Available online at: http://jurnal.uns.ac.id
Yustisia Jurnal Hukum
| ISSN (Print) 0852-0941 | ISSN (Online) 2549-0907 |

Aviation Cyber Security in India: Legal Gaps, International Frameworks, and Policy Reforms

Mohammad Owais Farooqui[1]; Adnan Sarhan[2]; Faizan Mustafa[3]
[1,2]College of Law, University of Sharjah, United Arab Emirates
[3]Chanakya National Law University, Patna, India
Corresponding author's email: mfarooqui@sharjah.ac.ae

Article Information
Received for publication: April 30, 2025
Accepted after corrections: August 30,2025

Keywords: *Aviation cyber security; legal liability; policy reform*

DOI:10.20961/yustisia. v14i2.101653

Abstract
Large passenger data breaches, ransomware attacks, and politically motivated Distributed Denial of Service attacks show that aviation faces cyber dangers to safety, national security, and consumer confidence. This article examines India's aviation cybersecurity governance, evaluates legal culpability in cyber incidents, and proposes worldwide best practices-based reforms. This study uses doctrinal and analytical legal methods. This study compares ICAO, EU, and US international frameworks, notably NIS2 and GDPR, to aviation and cybersecurity statutes, regulations, policy papers, and judicial interpretations. The findings reveal that India has fundamental cyber and data protection laws but no aviation-specific cybersecurity policies, unambiguous liability allocation, or strong enforcement. Institutional fragmentation and resource constraints increase these risks. Comparing India to other countries shows it violates worldwide laws, emphasising the need for accountability, supervision, and cyber risk management changes in the aviation sector. India can improve resilience, foster a proactive security culture, and assure passenger trust and operational safety in the digital age by following ICAO regulations and EU and US best practices.

I. Introduction

An increase in cyberattacks has been observed in India's civil aviation sector, including airline data breaches and airport system invasions. This circumstance has highlighted the prevalence of cyber risks and prompted

critical inquiries regarding legal liability and regulatory preparedness. SpiceJet, a significant airline in India, was the victim of a data breach in early 2020. The breach exposed the confidential information of more than 1.2 million passengers (Singh & Whittaker, 2020). In May 2021, Air India revealed that a hack on its passenger service system and the SITA data breach affected the data of approximately 4.5 million travellers (Singh, 2021). In May 2022, a ransomware attack on SpiceJet crippled the airline's IT systems, leaving flights delayed for hours and hundreds of passengers stranded at airports (Singh & Sharma, 2022). More recently, in April 2023, a hacker group launched coordinated Distributed Denial of Service (hereinafter written to DDoS) attacks against the websites of at least six major Indian airports, interrupting online services for about nine hours (Hummel, 2023). These real-world incidents illustrate the range of cyber threats facing Indian aviation, from massive data breaches and ransomware-induced operational paralysis to attacks aiming to turn off critical services, and highlight the potential consequences for safety, security, and consumer trust when aviation systems are compromised.

In addition to these prominent occurrences, broader data patterns from 2020 to 2025 indicate an increasing prevalence and magnitude of cyber threats aimed at Indian civil aviation. A pivotal study conducted in 2024 by the CyberPeace Foundation, utilising a simulated aviation network to lure attackers, documented over 80,000 cyberattack attempts within a mere three-month period (June–August 2024), signifying a substantial degree of hostile activity aimed at aviation systems (CyberPeace Foundation, 2025). The hackers in the study mostly went for communication and database services. For example, Telnet (an older networking protocol) had more than 64,000 intrusion attempts, and MySQL databases had more than 15,000 attempts (CyberPeace Foundation, 2025). These findings indicate that criminal entities are methodically investigating Indian aviation networks for vulnerabilities, frequently employing automated brute-force attacks on login credentials. The investigation identified over 16,000 distinct password attempts across numerous usernames (CyberPeace Foundation, 2025). The malicious traffic was traced to other countries, including China, South Korea, and the United States, highlighting the international character of the danger. Indian aviation systems face hundreds of illegal access attempts daily, highlighting the persistent strain on cybersecurity.

Recent national cybersecurity data highlight the prevalence of assaults and the susceptibility of essential sectors such as aviation. Official data presented in the Indian Parliament indicates that the overall number of cybersecurity events reported to India's Computer Emergency Response Team (hereinafter written to CERT-In) surged from around 394,000 in 2019 to 1.59 million in 2023, representing an increase of over fourfold (Agrawal, 2024). Even incidents specifically affecting government organisations (which include aviation agencies) more than doubled in the same period, rising from ~85,800 in 2019 to ~204,800 in 2023 (Agrawal, 2024). The significant increase in recorded occurrences signifies India's progressively

deteriorating danger landscape annually. India has emerged as one of the most frequent targets of cyberattacks worldwide. A recent threat landscape analysis identified India as the second most targeted nation globally for cyber-attacks in 2024, with 95 major Indian companies experiencing substantial data breaches that year, a figure exceeded only by the United States (Press Trust of India [PTI], 2025). Including aeroplanes and airports in India's vital infrastructure subjects them to persistent threats within the overarching surge in cybercrime, despite the data encompassing all sectors.

The risks to aviation are particularly severe and significant. Cyberattacks on airlines and airport networks can have far-reaching consequences beyond data loss, potentially delaying flight operations, threatening passenger safety, and inflicting extensive economic harm. The predominant attack vectors identified in the aviation sector encompass ransomware attacks (capable of encrypting essential systems and demanding payment), phishing and social engineering (frequently employed to acquire credentials or introduce malware), insider threats, supply-chain assaults on vendors, and DDoS attacks that inundate online services (ETCISO, 2023; Resecurity, 2024). For example, Eurocontrol (the European air traffic agency) reported that ransomware became the single largest threat to aviation in 2022, accounting for roughly 20–25% of reported incidents (Resecurity, 2024). Recent incidents in India exemplify this global trend, as ransomware and DDoS attacks have resulted in operational interruptions, while data breaches have compromised millions of records. State-sponsored espionage entities and politically motivated hacktivists have focused their efforts on the aviation sector. Intelligence analysts observe that advanced persistent threat (APT) actors associated with nation-states may focus on aviation for espionage or sabotage. In contrast, hacktivist groups regard airports and airlines as prominent targets for ideological expression (Resecurity, 2024). The April 2023 airport DDoS event was linked to an international hacktivist organisation responding to geopolitical factors, demonstrating that geopolitics may immediately manifest as cyberattacks on aviation infrastructure. The designation of aviation as essential infrastructure undoubtedly attracts such attacks; as noted by an industry leader, this classification "paints a target on [its] back for threat actors" aiming for maximum impact (Resecurity, 2024). The aviation threat landscape is varied and more sophisticated, encompassing financially motivated cybercriminals, state-sponsored hackers, and hacktivists, all of which can cause significant damage.

The aviation sector's significance to public safety and the economy renders cyber vulnerabilities more consequential. Aviation is designated as essential infrastructure in India; thus, successful assaults could jeopardise the airline sector, national security, and trade. Recent incidents indicate that defensive measures have not adequately matched the evolving threat. In March 2023, India's Parliamentary Standing Committee on Transport, Tourism and Culture, concerned by the increase in cyber incidents, urged the Ministry of Civil Aviation to implement a robust cyber defence mechanism, highlighting that Indian airports and airlines had officially reported at

least 13 cyber incidents over the past five years (Asian News International, 2023). The Committee proposed allocating a specific budget for aviation cybersecurity, indicating an increasing official acknowledgement that cyber threats represent a "real and present danger" to Indian aviation and that current measures may be inadequate. The increasing frequency of threats, the broadening attack surfaces resulting from digitisation and IoT integration in aviation, and inconsistent security readiness indicate a vulnerable sector. India's aviation expansion and dependence on technology enhance the potential repercussions of a cyber disaster. Conversely, enduring deficiencies—such as outdated IT systems, disparate security standards among operators, a scarcity of proficient cybersecurity professionals, and intricate supply chains—heighten the probability that attackers will identify and exploit vulnerabilities.

Simultaneously, these advancements prompt significant inquiries over legal accountability and regulatory readiness. Who bears responsibility when a cyber event inflicts damage in the aviation sector? Airlines and airport operators may incur obligations to passengers for data breaches or flight disruptions. At the same time, technology vendors and service providers, such as the compromised third-party SITA system in Air India's situation, could also be held accountable. Regulators must contemplate enforcement measures if operators do not comply with cybersecurity mandates. In India, the assignment of liability for aviation cyberattacks is complicated by a fragmented legal framework, encompassing the Information Technology Act of 2000, the Aircraft Act of 1934, along with its aviation safety regulations, and more recent data protection laws, none of which were specifically designed to address aviation cybersecurity. Simultaneously, international and comparative frameworks, such as the guidelines established by the International Civil Aviation Organisation (ICAO), the European Union's network security directives, and U.S. critical infrastructure regulations, present potential models for enhancing India's strategy. Legal studies have emphasised that conventional aviation law was not created to address cyber dangers and requires adaptation to this emerging risk landscape (Klenka, 2021).

The combination of widespread cyber threats and significant risks indicates that India's civil aviation sector functions within a hazardous cybersecurity landscape. This article critically analyses the efficacy of India's legal and regulatory framework in addressing aviation cybersecurity threats, identifies significant gaps that render the sector vulnerable, and proposes comprehensive legal and policy reforms to enhance accountability and cyber resilience in the aviation industry, utilising international best practices to inform these recommendations.

This study utilises a doctrinal and analytical legal technique. This entails thoroughly reviewing existing regulations and policy documents pertinent to cybersecurity in civil aviation, alongside an analysis of case law and recorded cyber incidents. The qualitative research relies solely on secondary sources such as law

texts, government publications, industry recommendations, and scholarly discussions, without incorporating fresh empirical data. A comparative methodology is incorporated into the analysis: international frameworks and exemplary practices (from jurisdictions such as the EU and US, along with guidelines from ICAO and IATA) are examined to evaluate India's regulatory stance. No interviews, questionnaires, or other forms of primary data collection were performed. This approach facilitates a comprehensive assessment of legal statutes and the recognition of deficiencies. The insights derived from analysing and contrasting these sources underpin the proposals for improvement. The technique aims to rigorously evaluate India's existing aviation cybersecurity framework's sufficiency and derive evidence-based recommendations for requisite legal and regulatory modifications.

II. Cybersecurity Risks in Indian Aviation

Indian civil aviation is experiencing great connectivity and passenger volume development, but this digital expansion has increased exposure to cyber risks. Modern aircraft and airport operations rely on complex, interconnected IT systems, ranging from reservation and baggage handling platforms to navigation, surveillance, and air traffic control networks. This interconnection creates a massive assault surface. According to one analyst, "almost all aspects of aviation infrastructure are receptive to cyber threats," including airport internet networks and in-flight Wi-Fi, which attackers may use to obtain unauthorized access to systems (Chande, 2023). Successful breaches can result in data theft, operational disruptions, safety accidents, and reputational harm (Chande, 2023).

Research suggests that the aviation industry has emerged as a profitable target for cybercriminals and state-sponsored hackers. A Eurocontrol (the European air traffic agency) report indicated that cyberattacks on aviation increased by more than 530% from 2019 to 2020, with airlines comprising 61% of the targets. The predominant attack vectors encompass ransomware, data breaches, phishing, and DDoS attacks. A 2024 investigation by the CyberPeace Foundation in India documented a significant increase in brute-force intrusion attempts on aviation systems from several global sources, indicating systematic probing of Indian aviation networks (CXOtoday News Desk, 2025). These threats are particularly alarming because, unlike many sectors, cyberattacks on aviation can have far-reaching consequences beyond data loss—potentially disrupting flight operations and jeopardising passenger safety.

The aviation sector is designated as essential infrastructure. Disruptions can yield significant economic and security ramifications, rendering them appealing targets for assailants aiming for maximal impact. India's vulnerabilities have been acknowledged: in March 2023, a Parliamentary Standing Committee on Transport, Tourism and Culture, concerned by the increase in incidents, urged the Ministry of Civil Aviation to implement a comprehensive cyber defence mechanism after discovering that 13 cyber incidents had been reported to the Airports Authority of India over the past five years (Asian News International, 2023). The Committee

suggested the allocation of a specific cybersecurity budget for the aviation sector (Asian News International, 2023), indicating an increasing official acknowledgement that cyber threats constitute a significant and imminent risk to Indian aviation and that current measures may be inadequate.

Consequently, Indian aviation confronts significant risks and substantial vulnerabilities in cyberspace. The sector's swift expansion and dependence on technology heighten the potential repercussions of cyber incidents; conversely, vulnerabilities in defences—such as outdated IT systems, inconsistent security protocols among airlines and airports, human error, and intricate supply chains—elevate the probability of successful attacks. This risk picture highlights the necessity of scrutinising how India's legal and regulatory structure responds to (or neglects) culpability for aviation cyberattacks.

III. Regulatory Framework for Aviation Cybersecurity in India

Currently, India does not have a single comprehensive aviation cybersecurity regulation. Instead, the legal system is fragmented, including general cyber laws, sectoral aviation laws, and growing data protection requirements. This section summarises the important Indian legislation and regulations governing cybersecurity responsibility and liability in the civil aviation context: The Information Technology Act (2000), which comprehensively addresses cybercrime and data protection, the Aircraft Act (1934) and related aviation safety/security rules, and the emerging personal data protection framework. We examine how each relates to aviation cyber events and find gaps.

A. Information Technology Act, 2000 and IT Rules

India's primary cyber law is the Information Technology Act of 2000 (IT Act), which was revised in 2008. The IT Act establishes fundamental legal definitions and punishments for unauthorised access, data theft, cyber terrorism, and related acts and requires enterprises to meet specific cybersecurity responsibilities. The legislation expressly describes "cyber security" as this: "protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction" (Information Technology Act, 2000, §2(1) (nb)). This broad definition, included in the 2008 amendment, emphasises that cybersecurity is a legal requirement for organisations operating computer systems in India, including airlines, airports, and other aviation service providers. Under the IT Act, cyberattacks can have civil and criminal consequences.

On the civil side, Sections 43(a)-(h) of the Act (as amended in 2008) establish liability for different acts of computer damage, such as hacking, virus introduction, and denial of service. More importantly, Section 43A establishes a type of data protection obligation: it provides that any corporate entity possessing sensitive personal data that fails to implement "reasonable security practices" and thus causes

wrongful loss or gain, is liable to pay damages as compensation to the affected persons (Information Technology Act, 2000, §43A; Chande, 2023). If an Indian airline or airport fails to secure sensitive customer data and a breach happens, victims may seek compensation for the resulting loss. This immediately applies to incidents like the Air India breach, in which impacted passengers may seek damages claiming the airline lacked proper protection. Section 43A is sometimes recognised as India's precursor to a data protection law, and it encourages businesses to implement security standards (e.g., ISO 27001 as "reasonable practices") to reduce liability (Ministry of Communications & IT, 2011). However, one limitation is that compensation under Section 43A requires proving negligence in maintaining security, which can be contested.

On the criminal side, the IT Act criminalizes various cyber activities that may occur in aviation settings. Section 66, for example, criminalizes dishonest or fraudulent acts of unauthorized access or damage to computer systems (punishable by up to three years in prison). If a hacker intrudes into an airline's reservation system or an airport's network, law enforcement may trigger Section 66 (Information Technology Act, 2000, §66). Sections 66C and 66D criminalise identity theft and cheating by impersonation using computer resources, which might include phishing or social engineering assaults on airline personnel or passengers. Importantly, Section 66F of the IT Act defines "cyber terrorism" as any act that causes denial of access, unauthorised access, or the introduction of malware with the intent to threaten India's unity, security, or sovereignty, or to cause death/injuries or damage to critical infrastructure, and is punishable with imprisonment for life (Information Technology Act, 2000, §66F). Given aviation's vital infrastructure status, a substantial hack on air traffic control systems or critical airport operations may be classified as cyber terrorism under this provision. For example, an attack intended to cause an aeroplane to crash or crippling airport operations might be tried as a kind of cyber terrorism. However, Section 66F has been rarely invoked. It is expected to apply primarily in extreme instances (e.g., a state-sponsored attack compromising flight safety), rather than more common data breaches or ransomware events. Furthermore, Section 65 of the Act criminalizes tampering with computer source documents (e.g., willfully modifying or concealing source code), which may apply if an insider at an airline or contractor maliciously manipulates aviation software (Information Technology Act, 2000, §65; Chande, 2023). Section 70 empowers the government to designate any computer resource as a “Protected System” if its incapacitation would have a debilitating impact on national security (Information Technology Act, 2000, §70). Many important aviation systems (radar networks, flight control systems, etc.) could be designated as protected systems, making unauthorised access to them a serious violation punishable by up to life in prison. Section 70B, which was enacted in 2008, established the national Computer Emergency Response Team (CERT-In) and requires incident reporting, which is extremely important for airline operators dealing with cyber problems. In April 2022, CERT-In issued binding Directions mandating all

service providers, corporations, and government organizations to report cyber incidents (such as targeted scanning, outages, breaches, and ransomware) to CERT-In within 6 hours of discovering them (CERT-In, 2022). Airlines and airports are subject to this mandate and hence have a legal need to swiftly disclose cyberattacks to authorities, a failure to which can result in penalties under the Information Technology Act. This reporting requirement tries to improve incident response and is an important regulatory instrument, although it focuses on reporting rather than preventing events.

Despite these measures, the IT Act's ability to address aviation cybersecurity is limited. While it allows offenders to be punished (usually after the fact) and compensated, it does not directly regulate aviation cybersecurity requirements. Enforcement has also been unequal, as victims of breaches have rarely invoked Section 43A in practice, and regulatory action for noncompliance is unusual (Duggal, 2019). Furthermore, the IT Act fails to specify the distribution of culpability among numerous parties implicated in a cyber incident (e.g., an airline, its third-party IT provider, and an airport authority). The existing gaps indicate that, while the IT Act constitutes the foundation of cyber law in India, it is not a comprehensive solution for the distinct challenges of aviation cyber threats.

B. Aircraft Act, 1934 and Civil Aviation Regulations

The Aircraft Act of 1934 and its subordinate regulations are the foundation of India's aviation legislation, addressing aircraft operation, safety, and security issues. Historically, these regulations emphasise physical safety and airworthiness. The Directorate General of Civil Aviation (DGCA) promulgates Civil Aviation Requirements (CARs) and additional regulations under this Act to oversee airlines, aircraft maintenance, crew licensing, and related matters. In contrast, the Bureau of Civil Aviation Security (BCAS) establishes aviation security regulations to prevent unlawful interference, such as hijackings. Until recently, neither the DGCA nor BCAS had established specific cybersecurity laws for aviation, as cyber risks had only recently been acknowledged as a significant concern in the aviation sector.

Certain current provisions may be construed to encompass cyber hazards. DGCA's CAR Section 3, Series C, Part II on Air Operator Certification mandates that airlines implement a security program and adhere to the National Civil Aviation Security Programme (NCASP). The NCASP, governed by BCAS, establishes standards for aviation security. The NCASP, traditionally centred on physical dangers, has started to recognise cybersecurity per ICAO Annexe 17 on Security. Recently, fundamental cyber safety measures have been incorporated into India's NCASP. BCAS has mandated that airports fortify their IT networks and essential systems as a component of comprehensive security certification. Nonetheless, these actions are frequently communicated as advisories or internal circulars instead of explicitly written as legislation.

Following the 2022 SpiceJet ransomware attack, the DGCA issued a show-cause

notice to the airline and requested a comprehensive report (Singh & Sharma, 2022), showing that authorities are prepared to regard significant cyber incidents as regulatory compliance breaches. However, no specific CAR or regulation exclusively pertaining to cybersecurity mandates for airlines or airports remains. If an airline's inadequate cybersecurity results in an incident, the DGCA could take action against it under general laws mandating safe operations or under the Aircraft Rules, 1937, which require adherence to DGCA orders. Likewise, BCAS may regard a cyber intrusion as a failure in the necessary security processes at an airport. However, without definitive cyber legislation, such enforcement is arbitrary and potentially constrained by the absence of explicit norms. This legislative deficiency complicates liability assessment: airlines or airport operators may contend they were not legally required to implement specific cybersecurity safeguards without statutory mandates.

Another consideration is the infrastructure controlled by the Airports Authority of India (hence referred to as AAI), which provides air traffic services and operates numerous airports. As a government body, AAI follows its internal regulations and generic critical infrastructure protection recommendations (some provided by authorities such as the National Critical Information Infrastructure Protection Centre, NCIIPC). The NCIIPC (under the National Technical Research Organisation) has recognized Civil Aviation as a vital information infrastructure sector, which means that important aviation IT systems may be subject to NCIIPC audits or advice. However, the processes and results are not transparent. The dearth of public information on any sector-specific audit results or sanctions imposed by the NCIIPC or DGCA for cybersecurity failures shows minimal aggressive enforcement thus far.

Consequently, the Aircraft Act and its accompanying regulations have not explicitly been updated to address cybersecurity. At best, the legal provisions that penalise or sanction operators for cyber lapses are indirect. Currently, there is no aviation cybersecurity regulation comparable to, for example, an airworthiness directive or a dedicated safety rule. This is an evident disparity compared to jurisdictions that have established specific cyber rules for aviation. This results in an enforcement deficit, in which regulators acknowledge the issue but lack the specialised legal instruments necessary to take decisive action.

C. Data Protection Law and Privacy Obligations

Aviation cyber incidents frequently lead to personal data breaches, such as exposing passengers' identities, passport information, credit card numbers, trip itineraries, or employee data. Consequently, data protection legislation is invoked. For an extended period, India lacked a specific data protection statute; the legal framework governing data breaches was predominantly Section 43A of the IT Act and the associated 2011 SPDI Rules, which delineated the protocols for companies in managing sensitive personal data (Ministry of Communications & IT, 2011). In accordance with the regulations, airlines were obligated to establish privacy policies, designate data officers, implement reasonable security protocols, and, in certain

instances, notify users in the event of a data breach. These airlines collect large quantities of sensitive personal data. The airline may be liable for compensation if it fails to comply with Section 43A, which defines negligence. Nevertheless, the enforcement of Section 43A and the SPDI Rules was primarily achieved through civil suits in India, as the country did not have an active data protection authority that could impose sanctions like the EU's GDPR. This circumstance meant that, for instance, there was no regulator in India to sanction Air India for the breach (although the data of EU citizens affected by the breach did trigger scrutiny under GDPR in Europe). Air India was compelled to implement remedial measures in response to reputational damage; however, the legal implications were restricted to prospective lawsuits (which were not disclosed in this instance).

The Digital Personal Data Protection Act, 2023 (hereinafter referred to as the DPDP Act) is transforming this landscape. The DPDP Act, which was enacted in August 2023, is India's first comprehensive data protection law. It imposes significant penalties on entities ("Data Fiduciaries") for failing to disclose breaches and protect personal data (Government of India, 2023). Airlines, airports, and any aviation service providers that process personal data will be considered Data Fiduciaries upon the full implementation of the DPDP Act. In the event of a significant personal data intrusion, they will be legally obligated to notify the Data Protection Board of India and affected individuals, secure the data with reasonable safeguards, and protect personal data by design and default (Digital Personal Data Protection Act, 2023, §8, §25). Crucially, the Act empowers the government to prescribe norms for "reasonable security safeguards" – which will effectively set baseline cybersecurity requirements across industries, likely referencing standards like ISO 27001 or sector-specific codes of practice. An airline suffering a hack due to poor security could face regulatory investigation and financial penalties up to ₹250 crore (approximately USD 30 million) under the DPDP Act's provisions (Government of India, 2023). This circumstance can potentially revolutionise the aviation sector regarding liability for data breaches resulting from cyberattacks. Air India may have been required to compensate passengers in addition to incurring an official penalty for the SITA data breach had the DPDP Act been in effect in 2021. In the event of an incident, an airline or airport must comply with government orders, such as directives to inform affected individuals or mitigate damage, under the new law. This introduces a regulatory enforcement layer absent from the previous IT Act-centric regime. It more closely aligns India with the EU approach (such as GDPR), in which data controllers (in this case, airlines or airport operators) are directly accountable for violations.

Acknowledging that the DPDP Act primarily pertains to digital privacy and personal data protection is important. It does not explicitly address cyberattacks that disrupt services or threaten safety without necessarily involving personal data, such as a ransomware attack that cripples an airline's operations but does not leak customer data. These scenarios would continue subject to sectoral aviation obligations and the IT Act. Nevertheless, the DPDP Act will significantly assign liability, as most

aviation cyber incidents involve data. It will compel aviation entities to enhance their IT security or face punitive penalties, indirectly enhancing their cybersecurity posture. However, overlap and coordination pose a challenge. A single cyber incident may now result in parallel legal repercussions, including a DPDP Act breach notification and fine, an IT Act offence (if the hacker is apprehended), a contract breach issue with service providers, and potentially passenger litigation. The manner in which these intersect will only become apparent upon implementing the new law.

In summary, India's data protection regime is transitioning from a light-touch, compensation-based model (in accordance with IT Act Section 43A) to a stricter compliance model (in accordance with the DPDP Act). This transition will increase the liability for data breaches in aviation. This development is a critical element of the comprehensive legal framework for aviation cyber liability, as it specifically addresses the personal data aspect, complementing the IT Act and aviation laws.

IV. Case Studies: Cyberattacks on Indian Aviation and Legal Fallout

The practical application of the aforementioned legal frameworks and the existence of voids are illuminated by an examination of recent cyber incidents involving Indian airlines and airports. This section examines a few notable cases, emphasising the nature of the attack, the damage it caused, and the legal or regulatory responses (if any). These cases exemplify the practical challenges of attribution, enforcement, and obtaining remedies under current laws.

A. **Air India Data Breach (2021).** Incident: In February 2021, a significant cyberattack was conducted against SITA, Air India's Passenger Service System (PSS) provider. SITA is a multinational information technology (IT) company that provides services to numerous airlines. The intrusion exposed the personal data of approximately 4.5 million Air India passengers over a 10-year period, which remained undetected for approximately one month (Singh, 2021). The compromised information included names, contact details, birth dates, passport and ticket details, and credit card numbers (excluding the CVV). The assault was a component of a more extensive supply-chain breach that impacted numerous international airlines via SITA. In May 2021, Air India publicly divulged the breach after investigating the affected servers' security (Singh, 2021).

Legal Consequences: The primary concerns regarding this breach were contractual liability and data protection. The personal data of affected passengers, including Indian and foreign passengers, was compromised. Air India was bound by Section 43A of the IT Act to implement reasonable security measures for sensitive personal data under Indian law at the time. If negligence is established, Air India may be required to provide compensation for damages. Nevertheless, Air India would likely contend that the intrusion was a sophisticated supply-chain exploit rather than negligence, as it occurred at SITA. This Swiss-headquartered vendor is not

under its direct control. In fact, there were no reports of any civil complaint filed by passengers in India, nor was any government enforcement action taken (India lacked a data protection authority in 2021). In contrast, European regulators under GDPR exercised jurisdiction due to the involvement of EU residents' data, underscoring the disparity with India's dearth of enforcement.

From a contract perspective, Air India likely sought recourse against SITA under their service agreements. Many such contracts have clauses on data security and liability for breaches. It is unknown if SITA compensated Air India or if any litigation ensued privately between them.

Regulatory Response: The incident was reported to India's CERT-In by Air India per the law. Thereafter, CERT-In would have provided the airline with any necessary coordination or advisory support; however, there was no penalty framework in place beyond that notification. The incident catalyzed a discussion in India regarding the need for more stringent regulatory oversight of critical systems, such as airline PSSs, and third-party risks (Ghosh, 2021). It also underscored the need for clearer rules: the forthcoming DPDP Act, had it been active in 2021, would have mandated Air India to notify affected individuals (which Air India did via press release) and could have imposed penalties for a breach at its vendor affecting Indian citizens' data.

In summary, the Air India case revealed a liability gap: passengers in India were subjected to a privacy violation, but their remedies were restricted and required proof of Air India's negligence. It underscored the necessity of more explicit obligations regarding data protection and more robust enforcement, which is the primary objective of the new data law. It also underscored the significance of supply-chain security in aviation. It posed the legal question of whether airlines should be held accountable for vulnerabilities at their outsourced partners (the argument that certain duties are "non-delegable" under privacy law?). To reduce this liability, airlines must demonstrate diligence in vendor supervision..

B. **SpiceJet Security Breaches (2020 & 2022).** Incident 1 – Data Breach (2020): In January 2020, a security researcher exposed the confidential data of approximately 1.2 million passengers of the Indian low-cost airline SpiceJet by discovering an unprotected SpiceJet server (Singh & Whittaker, 2020). The researcher could access a database backup file through a brute-force attack on SpiceJet's systems. Subsequently, the airline and authorities were informed. The disclosed records comprised the passengers' names, phone numbers, email addresses, and dates of birth (Singh & Whittaker, 2020). The breach was responsibly disclosed, and there was no evidence of data misuse. However, it indicated SpiceJet's inadequate IT infrastructure security measures, such as misconfigured servers or weak passwords.

Legal Consequences: SpiceJet, as a corporate entity that manages sensitive personal data (including contact information and potentially some payment data), was subject to the SPDI Rules and Section 43A of the IT Act. An evident failure to secure its server could be interpreted as negligence in implementing "reasonable security practices," rendering SpiceJet liable to the impacted passengers. Nevertheless, no known compensation claims have been made, as the breach was disclosed through a news report rather than user complaints. SpiceJet acknowledged that it had resolved the issue but refrained from disclosing the specifics, possibly to mitigate reputational harm. SpiceJet received no formal penalties in 2020, as no data regulator existed. Consequently, the incident was once again classified as an enforcement void. It is uncertain whether any government agency took notice; SpiceJet or the researcher may have informed CERT-In, but no public enforcement action was taken. A comparable breach today would necessitate SpiceJet to disclose it within strict timeframes and potentially incur substantial penalties for failing to safeguard personal data adequately under the new DPDP Act regime..

Incident 2 – Ransomware (2022): SpiceJet was the victim of a ransomware attack in May 2022 that affected Flight Operations systems (Chande, 2023). The airline characterised it as an "attempt at ransomware" that affected its IT infrastructure. Consequently, SpiceJet's check-in, cargo, and flight planning systems malfunctioned, delaying flights at numerous airports. Hundreds of passengers were left stranded. SpiceJet implemented manual procedures for critical operations during the interim period, as certain aircraft were suspended for hours. Normal operations were not restored until the following day. The airline did not disclose the attackers' identity or whether any ransom was paid, and it asserted that no passenger data was stolen.

Legal Implications: This incident largely caused service disruption, raising concerns about contractual and consumer protection liability rather than data privacy. Passengers who experience extended delays may be able to request compensation or refunds under the DGCA's Charter of Passenger Rights, which compels airlines to provide certain facilities (meals, lodging) and compensation for delays that are within the airline's control. SpiceJet initially described the outage as a technical issue, but later admitted it was a hack; if deemed within the airline's control (arguably yes, to the extent that stronger cybersecurity could have avoided it), regulators may compel the firm to pay customers. In legal terms, travellers may also claim inadequate service under the Consumer Protection Act of 2019, claiming SpiceJet failed to maintain secure systems, resulting in financial and time losses. There were media accounts of stranded flyers expressing frustration, but no significant lawsuit ensued.

Notably, DGCA stepped in as a regulator: it issued a notice to SpiceJet seeking an explanation and directing the airline to prevent future recurrences (Singh & Sharma, 2022). DGCA did not impose a fine in this instance, as it lacks a clear statutory authority to do so. However, it made it plain that IT security breaches are taken seriously. A grievous cyber breach could be regarded as a safety concern by the DGCA. If SpiceJet had failed to address the situation, the DGCA could have imposed operational restrictions on safety grounds, such as terminating flights until the systems were secured. The ransomware incident thus illustrated that operational cyber failures could result in regulatory and contractual repercussions, even in the absence of explicit cybersecurity laws. SpiceJet's stock price purportedly declined amid concerns regarding its cybersecurity readiness, negatively impacting its brand (Kapoor, 2022).

The unknown attackers in the SpiceJet case committed offences under Section 66 (unauthorised access causing disruption) and arguably Section 66F (if the attack could be viewed as an act likely to endanger safe operations, although fortunately no accidents occurred) from an IT Act perspective. Nevertheless, the identification and prosecution of the perpetrators were challenging; there is no public indication that they were identified. This highlights a typical obstacle: the airline is responsible for the majority of the harm, while the hackers frequently operate in secrecy and are beyond the jurisdiction of law enforcement.

C. **DDoS Attacks on Airports (2023).** Incident: On April 8, 2023, a hacker group identified as "Anonymous Sudan" conducted synchronized DDoS (Distributed Denial of Service) attacks on the public websites of numerous main Indian airports, including Delhi, Mumbai, Hyderabad, Goa, and Kochi. The airports' web servers were inundated with traffic for approximately nine hours due to the attack, which rendered online services (such as flight information displays, booking portals, and check-in systems) inaccessible (Hummel, 2023). The effects were restricted to the inconvenience of travellers who could not utilize the airports' digital services; there was no compromise of internal airport operating systems or any impact on air traffic control. However, the incident underscored the vulnerabilities of the outward-facing systems of critical transportation centres.

Legal Consequences: The airport DDoS incident serves as an illustration of an attack on critical infrastructure by potential foreign actors. Direct liability to third parties was restricted; passengers experienced inconvenience rather than tangible losses or injuries, and no personal data was misappropriated. The airport operators, many of whom are public-private collaborative ventures with AAI, were the primary beneficiaries of the impact. In theory, the operators could legally pursue action against the

assailants under the IT Act's provisions for denial of service (Section 43 and the corresponding criminal Section 66). However, in practice, pursuing an international hacker collective is impossible unless it is possible to identify them and establish jurisdiction. Rather, the incident's primary impact was to encourage the implementation of compliance and resilience measures. It emphasised the obligation of airport administrators to guarantee that reliable backup systems and DDoS protection safeguard critical services.

In terms of regulatory oversight, CERT-In likely treated this as a significant incident given the involvement of critical infrastructure. The NCIIPC may also have been involved, as protecting nationally significant systems (like major airports) falls under its mandate. There was immediate pressure on airport IT teams to upgrade their network defenses and possibly to engage specialist security vendors for DDoS mitigation. It is also possible that BCAS or AAI issued advisory guidelines (if not already in place) that airport websites and other internet-facing systems employ anti-DDoS services and maintain redundancy to handle such attacks.

One could imagine an extreme scenario: liability could have extended to safety and operational domains if the DDoS had been so severe as to disrupt core airport operations (e.g., by turning off internal communication networks or security systems). Airlines may have been compelled to delay flights, and passenger safety or security could have been jeopardized. Fortunately, this was not the situation in April 2023. However, the incident served as a cautionary tale: a relatively low-level assault could disrupt multiple airports simultaneously for several hours. Legally, it revealed that no specific accountability was allotted for the cyber resilience of airport operations beyond general expectations. There was no public inquiry or sanction for the disruption, and each airport operator responded individually. The lesson is that, even though passenger damage is minimal, such incidents expose deficiencies in oversight and preparedness that could be more severe in other situations.

Lessons from the Cases: These case studies reveal a few key patterns. First, the victims of cyberattacks (airlines, airports, and by extension their customers) bear the immediate costs – service disruption, recovery expenses, and reputational damage – while direct legal punishment of the attackers is rare due to problems of attribution and jurisdiction. Second, affected individuals (passengers) have historically had limited avenues for redress in India; this may improve under new laws like the DPDP Act and strengthened consumer protection, which empower regulators to act and consumers to claim compensation. Third, Indian regulators have responded in a somewhat reactive and piecemeal manner – issuing notices and ordering investigations – but lacked explicit protocols or rules, leading to uncertainty. This highlights the need for clearer incident-response procedures and liability frameworks specific to aviation cybersecurity.

V. Comparative Insights from International Frameworks

Cyber threats to aviation are a global concern, and numerous jurisdictions and international organisations have been attempting to establish legal obligations to mitigate this risk. The International Civil Aviation Organisation (ICAO), the European Union, and the United States can give India valuable insights. India is contemplating enhancing its regime, and these insights underscore the importance of addressing gaps and implementing best practices.

A. International Civil Aviation Organization (ICAO) Initiatives

ICAO, the U.N. specialised agency for civil aviation, has come to acknowledge cybersecurity's importance in aviation safety and security. In the past decade, ICAO member states have adopted a series of resolutions to encourage action on aviation cybersecurity. It is important to note that ICAO Assembly Resolution A40-10 (2019) and Resolution A41-19 (2022) encourage states to establish frameworks and capabilities to mitigate cyber threats in civil aviation. The 41st ICAO Assembly in 2022 took it a step further by encouraging states to adopt and implement the Beijing Convention 2010 to address cyberattacks against civil aviation (ICAO, 2022).

The Beijing Convention 2010 (formally the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation) is a treaty that criminalises specific acts of aviation terrorism and sabotage. ICAO maintains that cyberattacks that threaten aviation (e.g., hacking an aircraft's systems or air traffic control with the intention of causing accidents) are included in the category of unlawful acts addressed by the Convention. India is a signatory to the 2010 Beijing Convention but has not yet ratified it as of 2025. The ratification and implementation of its provisions would enhance India's capacity to prosecute aviation cyber offenders across borders, as the Convention simplifies the definition of offences and enables extradition.

ICAO has revised its technical standards in addition to international treaties. Provisions regarding cybersecurity were implemented by the International Civil Aviation Organisation (ICAO) in Annexe 17 (Security) to the Chicago Convention. For instance, Annexe 17's Standard 4.9.1 (amendment effective 2020) mandates that member states implement safeguards for critical information and communication technology systems utilised in civil aviation within their civil aviation security programs (ICAO, 2017). In practice, this means countries should incorporate cyber protections in airport and airline security regulations (e.g., BCAS should have guidelines for cyber resilience as part of the national aviation security program). ICAO has also developed detailed guidance materials – for instance, the ICAO Aviation Cybersecurity Strategy (initially adopted in 2019) which outlines a multi-pronged approach including governance, legal measures, technical protections, information-sharing, and incident response (ICAO, 2019). The strategy emphasizes international cooperation, given the interconnected nature of aviation systems.

Nevertheless, the ICAO's function is primarily normative and facilitative. It does not impose direct liability or enforce penalties but establishes expectations that states

must fulfil through their national laws and regulations. ICAO's standards and recommendations must be translated into domestic requirements by each country, including India. Some nations have taken this step proactively, while India is still establishing compliance in this area. For example, India has not yet explicitly integrated the cybersecurity standards of the International Civil Aviation Organisation (ICAO) into the enforceable regulations of the DGCA/BCAS, as envisioned in Annexe 17.

Mandatory cyber risk assessments for aviation entities, the establishment of an aviation sector Computer Security Incident Response Team (CSIRT), and active participation in international information-sharing mechanisms (such as aviation Information Sharing and Analysis Centres, or ISACs, and global CERT collaborations) are likely to be required to adopt ICAO's guidance. It is crucial to note that ICAO also promotes capacity building, acknowledging that legal frameworks are insufficient if authorities and industry lack technical capability. Consequently, the ICAO's impact on liability is indirect, as it establishes a global baseline and peer pressure. A state may be perceived as failing to fulfil its obligations under the security provisions of the Chicago Convention if it fails to address aviation cybersecurity adequately. In an extreme case, a significant cyber incident attributable to such negligence could even prompt inquiries regarding a state's accountability under international law. However, in practical terms, the ICAO's framework motivates states to implement best practices before the emergence of such issues.

B. European Union

The European Union has taken a proactive approach to establishing regulatory requirements for cybersecurity in critical sectors, such as aviation. General cybersecurity directives that encompass aviation as critical infrastructure and aviation-specific safety/security regulations that integrate cyber risk management are the two primary strands of EU law that are pertinent.

Aviation is classified as an essential service sector under the EU's NIS Directive (2016) and its subsequent amendment, the NIS2 Directive (2022). The original NIS Directive mandated that EU member states guarantee that operators of essential services, such as airlines and airport operators, implement minimum cybersecurity risk management measures and report significant cyber incidents to national authorities (European Parliament and Council, 2016). Regulators in each member state may implement enforcement actions and impose penalties for noncompliance. The NIS2, which was implemented in January 2023, strengthens and broadens the scope of these requirements. It classifies air transport as one of the "essential" sectors. It imposes even stricter obligations, such as executive accountability for cybersecurity, supply-chain security measures, and higher penalty caps (up to 2% of global annual turnover for companies) for violations. (European Parliament and Council, 2022). Thus, in Europe, liability for failing to prevent or mitigate cyberattacks is not just ex post (after an incident) but also ex ante in the form of regulatory fines if appropriate

safeguards are not in place.

The General Data Protection Regulation (GDPR) 2016 is another pillar of the EU's approach, which includes data protection. If data breaches involving personal data result from inadequate security, GDPR imposes substantial penalties (up to 4% of global turnover) on companies, including airlines. A notable example of this was the 2018 British Airways data compromise, in which hackers injected malicious code onto BA's website to steal the credit card details of approximately 380,000 customers. BA was fined £20 million in 2020 by the UK Information Commissioner's Office for failing to implement fundamental security measures that could have prevented the attack, as per GDPR. This illustrated an airline's tangible financial liability due to a cyber breach. The BA case is instructive for India, as in the past, an Indian carrier that encountered a comparable breach did not face an equivalent regulatory fine due to the absence of an empowered data protection authority in India. However, the DPDP Act has been implemented, and Indian regulators can impose penalties in similar situations.

In addition to these general laws, the EU implements aviation-specific regulations. The European Union Aviation Safety Agency (EASA) has incorporated cybersecurity into its supervision. EASA has mandated that aircraft manufacturers adhere to specific cybersecurity standards for new aeroplane designs since 2019, to safeguard avionics and onboard networks from cyberattacks. It also introduced regulations that required airlines to integrate cyber risk into their safety management systems. Additionally, it required national aviation authorities to conduct cybersecurity assessments of airports and airlines during their safety examinations.

The European Air Traffic Management Computer Emergency Response Team (EATM-CERT) is a dedicated CERT for European aviation, and European air navigation service providers comply with Eurocontrol's cybersecurity guidelines. These measures establish defined roles and preparedness expectations in the EU. An airline that disregards recognised cybersecurity best practices may be found to violate security and safety obligations, increasing its liability. The EU's strategy generally illustrates the efficacy of comprehensive regulation and enforcement. It emphasises that preventing aviation cyber incidents is considered a legal obligation, rather than a trivial IT concern. For India, implementing a comparable model, such as explicit mandates for airlines and airports to report incidents and implement cyber risk management, could substantially enhance accountability. Simultaneously, replicating the EU's model would necessitate the resolution of resource and capacity constraints within Indian institutions. Formulating regulations is a preliminary step; enforcing them with the same rigour as the EU, including audits and sanctions, necessitates a substantial regulatory capacity and an industry compliance culture.

C. United States

The United States has a somewhat fragmented but evolving approach to aviation cybersecurity, which involves the integration of voluntary frameworks with

progressively increasing regulatory requirements. Historically, the governance of U.S. aviation cybersecurity has been characterised by a partnership model. The Department of Homeland Security (particularly the Transportation Security Administration, TSA) and the Federal Aviation Administration (FAA) collaborated with industry through guidelines and information-sharing, rather than strict regulations. The NIST Cybersecurity Framework, a voluntary set of standards developed by the National Institute of Standards and Technology, has been extensively adopted by U.S. airports and airlines as a baseline for best practices (Norton Rose Fulbright, 2020). The aviation industry also established an Aviation Information Sharing and Analysis Center (A-ISAC) to share threat intelligence among airlines, aircraft manufacturers, airports, and federal agencies, thereby voluntarily enhancing collective security posture.

Nevertheless, the United States has initiated a transition to more prescriptive mandates in response to the escalating threats. The FAA was explicitly instructed by the FAA Reauthorization Act of 2018 to intensify its cybersecurity initiatives in the aviation sector. The Act mandated the FAA to establish a comprehensive cybersecurity and emergency response plan for air navigation systems and evaluate the implementation of new regulations to safeguard aircraft and avionics from cyber sabotage (FAA Reauthorization Act, 2018, §506). It also encouraged the FAA to incorporate cybersecurity into aircraft certification processes and to establish an expert task force (which later evolved into the Aviation Cybersecurity Initiative) to suggest risk mitigations (FAA, 2020).

Specifically, U.S. authorities issued emergency Security Directives for critical transport sectors in response to high-profile cyber incidents in other transportation modes (e.g., the 2021 Colonial Pipeline ransomware that impacted petroleum supply). In 2021–2022, the Transportation Security Administration (TSA), which oversees aviation security, issued directives mandating the implementation of particular cybersecurity protocols by all significant rail and aviation operators in the United States. TSA mandated network segmentation, access controls, continuous monitoring, and the prompt reporting of cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 24 hours for airports and certain aircraft operators (DHS, 2022). A distinct TSA directive mandating the appointment of a cybersecurity coordinator, the execution of a vulnerability assessment, and the implementation of remediation plans applied to airlines. Penalties or operational consequences may ensue if these directives are not adhered to. They effectively mandate specific baseline cybersecurity practices. For example, an airport that neglects to disclose a significant cyber incident or does not have an approved cybersecurity plan may be subject to penalties or a loss of federal support.

In addition to regulation, the United States continues to extensively rely on litigation and market forces from a liability perspective. Companies may be subject to negligence lawsuits if a cyber incident results in injury. For instance, a passenger may pursue a tort claim or a claim under the airline's contract of carriage if they are injured

or suffer losses due to a flight delay or disaster that can be attributed to a cyberattack. Internationally, the Montreal Convention (applicable in the United States and India) holds airlines accountable for flight delays and passenger injuries unless they can demonstrate that they either failed to take all necessary precautions or that it was impossible to do so. A cyberattack could be argued to be an "extraordinary circumstance" similar to terrorism, which could potentially excuse liability. However, liability may still apply if evidence demonstrates that the airline's inadequate cybersecurity made the attack possible. Although aviation does not yet have a precedent for this, there are examples of other industries in which companies have encountered negligence claims or shareholder lawsuits due to cyber incidents.

U.S. criminal law also offers opportunities for prosecution: the Computer Fraud and Abuse Act and other statutes permit the prosecution of cyber intrusions. Additionally, the Department of Justice has demonstrated a willingness to indict perpetrators of aviation system attacks, including foreign state-backed hackers, albeit frequently in absentia. Although these prosecutions do not directly compensate victims, they underscore the notion that cyberattacks on critical infrastructure are severe offenses. The U.S. government has instituted sanctions and diplomatic measures against state-sponsored cyber actors suspected of targeting sectors such as aviation.

In summary, the United States' approach is a hybrid model that prioritises industry-led best practices and information exchange, but also implements targeted regulation when necessary. It also relies on legal action (both civil and criminal) to assign responsibility and penalise wrongdoers following an incident. One lesson for India is the significance of cross-sector coordination and mandatory incident reporting. This is echoed by India's CERT-In directive 2022 and its endeavours to establish sectoral CERTs. Another option is the establishment of sector-specific directives or guidelines. In a manner similar to the TSA, India could empower DGCA/BCAS to issue binding cybersecurity requirements for aviation operators. Lastly, the A-ISAC fosters an information-sharing environment that can enhance preparedness without imposing formal liability. Companies that share and learn about threats are frequently more adept at prevention, reducing the likelihood of damage occurring in the first place. Implementing these measures in India will necessitate the development of the underlying capacity and culture, rather than merely replicating policies. The U.S. aviation industry is characterised by a compliance-driven culture influenced by litigation and reputation. U.S. agencies like the FAA and CISA possess significant technical expertise and resources. India will achieve the same benefits by investing in regulatory capacity and encouraging industry participation.

VI. Deficiencies and Obstacles in the Indian Framework

Comparing the above international practices to India’s current situation reveals several gaps and challenges that need addressing:

A. Lack of Sector-Specific Cybersecurity Regulations: India has not yet implemented aviation-specific cybersecurity standards, unlike the EU and the U.S. The IT Act and the forthcoming DPDP Act are generally applicable; however, the DGCA/BCAS have not issued specific, public guidelines or CARs that airlines and airports must adhere to regarding cybersecurity. This complicates determining negligence or noncompliance in the event of a breach, as Indian regulations do not establish a distinct industry "standard of care." It also results in inconsistent practices: some Indian airline members of global alliances may voluntarily comply with international cybersecurity standards, while others may not prioritise cybersecurity without regulation. For instance, the NIS Directive of 2016 of the European Union mandates that member states implement baseline cybersecurity measures and incident-reporting obligations in critical sectors such as aviation. This directive establishes a distinct standard of care that India currently lacks (European Parliament and Council, 2016).

B. Enforcement and Coordination Deficit: The responsibility for cyber supervision in Indian aviation is dispersed among numerous organizations. CERT-In is responsible for incident response coordination, DGCA for aviation safety and airworthiness, BCAS for aviation security, AAI (in conjunction with NCIIPC) for airport infrastructure protection, and the new Data Protection Board for personal data intrusions. The coordination among these entities is essential; however, it is ad hoc. The Parliamentary Committee's alarm in 2023, which necessitated the specific request of incident data and the encouragement of action, implies that oversight has been reactive and compartmentalised (Asian News International, 2023). There is no formal information-sharing mechanism or dedicated aviation cybersecurity cell that connects regulators and industry. The enforcement of existing mandates has also been inadequate: regulators have not imposed penalties on airlines or airports for cybersecurity breaches until recently. For instance, the Air India and SpiceJet incidents did not result in any substantial punitive measures being implemented in public, as opposed to the substantial fines or penalties common in jurisdictions such as the EU. The absence of tangible repercussions contributes to an enforcement deficit, as the laws enacted have not been followed through with effective enforcement.

C. **Institutional and Resource Constraints:** Practical obstacles exist in the implementation of comprehensive aviation cybersecurity supervision in India. The civil aviation regulator (DGCA) and other agencies frequently lack the necessary specialised personnel, budgets, and sometimes autonomy to proactively address cyber issues. The DGCA's capacity to enforce regulations and conduct comprehensive audits in a swiftly expanding aviation market is currently impeded because nearly 48% of

technical positions are vacant (Tripathi, 2025). In contrast to the U.S. FAA, which has a larger dedicated budget and personnel, the DGCA operates under the Ministry of Civil Aviation with limited financial and staffing independence. The development and maintenance of new initiatives, such as exhaustive audit programs or dedicated cyber units, are impeded by this resource constraint. Additionally, the private sector's competition with the government challenges retaining competent cybersecurity professionals in government positions. Budgetary support for aviation cybersecurity has been minimal, with no specific budget allocation to date, a need identified by the Parliamentary Committee. These structural constraints may result in the failure of even well-crafted policies to be implemented without substantial capacity-building.

D. Until recently, consumers had limited legal recourse: Aviation cyber incidents frequently led to personal data breaches or flight disruptions that affected passengers. However, Indian passengers who experienced personal data theft or travel disruptions had limited options before 2023. They could file civil suits or consumer complaints; however, such litigation is uncommon and time-consuming in cyber issues. In contrast to the EU's data protection authorities and the U.S. Department of Transportation for consumer aviation issues, no specialised regulator could advocate for their cause. This resulted in a significant number of victims not receiving compensation, and companies were not directly liable for the financial losses incurred by those affected. The DPDP Act (2023) is expected to enhance the situation by enabling a Data Protection Board to investigate data breaches, impose penalties, and implement generally stronger consumer protection norms. However, the development of awareness and the utilisation of these mechanisms will require time. Furthermore, India has no class-action or collective litigation for data breaches, which means that companies have not encountered the substantial damages payouts that drive cybersecurity investment in certain other jurisdictions. The historical low priority of cybersecurity among Indian aviation companies may be altered as new laws are implemented, as the absence of legal pressure from consumers and shareholders has arguably contributed to this.

E. Jurisdictional and Attribution Issues: Legal accountability is complicated because cyberattacks on aviation frequently originate from abroad or involve foreign actors. Indian law enforcement encounters substantial challenges in attributing attacks to specific individuals. Even when they do, prosecuting overseas perpetrators necessitates international cooperation that may be sluggish or unavailable. Cross-border investigations are greatly facilitated by global frameworks such as the Budapest Convention on Cybercrime. However, India is not a party to this

convention but relies on bilateral treaties for support. This restricts the capacity to discourage or penalise assailants who operate from abroad; numerous cybercriminals (often accurately) believe they are beyond the effective jurisdiction of Indian law if they are located outside India. If the attacks are severe, state-sponsored cyberattacks may pose even more complex issues, potentially involving questions of state responsibility or even the laws of armed conflict. Responses may be contingent upon diplomatic or covert measures rather than legal ones, as India's domestic legal system is inadequately prepared to manage such circumstances. In summary, India's cyber laws' deterrent effect is weakened by the low likelihood of prosecution for a determined attacker operating from foreign soil who targets Indian aviation. India's capacity for international legal cooperation in cyber cases is relatively limited and requires strengthening, even though this is a challenge that is shared globally.

F. **Third-party and supply-chain risks**: Modern aviation is dependent on a network of third-party purveyors, including aircraft manufacturers, cloud hosting services, and global distribution systems. An airline or airport can be directly compromised by a vulnerability in a vendor's system. In such instances, Indian law has not expressly defined how liability is distributed between an aviation company and its vendor. In practice, contracts allocate some risk (through indemnities, for example), but the airline or airport, as the certificate holder, is responsible for the overall operations from a regulatory perspective. Aviation companies are at risk of becoming overly dependent on outsourcing without proper supervision, which could form weak links. If a violation occurs, the airline may attribute the responsibility to the vendor, who may maintain that it fulfilled contractual obligations, leaving victims in a precarious position. In aviation, there is a lack of explicit legal or regulatory guidance regarding managing third-party cyber risk. In the absence of it, accountability may be impeded by the "blame game" that ensues following incidents. For instance, regulators could mandate that aviation companies incorporate cybersecurity clauses into their contracts and guarantee that critical IT providers comply with specific security protocols; however, these obligations have yet to be formalised.

G. **Inadequate Cyber Insurance Market**: Cyber insurance is one method of managing liability and encouraging improved security. Aviation companies are progressively acquiring cyber insurance policies that cover various costs, including legal liabilities, business interruption losses due to cyber incidents, and data breach notifications. This trend is occurring globally. These policies frequently require that the insured adhere to minimal security protocols (insurers may audit security or mandate compliance with standards to provide coverage). The aviation sector in

India has a limited adoption of cyber insurance. If airlines/airports are inadequately insured, the company may be required to assume the full cost of a significant cyber incident, including passenger compensation, system restoration, and revenue loss from outage (or the government if the company is bailed out due to its systemic significance).

Additionally, companies are deprived of an external incentive to enhance security in the absence of insurers' pressure. Promoting adherence to best practices and ensuring financial resilience could be achieved by encouraging or mandating cyber risk insurance for critical aviation entities. This is because insurers incentivise better risk management with reduced premiums. However, the legal frameworks in Indian aviation do not currently address cyber insurance, which is still in its infancy.

H. **Cultural and Training Gaps:** a non-legal but critical challenge is the level of cybersecurity awareness and culture within aviation organisations. A human element is present in numerous incidents, such as a successful phishing email to an airline employee or a misconfigured server by an IT contractor, which can provide an entry point for attackers. Ultimately, compliance is contingent upon daily vigilance and company culture, even though laws can mandate training and standards. In India, aviation organisations do not consistently implement cybersecurity exercises or third-party security audits. While Indian aviation's top executives have begun to express significant concern regarding cybersecurity risks (85% of Indian airline CEOs in a survey were concerned about cybersecurity risks, a substantially higher percentage than CEOs in other industries (PwC, 2018), this must be translated into action at all levels. At present, the organisation is responsible for cybersecurity errors, and individual employees are not subject to legal repercussions unless there is willful or gross negligence. That places the responsibility on corporate governance: airline and airport management must prioritise cybersecurity, allocate budgets, and hold staff accountable through performance metrics. Though not yet mandated in aviation, governance reforms may prove advantageous, such as mandating that company boards conduct regular cyber risk assessments or associating management incentives with safety and security outcomes. Ultimately, the enhancement of cybersecurity is not solely a matter of technology and laws, but also of individuals and procedures. A robust internal security culture can prevent numerous incidents, reducing the necessity to pursue legal liability after the fact.

VII. Recommendations for Legal and Policy Reform in India

To fortify the legal framework surrounding aviation cybersecurity and explicitly define liability, India should implement a combination of legislative updates, regulatory actions, and capacity-building initiatives. The following are the primary recommendations:

A. **Enactment of Comprehensive Aviation Cybersecurity Guidelines:** The

DGCA, in partnership with BCAS and CERT-In, should establish a comprehensive Civil Aviation Requirement (CAR) or comparable regulatory guideline specifically dedicated to cybersecurity. This should require all aviation stakeholders (airlines, airport operators, ground service providers, air navigation service providers, etc.) to adhere to baseline security controls and implement cybersecurity management systems. Regular cyber risk assessments, the implementation of cutting-edge security controls (such as firewalls, intrusion detection systems, and data encryption in transit and at rest), the maintenance of up-to-date software (including the prompt patching of known vulnerabilities), and the training of all personnel in cyber hygiene are all critical components. The guideline should be consistent with the security provisions of Annexe 17 and the Aviation Cybersecurity Strategy of ICAO (ICAO, 2017), and align with global standards like the NIST Cybersecurity Framework and ISO 27001. This regulation will facilitate the determination of whether an entity was negligent or compliant in the event of an incident by establishing a distinct baseline. DGCA/BCAS should be able to audit compliance through periodic cybersecurity inspections, similar to how they undertake safety audits. Non-compliance may result in penalties under the Aircraft Act/Rules, such as financial penalties or restrictions on operations or certifications until the issue is resolved.

B. Mandatory Incident Reporting and Information Sharing: The aviation sector should incorporate a layer of sector-specific reporting and collaboration, in addition to the 6-hour incident reporting mandate (CERT-In, 2022) applicable across sectors. To function as a sectoral cyber-coordination centre or CERT for aviation, it is recommended that a dedicated Aviation Cybersecurity Cell be established, either within DGCA or in collaboration with NCIIPC. All aviation entities must disclose any cyber incident, particularly those that impact operations or sensitive data, to this specialised cell in addition to CERT-In. The cell can subsequently issue sector-wide alerts, advise other airlines/airports of emergent threats, coordinate with law enforcement or intelligence agencies if necessary, and provide assistance in incident response. This cell can potentially develop into an Aviation-ISAC (Information Sharing and Analysis Centre) for India, where trusted stakeholders can exchange real-time information on threats, indicators of compromise, and best practices. ICAO has endorsed this collaborative approach, which has been effectively implemented in the United States. It can significantly mitigate the impact of attacks and potentially deter attackers if they know the sector's unified defence front. In particular, a policy paper has previously recommended the establishment of an Aviation-ISAC in India, emphasising its necessity and feasibility.

C. Clarify and Strengthen Legal Accountability for Cyber Lapses: Amendments to existing aviation regulations or laws should be considered to explicitly spell out cybersecurity obligations and liabilities. For example, the Aircraft Rules, 1937 could be amended to require that licensees (airlines, airport operators) "maintain robust cybersecurity measures to ensure the safety and security of operations," with failure to do so constituting a regulatory offense. This would give DGCA clear grounds to take action (e.g., impose fines, issue directives or even suspend licenses) if an investigation reveals that an airline or airport had egregiously poor security practices leading to an incident. Additionally, as India develops new critical infrastructure protection laws (such as the proposed Telecom Bill addressing internet resilience), civil aviation should be expressly listed as a critical sector requiring special protection (Ministry of Communications of India), 2022). This could impose duties on aviation operators (like mandatory risk mitigation steps) and empower the government to direct specific emergency actions during cyber crises (for instance, temporarily grounding flights or isolating systems if necessary to contain a cyber incident).

Contracts between aviation companies and their technology providers should also come under regulatory scrutiny. Regulators can issue guidance that any critical IT outsourcing or vendor contract in aviation include clauses on minimum security standards, breach notification, and shared liability in case of breaches. This would cascade cybersecurity obligations down the supply chain, ensuring vendors are also accountable. On the civil liability side, the government might explore establishing an expedited dispute resolution mechanism for cyber incidents in critical sectors – for instance, a fast-track tribunal or ombudsman for resolving passenger claims arising from cyber-related flight disruptions, or for companies to seek redress against negligent vendors. Such mechanisms could encourage victims to seek remedies and hold companies accountable without protracted litigation. Additionally, India's consumer courts and the new Data Protection Board should be sensitized to aviation scenarios: for example, if a passenger brings a complaint about a flight delay caused by a cyberattack, authorities should recognize it as a valid grievance and not automatically dismiss it as force majeure if it's shown the airline's inadequate security contributed to the incident.

D. Ratify and Implement International Conventions on Cybercrime in Aviation: India should give urgent consideration to ratifying the Beijing Convention (2010) on unlawful acts against civil aviation, as ICAO has urged (ICAO, 2022). Doing so would update India's international commitments by explicitly including cyberattacks against civil aviation as

offenses under the same legal framework as hijackings and bombings and would facilitate better cooperation with other countries in investigating and extraditing cyber criminals who target aviation. Domestically, necessary amendments to statutes (like the Aircraft Act or Penal Code) could follow to incorporate the Convention's provisions (for example, criminalizing attempts to use cyber means to damage air navigation facilities or an in-flight aircraft). In addition, India should strengthen its participation in international cybercrime efforts. Joining the Budapest Convention on Cybercrime or negotiating robust bilateral agreements focused on cybercrime can improve cross-border evidence sharing and assistance. This is crucial since many serious aviation cyber incidents have an international footprint. Furthermore, on the cyber-defense front, India could lead or join regional initiatives (at the SAARC or BIMSTEC level) for protecting aviation from cyber threats – sharing information about incidents like the "Anonymous Sudan" DDoS attacks, which could easily be replicated against neighboring states. In essence, international cooperation will enhance India's ability to deter and respond to aviation cyberattacks that originate outside its borders.

E. Impose Appropriate Consequences on Offenders and Negligent Parties: While external hackers (especially those backed by foreign states) may be beyond immediate reach, India should ensure it uses its existing laws to the fullest against those it can hold accountable. This means that when a cyberattacker is identified – even if overseas – Indian agencies should file charges under stringent provisions like Section 66F of the IT Act (cyber terrorism) or relevant penal laws, to signal that attacks on aviation are grave offenses. Even if such trials occur in absentia, they build a legal record and put perpetrators on notice (for instance, making them fugitives internationally). Domestically, for insiders or companies that willfully flout cybersecurity, regulators should consider stronger sanctions. For example, if an investigation finds that an airline repeatedly ignored basic cyber hygiene or a known DGCA directive on IT security, such failures could be made punishable under aviation regulations similar to how willful safety violations are penalized. The intent is not to punish victim companies for being attacked, but to target egregious negligence that heightens risk. A balanced approach is needed: the goal is to encourage transparency and improvement in security, not to create a climate of fear that dissuades companies from reporting incidents. Perhaps a tiered enforcement approach can work – minor first-time violations result in warnings and mandated improvements, whereas severe or repeated failures to maintain reasonable security result in fines or operational penalties.

F. Integrate Cybersecurity into Aviation Safety Management and Culture:

Cybersecurity should be formally integrated into the existing safety and security management frameworks of aviation. The concept of Safety Management Systems (SMS) is well ingrained in aviation – every airline and airport has processes to identify and mitigate safety risks. DGCA should update its regulations or advisory circulars to require that cyber risks (like possible GPS spoofing of navigation signals, malware in airline operational software, etc.) be included in hazard identification and risk assessment within SMS documentation (International Air Transport Association, 2021). Correspondingly, the mandatory training curricula for various aviation personnel (pilots, air traffic controllers, aircraft maintenance engineers, ground staff, etc.) should include cybersecurity awareness modules. Many breaches begin with phishing or social engineering, so a well-trained workforce is the first line of defense. Regulators can audit training records and SMS reports to ensure this integration is happening. By making cybersecurity a part of the everyday safety culture, it ceases to be viewed as solely an IT department issue and becomes everyone's responsibility. Over time, this can significantly reduce the number of incidents (and therefore reduce liability exposure), as employees are more likely to spot and prevent threats. Building a robust security culture also means encouraging internal reporting of cyber "near misses" or vulnerabilities, so that organizations can learn and improve proactively without the trigger of an external incident.

G. Mandate Incident Response and Continuity Planning: All major aviation entities should be legally required to maintain up-to-date incident response and business continuity plans for cyber events, and to rehearse them regularly. This would include having data backups, manual override or fallback procedures for critical operations, and clear communication protocols to manage an incident. For example, if an airline's reservation system is hit by ransomware, it should have a tested plan to quickly switch to a clean backup system or even revert to manual ticketing processes to continue essential operations (as SpiceJet attempted in 2022 by moving to manual check-ins). DGCA could enforce this by requiring airlines/airports to submit their cyber incident response and continuity plans for approval and to conduct periodic cyber drills. Indeed, just as emergency exercises are routinely conducted for scenarios like hijackings or aircraft crashes, cyber incident drills (simulating, say, a malware attack that affects airport operations or ATC communications) should be part of preparedness at major airports. Effective incident response can significantly limit the damage during a cyber crisis, thereby reducing knock-on liabilities (fewer flights canceled, less harm to passengers, quicker recovery). It also demonstrates due diligence – being able to show that a company had a robust response plan and executed it can be a strong

defense in legal or regulatory proceedings, evidencing that the company took reasonable actions under the circumstances.

H. Promote Cyber Insurance and Risk Financing: The government and industry associations (like the Confederation of Indian Industry's aviation group) should encourage greater uptake of cyber insurance in the aviation sector. This could involve creating an insurance pool or a government-backed scheme for critical infrastructure sectors, where companies can obtain cyber risk coverage at reasonable rates. Insurers, in turn, often enforce certain cybersecurity best practices as conditions for coverage (for example, requiring companies to maintain specific security certifications or conduct regular audits to remain insured). Thus, increasing cyber insurance coverage can indirectly raise security standards. Additionally, the government might consider establishing a contingency fund for critical infrastructure cyber incidents. Such a fund, fed by contributions from industry and/or government, could act as a financial safety net to provide quick relief to victims (e.g., compensating passengers or airports in the immediate aftermath of a major cyber disruption), with the fund then recovering costs from the responsible parties after investigation. While not a direct legal liability measure, this ensures timely compensation and maintains public trust, while still ultimately holding the liable entities accountable. Over the long term, a mature cyber insurance market will help normalize proactive cybersecurity investments (companies with better security could receive premium discounts) and provide expertise (insurers often conduct risk assessments of their clients). Currently, however, awareness and penetration of cyber insurance in Indian aviation remain low, so steps should be taken to educate and incentivize the sector about its benefits.

I. Encourage Public-Private Collaboration and Transparency: Cybersecurity in aviation cannot be improved by government mandate alone – it requires partnership between regulators and industry. Legal reforms should include incentives for transparency and cooperation. Regulators should adopt a cooperative posture where possible: for instance, DGCA/BCAS could establish a "safe harbor" policy for the voluntary reporting of minor cyber incidents or vulnerabilities. If an airline or airport promptly discloses an issue and demonstrates proactive mitigation, the regulator could agree to forgo or reduce penalties for that incident. This approach, akin to practices in some data protection regimes (where quick breach reporting can lead to lower fines), encourages organizations to come forward with information that can benefit the whole sector. It builds trust and helps regulators gather a more accurate picture of the threat landscape. Such a safe harbor could be formalized via rules stating that penalties may be waived if a company self-reports in

good faith and rectifies the issue. Furthermore, establishing joint industry-government working groups or advisory committees on aviation cybersecurity can help in formulating practical regulations and sharing best practices. In summary, the regulatory approach should balance stick and carrot: punish clear negligence or concealment, but reward transparency and proactive risk management.

J. Continuously Update the Legal Framework for Emerging Threats: Technology in aviation is rapidly evolving – from increased reliance on cloud-based systems and Internet of Things (IoT) devices in airports, to the rise of unmanned aircraft systems (drones) and potentially autonomous passenger aircraft. The legal framework must be agile enough to cover new threat scenarios. Regular reviews of laws and regulations should be mandated. For example, if airlines start using AI extensively for operations or if airports adopt 5G networks for critical communications, regulators should evaluate what new cyber vulnerabilities come with that and update requirements accordingly. If entirely novel attack vectors appear (say, hacking of satellite-based navigation or drone swarms causing airspace disruptions), laws might need amendments to clearly criminalize those and assign responsibility. India's existing mechanisms, like the expert committee reviewing cyber laws, should explicitly include civil aviation in their scope. By institutionalizing a process to update rules (perhaps through an annual or biennial review involving stakeholders), India can avoid its legal framework becoming obsolete. In essence, cybersecurity regulation should not be a one-off project but an ongoing process, just as aviation safety regulations continually evolve with new aircraft, technologies, and procedures.

VIII. **Implementing a Roadmap:** Translating these recommendations into action will require a clear roadmap with defined phases, responsible agencies, and resource allocation:

A. **Immediate (within 6–12 months):** The Ministry of Civil Aviation (MoCA) should convene a task force or working group (including DGCA, BCAS, CERT-In, NCIIPC, and industry representatives) to draft the new Civil Aviation Cybersecurity guidelines (Recommendation 1). Concurrently, DGCA can set up the Aviation Cybersecurity Cell (Rec 2) on a pilot basis, identifying staff (possibly seconded from CERT-In or NIC) and securing initial funding – which the government should allocate as per the Parliamentary Committee's advice. Quick wins in this phase could include issuing an interim circular to all operators to begin aligning with basic cyber hygiene practices and establishing communication channels for incident sharing.

B. **Short to Medium Term (1–2 years):** Finalize and formally adopt the Civil

Aviation Cybersecurity guidelines as a binding requirement, with a reasonable timeline for industry compliance (e.g., one year to implement key controls). In parallel, MoCA – in coordination with the IT Ministry and other relevant ministries – should draft necessary amendments to the Aircraft Rules or related laws to embed cybersecurity duties and penalties (Rec 3). Efforts to ratify the Beijing Convention and bolster international cooperation (Rec 4) should be initiated via the Ministry of External Affairs and Ministry of Home Affairs. Meanwhile, DGCA/BCAS should integrate cybersecurity into existing oversight processes (Recs 6 and 7): for example, adding cyber scenarios to safety audits and emergency drills by 2025, and requiring each airline and major airport to conduct at least one cyber incident drill per year. The Aviation Cybersecurity Cell should gradually evolve into a full-fledged ISAC, enrolling all airlines, airports, ATC units, and perhaps aircraft manufacturers active in India, and begin regular threat briefings or bulletins to the sector.

C. **Long Term (3–5 years):** Evaluate the effectiveness of the new regulations and structures and refine them. By year 3, data on compliance levels, incident frequency, and enforcement actions should be analyzed. DGCA can consider raising the bar on guidelines (e.g., requiring more advanced measures like periodic third-party penetration testing or certification for critical systems). Legislative work to address any remaining gaps (Rec 10) should be ongoing. The uptake of cyber insurance (Rec 8) and the viability of any cyber incident fund can be reviewed and adjusted. On enforcement, by this time one would expect to see some enforcement cases or penalties for non-compliance – these should be transparently reported to build credibility (while still protecting sensitive security details). Overall, clear ownership should be assigned for each task: DGCA and BCAS for drafting and enforcing aviation-specific rules; CERT-In/NCIIPC for technical support and incident response integration; MoCA for policy oversight and ensuring inter-agency cooperation; industry bodies for driving compliance and information-sharing; and the Data Protection Board for handling personal data breach cases. Regular public reports (perhaps an annual "State of Aviation Cybersecurity" report by MoCA or DGCA) could help maintain momentum and accountability.

IX. Research Findings and Recommendations for Developing Countries

The examination of India's aviation cybersecurity framework provides valuable insights that are broadly pertinent to developing countries. In the context of underdeveloped legal and regulatory structures, limited institutional capacity, and nascent recognition of cyber threats, common challenges include the rapid digitisation of aviation systems. Many developing countries encounter comparable deficiencies: their aviation laws and regulations were not developed with cyber threats in mind,

resulting in ambiguous accountability and liability for cyber incidents (Klenka, 2021). For instance, there are critical oversight voids in India due to a patchwork of general IT laws and traditional aviation regulations. India's experience demonstrates that the fragmentation of aviation cybersecurity responsibilities across agencies hampers incident response and enforcement. This fragmentation and the absence of a designated main authority or information-sharing mechanism are likely to be replicated in other developing countries. Moreover, resource constraints impede the effective implementation of cybersecurity measures: the supervision capacity of India's civil aviation regulator (DGCA) is undermined by the fact that nearly half of the technical positions are vacant (Tripathi, 2025). In developing contexts, such capacity deficits—regarding funding, technical expertise, and trained personnel—are prevalent and impede the implementation of even the most well-crafted policies. These results underscore the necessity of comprehensive enhancements in legal frameworks, regulatory measures, institutional arrangements, and capacity development to enhance aviation cybersecurity in developing countries.

A. **Strengthen Legal Frameworks and Clarify Liability:** To explicitly address aviation cybersecurity, developing countries should update and broaden their legislative frameworks. Legal scholarship has observed that conventional aviation laws are inadequately equipped to address cyber threats and must be updated to encompass digital hazards (Klenka, 2021). National aviation statutes and penal codes should explicitly define liability for operators and criminalise intrusions on aviation systems. Consider, for example, the ICAO Assembly resolutions of 2019 and 2022, which have encouraged states to enhance their legal frameworks: The 41st Assembly of the International Civil Aviation Organisation (ICAO) urged the adoption of the 2010 Beijing Convention, which classifies cyberattacks on aviation as offences analogous to unlawful interference (ICAO, 2019; ICAO, 2022). Resolution A40-10 also encourages states to establish frameworks against cyber threats. Developing countries should ratify and implement these international instruments to facilitate the prosecution of offenders and promote cross-border cooperation. They should also contemplate participating in the Budapest Convention or similar agreements to facilitate international cybercrime investigations. Accountability will be established by defining legal obligations and liabilities. Suppose airlines, airports, or vendors fail to maintain "reasonable security" and a breach occurs. In that case, the law should permit regulators or victims to hold them accountable (e.g., through regulatory penalties or negligence claims). In summary, implementing updated definitions of cyber offences and penalties and transparent legal accountability will encourage improved cybersecurity compliance.

B. **Implement Cybersecurity Regulations and Standards:** Concrete cybersecurity standards for the aviation sector must be mandated by

regulators in developing countries, in addition to broad laws. India's example demonstrated that security practices were inconsistent and enforcement was challenging without sector-specific regulations. Like the EU and the United States, developing states may establish regulations that mandate aviation operators to implement baseline security measures, conduct risk assessments, and report incidents. The European Union's Network and Information Security (NIS) framework is a model. The NIS Directive mandates that EU member states implement minimum cyber risk controls and incident reporting obligations in "essential" sectors, such as aviation transport (European Parliament and Council, 2016). This was further fortified by the NIS2 Directive in 2022, which strengthened the requirements for aviation and other critical sectors, such as executive accountability and supply-chain security (European Parliament and Council, 2022). These regulations establish a distinct standard of care for cybersecurity, which is accompanied by substantial fines for noncompliance (as evidenced by the enforcement of data-breach penalties under the EU's GDPR). Developing countries should also empower civil aviation authorities or cybersecurity agencies to issue binding guidelines or rules for airlines, airports, and air navigation service providers. Key mandates may include the following: adhering to international standards (e.g., ICAO Annex 17 provision 4.9.1, which mandates the protection of critical aviation ICT systems (ICAO, 2017), establishing an information security management system that is consistent with frameworks such as the NIST Cybersecurity Framework or ISO 27001, as well as with ICAO/IATA cybersecurity guidance), and promptly reporting significant cyber incidents to relevant authorities. Regulatory enforcement is essential; regulators should be permitted to conduct audits, mandate remedial actions, and impose penalties for cybersecurity lapses. The U.S. experience demonstrates the value of combining voluntary frameworks with targeted mandates: The U.S. Transportation Security Administration issued directives requiring airlines and airports to implement network segmentation, access controls, continuous monitoring, and 24-hour incident reporting in response to a surge in transportation-related attacks (DHS, 2022). Similarly, developing countries should transition from solely voluntary guidance to enforceable requirements that guarantee minimum cyber hygiene in aviation. Regulators will increase the priority of cyber safety within the industry by considering it as a legal obligation rather than a mere IT concern.

C. **Enhance Institutional Coordination and Oversight:** To ensure aviation cybersecurity, it is essential to establish a coordinated institutional framework. Developing countries must establish a distinct leadership structure and encourage collaboration among aviation authorities,

cybersecurity agencies, and industry stakeholders. Supervision has been siloed in India, with DGCA, BCAS, CERT-In, airport operators, and other entities participating in the process. This has led to ad hoc coordination. Countries may establish aviation cybersecurity task forces or bodies to prevent such voids. For instance, a national aviation cybersecurity committee could convene the civil aviation regulator, the national CERT, air navigation service providers, and major airlines to exchange information and collaborate on strategies. Threats and incidents are promptly disseminated throughout the sector through regular communication channels (or an industry ISAC). Useful models for such collaboration are provided by the U.S. Aviation ISAC and Europe's aviation CERT (EATM-CERT) (Norton Rose Fulbright, 2020). Similarly, developing countries could establish a sector-specific aviation CERT team or a cybersecurity branch within the civil aviation authority dedicated to monitoring cyber threats and responding to incidents. In addition, governments should establish a national aviation cybersecurity strategy or action plan that delineates roles and coordination mechanisms, similar to the U.S. FAA's comprehensive Cybersecurity Plan for the national airspace (FAA, 2020). This plan would delineate how various institutions collaborate during a cyber crisis and how critical systems will be restored. It would also provide a clear understanding of the chain of command and communication protocols to prevent confusion during incidents. Enhancing oversight may also necessitate legal modifications that grant the aviation regulator explicit authority over cybersecurity compliance and mandate that operators undertake periodic cybersecurity audits. Developing countries can transition from a reactive to a more proactive and organised defence by enhancing inter-agency coordination and dedicating institutional attention to cyber threats.

D. **Build Capacity and Foster a Security Culture:** To effectively implement aviation cybersecurity measures, developing countries require significant capacity-building. This encompasses acquiring technology, awareness, training, and competent human resources. The Indian case illustrates the potential for policy enforcement to be undermined by a lack of qualified personnel and restricted budgets (Tripathi, 2025). To resolve this issue, governments should designate specific funding for cybersecurity in the aviation sector. For instance, budgets should be allocated to recruiting cyber experts within aviation agencies and upgrading critical systems. Regular staff training on cybersecurity best practices and cybersecurity exercises or simulations (e.g., at airports) should be conducted by regulators and aviation operators to assess readiness and enhance incident response plans. ICAO underscores that legal frameworks are insufficient without technical capacity on the ground. Therefore, states

must enhance the number of aviation professionals proficient in cybersecurity and establish an organisational culture that prioritises security (ICAO, 2022). Developing countries may collaborate with more advanced jurisdictions to facilitate knowledge exchange or request assistance from ICAO's capacity-building programs. It is equally crucial to cultivate a "cyber safety" culture. In the same way that civil aviation has a pervasive safety culture, organisations must inculcate the belief that cybersecurity is everyone's responsibility (IATA, 2021; ICAO, 2022). This necessitates executive support – airline and airport leadership should regard cyber risks as strategic risks – and accountability mechanisms, such as appointing a Chief Information Security Officer (CISO) or equivalent for aviation organisations. Baseline cybersecurity practices for airlines have been published by industry associations such as IATA (IATA, 2021), which regulators may either require or promote. The disparity between policy and practice will be bridged over time by enhancing human capital and awareness, ensuring that the rules on paper are translated into meaningful risk reduction.

E. **Comply with international standards and foster collaboration:** Lastly, developing countries should participate in global cooperation and align their aviation cybersecurity initiatives with international frameworks. The vulnerability of all individuals is exacerbated by the transnational nature of cyber threats to aviation, which are addressed through a patchwork approach by individual states. For instance, ICAO Annexe 17 mandates that states incorporate cybersecurity into their national civil aviation security programs (ICAO, 2017), a foundation for the organisation's standards and strategies. To ensure that their aviation systems meet the globally anticipated level of protection, states should implement these standards domestically. Moreover, the 2019 Aviation Cybersecurity Strategy of the International Civil Aviation Organisation (ICAO) (adopted at the 40th Assembly) delineates the primary pillars of international cooperation, governance, legislation, information-sharing, incident response, and capacity-building, which can serve as a foundation for national policies (ICAO, 2022). Developing countries are encouraged to adopt best practices disseminated by ICAO, IATA, and other bodies, share data on threats, and participate in ICAO's initiatives. International cooperation is also essential when incidents occur: mechanisms for cross-border information exchange and mutual assistance through CERT networks and INTERPOL should be strengthened. Countries should not hesitate to request assistance from more experienced partners in investigating and mitigating attacks. Developing states can guarantee that the airlines and airports under their jurisdiction are not vulnerable segments of the global aviation network by aligning their regulations with

global best practices, such as the EU and US frameworks for critical infrastructure protection. In conclusion, a globally informed approach will enhance domestic resilience and contribute to the collective security of international civil aviation.

Implementing the earlier measures will enable developing countries to manage cyber risks in aviation more effectively. These states can address the legal and policy gaps identified in India's case by enacting clear laws and standards, creating robust institutions, enhancing capacity, and cooperating internationally. This will lead to a more cohesive and robust approach to aviation cybersecurity, safeguarding critical aviation services, enhancing passenger confidence, and ensuring that developing nations follow the changing global standards of cyber resilience in civil aviation.

X. Conclusion

Cybersecurity has become as critical to the safety and reliability of aviation as aircraft maintenance or physical security, as a result of the numerous cyberattacks on the aviation industry, including enormous data breaches, crippling ransomware, and DDoS disruptions. India is currently at a critical juncture in safeguarding its aviation sector. The analysis demonstrates that India's legal and regulatory system is inadequately equipped to address this novel threat environment. A mishmash of regulations with unclear reach and ineffective enforcement resulted from the Information Technology Act 2000 and the Aircraft Act 1934 not being designed for aviation hacking. Recent examples demonstrated the impact of these deficiencies on real-world outcomes: victims were not compensated, accountability for breaches was unclear, and lessons learned were rarely implemented to enhance preparedness. Proactive risk management is impeded by a lack of institutional control and an immature cybersecurity culture among aviation stakeholders. The absence of best practices and standards in India's aviation sector is underscored by global frameworks such as the ICAO's guidance and the EU and US aviation cybersecurity initiatives, which underscore the country's inadequate defences compared to international standards.

Legislation and policy reforms are needed to close these gaps and improve accountability and resilience in Indian aviation cybersecurity. The proposed reforms, based on international best practices and India's recent initiatives like the Digital Personal Data Protection Act 2023, require clearly defining liability for cyber incidents, mandating rigorous cyber risk management across airlines, airports, and other aviation players, improving inter-agency coordination and regulatory oversight, and fostering a security-first culture in the industry. Since cyber threats cross borders, India's strategy must include international cooperation, such as aligning with ICAO guidelines, sharing information across borders, and adopting EU and US best practices. Urgency is needed for this reform plan. Indian rules and procedures may be updated quickly to protect passengers and operations better, maintain public faith in this vital sector, and meet international commitments to secure the skies in the

digital age. Strong cybersecurity in Indian aviation would help stakeholders identify attacks before they cause considerable harm, making legal liability a rare backup rather than a frequent battleground.

Acknowledgments:

The authors are sincerely appreciative of the University of Sharjah, United Arab Emirates, for its institutional support during the duration of this research. The successful completion of this study was significantly influenced by the University's dedication to academic excellence, its collaborative environment and comprehensive research resources. The authors also thank the faculty and administrative staff for their guidance and encouragement, which have been instrumental in developing this work on aviation cybersecurity and legal liability.

References:

Agrawal, A. (2024, December 7). *Cybersecurity incidents tracked by CERT-In quadrupled in last 5 years*. Hindustan Times. https://www.hindustantimes.com/india-news/cybersecurity-incidents-tracked-by-cert-in-quadrupled-in-last-4-years-101733512342858.html

Aircraft Act, 1934 (India). No. 22 of 1934, as amended. Retrieved from http://www.indiacode.nic.in/

Asian News International. (2022, May 25). *SpiceJet faces ransomware attack; flights impacted*. The Economic Times. https://economictimes.indiatimes.com/industry/transportation/airlines-/-aviation/spicejet-faces-ransomware-attack-flights-impacted/articleshow/91780385.cms

Asian News International. (2023, March 14). Parliamentary committee recommends separate budget for cyber security system in aviation sector. *ThePrint*. https://theprint.in/india/parliamentary-committee-recommends-separate-budget-for-cyber-security-system-in-aviation-sector/1442660/

CERT-In. (2022). Directions under sub-section (6) of section 70B of the IT Act, 2000 (No. 20(3)/2022-CERT-In). Ministry of Electronics and Information Technology, Government of India.

Chande, R. (2023). Cyber crime in aviation industry: The sky's the limit? *Legal Service India*. https://www.legalserviceindia.com/legal/article-11873-cyber-crime-in-aviation-industry-the-sky-s-the-limit-.html

CXOtoday News Desk. (2025, March 4). CyberPeace unveils critical report on over 80,000 cyber threats in India's aviation sector. *CXOtoday*. https://cxotoday.com/press-release/cyberpeace-unveils-critical-report-on-over-80000-cyber-threats-in-indias-aviation-sector/

Duggal, P. (2019). *Cyber security law* (2nd ed.). New Delhi: Saakshar Law Publications.

ETCISO. (2023, April 13). DDoS attacks strike Indian airports: Here's how the threat was mitigated. *ETCISO – Economic Times*.

https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/ddos-attacks-strike-indian-airports-heres-how-the-threat-was-mitigated/99461876

European Parliament and Council. (2016). Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems (NIS Directive). *Official Journal of the European Union*, L 194/1.

European Parliament and Council. (2022). *Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union* (NIS2 Directive). *Official Journal of the European Union*, L 333/80.

FAA Reauthorization Act of 2018 (U.S.). Pub. L. No. 115–254, §506, 132 Stat. 3186 (2018). *(U.S. federal law enacted Oct. 5, 2018.)* Retrieved from **GovInfo**: https://www.govinfo.gov/content/pkg/PLAW-115publ254/pdf/PLAW-115publ254.pdf

Ghosh, S. (2021, May 30). Air India data breach highlights concerns around third-party risk and supply-chain security. *CSO Online*. https://www.csoonline.com/article/570797/air-india-data-breach-highlights-concerns-around-third-party-risk-and-supply-chain-security.html

Government of India. (2023). *Digital Personal Data Protection Act, 2023* (No. 22 of 2023). *Gazette of India: Extraordinary*, Part II, Section 1 (August 11, 2023). https://indiankanoon.org/doc/185806268/

Hummel, R. (2023, April 25). *100% increase in DDoS attacks against India*. NETSCOUT Blog. https://www.netscout.com/blog/asert/100-increase-ddos-attacks-against-india

Information Technology Act, 2000 (India). Act No. 21 of 2000, as amended by Act 10 of 2009. Ministry of Law and Justice, Government of India. https://www.meity.gov.in/content/information-technology-act

International Air Transport Association. (2021). *Guidance on Aviation Cybersecurity*. Montreal/Geneva: IATA.

International Civil Aviation Organization. (2017). *Annex 17 to the Chicago Convention: Security* (16th ed., Amendment 16). Montreal: ICAO.

International Civil Aviation Organization. (2019). *Assembly Resolution A40-10: Addressing cybersecurity in civil aviation*. Montreal: ICAO.

International Civil Aviation Organization. (2022). *Aviation cybersecurity strategy and action plan*. Montreal: ICAO.

International Civil Aviation Organization. (2022). *Assembly Resolution A41-19: Addressing Cybersecurity in Civil Aviation*. Montreal: ICAO.

International Civil Aviation Organization. (2025). Aviation Cybersecurity. Retrieved April 30, 2025, from https://www.icao.int/aviationcybersecurity/

Kapoor, M. (2022, May 28). SpiceJet ransomware attack: Questions raised about airline's IT security. *Business Today*. https://www.businesstoday.in/latest/in-

focus/story/spicejet-ransomware-attack-questions-raised-about-airlines-it-security-336873-2022-05-28

Klenka, M. (2021). Aviation cybersecurity: Legal aspects of cyber threats. *Journal of Transportation Security, 14*(3), 177–195. https://doi.org/10.1007/s12198-021-00232-8

Ministry of Communications & IT (India). (2011). *Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011* (SPDI Rules) under IT Act 2000. Ministry of Communications and IT, Government of India.

Ministry of Communications (India). (2022). *The Indian Telecommunication Bill, 2022* (Draft for consultation). New Delhi: Government of India.

Norton Rose Fulbright. (2020). Cybersecurity law in the aviation sector. https://www.nortonrosefulbright.com/en/knowledge/publications/fc813c25/cybersecurity-law-in-the-aviation-sector

Press Trust of India (PTI). (2025, January 2). *India second most targeted nation in terms of cyber attacks: CloudSEK*. The Economic Times. https://economictimes.indiatimes.com/tech/technology/india-second-most-targeted-nation-in-terms-of-cyber-attacks-cloudsek/articleshow/116890873.cms

PwC. (2018). *Airline CEOs survey – Aviation perspectives*. PricewaterhouseCoopers. https://www.pwc.in/assets/pdfs/publications/2018/airline-ceos-survey-aviation-perspectives.pdf

Resecurity. (2024, March 16). *The aviation and aerospace sectors face skyrocketing cyber threats* (Cyber Threat Intelligence Report). Resecurity Blog. https://www.resecurity.com/blog/article/the-aviation-and-aerospace-sectors-face-skyrocketing-cyber-threats

Singh, M. (2021, May 23). Air India passenger data breach reveals SITA hack worse than first thought. *TechCrunch*. https://techcrunch.com/2021/05/23/air-india-passenger-data-breach-reveals-sita-hack-worse-than-first-thought/

Singh, M., & Sharma, A. (2022, May 27). SpiceJet ransomware attack led to delayed flights; DGCA issues notice. *The Indian Express*. https://indianexpress.com/article/india/spicejet-ransomware-attack-delayed-flights-dgca-notice-7938021/

Singh, M., & Whittaker, Z. (2020, January 30). Breach at Indian airline SpiceJet affects 1.2 million passengers. *TechCrunch*. https://techcrunch.com/2020/01/30/spicejet-breach-millions-passengers/

Tripathi, N. L. M. (2025, July 20). Nearly half of technical posts in DGCA vacant. *Hindustan Times*. https://www.hindustantimes.com/india-news/nearly-half-of-technical-posts-in-dgca-vacant-101752951059224.html

U.S. Department of Homeland Security (DHS). (2022, October 19). DHS statement on TSA Security Directive Pipeline-2021-02D and aviation SDs [Press release]. Washington, DC: DHS.

U.S. Federal Aviation Administration (FAA). (2020). *FAA Cybersecurity Plan for*

National Airspace Systems. Washington, DC: FAA.