INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

LEGAL GAPS IN PROSECUTING CYBERATTACKS ON AIRCRAFT: ADDRESSING JURISDICTIONAL AND EVIDENTIARY CHALLENGES IN AVIATION CYBERCRIME CASES

AUTHORED BY - PRANATHI V

Abstract

The digitization of the aviation industry, marked by reliance on avionics, satellite navigation, and real-time communications, has introduced new vectors for cybercrime, outpacing the capabilities of existing international aviation and cyber law. This paper interrogates the legal vacuum surrounding the prosecution of cyberattacks on aircraft by analytically dissecting jurisdictional conflicts and evidentiary barriers in transnational aviation cybersecurity enforcement. Despite global conventions such as the **Chicago Convention (1944)** and **Montreal Convention (2010)**, their doctrinal and textual silence on aviation-specific cyber intrusions has created loopholes exploitable by cyber offenders operating across borders. Territorial jurisdiction, once sufficient in physical hijackings, is rendered obsolete in the intangible yet catastrophic realm of *"digital aircraft piracy."*

The Budapest Convention (2001), while pioneering in cross-border cooperation, suffers from limited signatory participation and weak enforcement mechanisms against cyber actors shielded by non-cooperative states like Russia and China. This paper argues for the adoption of **universal jurisdiction** for cyber hijackings, akin to maritime piracy or terrorism, under a proposed **ICAO-led international cybercrime protocol**, to harmonize legal standards and facilitate extradition and evidence sharing.

Furthermore, the study critiques the evidentiary crisis arising from fragmented forensic protocols and digital sovereignty claims that impede real-time investigations. Through doctrinal analysis and comparative case studies, including the **Chris Roberts aircraft hacking case (2015)** and **Boeing cyber espionage incident (2018)**, this paper exposes the procedural disconnects between national cybersecurity laws and aviation regulatory frameworks.

Lastly, the work innovatively explores **shared liability frameworks** among airlines, aircraft manufacturers, and IT vendors, advocating for an expansion of the Montreal Convention to

 ISSN: 2582-6433

codify cyber-risk obligations, breach notification duties, and indemnification clauses. The redefinition of cyberattacks as acts of cyberterrorism or digital piracy, supported by revised interpretive guidelines, is proposed to close normative gaps in prosecuting such transnational threats.

Keywords: *Digital Aircraft Piracy, Universal Jurisdiction, Cybersecurity, Unlawful Interference, Transnational Regulation.*

This research bridges theory and practice by integrating principles of **universal jurisdiction, transnational digital forensics, and cyber-resilience governance**, underscoring the urgency for a unified and enforceable aviation cybersecurity regime. In doing so, it contributes to the international legal discourse on aviation security and offers tangible legal reforms aimed at mitigating future threats to global civil aviation.

1. Methodology and Legal Research Style

This research adopts a **doctrinal legal methodology** grounded in black-letter law analysis, critical theory, and comparative jurisprudence. The doctrinal method is chosen due to its capacity to interrogate the text, context, and application of legal rules as found in statutes, treaties, and case law. Supplemented by qualitative insights and empirical references, the study proceeds in three major research phases:

1.1. Treaty and Statutory Analysis

1.1.1. Primary Sources: Examination of key international conventions including the *Convention on International Civil Aviation (Chicago Convention, 1944)*, *Montreal Convention (1971 and 2010)*, *Tokyo Convention (1963)*, and *Budapest Convention (2001)*.

1.1.2. Secondary Sources: Analysis of ICAO working papers, cybersecurity directives (FAA, EASA), and relevant international resolutions.

1.2. Case Law Analysis

1.2.1 Chris Roberts Hacking Incident (2015): An onboard cyber intrusion that revealed legal ambiguity regarding unauthorized access to avionics systems.

1.2.2. Chinese State-sponsored Hack on Boeing (2018): Highlighting state immunity and extradition failure.

1.2.3. easyJet Data Breach (2019): Illuminating gaps in liability assignment under

 ISSN: 2582-6433

airline cybersecurity protocols.

1.3. Comparative and Empirical Inquiry

- Assessment of cybersecurity incident trends (2014–2024) and state-specific enforcement mechanisms.
- Comparative legal analysis of extradition practices, forensic protocols, and sovereign limitations across jurisdictions including the U.S., EU, China, and Russia.

2. Theoretical Focus

2.1 Territorial Jurisdiction vs. Universal Jurisdiction: Challenges in applying territorial principles to transboundary cyber intrusions; necessity for universal jurisdiction analogous to maritime piracy.

2.2. Digital Sovereignty and Evidentiary Sovereignty: Conflicts over data localization, state control of cyber evidence, and non-cooperation in transnational investigations.

2.3. Cyberterrorism Theory: Reconceptualizing cyber hijacking as a terrorist act or act of unlawful interference, meriting prosecution under expanded definitions of aerial piracy.

2.4. Public-Private Liability Model: Redefining cybersecurity responsibilities in light of tort principles, regulatory compliance doctrines, and global cyber resilience benchmarks.

3. Legal Framework Governing Aviation Cybercrime

Aviation cyberattacks challenge the structural integrity of both air law and cyber law by exploiting gaps in jurisdiction, enforcement, and digital evidence protocols. Current legal instruments, international, regional, and domestic, fail to adequately address cyberthreats that are transnational, stealthy, and evolving. Below is an analytical framework identifying existing laws, their scope, and limitations.

3.1. International Civil Aviation Law

3.1.1. Chicago Convention on International Civil Aviation (1944)

The scope of this regulation establishes that each state has complete and *exclusive sovereignty* over the airspace above its territory **(Art. 1),** and governs technical, navigational, and operational aspects of civil aviation. However, the convention predates the concept of cybercrime. It assumes physical proximity to the offense, thereby rendering cyberattacks that originate remotely, often from foreign jurisdictions, beyond the reach of territorial enforcement. Modernization through an ICAO protocol recognizing “cyber interference” as a

 ISSN: 2582-6433

threat to aviation sovereignty is required.[1]

3.1.2. Tokyo Convention (1963)

The Tokyo Convention grants the state of aircraft registration primary jurisdiction over crimes committed onboard an aircraft in flight (Art. 3). However, it does not apply to external cyber intrusions, such as remotely disabling navigation systems or uploading malware into communication systems. No provision is made for attributing criminal responsibility to actors outside the aircraft.

Case Example: In 2015, hacker Chris Roberts claimed to have accessed in-flight systems via the in-flight entertainment system. Legal ambiguity followed because his actions, though severe, did not fall clearly under Tokyo Convention offenses. [2]

3.1.3. Montreal Convention (1971; amended 2010)

It criminalizes acts of unlawful interference with civil aviation (e.g., bombings, hijackings). However, its definition of interference emphasizes physical violence or seizure; cyberattacks such as GPS spoofing, data corruption, or remote access to avionics systems are not explicitly covered. The Proposed Legal Innovation includes that cyber hijacking could be conceptualized as "digital aircraft piracy," extending the piracy model from maritime to aerial domains. However, without legal recognition as terrorism or interference, such attacks do not trigger international extradition or counterterrorism protocols.[3]

3.2. International Cybercrime Instruments

3.2.1. Budapest Convention on Cybercrime (2001)

It addresses crimes such as illegal access, data interference, and system interference and facilitates cross-border cooperation in evidence collection. It also provides mechanisms for mutual legal assistance, digital forensics, and extradition for cyber offenses. However, it is not ratified by Russia, China, India, and several Southeast Asian nations, who are all key players in cyber activities. It also lacks provisions tailored to critical infrastructure attacks, like those on aviation. In cases where aviation systems are attacked from a non-signatory jurisdiction,

[1] Convention on International Civil Aviation art. 1, Dec. 7, 1944, 15 U.N.T.S. 295.
[2] Convention on Offences and Certain Other Acts Committed on Board Aircraft, Sept. 14, 1963, 704 U.N.T.S. 219.
[3] Convention for the Suppression of Unlawful Acts Relating to International Civil Aviation, Sept. 10, 2010, ICAO Doc. 9946.

 ISSN: 2582-6433

cooperation is voluntary, often delayed, or denied.[4]

Example: During the 2018 Boeing cyber espionage incident involving Chinese hackers, the lack of binding extradition and cybercrime cooperation rendered U.S. prosecutorial efforts ineffective.

3.3. Regional and Domestic Cybersecurity Regulations

3.3.1. EU General Data Protection Regulation (GDPR) (2016)

It enforces strict rules for data handling, breach notification, and user consent. Airlines handling passenger data must report data breaches, but GDPR focuses on privacy, not the security of aircraft operational systems. However, GDPR does not require cybersecurity standards for aircraft IT systems, avionics software, or communication nodes.[5]

3.3.2. EU NIS Directive (2016)

It requires operators of essential services (including air transport) to ensure network and system security. It also supports incident reporting and baseline security standards. However, it lacks enforcement uniformity across EU member states. Also, compliance often targets airport and airline networks, not airborne systems.[6]

3.3.3. U.S. FAA Aircraft Systems Information Security Protection Rule (ASISP, 2019)

It mandates manufacturers to demonstrate the protection of aircraft systems from unauthorized external access during certification. However, the focus is preventive, not punitive, it does not address criminal prosecution or cross-border enforcement. It leaves post-certification cybersecurity governance largely to private actors.[7]

3.4. Customary International Law and Emerging Norms

3.4.1. Universal Jurisdiction

It allows states to prosecute certain crimes regardless of where they occurred. However, it has not yet extended to aviation cyberattacks, but analogous to piracy or terrorism, given its transnational, anonymous, and high-risk nature. Bassiouni and others advocate expanding universal jurisdiction to cover global security threats, including cyber interference with critical

[4] Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167.
[5] Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1.
[6] Directive (EU) 2016/1148, 2016 O.J. (L 194) 1.
[7] Federal Aviation Administration, Aircraft Systems Information Security Protection (ASISP), 14 C.F.R. § 25.1316 (2019).

 ISSN: 2582-6433

infrastructure.[8]

3.4.2. UN GGE Norms & Draft Articles on State Responsibility (ARSIWA, 2001)

GGE norms emphasize responsible state behavior in cyberspace, including due diligence and cooperation. ARSIWA provides legal bases for holding states internationally responsible for wrongful acts, including failure to prevent cyberattacks.[9] However, these are soft law instruments, non-binding, with no dispute resolution or enforcement mechanisms. The States harboring cybercriminals may avoid liability by invoking plausible deniability or sovereignty.[10]

3.5. Institutional Gaps and Need for Reform

ICAO, the global civil aviation regulator, lacks a dedicated legal instrument on aviation cybersecurity. There is no standardized evidence-sharing or incident reporting system at the global level.

The suggested Reform Directions include:

- ICAO-led treaty or protocol on aviation cybercrime.
- Expansion of the Montreal Convention to include "cyber interference."
- Establishment of an international aviation cybersecurity incident database and forensic evidence cooperation agreement.

The global legal framework remains fragmented and outdated in addressing cyberattacks on aircraft. International aviation law is rooted in territorial sovereignty and physical threats, while cyber law lacks aviation specificity and universal enforceability. The interplay between jurisdictional uncertainty, evidentiary complexity, and lack of treaty coverage creates an urgent extraterritorial jurisdiction, liability attribution, and evidence cooperation.

4. Jurisdictional Challenges in Prosecuting Aviation Cyberattacks

4.1. Territorial Jurisdiction: Inadequacy in the Digital Age

One of the most significant obstacles in prosecuting aviation cyberattacks stems from the reliance of international aviation law on territorial jurisdiction, a principle increasingly obsolete in cyberspace. *The Chicago Convention (1944),* the foundational treaty governing international civil aviation, enshrines the notion that "every state has complete and exclusive sovereignty

[8] M. Cherif Bassiouni, *Universal Jurisdiction for International Crimes: Historical Perspectives and Contemporary Practice*, 42 Va. J. Int'l L. 81 (2001).
[9] Draft Articles on Responsibility of States for Internationally Wrongful Acts, [2001] 2 Y.B. Int'l L. Comm'n 31, U.N. Doc. A/56/10.
[10] G.A. Res. 73/27, U.N. Doc. A/RES/73/27 (Dec. 5, 2018).

 ISSN: 2582-6433

over the airspace above its territory" (Art. 1).[11] This state-centric framework assumes that offenses against aircraft occur physically within a state's territory, or at least within the spatial jurisdiction of the aircraft's registered nation.

However, cyberattacks defy these assumptions. Consider a scenario in which a hacker in Country A transmits malicious code to remotely interfere with the avionics of an aircraft registered in Country B, while the aircraft is flying over Country C's airspace. Each of these states has a partial nexus to the offense, yet none has a clearly superior claim to jurisdiction under existing aviation treaties. The Tokyo Convention (1963) grants primary jurisdiction to the state of aircraft registration over onboard offenses, but this is inadequate when the attack originates from outside the aircraft, potentially thousands of miles away.[12]

This jurisdictional fragmentation results in prosecutorial paralysis, with states often unwilling or unable to assert extraterritorial claims for fear of violating international norms of sovereignty or due to domestic legal limitations. Furthermore, traditional doctrines of active personality, passive personality, or protective jurisdiction are rarely invoked in cyber contexts due to evidentiary challenges and state reluctance to establish controversial precedents. The lack of harmonization in domestic cybersecurity laws only compounds this problem, as different nations define cyber offenses, digital evidence admissibility, and extradition criteria in vastly divergent ways.

Aviation cybercrime, therefore, occupies a legal grey zone, unaddressed by both classical territorial frameworks and current extradition and enforcement mechanisms. Without explicit provisions enabling extraterritorial prosecution of cyberattacks affecting civil aviation, offenders can exploit jurisdictional loopholes to operate with near impunity.

4.2. The Case for Universal Jurisdiction

In light of the inadequacies of territorial jurisdiction, legal scholars and policymakers have increasingly advocated for the extension of universal jurisdiction to aviation cyberattacks. Universal jurisdiction allows any state to prosecute certain grave crimes, regardless of where the crime occurred or the nationality of the offender or victim, on the theory that such crimes threaten the international community as a whole. Traditionally, this principle has been applied

[11] [Chicago Convention, Dec. 7, 1944, 15 U.N.T.S. 295]
[12] [Tokyo Convention, Sept. 14, 1963, 704 U.N.T.S. 219]

 ISSN: 2582-6433

to offenses like piracy, genocide, war crimes, and terrorism.[13]

Drawing a parallel with maritime piracy, aviation cyberattacks, particularly those aimed at hijacking or disrupting the navigation of aircraft, can be analogized to aerial piracy committed via digital means. Like high seas piracy, these attacks are often perpetrated by anonymous actors beyond the effective control of any single jurisdiction. Moreover, when such attacks threaten the safety of hundreds of passengers, the economic infrastructure of global aviation, and international peace, they meet the threshold of gravity and transnational impact that typically justifies universal jurisdiction.

Further justification can be found in the evolving norms of international cybersecurity governance. The United Nations Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG) have recognized that cyberattacks on critical infrastructure, including transportation systems, may constitute violations of international peace and security. Although these norms are not binding, they underscore a growing international consensus that state sovereignty must not shield cyber aggressors from accountability.[14]

In this context, the International Civil Aviation Organization (ICAO) emerges as a logical forum for coordinating a cyber-specific universal jurisdiction regime. ICAO has the institutional legitimacy and technical expertise to draft a new international protocol or treaty that

- criminalizes aviation cyberattacks,
- defines digital aircraft interference, and
- confers universal jurisdiction upon states to prosecute such crimes regardless of location or nationality.

This model could mirror the 1988 Montreal Protocol, which extended jurisdiction over unlawful acts of violence at airports. Such a legal instrument would fill the jurisdictional vacuum left by the Chicago, Tokyo, and Montreal Conventions, empowering states to investigate and prosecute aviation cybercrimes in the same manner as they would acts of traditional terrorism or piracy. It would also signal a shift from reactive, fragmented enforcement to proactive, harmonized global legal governance of aviation cybersecurity.

[13] [M. Cherif Bassiouni, *Universal Jurisdiction for International Crimes: Historical Perspectives and Contemporary Practice*, 42 Va. J. Int'l L. 81 (2001)].
[14] [G.A. Res. 73/27, U.N. Doc. A/RES/73/27 (Dec. 5, 2018).

 ISSN: 2582-6433

The failure of territorial jurisdiction to address the realities of aviation cyberattacks exposes a profound structural weakness in international law. In the absence of enforceable extraterritorial or universal jurisdictional standards, legal systems are poorly equipped to deal with crimes that transcend both physical borders and traditional legal categories. A move toward universal jurisdiction through an ICAO-led cybercrime treaty offers a legally viable and globally equitable response to this growing threat, one that protects not only states but also the integrity of international civil aviation.

5. Evidentiary Barriers in Cross-Border Aviation Cybercrime Investigations

5.1. Forensic Data Collection Challenges

The successful prosecution of aviation cyberattacks hinges on timely access to digital forensic evidence, yet such access remains fraught with legal, technical, and political obstacles. Unlike conventional crimes, cyberattacks rarely leave behind tangible evidence; instead, investigators must gather real-time data trails, system logs, IP records, and network traffic patterns that are often stored across multiple jurisdictions and cloud-based platforms. These platforms may fall under differing data protection regimes, such as the *EU General Data Protection Regulation (GDPR),* which restricts the flow of personal or operational data across borders without strict safeguards.[15]

This legal fragmentation creates a paradox: The very tools needed to trace and prosecute the cybercriminal may be legally inaccessible due to data sovereignty concerns. For instance, if an airline stores navigation system logs in servers located in the United States but the affected aircraft is registered in a European Union state, the prosecuting authority must navigate a complex web of national security laws, privacy regulations, and corporate secrecy before accessing such data.

Moreover, the aviation industry's heavy reliance on multiple private actors, including airlines, aircraft manufacturers (e.g., Boeing, Airbus), and third-party IT vendors, further complicates forensic access. These entities often prioritize corporate liability protection and reputation management over investigative transparency, leading to non-cooperation or delay. The easyJet

[15] [Regulation (EU) 2016/679, 2016 O.J. (L 119) 1]

 ISSN: 2582-6433

data breach in 2019, affecting over 9 million customers, illustrates how corporations may withhold full details of cybersecurity lapses until compelled by public outcry or regulatory pressure.[16] Additionally, there is no standardized framework within the aviation sector for the collection, preservation, or admissibility of cyber forensic evidence, leading to inconsistencies in the treatment of digital evidence across jurisdictions. Without uniformity in evidence standards and protocols, prosecutions are frequently derailed on procedural grounds.

5.2. The Budapest Convention and Its Shortcomings

The Budapest Convention on Cybercrime (2001) remains the principal international legal instrument facilitating cross-border cybercrime investigation. It provides mechanisms for mutual legal assistance, expedited preservation of stored data, and cross-border access to computer systems with the consent of the lawful owner.[17] However, the Convention's effectiveness is significantly curtailed in the aviation context for three key reasons.

First, not all major cyber powers are parties to the Convention. Countries such as Russia, China, and India have not ratified it, citing concerns about sovereignty, Western legal hegemony, and the lack of international consensus on cyber norms. This non-participation limits cooperation in investigating aviation-related cyberattacks originating from these jurisdictions. The 2018 cyber espionage attack on Boeing, attributed to Chinese hackers, highlighted this limitation. Despite clear digital signatures pointing to state-linked actors, the United States faced significant hurdles in extraditing suspects and obtaining digital evidence from Chinese authorities, who rejected requests for cooperation on the basis of non-membership and national interest.[18]

Second, the Convention does not specifically address critical infrastructure sectors such as aviation, nor does it mandate data sharing from private sector actors involved in aviation, like airline vendors and aerospace contractors. The result is an enforcement void, where investigators may have the legal tools but not the jurisdictional reach or institutional cooperation to deploy them effectively.

[16] [Cooper, P., *The Foundations of Aviation Cyber Safety and Security*, ATLANTIC COUNCIL (2017), https://www.jstor.org/stable/resrep16767.16].
[17] [Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167]
[18] [Kramer & Butler, *CYBERSECURITY: CHANGING THE MODEL*, ATLANTIC COUNCIL (2019), https://www.jstor.org/stable/resrep20932.4].

 ISSN: 2582-6433

Third, even among signatory states, the interpretation and implementation of the Convention vary, especially regarding the scope of data requests and the definition of cybercrime. This leads to inconsistent enforcement and prolonged investigation timelines, which are detrimental in aviation contexts where real-time responsiveness is crucial to prevent ongoing or future attacks.

5.3. The Need for an ICAO-led Cyber Incident Sharing Mechanism

Given the shortcomings of current legal instruments and enforcement mechanisms, there is an urgent need for a sector-specific, aviation-oriented cyber forensic protocol. The International Civil Aviation Organization (ICAO) is uniquely positioned to lead this initiative, given its global membership and existing authority over international civil aviation safety standards.

This research proposes the creation of an ICAO-led Cyber Incident Sharing Mechanism (CISM), a legally binding protocol or annex to the Chicago or Montreal Conventions. This mechanism would require all contracting states and their national aviation authorities to:

- Report cyber incidents affecting civil aviation infrastructure, onboard systems, and ground-to-air communication networks;
- Preserve and share forensic data, including attack vectors, malware signatures, and intrusion methods, within 24 to 48 hours of detection;
- Establish legal pathways for cross-border evidence sharing between aviation regulators, airline cybersecurity units, and law enforcement bodies;
- Mandate airlines and aircraft manufacturers to maintain secure, interoperable logging systems that can capture and store cyber event data in forensically admissible formats.

The model could draw from existing regional examples like the EU Aviation ISAC (Information Sharing and Analysis Centre), but would require global harmonization. By centralizing cybersecurity event reporting and standardizing forensic protocols, ICAO can promote a culture of transparency, rapid response, and legal accountability in aviation cyber governance.

Such a framework would also help mitigate the “data hoarding” culture prevalent among private aviation entities and ensure that digital evidence is not lost, tampered with, or rendered inadmissible due to non-standardized collection procedures.

In an environment where cyberattacks on aircraft can originate anywhere, occur

 ISSN: 2582-6433

instantaneously, and leave few physical traces, the ability to gather, preserve, and share digital evidence becomes the linchpin of successful prosecution. Yet, the current global legal architecture, fragmented across jurisdictions, hampered by non-cooperation, and blind to aviation-specific needs, undermines this ability at every turn. The failure of the Budapest Convention to accommodate non-signatory states and the absence of aviation-specific enforcement mechanisms point to a profound evidentiary gap.

Addressing this gap requires a new paradigm of legal and institutional cooperation, led by ICAO and embedded in a binding international protocol. Only by elevating aviation cybersecurity from a technical afterthought to a legal imperative can the global community respond effectively to the growing threat of aviation cybercrime.

6. Legal Classification: Is Cyber Hijacking a Form of Terrorism or Piracy?

6.1. Conceptual Ambiguity in the Montreal Convention

The **Montreal Convention of 2010**, formally the *Convention for the Suppression of Unlawful Acts Relating to International Civil Aviation*, serves as the primary international legal instrument addressing aviation security threats such as hijackings, bombings, and sabotage. However, its language is tailored almost exclusively to **physical acts of violence or coercion** and does not recognize **digital intrusions or cyber interference** as forms of "unlawful interference" with aircraft systems.[19]

For example, Article 1 criminalizes intentional acts that “destroy” or “damage” aircraft or navigation facilities, or that endanger safety through **use of force or threat thereof**. Yet, the Convention remains silent on **non-kinetic disruptions**, such as remotely hacking into avionics systems, disrupting GPS signals, or uploading malware that manipulates flight data. These acts, although potentially catastrophic, do not fall neatly within the Convention’s definitions because they **lack a physical or visible act of violence**.

This **doctrinal blind spot** is problematic in the age of networked aviation, where cyberattacks can be more destructive than conventional hijackings. The 2015 **Chris Roberts aircraft hacking incident**, where a cybersecurity researcher claimed to have accessed in-flight systems and manipulated thrust settings, illustrates how such intrusions are not prosecutable under

[19] [Montreal Convention, Sept. 10, 2010, ICAO Doc. 9946]

 ISSN: 2582-6433

existing international aviation security conventions due to their ambiguous classification.[20]

The **failure to legally classify cyber hijacking as an act of unlawful interference** not only impedes enforcement but also sends a troubling message that **digital threats to aviation systems are secondary or less serious**, despite their potential to endanger hundreds of lives.

6.2. Cyberterrorism and Digital Piracy

The **redefinition of hijacking in the cyber age** is both a legal necessity and a policy imperative. The **conceptual boundaries between cybercrime, terrorism, and piracy have become increasingly porous**, especially when cyberattacks are used to exert control over critical systems like aircraft navigation. Cyber hijacking can, in effect, replicate the effects of a traditional hijack: diverting aircraft, disabling controls, or inducing chaos, all without physical presence onboard.

From a legal perspective, cyber hijacking could be subsumed under the growing body of international law surrounding **cyberterrorism**. The **International Institute for Counter-Terrorism (ICT)** defines cyberterrorism as the "use of computer networks to cause disruption or fear to achieve political, religious or ideological goals". If an actor gains unauthorized access to flight systems and manipulates aircraft controls, particularly for coercive or ideological purposes, such an act clearly satisfies the elements of both **terrorism and unlawful interference**, albeit through **digital, rather than physical** means.[21]

Moreover, cyber hijacking aligns conceptually with **piracy** under customary international law. Piracy, as defined in **Article 101 of the United Nations Convention on the Law of the Sea (UNCLOS)**, includes illegal acts of violence or detention committed for private ends on the high seas. This definition has been analogously applied in aviation law to justify **universal jurisdiction over aircraft hijacking**, particularly under the **Hague Convention (1970)** and the **Montreal Convention (1971)**. A **digital hijack**, where an actor illegally takes control of an aircraft's direction, trajectory, or systems remotely, mimics the effect of piracy, only through **electronic capture** instead of armed coercion.

[20] [Cooper, P., *The Foundations of Aviation Cyber Safety and Security*, ATLANTIC COUNCIL (2017), https://www.jstor.org/stable/resrep16767.16]
[21] [ICT, *Cyber-Crime and Cyber-Terrorism*, Cyber Report, 2018, https://www.jstor.org/stable/resrep17687.7]

 ISSN: 2582-6433

Recognizing cyber hijacking as **"digital aircraft piracy"** not only facilitates the use of **universal jurisdiction** but also allows international agencies to treat cyberattackers with the same level of scrutiny and urgency as terrorists or armed hijackers. This shift in classification is critical for deterrence, extradition, and international legal cooperation.

Furthermore, without reclassification, enforcement legitimacy remains weak. Prosecutors may struggle to frame charges under traditional legal categories, and extradition requests can be denied on grounds of **non-recognition** of cyber hijacking as an extraditable offense. As cyberattacks grow more sophisticated and widespread, failing to adapt our legal categories invites impunity.

6.3. Proposed Doctrinal Amendments

To bridge the definitional and enforcement gap, this research proposes that **cyber hijacking be expressly included within the scope of "unlawful interference"** under the Montreal Convention or, alternatively, through a new ICAO-led protocol dedicated to aviation cybercrime.

Such doctrinal amendments could take several forms:

1. **Expanded Definition of Unlawful Interference**: The term should be revised to include "any unauthorized digital intrusion, manipulation, or obstruction of aircraft systems, air traffic control infrastructure, or navigation facilities that compromises the safety or operability of civil aviation."
2. **Cyber Piracy Clause**: Drawing from the piracy analogy, a clause can be included defining "digital seizure or manipulation of an aircraft's systems from a remote or onboard electronic source" as an act tantamount to hijacking.
3. **Terrorism Linkage**: The preamble or purpose clause of the Montreal Convention should clarify that **cyber acts** committed with the intention of inducing public fear or coercing governments fall within the broader spectrum of terrorism.

These amendments would serve **multiple legal purposes**:

- They would **enable prosecutors to apply counterterrorism and anti-piracy statutes** to cyber hijackers.
- They would **trigger extradition treaties**, which often require dual criminality or recognition under international law.
- They would **legitimize multilateral responses**, such as sanctions, asset freezes, and preventive cyber defense coordination.

 ISSN: 2582-6433

The inclusion of such language within the Montreal Convention or a standalone cyber aviation treaty would also **promote legal certainty and procedural fairness**, ensuring that cybercriminals are subject to due process under a clear and defined offense structure.

7. Cross-Border Extradition and State Non-Cooperation

7.1. Political Barriers to Extradition

One of the most intractable challenges in prosecuting aviation cyberattacks is the geopolitical friction surrounding extradition, especially when cybercriminals are state-sponsored or reside in nations hostile to extradition requests. Extradition in cybercrime cases is already fraught with complications due to divergent legal systems, but when aviation security intersects with national intelligence, espionage, or strategic interests, cooperation becomes virtually nonexistent.

The 2018 Boeing cyberattack is illustrative. A group of Chinese state-linked hackers infiltrated Boeing's computer systems to steal proprietary aviation data. Despite identification and evidence provided by U.S. authorities, China refused to extradite the suspects, citing the absence of a bilateral treaty and national security concerns. Similarly, Russia has repeatedly refused to extradite cybercriminals accused of launching ransomware and infrastructure attacks from within its territory, shielding them through domestic legislation and asserting national sovereignty.[22]

In such cases, the lack of universal standards for cybercrime extradition, particularly for aviation-related offenses, enables impunity. The Budapest Convention contains provisions on international cooperation, but is ineffective against non-signatory states like Russia and China.[23] Moreover, without reciprocal legal definitions or shared recognition of cyber hijacking as a serious offense under international law, extradition requests are often denied on procedural or political grounds.

7.2. Legal Limitations Under Existing Mutual Legal Assistance Treaties (MLATs)

Mutual Legal Assistance Treaties (MLATs) are bilateral or multilateral instruments designed to facilitate the sharing of evidence, execution of search warrants, and transfer of suspects

[22] [Kramer & Butler, *CYBERSECURITY: CHANGING THE MODEL*, ATLANTIC COUNCIL (2019), https://www.jstor.org/stable/resrep20932.4]
[23] [Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167]

 ISSN: 2582-6433

between jurisdictions. While effective in traditional criminal matters, MLATs are slow, bureaucratic, and ill-suited for cyber investigations, where data is volatile, encrypted, and often disappears within hours of the attack.

Aviation cyberattacks further strain MLATs due to their multi-jurisdictional nature. For example, a cyberattack may involve:

- A hacker operating from a non-MLAT partner state.
- An aircraft registered in another.
- A cloud server storing the evidence in a third country.

MLATs typically lack the agility required to process such requests within actionable timelines. Furthermore, the lack of aviation-specific MLAT clauses means that cybercrimes affecting aircraft systems are often deprioritized, particularly when no physical harm has occurred.

The United Nations Office on Drugs and Crime (UNODC) and the Council of Europe have acknowledged these limitations, calling for faster, harmonized, and tech-sensitive legal frameworks for cybercrime cooperation.[24]

7.3. Proposed Reforms

To overcome these limitations, this paper proposes the development of an Aviation Cyber MLAT Network (ACMN), a multilateral legal assistance mechanism designed specifically for aviation cybersecurity. Administered under the ICAO's legal affairs bureau, the ACMN would:

- Standardize definitions of aviation cybercrime and digital hijacking.
- Mandate expedited digital evidence sharing within 48 hours of request.
- Enable emergency cooperation between air traffic control authorities, airlines, and national cybercrime units.

In addition to the ACMN, Interpol Red Notices could be expanded to cover aviation-specific cybercriminals, even in the absence of dual criminality. Red Notices serve as alerts to arrest individuals pending extradition and are already used in cases of transnational crime. Formal recognition of aviation cybercrime under Red Notice parameters would enhance global enforcement.

[24] [UNODC, *Comprehensive Study on Cybercrime*, 2013]

 ISSN: 2582-6433

Further, the United Nations Security Council (UNSC) could be petitioned under Chapter VII authority to treat mass-scale aviation cyberattacks, especially those state-sponsored, as threats to international peace and security. Such a move would allow for the imposition of binding resolutions, sanctions, or international investigative tribunals, thereby bypassing bilateral bottlenecks.

8. Regulatory Liability: Who Is Responsible When Aviation Cyberattacks Occur?

8.1. Airlines, Manufacturers, and Third-Party Vendors

Aviation cybersecurity is not only a matter of enforcement, it is also a regulatory liability issue. Currently, no comprehensive legal framework establishes clear cybersecurity obligations for airlines, aircraft manufacturers (e.g., Boeing, Airbus), or the myriad of IT vendors who provide onboard and offboard digital infrastructure.

From a tort and contract law perspective, these stakeholders may owe duties of care, arising from:

- Negligence in failing to implement basic cybersecurity standards.
- Breach of contract in not fulfilling technical service level agreements (SLAs).
- Product liability, particularly when flawed avionics systems expose passengers to harm.

Yet the absence of a global compliance code means that standards vary widely across jurisdictions. In many cases, blame-shifting occurs after incidents, with airlines blaming manufacturers, who in turn blame third-party software providers. This legal diffusion of responsibility undermines accountability and incentivizes minimal compliance over robust prevention.

8.2. Comparative Liability Frameworks

The European Union's GDPR and NIS Directive provide some insight into how liability can be codified. Under GDPR, entities can be fined up to 4% of their global turnover for failing to protect personal data, a model that could be applied to passenger manifests, aircraft telemetry, and sensitive operational data.[25]

The NIS Directive (2016) requires that operators of essential services, including air transport

[25] [Regulation (EU) 2016/679, 2016 O.J. (L 119) 1].

 ISSN: 2582-6433

providers, implement appropriate security measures and report serious incidents.[26] However, the directive stops short of defining technical standards or assigning tiered liability among actors.

In the United States, the FAA's Aircraft Systems Information Security Protection (ASISP) Rule governs the certification of new aircraft systems but does not impose post-certification cybersecurity obligations or penalties.[27] This narrow scope leaves open significant regulatory gaps.

These comparative models show that while sector-specific cyber liability is emerging, there is no globally harmonized legal mechanism for the aviation industry that allocates liability proportionately.

8.3. Proposal for an ICAO Global Aviation Cybersecurity Compliance Code

To close this regulatory gap, this paper proposes the development of an ICAO Global Aviation Cybersecurity Compliance Code (GACCC). Modeled on the GDPR and ISO cybersecurity standards, this code would:

1. Define cybersecurity obligations across the aviation supply chain.
2. Mandate end-to-end encryption of onboard and ground communication.
3. Require incident disclosure within a standardized timeframe (e.g., 48 hours).
4. Establish tiered liability:
    - Airlines for failure to secure data transmissions.
    - Manufacturers of software vulnerabilities in flight systems.
    - IT vendors for failing to update or patch known system weaknesses.
5. Enable cross-border inspections and audits of aviation cybersecurity systems.

Incorporating such a compliance code into an ICAO annex or multilateral agreement would not only standardize expectations but also allow for enforcement through aviation safety audits, compliance ratings, and potential sanctions for non-compliance.

The regulation of aviation cybersecurity must extend beyond enforcement to include preventive liability frameworks that allocate responsibility across all actors involved in flight operations. As attacks become more sophisticated and multi-layered, so too must the legal architecture that

[26] [Directive (EU) 2016/1148, 2016 O.J. (L 194) 1]
[27] [14 C.F.R. § 25.1316 (2019)]

 ISSN: 2582-6433

governs accountability. By reforming extradition protocols and establishing a global compliance code, the international community can transition from fragmented responses to a cohesive, risk-based governance model for aviation cybercrime.

9. Case Studies and Precedents

9.1. Chris Roberts Aircraft Hacking Case (2015)

In 2015, cybersecurity expert Chris Roberts publicly claimed to have accessed the in-flight entertainment (IFE) system of a United Airlines aircraft and manipulated its engine controls via the aircraft's onboard network. According to his statements, he exploited known vulnerabilities in the aircraft's Seat Electronic Box (SEB) to access critical flight data systems, including the thrust management system.[28]

Despite the apparent seriousness of the intrusion, **no criminal charges were filed**, and Roberts was temporarily detained by the FBI and barred from future United flights. This incident highlights **legal ambiguity in classifying unauthorized digital access** as a criminal act in aviation contexts. While the Computer Fraud and Abuse Act (CFAA) in the U.S. criminalizes unauthorized access to protected systems, there was **no specific aviation law** addressing such intrusions at the time, nor was there a precedent for applying anti-hijacking laws to cyber actions that lacked physical violence or intent to harm.

This case demonstrates a critical **gap in jurisdiction, terminology, and prosecutorial clarity**, as cybersecurity testing and malicious hacking were not sufficiently differentiated in legal terms, and aviation-specific cyber offenses had not yet been codified.

9.2. Boeing Cyberattack by Chinese Hackers (2018)

In 2018, U.S. federal authorities charged several Chinese nationals affiliated with the Ministry of State Security for **cyber espionage targeting Boeing**, specifically to steal sensitive data related to military and civil aviation technology. The attackers infiltrated Boeing's servers, downloaded proprietary aircraft blueprints, and compromised the cybersecurity of a major supplier.[29]

[28] [Cooper, P., *The Foundations of Aviation Cyber Safety and Security*, ATLANTIC COUNCIL (2017), https://www.jstor.org/stable/resrep16767.16]
[29] [Kramer & Butler, *Cybersecurity: Changing the Model*, ATLANTIC COUNCIL (2019), https://www.jstor.org/stable/resrep20932.4]

 ISSN: 2582-6433

Despite the indictment, the United States was **unable to extradite the accused** from China due to the absence of an extradition treaty and the **Chinese government's refusal to cooperate**, citing national sovereignty and political tension. This case is a textbook example of **extradition failure and state-sponsored cybercrime**, where the existing legal infrastructure proved wholly inadequate to ensure accountability. It also showcases how **espionage overlaps with aviation cybersecurity**, revealing vulnerabilities not only in aircraft operations but also in design and manufacturing processes, which can be weaponized in cyber warfare.

9.3. easyJet Data Breach (2019)

In 2019, British airline easyJet disclosed that a **sophisticated cyberattack compromised the personal data of over 9 million customers**, including email addresses and travel information. About 2,200 customers had their credit card details exposed. While easyJet cited compliance with the EU General Data Protection Regulation (GDPR), it delayed notification to affected users and regulators by several months, drawing criticism from data protection authorities and customers alike.[30]

This breach exposed serious **accountability gaps** within aviation cybersecurity frameworks. Although GDPR allows regulators to impose heavy fines for data protection failures, easyJet's incident pointed to a **lack of sector-specific cybersecurity mandates**. There was **no regulatory requirement** for securing operational systems like IFE or communication links, nor were there legal consequences under aviation law, underscoring the need for **overlapping enforcement across aviation and data privacy regimes**.

9.4. Analytical Summary of Case Outcomes and Gaps

These case studies collectively reveal a pattern of **legal inertia and reactive enforcement** in the face of sophisticated aviation cyber threats. The Chris Roberts case shows that cyber interference is often **outside the jurisdictional scope of anti-hijacking laws**. The Boeing incident reveals **extradition paralysis in geopolitically sensitive cases**, and the easyJet breach highlights **regulatory voids and delayed enforcement**.

Across all three, **evidentiary hurdles, definitional ambiguity, and jurisdictional misalignment** prevent consistent accountability. This supports the core thesis of this research:

[30] [Regulation (EU) 2016/679, 2016 O.J. (L 119) 1]

 ISSN: 2582-6433

that **international aviation law must evolve to recognize and respond to cyber threats through legal innovation, harmonized frameworks, and proactive institutional mechanisms.**

10. Reform Proposals and the Way Forward

10.1. Treaty Reform Proposals

The most urgent legal reform is the **expansion of international treaties** to address aviation cybercrime explicitly. This includes:

- Drafting a new **ICAO Cybersecurity Protocol**, to be annexed to the Chicago or Montreal Convention, that criminalizes cyber intrusions into aircraft systems, ATC infrastructure, and airline databases.
- Amending the **Montreal Convention (2010)** to redefine "unlawful interference" to include **digital acts** such as unauthorized access, cyber hijacking, and disruption of navigational or operational systems.

Such treaty reforms would not only create **uniform legal definitions** but also provide **jurisdictional clarity**, facilitate **extradition**, and **mandate state cooperation**. By recognizing cyber hijacking as a form of digital piracy or terrorism, these instruments would align legal tools with modern technological threats.[31]

10.2. Institutional Innovations

The ICAO should establish an **Aviation Cybercrime Unit (ACU)** under its Legal Bureau or Air Navigation Bureau. The ACU would:

- Monitor aviation-related cyber threats globally.
- Coordinate with Interpol and national cybercrime units.
- Develop technical standards and forensic protocols for evidence collection.
- Maintain a **global incident database** to track cyber threats and responses.
- Chain of custody requirements.
- Data integrity protocols.

Additionally, ICAO should issue **standard forensic cooperation guidelines**, akin to those under the Budapest Convention but adapted for aviation, covering:

[31] Convention for the Suppression of Unlawful Acts Relating to International Civil Aviation, Sept. 10, 2010, ICAO Doc. 9946.

 ISSN: 2582-6433

- Multi-jurisdictional access to cloud-based evidence.[32]

10.3. Multilateral Diplomacy Pathways

Legal reform must be supplemented by **diplomatic coordination** through existing international forums:

- The **United Nations**, via the Group of Governmental Experts (GGE), should recognize aviation cybersecurity as a **threat to international peace and security**.
- The **G20 and ASEAN** can facilitate **regional aviation cyber readiness** and promote legal harmonization.
- The **Council of Europe** should collaborate with ICAO to extend the **Budapest Convention's mechanisms** to aviation-specific threats.

These forums can drive consensus on **minimum cybersecurity standards**, **lawful evidence sharing protocols**, and **non-refoulement exceptions for cybercriminals** when national protections obstruct global justice.

10.4. Strengthening National Aviation Cybersecurity Laws

On the domestic front, states must adopt a **model aviation cybersecurity law**, harmonized with international norms, to:

- Criminalize unauthorized access to aviation systems.
- Mandate breach reporting and forensic preservation.
- Allow extraterritorial application to foreign actors who compromise nationally registered aircraft.
- Integrate cybersecurity obligations into **civil aviation codes, tort statutes, and criminal laws**.

This law should also create **national aviation cybersecurity enforcement units**, ensuring rapid coordination between **aviation authorities, cybersecurity regulators, and law enforcement.[33]**

Model frameworks can draw from the **NIS Directive (EU)** and **FAA cybersecurity standards (U.S.)**, but must be aviation-specific to ensure operational resilience.[34]

[32] Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167.
[33] 14 C.F.R. § 25.1316 (2019).
[34] Directive (EU) 2016/1148, 2016 O.J. (L 194) 1.

 ISSN: 2582-6433

11. Conclusion

In the digital age, where aircraft are increasingly integrated with complex software, communication systems, and real-time data processing platforms, the skies have become **not only a physical domain but a cyber domain**. Yet, international aviation law has failed to keep pace. This research has demonstrated that the legal frameworks governing civil aviation, rooted in territoriality and physical interference, are **inadequate to address the invisible, borderless, and technically sophisticated nature of cyberattacks on aircraft**.

Through doctrinal analysis and case study evaluation, the research identified fundamental gaps in **jurisdiction, extradition, evidentiary access, and classification of cyber offenses**. The current treaties, most notably the Chicago Convention (1944), Tokyo Convention (1963), and Montreal Convention (2010), remain grounded in 20th-century threats and offer **no substantive response to aviation cybercrime**. The Budapest Convention (2001), while significant, lacks both universal adoption and aviation specificity, rendering it ineffective against non-cooperative cyber powers and critical infrastructure attacks.

The challenges posed by cyber hijacking, unauthorized access, and manipulation of aircraft systems have shown how **traditional legal categories, such as terrorism or piracy, are no longer adequate without digital reinterpretation**. Likewise, the persistent failure to extradite offenders due to political shielding or treaty absence highlights the need for **a new enforcement paradigm**.

This paper proposes a comprehensive reform strategy that is both **legal and institutional**:

- Treaty modernization through an **ICAO Cybersecurity Protocol** and expansion of the Montreal Convention to include **digital piracy**;
- Institutional mechanisms such as an **ICAO Aviation Cybercrime Unit** and forensic cooperation protocols;
- Multilateral diplomacy to harmonize standards through the **UN, G20, ASEAN, and the Council of Europe**;
- National-level reform through model aviation cybersecurity laws with clear liability frameworks for **airlines, manufacturers, and IT vendors**.

Beyond legal texts, this paper calls for a **jurisprudential shift**—one that treats cyberattacks on aircraft not merely as technical anomalies, but as direct threats to international civil order and human life. If aviation law is to remain a cornerstone of international cooperation and safety,

 ISSN: 2582-6433

it must evolve to **recognize the aircraft as both a vessel of flight and a node in the global digital network**.

In a world where a keystroke can be as dangerous as a cockpit takeover, the law must speak the language of code, jurisdiction, and accountability. Anything less leaves the future of aviation flying blind.

12. Bibliography

12.1. International Conventions & Legal Instruments

1. *Convention on International Civil Aviation*, Dec. 7, 1944, 15 U.N.T.S. 295 (Chicago Convention).
2. *Convention on Offences and Certain Other Acts Committed on Board Aircraft*, Sept. 14, 1963, 704 U.N.T.S. 219 (Tokyo Convention).
3. *Convention for the Suppression of Unlawful Acts Relating to International Civil Aviation*, Sept. 10, 2010, ICAO Doc. 9946 (Montreal Convention 2010).
4. *Convention on Cybercrime*, Nov. 23, 2001, 2296 U.N.T.S. 167 (Budapest Convention).
5. *United Nations Convention on the Law of the Sea*, Dec. 10, 1982, 1833 U.N.T.S. 397 (UNCLOS).
6. *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Int'l Law Comm'n, U.N. Doc. A/56/10 (2001).
7. G.A. Res. 73/27, *Advancing Responsible State Behavior in Cyberspace in the Context of International Security*, U.N. Doc. A/RES/73/27 (Dec. 5, 2018).

12.2. National and Regional Regulations

8. Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1 (General Data Protection Regulation – GDPR).
9. Directive (EU) 2016/1148, 2016 O.J. (L 194) 1 (Directive on Security of Network and Information Systems – NIS Directive).
10. Federal Aviation Administration, Aircraft Systems Information Security Protection (ASISP), 14 C.F.R. § 25.1316 (2019).

12.3. Scholarly Articles and Reports

11. M. Cherif Bassiouni, *Universal Jurisdiction for International Crimes: Historical Perspectives and Contemporary Practice*, 42 Va. J. Int'l L. 81 (2001).

 ISSN: 2582-6433

12. Deborah Housen-Couriel, *The Evolving Law on Cyber Terrorism: Dilemmas in International Law and Israeli Law*, Int'l Inst. for Counter-Terrorism (ICT) (2013), https://www.jstor.org/stable/resrep09430.
13. Pete Cooper, *The Foundations of Aviation Cyber Safety and Security*, in *Aviation Cybersecurity: Finding Lift, Minimizing Drag*, Atlantic Council 57 (2017), https://www.jstor.org/stable/resrep16767.16.
14. Franklin D. Kramer & Robert J. Butler, *Cybersecurity: Changing the Model*, Atlantic Council 2–4 (2019), https://www.jstor.org/stable/resrep20932.4.
15. International Institute for Counter-Terrorism (ICT), *Cyber-Crime and Cyber-Terrorism*, in *Cyber Report: Sept.–Nov. 2017*, at 23–27, https://www.jstor.org/stable/resrep17687.7.
16. SAALMAN, L. (Ed.), *Integrating Cybersecurity and Critical Infrastructure: National, Regional and International Approaches*, Stockholm Int'l Peace Research Institute xi–xvi (2018), https://www.jstor.org/stable/resrep24516.6.
17. Jan Kallberg, *Strategic Cyberwar Theory – A Foundation for Designing Decisive Strategic Cyber Operations*, 1 Cyber Def. Rev. 113–28 (2016), https://www.jstor.org/stable/26267302.

12.4. Institutional & Governmental Publications

18. United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, U.N. Doc. CTOC/CY/2013/CRP.5 (2013).
19. European Union Aviation Safety Agency (EASA), *Cybersecurity in Civil Aviation: Safety Information Bulletin*, SIB No. 2019-05.
20. International Civil Aviation Organization (ICAO), *Manual on Cybersecurity*, Doc 9985, 2nd ed. (2020).

12.5. Case References and Notable Incidents

21. Chris Roberts Aircraft Hacking Case, FBI Investigation, 2015 (unofficial case documents and media coverage).
22. *United States v. Su Bin*, Criminal No. 14-174 (C.D. Cal. 2014) (involving cyber theft from Boeing).
23. *easyJet Cyber Breach Incident*, ICO Investigation Report, 2019, https://www.ico.org.uk/news/press-releases/2020/easyjet-investigation/.

 ISSN: 2582-6433

12.6. Additional Resources

24. Air University Press, Convertino II et al., *Flying and Fighting in Cyberspace*, Air & Space Power Journal, https://www.jstor.org/stable/resrep13680.
25. Woods, B., *Confronting Transatlantic Cybersecurity Challenges in the Internet of Things*, Atlantic Council (2017), https://www.jstor.org/stable/resrep03490.