IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Recent Developments In Aviation Security In India – A Critical Analysis

Shudharshini E

Student

School of Excellence in Law, Tamil Nadu Dr. Ambedkar Law University

Introduction

India, as one of the fastest-growing aviation markets in the world, has faced multifaceted challenges in securing its civil aviation sector. With the exponential growth in air traffic, ensuring the safety and security of passengers, aircraft, airport infrastructure, and aviation data has become paramount. Over the past decade, and especially in recent years, India has taken significant strides to revamp its aviation security architecture. This write-up critically examines the major developments, including institutional reforms, technological advancements, regulatory initiatives, and challenges ahead.

Overview of Aviation Security in India

Aviation security in India operates within a framework governed by international obligations (like those under the International Civil Aviation Organization – ICAO), domestic laws, and national policies. The Bureau of Civil Aviation Security (BCAS) is the nodal agency under the Ministry of Civil Aviation, responsible for laying down security standards and monitoring implementation at all civil airports in India. Historically, India has suffered security breaches, most notably the hijacking of Indian Airlines Flight IC-814 in 1999, which brought aviation security into national consciousness and policy reform[1].

Over the years, threats have evolved from conventional hijackings to more complex challenges like cyberattacks, drone incursions, insider threats, and terrorism through unmanned means. Thus, recent developments reflect the shift in security strategy from reactive to preventive and intelligence-driven approaches.[2]

[1] ICAO, *Annex 17 to the Convention on International Civil Aviation – Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, 11th Edition, 2020.

[2] Bureau of Civil Aviation Security, Ministry of Civil Aviation. *National Civil Aviation Security Programme (NCASP)* – Revised 2022.

Institutional and Policy Developments

In response to global trends and ICAO audits, India has revised its National Civil Aviation Security Programme (NCASP) multiple times, with the most recent amendment aligning with ICAO Annex 17 standards. The NCASP mandates enhanced screening, staff vetting, and security culture training.

Furthermore, BCAS has expanded its oversight capacity and integrated with intelligence agencies to address evolving threats. In 2022, India introduced the National Counter Rogue Drone Guidelines, empowering security agencies to neutralize suspicious drones, especially near airports. This was a landmark policy following incidents of drone sightings near vital installations and airports, particularly in border states. Additionally, in 2023, the Ministry of Civil Aviation initiated a comprehensive Security Audit Program involving third-party auditors to assess compliance and recommend site-specific enhancements. These audits have revealed gaps in smaller regional airports, prompting more inclusive security planning under the UDAN (Ude Desh ka Aam Naagrik) scheme.

Technological Integration in Aviation Security

A major thrust in recent reforms has been the adoption of smart technologies. The DigiYatra initiative, launched in December 2022, integrates facial recognition systems for seamless and contactless passenger processing. While enhancing convenience, it also introduces biometric-based passenger tracking, allowing pre-emptive threat identification.[3]

Moreover, modern explosive detection systems (EDS), advanced imaging technology (AIT) scanners, and full-body scanners have been introduced in major airports, especially those operated under the PPP model like Delhi and Mumbai. Surveillance has been upgraded with AI-based CCTV monitoring systems that can detect unattended baggage, suspicious movement, and perimeter breaches in real-time.

In cargo security, Radio Frequency Identification (RFID) tags and blockchain tracking for high-value cargo have been piloted in some airports, improving traceability and reducing risks of tampering or theft.

Legal and Regulatory Developments (Elaborated)

Over the last few years, India's legal and regulatory framework governing civil aviation security has undergone a significant transformation to address the growing spectrum of threats in a rapidly evolving global environment. The shift is evident in the strengthening of statutory powers, incorporation of international legal standards, and increased emphasis on compliance and enforcement.

Aircraft (Amendment) Act, 2020

One of the most critical legislative changes was the enactment of the Aircraft (Amendment) Act, 2020, which updated several aspects of the Aircraft Act, 1934. This amendment was driven by the need to enhance India's compliance with International Civil Aviation Organization (ICAO) audit recommendations. Key features of this amendment include:

- Increased Penalties: The amendment significantly raised penalties for aviation security breaches. For instance, carrying prohibited items, obstructing security personnel, or violating safety instructions now attracts fines of up to ₹1 crore.

[3] Ministry of Civil Aviation, "DigiYatra Rollout and Data Privacy Measures," Press Note, December 2022.

- Enhanced Enforcement Powers: BCAS inspectors and DGCA officials were empowered to impose penalties, conduct on-the-spot investigations, and seize documents in the event of suspected violations.[4]
- Recognition of International Obligations: The amendment brought Indian law in closer alignment with ICAO's safety and security standards, thereby improving India's audit scores in the Universal Security Audit Programme (USAP).

This reform signalled a more proactive legal posture and aimed at deterrence through stricter accountability measures.

Civil Aviation Security (Amendment) Regulations, 2023

In response to the insider threat and increasing privatization of airport operations, the Civil Aviation Security (Amendment) Regulations, 2023, were notified by BCAS. This regulatory reform introduced a system of mandatory security clearance for all personnel and entities working within sensitive airport zones. Key provisions include:

- Background Verification: Contractors, vendors, and employees working in areas like baggage handling, catering, and aircraft servicing are now subject to comprehensive police verification.
- Security Clearance as Precondition: Security clearance from BCAS is mandatory for license issuance or renewal for Ground Handling Agencies (GHAs), maintenance agencies, and private airport operators.
- Audit-Based Enforcement: Random and periodic audits by BCAS officials are allowed under the regulation to monitor compliance with screening and clearance norms.

This regulation is particularly important considering increasing subcontracting in Indian airports, where outsourced employees sometimes escape the scrutiny applicable to government or CISF personnel.

Strengthening Anti-Terror Legislation

The aviation sector is also covered under broader national security legislation. Amendments to the Unlawful Activities (Prevention) Act (UAPA) have widened the scope of what constitutes a terrorist act, including sabotage of critical infrastructure like airports and aircraft. Under this framework:

- Pre-Emptive Detention: Law enforcement agencies can detain suspects on grounds of planning or supporting acts that endanger civil aviation.
- Designation of Individuals as Terrorists: Unlike earlier provisions that targeted organizations, individuals planning or attempting to disrupt aviation operations can be designated as terrorists.

This change facilitates international cooperation, asset freezing, and extradition in cross-border aviation-related terror cases.

[4] Directorate General of Civil Aviation (DGCA), "Cybersecurity Guidelines for Civil Aviation Stakeholders," July 2023.

Drone Regulations and Security

Given the emergence of drones as potential threats to aviation security, the Ministry of Civil Aviation has framed Drone Rules, 2021 and accompanying Counter Rogue Drone Technology Guidelines (2022). While these are not security laws per se, their implications are critical for airport safety. Features include:

- Restricted Zones: The rules prohibit flying drones within 5 km of airport perimeters without prior approval.
- Penalties and Enforcement: Violations of no-fly zones attract penalties under both the Aircraft Act and Information Technology Act, depending on whether the drone is manually or remotely operated.
- Empowerment of Local Police and Airport Authorities: For immediate action, airport directors and local law enforcement are authorized to neutralize rogue drones using jamming, spoofing, or kinetic systems.

The Civil Aviation Ministry has also encouraged indigenous development of anti-drone systems in collaboration with DRDO and Bharat Electronics Limited.

Compliance with International Aviation Security Conventions

India is a signatory to several international conventions that shape its domestic aviation security regulations:

- Tokyo Convention (1963) – Deals with offenses on board aircraft and jurisdictional matters.
- Hague Convention (1970) – Focuses on unlawful seizure of aircraft (hijacking).
- Montreal Convention (1971 and 1999) – Addresses acts of sabotage, bomb threats, and destruction of aircraft or airport facilities.

These conventions are increasingly being referenced in domestic judicial decisions and enforcement actions, especially when dealing with international crimes like cross-border hijackings or threats originating from foreign jurisdictions. The incorporation of such instruments provides a transnational legal basis for cooperative enforcement and extradition efforts.

Cybersecurity and Data Protection Regulations

The aviation sector's growing reliance on digital infrastructure has necessitated the development of cybersecurity-specific legal mechanisms. Although India's data protection regime is still evolving, certain regulatory steps have been taken:

- DGCA Guidelines (2023) mandate periodic cybersecurity audits for airports and airline software systems, including Passenger Service Systems (PSS), Flight Operations Software (FOS), and Cargo Tracking Systems.
- CERT-In Advisories require all aviation entities to report cybersecurity breaches within 6 hours and maintain logs for forensic audits.
- Proposed Data Protection Act (Digital Personal Data Protection Act, 2023) includes obligations for aviation companies handling biometric data (e.g., under DigiYatra) to obtain explicit consent and ensure data minimization.

These frameworks, while not sector-specific, are legally binding and have a significant bearing on aviation security in India.

Human Resource and Capacity Building

Security personnel remain the backbone of aviation security. The Central Industrial Security Force (CISF) continues to guard India's major airports, but new recruitment and training modules have been rolled out focusing on behavioural detection techniques and use of non-lethal technologies. India has also collaborated with global agencies like ICAO, INTERPOL, and the U.S. TSA for training programs. Simulation-based learning and cyber-awareness training have been made compulsory for airport security staff. Furthermore, India has initiated programs to include female officers in sensitive screening roles to balance operational efficiency with privacy and gender sensitivity.

There has also been a growing emphasis on **passenger awareness programs** — signage, public announcements, and app-based alerts are now part of integrated airport operations to ensure greater public involvement in security.

Cybersecurity in Civil Aviation

In an increasingly digitized ecosystem, cyber threats pose a serious risk to aviation operations. Airports and air traffic control systems have become attractive targets for ransomware, data breaches, and malware attacks. Recognizing this, the Directorate General of Civil Aviation (DGCA), in coordination with CERT-In, issued new guidelines in 2023 mandating vulnerability assessments and penetration testing (VAPT) for all civil aviation stakeholders.

The Cybersecurity Policy for Civil Aviation (drafted in 2023) outlines mandatory encryption standards, endpoint protection, and audit trails for all digital operations, including passenger data management, flight operation systems, and baggage handling software. This is a critical development given previous cyber threats reported at Mumbai and Hyderabad airports.

India also became a member of the ICAO's Aviation Cybersecurity Strategy Working Group, contributing to global policy discussions and enabling shared threat intelligence.

Critical Challenges and Security Gaps

Despite these advancements, several challenges remain. First, India's regional airports, many under UDAN, often lack adequate security infrastructure and trained personnel, making them soft targets. While major airports are well-equipped, security disparity across the aviation ecosystem dilutes the overall national risk profile.

Second, the issue of insider threats — be it ground staff, catering vendors, or cleaning contractors — continues to be inadequately addressed in smaller airports. Though background checks are mandatory, enforcement remains inconsistent.

Third, drone threats are still evolving faster than regulatory response. While anti-drone technology is being piloted, high costs and technical barriers prevent large-scale deployment, especially in lower-tier airports.

Fourth, India still lags in implementing a **comprehensive passenger redressal mechanism** for security grievances, particularly regarding the right to privacy, profiling, and security-related harassment.

Lastly, the lack of a unified command and control centre at the national level for civil aviation security limits real-time threat coordination and data integration among airports.

Strategic Recommendations

To build a resilient aviation security ecosystem, India must undertake several key initiatives:

- Establish a National Aviation Security Command Center (NASCC) to centralize intelligence, operational decisions, and emergency coordination.
- Scale anti-drone technology deployment through public-private funding and indigenization to make it cost-effective.
- Strengthen regional airports by providing modular security equipment and mobile security units.
- Institutionalize passenger privacy frameworks in the DigiYatra and biometric data ecosystem to prevent surveillance overreach.
- Foster public-private partnerships in aviation cybersecurity innovation, ensuring indigenous solutions for SCADA systems, AI surveillance, and data integrity.

Conclusion

India's aviation security landscape has undergone a notable transformation, propelled by both external threats and internal reforms. While progress has been commendable, especially in technological integration and international alignment, structural vulnerabilities and inconsistent implementation remain. A critical analysis reveals that a layered, adaptive, and intelligence-led approach, inclusive of regional disparities, cyber risks, and emerging threats, is the need of the hour. Only then can India truly secure its skies in an era of high-altitude ambition and unpredictable threats.