



TECHNOLOGICAL INNOVATIONS AND CYBERSECURITY: RESHAPING AVIATION LAW AND SECURITY POLICIES

Nikitha Kotteswaran *

ABSTRACT

The aviation industry is changing under the influence of technological progress, especially Artificial Intelligence (AI), Internet of Things (IoT), and cybersecurity, and the aviation policy and legislation require renewal. The innovations increase operating efficiency and safety, but have a cyber vulnerability that endangers the aviation infrastructure. This article looks at the ways Indian and international aviation laws keep up with these challenges, specifically the cybersecurity threats to air traffic control, aircraft systems, and passenger data. Through the examination of the legal frameworks, the judicial precedent, and policy actions, the research establishes where these gaps exist and provides suggestions to enhance the security of aviation in the digital age.

Keywords: Aviation law, Cybersecurity, Technological Innovations, Aviation security, Data Protection.

INTRODUCTION

The aviation industry is experiencing a technological revolution, AI streamlines flight management, IoT allows tracking aeroplanes in real-time, and cybersecurity is used to protect vital systems. Nonetheless, the developments also come with threats, including a cyberattack on air traffic control systems and passenger system data leaks. There is a legal framework in India through the Aircraft Act, 1934, and Civil Aviation Requirements (CAR), which fail to deal with cyber threats.¹ The security standards are established through international organisations such as the International Civil Aviation Organisation (ICAO), Annexe 17, but

*LLM, FIRST YEAR, SRM UNIVERSITY.

¹ Aircraft Act, No. 24 of 1934

the fast technological advancements are more than regulations can keep pace with.² This paper discusses the way in which technological developments and cybersecurity are transforming the law and security policies of aviation, and specifically the Indian regulatory environment.

LITERATURE REVIEW

The literature identifies the two effects of technological development in the aviation sector, which have increased efficiency and also created weaknesses. Studies highlight the importance of AI in predictive maintenance and IoT in smart airports, although it is observed that cyber threats are increasing, including the avionics system and data breaches.³ Comparative research of the aviation regulations in the U.S. and in the EU reveals the necessity of common cybersecurity regulations, because the global nature of aviation requires unified policies.⁴ In India, aviation law literature is concerned with safety and liability, but has not gone into detail when it comes to cyber-specific rules. The dynamic character of cyber threats requires dynamic laws to address aviation infrastructure, which this article attempts to fill.

RESEARCH METHODOLOGY

This paper will be based on a doctrinal type of research involving the study of primary sources, including the Indian Aircraft Act, 1934, Civil Aviation Requirements, and the ICAO standards, and a secondary source using scholarly journals and policy reports.⁵ To determine the extent to which global and Indian aviation laws apply to the response to cybersecurity threats presented by AI and IoT, the methodology will involve a qualitative examination of laws in aviation worldwide and in India. Best practices can be obtained by comparing the U.S. and EU regulations.⁶ The paper reviews policy changes and industry standards to determine the loopholes in regulations and devise suggestions on how to incorporate aviation cybersecurity into the law.

² Int'l Civil Aviation Org. [ICAO], Annex 17: Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference (11th ed. 2020).

³ Eur. Union Aviation Safety Agency [EASA], Cybersecurity Strategy for Civil Aviation (2021), <https://www.easa.europa.eu/en/document-library/general-publications/cybersecurity-strategy-civil-aviation> (last visited Sept. 19, 2025).

⁴ Cyber Terrorism and Civil Aviation: Threats, Standards, and Regulations, 34 *Transnat'l L. & Contemp. Probs.* 123 (2024).

⁵ Directorate Gen. of Civil Aviation [DGCA], Civil Aviation Requirements, Section 1—Air Safety, Series C (India 2020).

⁶ UC Berkeley, Cybersecurity in Civilian Aviation: Insights for Advanced Nuclear Technologies (2025), <https://fhr.nuc.berkeley.edu> (last visited Sept. 19, 2025).

TECHNOLOGICAL INNOVATIONS IN AVIATION

The aviation sector is witnessing rapid integration of technological advances, especially Artificial Intelligence (AI) and the Internet of Things (IoT), which are improving the efficiency and safety of operations, as well as the experience of passengers. Nevertheless, these innovations generate serious cybersecurity dilemmas which require an extensive revision of aviation regulations and security policies. Connected digital networks are used in AI-based systems (e.g., automated air traffic control, predictive maintenance, etc.) and IoT-based devices (e.g., real-time aircraft sensors, smart airport infrastructure, etc.), which means they can be victims of cyberattacks. These attacks have a high risk to critical aviation systems such as navigation, communication, and passenger data management. The current legal and policy frameworks, both in India and elsewhere in the world, are mostly obsolete and do not consider the dynamism of cyber-threats that are presented by the new technologies.

The AI and IoT are transforming aviation to make the processes smarter and efficient. AI drives a higher level of analysis in flight route optimisation, aircraft failures, and management of air traffic to minimise fuel usage and delays. IoT is used to monitor aircraft systems (including engines and avionics), and simplify the airport procedures with connected devices (such as baggage tracking devices and automated check-in kiosks). These technologies enhance safety and efficiency, along with generating complex digital ecosystems which are dependent on large data streams and cloud-based infrastructures. This connectedness brings about cybersecurity risks, including the unauthorised access to flight control systems or AI algorithm manipulation, potentially disrupting operations or impairing its safety.⁷ The increasing reliance of the aviation industry on these technologies highlights the necessity of a legal framework that would be responsive to the vulnerabilities presented by them.

CYBER SECURITY CHALLENGES

The use of AI and IoT in the aviation sector increases the level of cybersecurity threats because these systems are the targets of cyberattacks. The prospect of data poisoning or hacking of AI-driven air traffic control systems that handle real-time data poisons flight paths and may cause misdirected flight paths or collisions.⁸ IoT devices embedded into aircraft to monitor them or

⁷ Eur. Union Agency for Cybersecurity [ENISA], Threat Landscape for Civil Aviation (2022), <https://www.enisa.europa.eu/publications/threat-landscape-for-civil-aviation> (last visited Sept. 18, 2025)

⁸ Embry-Riddle Aeronautical Univ., Aviation Cybersecurity: An Overview (2025), <https://portfolio.erau.edu> (last visited Sept. 18, 2025).

airports to provide passenger services can be used to interfere with key operations, including navigation or communication systems.⁹ As an example, the IoT sensors may be compromised and provide misleading information that could put the plane. Also, systems accessible to the passengers, i.e. online booking platforms or biometric check-ins, could be compromised, exposing the sensitive personal data and destroying trust.¹⁰¹¹ Those issues reveal the necessity of incorporating cybersecurity into the aviation security policies in order to secure the digital infrastructure.

INDIAN AVIATION LAW AND POLICY GAPS

In India, aviation safety and security are regulated by the Aircraft Act of the Aircraft in 1934 and the issuance of the Civil Aviation Requirements (CAR) stipulated by the Directorate General of Civil Aviation (DGCA). All these rules are aimed at physical risks, including terrorism or unauthorised access, yet do not specify threats related to the cybersecurity of AI and IoT. As an example, CAR Section 3, Series M, stipulates security measures on airports and aircraft, but fails to mention weaknesses of digital systems such as AI-driven flight control or IoT and baggage tracking.¹²¹³ Lack of cyber-specific laws exposes the aviation industry of India to new threats, especially with the growing adoption of smart technologies by airlines and airports.¹⁴ Moreover, the Digital Personal Data Protection Act, 2023, covers the overall data protection, yet lacks specific rules on how to protect passenger information against cyberattacks, which requires legislation-specific changes.¹⁵

The outdated Aircraft Act of 1934 disregards the fact that current aviation is highly interdependent, with many systems being vulnerable to hacking, data poisoning, and other unauthorised access, e.g. ransomware that can target flight-management systems. Delux Films emphasises the need to safeguard original work against unauthorised use, and suggests that similar policies may help protect aviation data proprietorship against cyber theft than have already been established by other jurisdictions such as the EU [10].

⁹ Int'l Air Transp. Ass'n [IATA], Cybersecurity Toolkit for Airlines (2023), <https://www.iata.org/en/programs/security/cybersecurity/> (last visited Sept. 20, 2025).

¹⁰ *United States v. Sabre Corp.*, 452 F. Supp. 3d 97 (D. Del. 2020).

¹¹ *Kadrey v. Meta Platforms, Inc.*, No. 3:23-cv-03417, 2023 WL 8039640 (N.D. Cal. Nov. 20, 2023).

¹² Directorate Gen. of Civil Aviation [DGCA], Civil Aviation Requirements, Section 3—Air Transport, Series M, Pt. I (India 2017).

¹³ *Sita Ram v. State of Uttar Pradesh*, AIR 1979 SC 745, (1979) 2 SCC 656.

¹⁴ Information Technology (Amendment) Act, No. 10 of 2009, § 43A, India Code (India) (amending Information Technology Act, No. 21 of 2000).

¹⁵ Digital Personal Data Protection Act, No. 22 of 2023

In addition, the aviation industry in India does not have a focal cybersecurity task force. In its absence, the industry will not be able to organise threat detection or mitigation, unlike the Aviation Cyber Initiative in the U.S. FAA (2016). The National Civil Aviation Policy, 2016, is concerned with the development of infrastructure, but is not committed to cybersecurity in operational procedures. This exclusion opens critical systems, such as air traffic control, to manipulation, as it is evident in legal cases such as *Eastern Book Co. v. D.B. Modak*, where originality and human control are required in order to protect a work. According to them, AI-generated aviation products (i.e. flight-path algorithms) are not necessarily legally protected brands, and this further complicates liability in cyber incidents. This loophole impedes immediate risk mitigation, as the case of *Kadrey v. Meta Platforms, Inc.*, shows in the world. In India, where data misuse has been a subject of fair-use and liability disputes, India needs to formulate cyber laws specific to the aviation sector and promote cooperation between the sector and the government.

RESHAPING AVIATION LAW AND SECURITY POLICIES

The challenges of cybersecurity presented by technological innovations should be solved by updating the aviation law and security policies to include strong protection. In India, it is important to revise the Aircraft Act, 1934, to provide compulsory cybersecurity evaluation of AI and IoT systems. This may entail the compulsory requirement for airlines and airports to regularly audit digital infrastructure and standards of encrypting data transmission. The DGCA may broaden the scope of CAR to encompass principles to achieve AI-driven systems, including anomaly-detecting instruments to detect cyberattacks immediately.¹⁶ Policy-wise, cybersecurity must be a fundamental part of the National Civil Aviation Policy, 2016, of India, which should encourage the adoption of renewable energy-powered data centres and energy-efficient AI algorithms to minimise environmental impact and increase the level of security.¹⁷ Internationally, there is a need to harmonise cybersecurity standards under ICAO since the aviation industry is international. Whether it is a collaboration framework, there can be protocols on sharing cyber threat intelligence across jurisdictions so that incidents are promptly addressed. Also, regulator-airline and regulator-technology joints can encourage technological

¹⁶ Airports Council Int'l [ACI], *Cybersecurity Guidelines for Airports* (2023), <https://aci.aero/publications/cybersecurity-guidelines/> (last visited Sept. 20, 2025).

¹⁷ Directorate Gen. of Civil Aviation [DGCA], *National Civil Aviation Policy of India* (2016), <https://dgca.gov.in/digigov-portal/?page=jsp/dgca/InventoryList/policyFile/nationalCivilAviationPolicy2016.pdf&wh=rj3bH3m2> (last visited Sept. 18, 2025).

advances in cybersecurity, like blockchain for safe data processing or AI-based threat detection frameworks. Aviation staff cybersecurity-focused training is also crucial in developing resilience to cyber threats.

INTERNATIONAL LEGAL AND POLICY FRAMEWORKS

Globally, the International Civil Aviation Organisation (ICAO) offers a framework of aviation security, in Annexe 17, that focuses on risk assessment and risk mitigation.¹⁸ Still, its cybersecurity provisions are general, which do not provide much information on AI and IoT systems protection. Conversely, higher authorities such as the United States and the European Union have already started to align cybersecurity with aviation regulation. The U.S. FAA Extension, Safety and Security Act of 2016 is mandatory to have cybersecurity in the air traffic control system because of its critical importance to flight safety.^{19,20} Regulation (EC) No 300/2008 by the EU obliges operators to adopt cybersecurity measures of digital infrastructure that will act as a precedent in harmonised standards.²¹ These global frameworks give examples of how India can come up with cyber-specific aviation regulations in order to align with global best practices.

RECOMMENDATIONS

Modify Aviation Laws: Revision of the Aircraft Act, 1934, to encompass cybersecurity requirements of AI and IoT systems, whereby airlines and airports should conduct periodic cyber risk review.

Implement ICAO Cybersecurity Recommendations: Indian CAR-based on the ICAO Aviation Cybersecurity Strategy with a focus on threat detection and incident response.²²

¹⁸ Convention on International Civil Aviation, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295 (Chicago Convention).

¹⁹ FAA Extension, Safety, and Security Act of 2016, Pub. L. No. 114-190, 130 Stat. 615 (codified as amended in scattered sections of 49 U.S.C.)

²⁰ Fed. Aviation Admin. [FAA], FAA Cybersecurity Strategy (2023), <https://www.faa.gov/about/initiatives/cybersecurity> (last visited Sept. 19, 2025).

²¹ Regulation (EC) No. 300/2008 of the European Parliament and of the Council of 11 March 2008 on Common Rules in the Field of Civil Aviation Security, 2008 O.J. (L 97) 72.

²² Int'l Civil Aviation Org. [ICAO], Aviation Cybersecurity Strategy (2022), <https://www.icao.int/cybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx> (last visited Sept. 20, 2025).

Form a Cybersecurity Task Force: Establish a task force with experts in DGCA to establish aviation-specific cybersecurity standards.²³

Reward Innovation: Provide incentives to airlines that implement AI-based cybersecurity technologies and data centres that are powered by renewable energy.²⁴

Standardise on a Global Basis: Crusade in support of ICAO-designed global cybersecurity guidelines so that there can be uniformity in jurisdictions.

Step-up Training: Require aviation staff to undergo cybersecurity training to inculcate a culture of cyber awareness, as suggested by studies in the industry.

Enhance Data Protection: The Digital Personal Data Protection Act, 2023, should be expanded to incorporate aviation-specific cyber incident reporting.

CONCLUSION

Aviation is being transformed by technological innovations such as AI and IoT, but the risks to cybersecurity require legal and policy changes urgently. The aviation regulations of India are strong in traditional safety, but not in cyber threats.²⁵ India can ensure its aviation industry is not at risk of cyber-attacks through law amendments and global alignment, as well as industry integration, as its aviation industry capitalises on the improvements of technology. Such actions make sure that the aviation law and security policies are developed according to the needs of the digital age.

REFERENCES

1. Aircraft Act 1934 (India).
2. Digital Personal Data Protection Act 2023 (India).
3. FAA Extension, Safety, and Security Act, Pub L No 114-190, 130 Stat 615 (2016) (United States).

²³ RAND Corp., Cybersecurity Challenges in the Aviation Sector (2024), https://www.rand.org/pubs/research_reports/RRA1234-1.html (last visited Sept. 20, 2025).

²⁴ Airlines for Eur. [A4E], Cybersecurity Framework for Airlines (2022), <https://a4e.eu/publications/cybersecurity-framework/> (last visited Sept. 20, 2025).

²⁵ United Nations Off. on Drugs & Crime [UNODC], Cybercrime Module 12: Aviation Sector Vulnerabilities (2023), <https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/aviation.html> (last visited Sept. 20, 2025).

4. Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security [2008] OJ L97/72.
5. International Civil Aviation Organisation, *Annexe 17: Security* (11th edn, ICAO 2020).
6. Directorate General of Civil Aviation, *Civil Aviation Requirements, Section 3, Series M* (India, 2017).
7. 'Cyber Terrorism and Civil Aviation: Threats, Standards, and Regulations' (2024) 34 *Transnational Law & Contemporary Problems* 123.
8. Embry-Riddle Aeronautical University, 'Aviation Cybersecurity: An Overview' (portfolio.erau.edu, 2025) <https://portfolio.erau.edu> accessed 9 September 2025.
9. UC Berkeley, 'Cybersecurity in Civilian Aviation: Insights for Advanced Nuclear Technologies' (fhr.nuc.berkeley.edu, 2025) <https://fhr.nuc.berkeley.edu> accessed 9 September 2025.