Flying Without Accountability: Cybersecurity and Liability under India's Aviation Law

Rohn Mathew John[56] & *Mathews P Cherian* [57]

ABSTRACT

The increasing digitalisation of civil aviation has transformed aircraft operations, air traffic management, and airport infrastructure into cyber-physical systems that are vulnerable to non-kinetic attacks. While cyber incidents in aviation may not always result in physical damage, they are capable of causing serious operational disruption, safety risks, and economic loss. In response to the need for regulatory modernisation, India enacted the Bharatiya Viman Adhiniyam, 2024, replacing the Aircraft Act, 1934. Although the new legislation strengthens regulatory oversight and updates aviation governance, it continues to conceptualise aviation security primarily in physical and state-centric terms. This essay argues that the Bharatiya Viman Adhiniyam, 2024 creates a liability vacuum with respect to private cyber attacks on aviation infrastructure. The Act does not expressly impose cybersecurity obligations on aircraft operators, service providers, or technology vendors, nor does it allocate responsibility for cyber-induced disruptions caused by non-state actors. As a result, in the event of a cyber incident, there is no clear statutory basis for determining regulatory, civil, or operational liability within the aviation framework. The essay further demonstrates that this gap is not adequately addressed by existing general cyber legislation, particularly the Information Technology Act, 2000. While the IT Act criminalises cyber offences and regulates certain aspects of digital conduct, it does not function as a sector-specific safety regime capable of allocating liability for systemic risks in aviation. The absence of integration between cyber law and aviation safety regulation leaves enforcement fragmented and accountability uncertain. By analysing the structure and silences of India's aviation law alongside the limits of general cyber regulation, this essay highlights the legal and practical consequences of unresolved liability in the aviation cybersecurity context. It concludes by proposing targeted reforms aimed at recognising cyber threats as aviation safety risks, imposing enforceable cyber duties within aviation law, and clarifying responsibility for private cyber attacks in order to enhance regulatory certainty and passenger safety.

[56] Student at School of Law, CHRIST (Deemed to be University), Bangalore.
[57] Student at School of Law, CHRIST (Deemed to be University), Bangalore.

I. INTRODUCTION

Civil aviation has increasingly evolved into a complex cyber-physical system in which aircraft operations, air traffic management, navigation, and airport infrastructure depend heavily on digital networks and software-driven processes. While traditional aviation security frameworks were designed to address physical threats such as sabotage, hijacking, and unlawful interference, contemporary risks are increasingly non-kinetic. Cyber attacks targeting aviation systems are capable of disrupting flight operations, grounding fleets, interfering with communication systems, and undermining safety without causing immediate physical damage.[58] Recognising the need to modernise aviation regulation, India enacted the Bharatiya Viman Adhiniyam, 2024, replacing the colonial-era Aircraft Act, 1934.[59] The new legislation aims to strengthen regulatory oversight, streamline certification processes, and enhance safety and security governance within the civil aviation sector. However, despite its reformist intent, the Act largely retains a traditional understanding of aviation security that prioritises physical threats and state-centric risks. The regulatory architecture it establishes does not expressly engage with cybersecurity as a distinct component of aviation safety. This omission has significant legal implications in the context of cyber attacks carried out by private actors. Unlike conventional security threats, private cyber attacks operate remotely, often across jurisdictions, and do not fit neatly within existing aviation security classifications. The Bharatiya Viman Adhiniyam, 2024 does not impose explicit cybersecurity obligations on aircraft operators, air navigation service providers, or technology vendors, nor does it provide a statutory framework for allocating responsibility when aviation operations are disrupted due to cyber incidents. As a result, the law offers limited guidance on regulatory accountability and civil liability in such scenarios. This essay argues that the Bharatiya Viman Adhiniyam, 2024 creates a liability vacuum with respect to private cyber attacks on aviation infrastructure. It contends that this vacuum cannot be effectively addressed through general cyber legislation, particularly the Information Technology Act, 2000, which lacks the sector-specific orientation required for aviation safety regulation. By examining the structure and silences of India's aviation law alongside the limitations of existing cyber law, the essay seeks to highlight the consequences of unresolved liability and the need for targeted legal reforms to ensure regulatory certainty and aviation safety in an increasingly digital environment.

[58] ICAO Civil Aviation Cybersecurity Strategy (2019)

[59] Bharatiya Viman Adhiniyam, 2024

II. LIABILITY ARCHITECTURE UNDER THE BHARATIYA VIMAN ADHINIYAM, 2024

The Bharatiya Viman Adhiniyam, 2024 was enacted with the objective of modernising India's civil aviation regulatory framework by strengthening institutional oversight, updating safety and security governance, and enhancing regulatory efficiency.[60] The Act expands the statutory role of aviation authorities, reinforces certification and compliance mechanisms, and consolidates regulatory powers within the civil aviation administration. In doing so, it reflects a clear legislative intent to move away from the outdated structure of the Aircraft Act, 1934 and respond to contemporary aviation needs.

Within this framework, the Act conceptualises aviation safety and security through a predominantly traditional lens. Its provisions are oriented towards the regulation of aircraft operations, airworthiness, licensing, aerodrome standards, and the prevention of unlawful interference with civil aviation.[61] Security obligations under the Act are framed around physical risks and operational compliance, consistent with long-standing aviation law assumptions that prioritise tangible threats such as sabotage, terrorism, and mechanical failure. Liability mechanisms embedded within this structure are therefore implicit, sector-specific, and closely tied to physical safety outcomes.

However, the Act does not expressly recognise cybersecurity as an independent dimension of aviation safety. It does not define cyber threats, prescribe minimum cybersecurity standards, or impose affirmative statutory duties on regulated entities to prevent or mitigate cyber risks. More importantly, the Act does not articulate a framework for allocating responsibility or liability in the event that aviation operations are disrupted due to cyber attacks carried out by private actors. The absence of such provisions is significant given the increasing reliance of aviation systems on digital infrastructure and networked technologies.

The regulatory model under the Act relies substantially on delegated legislation and administrative oversight exercised through authorities such as the Directorate General of Civil Aviation.[62] While this enables flexibility in rule-making and operational guidance, it also highlights a structural limitation. Delegated regulations and circulars may prescribe best

[60] Bharatiya Viman Adhiniyam, 2024, Statement of Objects and Reasons
[61] Bharatiya Viman Adhiniyam, 2024 (security and safety provisions)
[62] DGCA statutory role

practices or advisory measures, but they cannot substitute for clear statutory allocation of liability. In the absence of explicit legislative direction, regulatory responses to cyber incidents remain discretionary and fragmented. As a result, the liability architecture under the Bharatiya Viman Adhiniyam, 2024 is ill-equipped to address cyber-induced disruptions that do not involve physical damage or traditional security breaches. The Act establishes a comprehensive regulatory framework for conventional aviation risks but leaves unresolved the question of who bears legal responsibility when private cyber attacks interfere with aviation safety and operations. This statutory silence forms the foundation of the liability vacuum that becomes particularly evident when cyber threats originate outside the state-centric security paradigm assumed by aviation law.[63]

III. THE PRIVATE CYBER ATTACKER PROBLEM

Aviation security law has historically been structured around identifiable and tangible threats.[64] Conventional regulatory frameworks assume that risks to civil aviation arise from physical sabotage, hijacking, terrorism, or hostile state action. These assumptions inform how duties are imposed, how security is enforced, and how responsibility is allocated when incidents occur. Cyber attacks carried out by private actors, however, do not conform to this threat model, creating a structural mismatch between contemporary risks and existing legal frameworks. This disconnect becomes most apparent when liability is examined within the statutory framework outlined in the previous section. Private cyber attackers operate remotely, often anonymously, and frequently across national borders.[65] Their actions may target flight management systems, airline reservation platforms, air traffic control networks, or airport operational technology without direct physical interference. While such attacks can cause severe operational disruption, safety risks, and economic loss, they may not trigger the traditional security responses envisaged under aviation law. As a result, cyber incidents fall into a regulatory grey area where the nature of the harm does not align with the assumptions underlying aviation security regulation.

This misalignment becomes particularly problematic when questions of liability arise. The Bharatiya Viman Adhiniyam, 2024 does not specify whether responsibility for preventing or

[63] In re Delhi Laws Act AIR 1951 SC 332
[64] Dempsey, Public International Air Law
[65] Brenner, 'Cybercrime Jurisdiction'

mitigating cyber attacks rests with aircraft operators, air navigation service providers, airport authorities, or third-party technology vendors. Nor does it establish a clear duty of care with respect to cybersecurity that can be enforced through regulatory or civil mechanisms. In the absence of such duties, liability for cyber-induced disruptions remains uncertain and contested. Criminal law responses to cyber attacks, while relevant, do not resolve this uncertainty.[66] Identifying and prosecuting private cyber attackers is often difficult due to jurisdictional constraints and technical complexity. Even where prosecution is possible, criminal liability does not address the allocation of regulatory or civil responsibility within the aviation ecosystem. Aviation law traditionally emphasises preventive regulation and operator accountability in safety-critical contexts, yet this logic is not extended to cybersecurity risks under the current statutory framework.

The result is a liability vacuum in which no actor bears clearly defined responsibility for cyber resilience in aviation operations. Operators may argue that cyber incidents fall outside their statutory obligations, regulators may rely on discretionary guidance rather than enforceable duties, and service providers may escape accountability due to the absence of sector-specific standards. This diffusion of responsibility undermines the preventive logic of aviation safety regulation and leaves aviation systems vulnerable to cyber threats that do not fit within the conventional state-centric security paradigm. By failing to adapt liability structures to account for private cyber attacks, the Bharatiya Viman Adhiniyam, 2024 exposes a critical weakness in India's aviation law. The Act's reliance on traditional security assumptions renders it ill-suited to address non-kinetic threats, thereby reinforcing legal uncertainty at precisely the point where clarity is most necessary for effective risk management and accountability.

IV. WHY GENERAL CYBER LAW DOES NOT CURE THE LIABILITY GAP

In the absence of aviation-specific cybersecurity provisions, it may be argued that existing cyber legislation is capable of addressing cyber threats affecting aviation operations. In India, this role is primarily performed by the Information Technology Act, 2000, which establishes offences relating to unauthorised access, data interference, and computer-related misconduct.[67]

[66] IT Act 2000, ss 43, 66
[67] IT Act 2000, ss 43, 66

While the Act provides a general framework for regulating cyber activity and penalising wrongful conduct, it is not designed to function as a sector-specific safety regime for civil aviation. The Information Technology Act operates as a horizontal statute that applies uniformly across sectors, irrespective of the nature of the infrastructure involved.[68] Its primary focus lies in criminalising cyber offences, regulating intermediaries, and providing limited civil remedies for certain forms of digital harm. This framework is effective in addressing individual instances of cyber wrongdoing, but it does not allocate responsibility for managing systemic risks in safety-critical sectors such as aviation. As a result, the Act does not impose affirmative cybersecurity duties tailored to the operational realities of aviation systems. More importantly, the Information Technology Act does not integrate cybersecurity compliance with aviation safety certification or regulatory oversight.[69] Aviation regulation traditionally relies on ex ante safety mechanisms, including licensing, continuous compliance monitoring, and preventive standards enforced by specialised regulators. Cyber law, by contrast, is largely reactive, addressing violations after harm has occurred rather than embedding cybersecurity into operational safety requirements. This structural difference limits the ability of general cyber law to function as a substitute for sector-specific aviation regulation.

The reliance on general cyber legislation also fails to resolve questions of liability following a cyber incident. While the Information Technology Act may facilitate the prosecution of attackers, it does not clarify whether aviation operators, service providers, or technology vendors bear responsibility for failing to prevent or mitigate cyber risks. Nor does it establish standards against which regulatory negligence or breach of duty can be assessed within the aviation context. Consequently, the application of general cyber law does little to address the diffusion of responsibility created by statutory silence in aviation law. This fragmentation is particularly problematic in an industry where safety regulation depends on clearly defined roles and accountability structures. Without explicit statutory linkage between cyber compliance and aviation safety obligations, enforcement remains inconsistent and discretionary. The absence of coordination between cyber law and aviation regulation reinforces the liability vacuum identified earlier, leaving aviation cybersecurity governed by a patchwork of general legal provisions rather than a coherent, sector-specific framework. Accordingly, while the

[68] Gulati & John, NUJS Law Review

[69] Lessig, Code and Other Laws of Cyberspace

Information Technology Act, 2000 plays an important role in addressing cyber offences, it cannot cure the liability gap created by the Bharatiya Viman Adhiniyam, 2024. The lack of aviation-specific cybersecurity duties and liability allocation underscores the need for targeted legal intervention within aviation law itself, rather than reliance on general cyber legislation to address risks it was never designed to manage.

V. PRACTICAL CONSEQUENCES OF THE LIABILITY VACUUM

The absence of clear liability allocation for private cyber attacks under India's aviation law has tangible legal and operational consequences. Aviation regulation is premised on preventive accountability, where defined duties and enforceable standards incentivise compliance and risk mitigation. When statutory obligations are unclear, this preventive logic weakens, leaving cyber risks to be managed inconsistently across the aviation ecosystem. One immediate consequence of the liability vacuum is regulatory uncertainty following a cyber incident.[70] In the event of a disruption caused by a private cyber attack, it is unclear which entity bears primary responsibility for the failure to prevent or contain the incident. Aircraft operators may contend that cybersecurity falls outside their statutory obligations, while service providers and technology vendors may deny responsibility due to the absence of sector-specific duties. Regulators, in turn, may lack a clear legal basis to impose sanctions or corrective measures. This uncertainty delays enforcement and undermines regulatory credibility.

The liability gap also complicates civil claims and insurance arrangements.[71] Aviation insurance and risk allocation mechanisms depend on predictable liability standards to assess exposure and determine coverage. When cyber incidents are not clearly linked to statutory duties, insurers may dispute claims on the ground that cyber risks were not contemplated within existing aviation liability frameworks. Passengers and affected stakeholders may similarly face difficulty in identifying responsible parties, resulting in prolonged litigation and inconsistent outcomes. From a safety perspective, the diffusion of responsibility weakens incentives for proactive cybersecurity investment.[72] Aviation operators and service providers may prioritise compliance with explicitly mandated safety requirements while treating cybersecurity as a secondary or discretionary concern. In the absence of enforceable obligations, cybersecurity

[70] OECD Cyber Risk Report
[71] IATA Aviation Cybersecurity Report
[72] Hodges, Law and Corporate Behaviour

measures are more likely to be driven by cost considerations rather than safety imperatives. This creates uneven standards across the sector, increasing systemic vulnerability to cyber threats.

The liability vacuum further undermines coordination between regulators and regulated entities. Effective aviation safety regulation relies on continuous oversight, reporting, and compliance monitoring. When cybersecurity is not formally integrated into the aviation safety framework, regulatory engagement remains ad hoc and reactive. This limits the ability of authorities to assess sector-wide cyber resilience or respond effectively to emerging threats. Taken together, these consequences illustrate that the absence of clear liability for private cyber attacks is not merely a doctrinal concern but a practical regulatory weakness. The lack of statutory clarity affects enforcement, risk allocation, and safety governance, reinforcing the need for aviation-specific legal mechanisms that recognise cybersecurity as an integral component of aviation safety rather than a peripheral concern.

VI. TARGETED LEGAL REFORMS

Addressing the liability vacuum surrounding private cyber attacks in aviation does not require an overhaul of India's aviation law framework. Rather, it requires targeted and carefully calibrated reforms that recognise cybersecurity as an integral component of aviation safety and allocate responsibility in a manner consistent with the preventive logic of aviation regulation. First, aviation legislation must explicitly acknowledge cybersecurity as a safety risk within the statutory framework. The Bharatiya Viman Adhiniyam, 2024 should be amended to recognise cyber threats to aviation systems as capable of endangering safety and operational integrity. Such recognition would establish a clear legal basis for treating cybersecurity on par with other safety-critical risks and would avoid reliance on discretionary interpretation by regulators.

Second, the Act should impose affirmative cybersecurity duties on key aviation stakeholders, including aircraft operators, air navigation service providers, airport authorities, and relevant technology service providers. These duties need not prescribe technical standards in detail but should mandate compliance with sector-specific cybersecurity requirements issued by the aviation regulator. Statutory recognition of such duties would ensure that cybersecurity obligations are enforceable rather than merely advisory.

Third, the regulatory framework should provide for clear allocation of responsibility following cyber incidents. While private attackers may remain the primary wrongdoers under criminal law, aviation law must clarify the circumstances under which regulated entities may be held accountable for failures in cyber preparedness, risk management, or incident response. This would enable regulators to impose proportionate sanctions and corrective measures based on defined standards rather than ad hoc discretion.

Fourth, cybersecurity compliance should be integrated into existing aviation safety oversight mechanisms. This includes incorporating cyber risk assessment into certification, licensing, and continuous compliance monitoring processes. Embedding cybersecurity within established safety governance structures would align cyber risk management with the preventive and supervisory approach that characterises aviation regulation.

These reforms do not seek to displace general cyber legislation or impose unrealistic compliance burdens. Instead, they aim to bridge the gap between aviation safety law and cyber risk governance by clarifying duties and liability within the sector. By addressing statutory silence and reducing regulatory ambiguity, such targeted measures would strengthen accountability, enhance safety outcomes, and ensure that India's aviation law framework remains effective in an increasingly digital operational environment.

LAW JURIST LEGAL JOURNAL