INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

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

CRITICAL ANALYSIS ON AVIATION CYBERSECURITY IN INDIA

AUTHORED BY - NAVEENA G.J & LAKSHMI .K

Abstract

The unprecedented rate of digitization and technological automation in aviation, the sector faces various challenges to keep sensitive operational and passenger data safe. In aviation, cyber threats could affect safety, operational continuity, regulatory compliance, and economic stability, and cybersecurity needs to be all-encompassing in modern air transport. This paper presents a critical assessment of the present state of the cybersecurity framework concerning aviation in India- different sources and types of cyber threats that the industry is exposed to, such as hacking, ransomware, supply chain attack, and insider threat. It also assesses the current legal and regulatory regime comprising the IT Act, sectoral aviation laws, and emerging guidelines and identifies the areas wherein the said framework falls short in responding appropriately to sector-specific risks. Presently, there is no specific unified and comprehensive aviation cybersecurity regulation in India, but rather a fragmented approach whereby general cyber laws, sector-specific aviation legislation, and emerging data protection requirements apply. The aim of this research paper is to delve into the concept and role of cybersecurity in the aviation sector; identify the gaps in its implementation and legislative oversight; and propose recommendations to upgrade standards and legislative measures in pursuit of ensuring an adequate level of aviation cybersecurity. Moreover, our study discusses feasible measures for its implementation to enhance cybersecurity, such as robust policies and procedures, adoption of international best practices, and development of a dedicated cybersecurity framework for aviation. Based on an analysis of the impact of cyber incidents and current defences, the paper gives reasons for a necessary comprehensive, proactive, and coordinated approach to protecting India's aviation sector from evolving cyber threats.

Introduction

Airports have evolved from being principally physical infrastructures into highly networked digital ecosystems. Most critical operations today, including passenger processing, baggage handling, flight information systems, energy and building management, and air traffic control,

ISSN: 2582-6433

are exceedingly reliant on networks, cloud services, and IoT devices[1].

A major study found that over 80,000 cyberattack incidents were recorded in the Indian aviation network in 2024, Recent security assessments have exposed some shocking vulnerabilities. For example, automated brute-force attacks were recorded using 296 unique usernames and 15,928 passwords-a sure sign that something has gone wrong with the authentication mechanisms. The sources of malicious traffic have been traced to several countries including China, India, the United States, South Korea, and Taiwan, indicating the global spread and reach of these threats. Major Vineet, founder and global president of Cyber Peace, said, "This report is a wake-up call for the Indian aviation industry. Cybersecurity has ceased to be an option; it is a core pillar of aviation safety and operational resilience. Immediate action is needed to harden systems against evolving cyber threats."

On a global scale, the aviation sector has become an attractive target for both cybercriminals and state-sponsored actors. Indeed, modern aviation networks, supporting air traffic control, flight operations, passenger management, and airport security, are highly interconnected, establishing a wide, complex attack surface.[2] Such digital transformation, while fostering efficiency, requires stringent cybersecurity measures in terms of proactive measures to protect this critical aviation infrastructure. Cyber threats largely intend to gain unauthorized access to key information in different fields through the internet. Recently, the rate of cyberattacks has increased tremendously over other industries, while aviation, due to its multidimensional, interactive, and global nature, tends to be the main target. Being a significant concern in economic and social development, its cybersecurity concern is raised at an international level.

Although design, technology, and efficiency in aviation operations have been improving continuously, the sector remains highly prone to cyber threats. With rapid growth in global connectivity using information and communication technologies, not all relevant disturbances can be foreseen or prevented in advance[3]. In essence, the increased electronic interconnectivity

[1] Pathare, Shirin, *The Rising Tide of Cyberattacks in Indian Aviation: Are We Prepared?*, 63 SATS Cybertech (Blog, Apr. 22, 2025), https://63sats.com/blog/the-rising-tide-of-cyberattacks-in-indian-aviation-are-we-prepared/

[2] Over 80,000 Cyber Threats in India's Aviation Sector — Study," *ET Edge Insights* (Mar. 4, 2025), https://etedge-insights.com/trending/over-80000-cyber-threats-in-indias-aviation-sector-study

[3] Singh, Satyarth, Cyber Security Laws in Civil Aviation in India: A Critical Analysis, (LL.M. dissertation, CHRIST (Deemed to be University) May 19, 2023) (on file with CHRIST University Institutional Repository), https://archives.christuniversity.in/items/show/2689

ISSN: 2582-6433

of aircraft systems with ground systems increases the risk to the safety and security of aviation. Threat actors, including terrorists, hacktivists, and organized crime groups, have begun to exploit cyberspace as a weapon to compromise aviation operations. As the industry moves toward automation and further technological dependency, protection of the aviation ecosystem becomes increasingly important. The IT infrastructure forms the backbone of both ground and flight operations, directly influencing the industry's safety, efficiency, and financial stability. It is thus important to take early steps in their detection and prevention to ensure sustained growth and security of the aviation sector.

Research problem

The existing legal framework primarily governed by the Aircraft Act, 1934 and the Information Technology Act, 2000 lacks a unified and aviation specific regulatory mechanism to address cyber risks. The absence of clear provisions defining liability, reporting obligations, creating challenges like security, privacy balance. This gap results in amending existing data protection laws to incorporate aviation focused safeguards is essential for ensuring secure and accountable data governance in the aviation sector.

Research Objective

- The current cyberthreats landscape and vulnerabilities within India's civil aviation sector
- Analyse gaps in existing Indian cybersecurity laws, regulations, and institutional frameworks related to aviation security.
- Research the scope of the existing legal framework to deal with cyberattacks in the aviation industry.
- The alignment of Indian aviation cybersecurity practices with international standards and ICAO guidelines.

Research Methodology

The research adopts a doctrinal methodology, the analysis of existing legal and regulatory frameworks governing cybersecurity in civil aviation.

Research Question

I. Whether the Civil Aviation & Cyber Security Laws in India need to be modified with respect

ISSN: 2582-6433

to the legislation with International Standards?

II. How far the existing legal framework is enabling to prevent cyber risks in civil aviation?

Literature review

1) Anjan Sinha et al. (2018) discuss the growing cyber vulnerabilities in India's aviation sector, highlighting risks in air traffic control, airline networks, and aviation websites. They emphasize the need for secure communication systems and promoting a cybersecurity culture through training and regular assessments. The authors also stress improving air traffic surveillance to prevent hacking threats. However, the study lacks specific guidelines or standardized frameworks for ensuring cybersecurity across airlines, making it more conceptual than policy-oriented.
2) Calvin N.M.N. Nobles et al. (2022) emphasize the urgent need for a "global aviation cybersecurity defence policy" to address vulnerabilities in the interconnected aviation ecosystem. They argue that cybersecurity gaps pose serious risks to the global aviation industry's economic stability and safety. The study highlights the importance of international cooperation, information sharing, and strong defensive strategies to combat evolving cyber threats. The authors suggest that a unified global policy could effectively close security gaps and prevent malicious exploitation of aviation systems.
3) Rajesh Kumar et al. (2023) survey cybersecurity challenges in India's aviation sector, emphasizing vulnerabilities in air traffic control systems and airline operations. They underscore the need for secure communication protocols, real-time threat detection, and incident response mechanisms.
4) Vivek Singh and Meera Joshi (2022) provide an overview of cybersecurity strategies in Indian aviation, with a focus on recent cyber incidents and their operational impact. They review the role of governmental agencies and existing cyber laws, highlighting gaps in specialized aviation cybersecurity policies.

Regulatory and Legal Framework Governing Aviation in India

The Aircraft Act, 1934

The Aircraft Act, 1934 is the foundational Act that laid the basis of civil aviation in India for several decades. It provided a legal framework to control all activities concerning flying, including the regulation of aircraft manufacture and registration, licensing of flight personnel, air traffic control, and even the safety of navigation. It gave the Central Government the power to make detailed rules regarding the manufacture, operation, and maintenance of aircraft,

ISSN: 2582-6433

covering the areas necessary for aviation safety and security[4] which empowered the DGCA to issue directives concerning any matter relating to airworthiness certification, operational control, and safety management[5]. The Bill titled the Bharatiya Vayuyan Adhiniyam, 2024 was introduced in the Lok Sabha on 31 July 2024. The New Act explicitly brings within its scope regulation of design, manufacture, maintenance, possession, use, operation, sale, export and import of aircraft. The 1934 Act focused more on manufacture, possession, use, operation, sale, import and export. It aims to align India's legal framework with contemporary aviation realities (maintenance, manufacturing) and international best- practices under ICAO norms.

Relation To Information Technology Act, 2000

The Information Technology Act, 2000 is the cornerstone of India's cybersecurity legal framework, extending its applicability to all sectors, including aviation. In tune with growing reliance on digital systems for air traffic management, passenger data handling, and airport operations, the IT Act essentially provides a legal safeguard against cyber-attacks on these critical infrastructures.[6]

Section 43 prescribes punishment for unauthorized access, data theft, hacking, or disrupting computer systems, thus covering the malicious intrusion into the databases of airlines, manipulation of information related to flights, interference with airport IT networks, and so on. Section 43A imposes a direct obligation on corporate bodies, including airlines and airport operators, to adopt "reasonable security practices" while dealing with sensitive personal data. Any negligence leading to data loss or damage renders the entity liable to compensate the affected party[7]. Moreover, Section 65 criminalizes tampering with computer source documents, an important safeguard against unauthorized modifications of aviation software or operational data. Sections 66, 66B, 66C, and 66D deal with various computer- related offenses like identity theft, phishing, and unauthorized access to records—of particular relevance to passenger information systems and online ticketing platforms. Section 66F defines cyberterrorism, which has particular significance for aviation because it encompasses cyberattacks against critical

[4] Sarosh Damania, Aviation Law in India: Guide to Regulations & Legal Framework, Sarosh Damania & Co. Blog (Aug. 9, 2024), https://saroshdamania.com/aviation-law-in-india/
[5] *The Legal Framework for Commercial Aviation in India*, The Law Communicants (Jul. 1, 2024), https://thelawcommunicants.com/the-legal-framework-for-commercial-aviation-in-india/ (last visited Nov. 2, 2025)
[6] *Aviation Laws and Regulations — India*, ICLG (Mar. 7, 2025), https://iclg.com/practice-areas/aviation-laws-and-regulations/india (last visited Nov. 2, 2025).
[7] *Aviation Laws and Regulations — India*, ICLG (Mar. 7, 2025), https://iclg.com/practice-areas/aviation-laws-and-regulations/india (last visited Nov. 2, 2025).

ISSN: 2582-6433

systems such as air traffic control, radar networks, or airport communication systems, hence attracting sentences of life imprisonment.

These sections, 69, 69A, and 69B, respectively, give the government authority to intercept, monitor, or block electronic information in the interest of national security, thus facilitating timely action against cyber incidents that could affect aviation safety. Sections 72 and 72A deal with the protection of confidentiality by imposing penalties for disclosure of sensitive and personal information without consent, which is an essential requirement for protecting passenger and operational data. The IT Act has indeed provided a broad legal framework for aviation cybersecurity in India, pertaining to data protection, system integrity, and government oversight[8]. It criminalizes unauthorized access to information, identity theft, cyberterrorism, and data breaches, thus holding people responsible and deterring them. In the context of rapidly changing technology, legal measures put in place by the IT Act enhance resilience within India's aviation ecosystem and reinforce the commitment to safety, security, and reliability within air transport operations.[9]

The Airports Authority Act,1994

The Airports Authority of India Act, 1994 serves as the principal legislation establishing the Airports Authority of India (AAI), the statutory body responsible for the management, development, and modernization of civil aviation infrastructure across the country[10]. Enacted to ensure efficient and coordinated administration of airport operations, the Act provides for the constitution, powers, and functions of the AAI with the objective of enhancing the safety, efficiency, and accessibility of India's aviation sector.

Under this Act, the AAI is entrusted with a broad range of responsibilities, including the creation, upgradation, maintenance, and management of civil aviation infrastructure such as airports, airstrips, and civil enclaves throughout India.[11] It also oversees the establishment and

[8] *Aviation Laws in India* (June 2025), available at https://vakeellaw.com/wp- content/uploads/2025/06/Aviation-Laws-in-India.pdf
[9] Poonam Dwivedi, *Navigating the Skies: An Overview of Aviation Law in India*, 5 Int'l J. for Multidisciplinary Research (IJFMR) 6 (Nov.–Dec. 2023), https://www.ijfmr.com/papers/2023/6/11387.pdf (last visited Nov. 2, 2025
[10] The Airports Authority of India Act, 1994, Act No. 55 of 1994 (Sept. 12, 1994) (India), available at https://www.indiacode.nic.in/bitstream/123456789/1979/1/AAairpoert1994_55.pdf.
[11] *Regulatory Frameworks in India's Aviation Sector*, Wright Research (last visited Nov. 2, 2025), https://www.wrightresearch.in/encyclopedia/chapter-report/chapter-4-regulatory-frameworks-in-indias-aviati on-sector

ISSN: 2582-6433

operation of aeronautical communication systems, navigational aids, and air traffic management services, except where such functions fall under the control of the armed forces.

Major Cyber Threats in Aviation Sector

In recent years, airports and aviation systems have emerged as prime targets for cybercriminals due to their reliance on digital infrastructure and the potential for large-scale disruption[12]. Among the most pressing threats are ransomware attacks, which can shut down airport operations, delay passenger and baggage screening, and induce widespread public panic often compelling authorities to meet ransom demands to quickly restore systems.

Globally, ransomware attacks in the aviation sector have increased by 600% year-on-year, and India has also been affected, with at least 27 significant incidents between 2024 and 2025 involving ransomware or credential theft.[13] Attackers are increasingly leveraging AI- generated phishing, advanced social engineering techniques, and zero-day vulnerabilities to compromise systems. Similarly, data breaches affecting critical systems, such as flight information displays or communication networks, underscore the urgent need for robust cybersecurity frameworks in aviation management.

Air Traffic Control (ATC) systems in India face growing cyber threats due to aging infrastructure and increasing digitalization. Many systems lack encryption and strong access controls, making them vulnerable to ransomware and unauthorized access[14]. Flat network designs and weak authentication allow attackers to move within systems, while insider threats and phishing further heighten risks. Malware infections can disrupt navigation and radar operations, causing flight delays or cancellations. Strengthening cybersecurity and modernizing ATC infrastructure are crucial for ensuring aviation safety and continuity.

The interconnected nature of global aviation means that any major cyber incident at an airport can have a domino effect on international travel and trade. Recent data indicates that

[12] *The State of Cybersecurity in Airports*, White Paper, Armis Inc. (May 2025), https://media.armis.com/wp-state-of-cybersecurity-in-airports-en.pdf (last visited Nov. 2, 2025)
[13] Rosehana Amin & Tom van der Wijngaart, *Cyber Threats in the Aviation Industry*, Clyde & Co (Nov. 2024), https://www.clydeco.com/en/insights/2024/11/cyber-threats-in-the-aviation-industry/ (last visited Nov. 2, 2025)
[14] John China, *The Current Cybersecurity Landscape, Explained*, J.P. Morgan (May 27, 2025), https://www.jpmorgan.com/insights/cybersecurity/phishing/the-current-cybersecurity-landscape-explained (last visited Nov. 2, 2025)

ISSN: 2582-6433

cyberattacks within the aviation industry increased by 131% between 2022 and 2023, with a significant proportion targeting airspace users. The financial, operational, and reputational damage caused by such incidents is immense. Cyber incidents in aviation are typically high-profile, attracting media attention and regulatory scrutiny. They often involve multiple jurisdictions, given the cross-border nature of air transport, and can lead to heavy regulatory fines and costly legal actions from affected passengers and stakeholders.

Among the most sophisticated adversaries are nation-state actors, who pose long-term and highly resourced threats to aviation infrastructure.[15] The complexity and interdependence of Communication, Navigation, and Surveillance (CNS) infrastructure magnify the potential scope and impact of these attacks, as disruptions in one component can cascade across the entire aviation ecosystem.

Equally concerning are insider threats, which are often underestimated compared to external cyber risks. Insiders' employees, contractors, or third-party vendors possess legitimate access credentials and detailed knowledge of internal systems, making them capable of bypassing traditional security defences.[16] Unlike external hackers who rely on phishing or malware, insiders exploit their authorized privileges and operational familiarity to conduct covert actions. Such breaches can be devastating, as seen in cases involving major corporations and government agencies worldwide.

The threat landscape continues to evolve rapidly. In 2024 alone, there were 3,158 recorded data compromises, matching the record-high numbers from the previous year. However, victim notifications surged by 211%, largely driven by a few mega-breaches, each affecting over 100 million individuals[17]. These figures reflect the growing frequency, sophistication, and impact of cyber incidents across industries including aviation emphasizing the urgent need for a comprehensive, technology-driven, and resilient cybersecurity framework.

Automated attacks target databases and servers by systematically cycling through millions of

[15] Akshay Joshi, *The Current Cybersecurity Landscape Explained*, World Economic Forum (Feb. 2025), https://www.jpmorgan.com/insights/cybersecurity/phishing/the-current-cybersecurity-landscape-explained
[16] *What Is the Cyber Threat Landscape?* UpGuard Blog (last visited Nov. 2, 2025), https://www.upguard.com/blog/cyber-threat-landscape
[17] George Prichici, Opinion: How Can Airports Boost Their Cybersecurity in 2024?, Passenger Terminal Today (Jan. 10, 2024), https://www.passengerterminaltoday.com/opinion/opinion-how-can-airports-boost-their-cybersecurity-in-2024.html

ISSN: 2582-6433

username-password combinations and exploiting unsecured protocols. In mid-2024, a simulated study of the Indian aviation network recorded over 80,000 such incidents.

Supply chain cyberattacks pose a major risk to airport networks that Hackers often exploit third-party vendors that maintain digital connections with airports or airlines, using them as entry points to spread malware or gain access to sensitive operational data as airports operate within complex ecosystems that depend heavily on external service providers. By targeting vulnerable vendors, attackers can indirectly compromise critical airport operations.

Challenges in Aviation Cybersecurity

The aviation industry faces critical cybersecurity challenges that could impact safety and the efficiency of operations. Onsite security remains highly important. Airlines and aircraft are areas of vulnerability for those seeking to gain unauthorized access, interfere with systems, or attack on the ground[18]. The sector is digitizing to enhance the flying experience utilizing advancements such as fifth-generation wireless technology, biometric identification, and the transition to ticketless travel. Implementing this introduces opportunities for hackers to get in and target key infrastructure.

A significant challenge concerns the fact that cyber and physical safeguards do not effectively integrate, resulting in weaknesses for malicious activities. Many online systems, like remote desktops and flight information displays, are publicly available on the internet lacking adequate safeguards, which renders them vulnerable to attack[19]. Relying on older technology on aircraft creates greater risks because these outdated technologies are inadequate for addressing today's cyber security landscape. Even modern aircraft equipped with Android based infotainment could accidentally produce further security flaws, increasing the threat of a cybersecurity breach.

Aircraft uses GPS information for accurate and continuous position computation during all Phases of flight that this position computation is used for aircraft navigation GPS also provides reference time information for the aircraft's clocks different systems on an aircraft such as ADS-

[18] P.J. Orretjer, *A Cybersecurity Analysis of Today's Commercial Aircrafts and Aviation Industry Systems* 22 (M.S. thesis, Utica Coll., 2018).
[19] E. Ukwandu et al., *Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends*, **Info.** 13 (3) 146 (2022), https://doi.org/10.3390/info13030146

ISSN: 2582-6433

B (Automatic Dependent Surveillance-Broadcast)[20] fuel data communication backup speed enhanced Ground Proximity Warning System use GPS information[21] which states that[22] GPS spoofing refers to sending false GPS information to an aircraft when an aircraft uses this signal the aircraft senses that it is at a different location although the aircraft is in its correct position this has an impact on performance-based navigation routes[23] GPS interference both GPS jamming and GPS spoofing are a part of GPS interference effects to fly safely out of the interference effects it would require timely detection and intervention by the flight crew a few General techniques would be to cross check the aircraft position by manually tuning a ground navigation Aid or deselecting[24].

International Perspectives on Aviation Cybersecurity

ICAO recognizes cybersecurity as one of the most pressing challenges in global aviation. In 2019, ICAO adopted the Aviation Cybersecurity Strategy, which emphasizes a risk-based and collaborative approach. It calls for shared responsibilities among states, industry, and international organizations this strategy focuses on building capacity, enhancing information sharing, and ensuring that cybersecurity is integrated into the overall aviation safety and security framework[25]. The European Strategic Framework for Aviation Cybersecurity, which provides guidance for states and stakeholders in Europe. It focusses has been on promoting harmonization across member states, facilitating exchanges of best practices, and ensuring consistent implementation of cybersecurity measures in line with ICAO's global strategy[26].

The UAE recognizes that cybersecurity is a shared responsibility. The key has been collaboration not only within the aviation sector but also across other critical infrastructure sectors. In France, they have established a national aviation cybersecurity framework that brings together civil aviation, defence, and cybersecurity agencies. The main aim is to ensure coherence between national policies and international obligations and also actively contribute

[20] M. Ellinor, *Report: Hackers Broke into FAA Air Traffic Control Systems* (CNET, 2009), https://tinyurl.com/y3yb2lmc
[21] L. Jones & R. Patel, *Enhancing Cybersecurity Measures in Airport Systems*, **Cybersecurity Rev.** (2023)
[22] D. McCallie, J. Butts & R. Mills, *Security Analysis of the ADS-B Implementation in the Next Generation Air Transportation System*, **4 Int'l J. Critical Infrastructure Prot.** 78, 78–87 (2011).
[23] N. Kagalwalla & P.P. Churi, *Cybersecurity in Aviation: An Intrinsic Review*, in *Proceedings of the 2019 5th Int'l Conf. on Computing, Communication, Control & Automation (ICCUBEA)* 1, 6 (IEEE 2019).
[24] U.K. Gov't, *International Scientific Report on the Safety of Advanced AI: Interim Report* (May 16, 2024), https://www.gov.uk/government/publications/international-scientific-report-on-the-safety-of-advanced-ai/international-scientific-report-on-the-safety-of-advanced-ai-interim-report
[25] *The Dark Side of DarkTrace – Five Takeaways for Customers and Partners* (Feb. 8, 2023), https://cyglass.com/newsand-events/dark-side-darktrace/
[26] International Civil Aviation Organization (ICAO). *Cybersecurity in Civil Aviation.* 2020. https://www.icao.int/

ISSN: 2582-6433

to ICAO and ECAC initiatives. The key takeaways are the need to maintain a balance between security requirements and operational efficiency, especially as new technologies like AI and remote towers emerge. Cybersecurity in aviation is not merely a technical issue it is a global governance challenge requiring coordination among states, industry, and international organizations. To address existing threats and risks, civil cybersecurity needs to be agreed upon at national, regional, and international levels. For this, ICAO serves as a top forum and the best platform for discussing cybersecurity issues globally. The organization holds various meetings, seminars, and other events to facilitate these discussions.

AIR INDIA CYBER BREACH

In May 2021, Air India experienced a significant data breach affecting millions of passengers. The breach involved unauthorized access to the airline's database, which contained a wide range of personal information collected from customers. The compromised data spanned a period from August 2011 to February 2021. The data exposed in the breach included names, dates of birth, contact details, passport information, and Social Security Numbers of affected passengers. The Air India data breach occurred when cyber attackers targeted the airline's passenger service system, managed by Swiss technology company SITA. Specific methods used by the hackers have not been disclosed, but the incident underscores the importance of robust cybersecurity measures to protect sensitive customer information. In response to the hacking incident, Air India took several measures to secure its platform and prevent future breaches[27]. These actions included securing the compromised servers, engaging external data security specialists, and notifying affected customers. Although passwords were not accessed by the hackers, Air India encouraged passengers to change their passwords as a precaution.

Additionally, the airline strengthened cybersecurity protocols, implemented regular employee training, improved data protection measures, conducted a thorough review of third-party vendors, and formulated an effective incident response plan to mitigate the damage from potential cyberattacks in the future[28].

AKASA AIR CYBER BREACH

The Akasa Air cyber breach, caused by a temporary technical configuration error in August

[27] Tommaso De Zan, Fabrizio d'Amore & Federica Di Camillo, *The Defence of Civilian Air Traffic Systems from Cyber Threats* (2015).
[28] E. Mazareanu, *Leading Airports Worldwide by Aircraft Movements* (Oct. 2020), https://www.statista.com/statistics/226823/largest-airports-worldwide-by-flight-operations

ISSN: 2582-6433

2022, exposed personal information of over 34,000 customers, including names, gender, email addresses, and phone numbers. Although no travel-related data or payment information was compromised, the incident posed significant risks of phishing and privacy violations. The airline swiftly responded by shutting down the affected systems, enhancing security measures, notifying the Indian Computer Emergency Response Team and informing impacted customers to be cautious of potential phishing attempts[29].

Suggestions

India requires a dedicated and comprehensive legal framework to strengthen cybersecurity in civil aviation. A specialized national aviation cybersecurity monitoring body should be established to oversee digital security across airlines, airports, and Air Traffic Control (ATC). This body must develop sector-specific cybersecurity policies, conduct regular assessments, Update security protocols regularly, encourage timely report of cyber incidents and ensure compliance with international standards such as ICAO Annex 17 and Annex 10.

To enhance accountability, the Aircraft Act, 1934 should be amended to include mandatory cybersecurity standards for all aviation operators, compulsory reporting of cyber incidents, and the requirement of regular vulnerability audits. It must also empower DGCA and BCAS to issue binding cybersecurity directives and impose clear penalties for non-compliance. At present, the Act focuses largely on physical safety and technical airworthiness, overlooking the digital dimension of aviation safety.

Similarly, the Information Technology Act, 2000 should be amended to include aviation-specific protections. This includes declaring aviation digital systems such as avionics, air traffic management systems, and airport networks as "critical information infrastructure,"

mandating cyber incident reporting to civil aviation authorities, and creating special penalties for attacks that endanger flight operations or passenger data. The Act's current provisions are too general and fail to address the high risk, safety critical nature of aviation systems.

India needs to address the gaps where it does not fully implement ICAO Annexes, especially in areas critical to aviation safety and security. It falls short of ICAO Annex 17 requirements.

[29] Int'l Civil Aviation Org. (ICAO), *Initial Capability for Ground Surveillance*, in *Global Air Navigation Plan 2013– 2028* (2013).

ISSN: 2582-6433

The Annex defines key terms like “acts of unlawful interference,” “screening,” and “security control”, “Aircraft security check”. Chapter 4 of Annex 17 focuses extensively on preventive security measures, including cybersecurity frameworks to protect critical aviation infrastructure such as avionics, air traffic control systems, and airport IT infrastructure. India currently lacks aviation-specific cybersecurity legislation aligned with these requirements, such as detailed risk assessments, incident reporting protocols, and resilient response systems as specified by ICAO. The IT Act offers a more general cybersecurity framework but does not address the sector-specific complexities of aviation cybersecurity detailed in Annex 17. India’s current legislative framework significantly lacks in fully adopting these Chapter 5 provisions. India does not have one clear law that brings together all aviation security agencies like DGCA, BCAS, CISF, and intelligence departments to work in a coordinated way during a crisis. ICAO requires countries to have such a unified, legally mandated crisis- management system, but India’s laws do not provide this. The laws also do not explicitly require standardized, timely reporting of unlawful interference incidents to ICAO or establish robust, legally binding information sharing protocols between aviation stakeholders and enforcement agencies. While operational emergency response practices exist in India, comprehensive statutory backing enforcing standardized aviation security emergency preparedness and continuous evaluation is missing. Moreover, the Aircraft Act does not clearly specify enforcement or accountability mechanisms for failure to respond effectively to such interference. The absence of these comprehensive, codified standards limits the effectiveness of India's aviation security framework in fully aligning with ICAO India’s aviation laws do not fully cover the specific requirements of ICAO Annex 10 Volume II Chapter 3. This chapter asks countries to ensure that all aeronautical messages are securely sent, received, and protected from tampering, but Indian Acts do not clearly mandate this. It also requires strict logging of all communications, proper record-keeping, and clear emergency communication procedures to maintain safe operations none of which are fully written into Indian law. The rules for coordination between communication units and aviation-specific cybersecurity measures are also not clearly defined. In India, the laws do not clearly cover the emergency communication requirements needed for aviation. Even though different aviation and telecom departments have their own operational response systems, there is no specific law in the IT Act, Telecommunications Act, or Aircraft Act that makes these emergency procedures mandatory or standardized for aeronautical communication. Because of this, India does not have a uniform national system to handle communication disruptions, including cyberattacks that could affect critical aviation signals. There are also no legally defined rules for how communication stations and agencies should

ISSN: 2582-6433

coordinate during emergencies, and no clear legal requirements for cybersecurity measures to protect aviation communication systems. This creates important gaps in ensuring safe and reliable aeronautical communication.

In India, basic safety management exists through DGCA rules that require airlines and airports to have Safety Management Systems (SMS), but there are still major gaps compared to ICAO Annex 19. India does not have a single, fully written law covering a State Safety Program (SSP) for all aviation sectors with clearly defined roles. Rules for sharing safety data, protecting it, and building a strong safety intelligence system are not enough, which makes proactive safety management difficult. Continuous monitoring of safety performance and enforcing rules at the state and operator level are not strongly backed by law. Promotion of safety culture and mandatory safety training also need improvement. New ICAO requirements for drones (RPAS) and certified heliports have not yet been fully included in Indian regulations.

In conclusion, India's aviation cybersecurity requires both legislative reform and institutional modernization. Amendments to the Aircraft Act and IT Act, creation of a dedicated aviation cybersecurity authority, mandatory independent audits, and legally codified reporting and crisis management systems are crucial to align India's aviation safety architecture with ICAO standards and global best practices.

Further, the judicial approach and legal framework must evolve to impose strict liability on entities responsible for cybersecurity breaches, acting as a deterrent against negligence. Laws should also mandate timely reporting of cybersecurity incidents to national authorities such as the National Cyber Security Coordinator ensuring swift response and mitigation.

Conclusion

The aviation sector is an area where technological advances face cybersecurity concerns. Air transportation is being transformed by computers and also robots, but this also means things are easier to hack, and aviation infrastructure are open to cyber-attacks. So, instead of merely dealing with physical dangers, it is important to improve our ability to handling system malfunctions to ensure aviation secure, according to schedule, and reliable. The analysis demonstrates that India's legal and regulatory system is inadequately equipped to address this novel threat environment.