# AVIATION SECURITY: A CRITICAL NON-TRADITIONAL SECURITY HOTSPOT

**INGUDAM YAIPHAREMBA SINGH**

The concept of security is an enormous area of central examination. Every aspect of it emerged with a new definition of threats, whether conventional or non-conventional. Aviation security is one of the elements of security that needs extreme protection—the approach of Aviation security by and large picked up pace after the 9/11 terrorist strikes. The aviation world shakes violently due to its easy access to the so-called foolproof security measures at the airport's multilayer security system. After the incident, many countries, including India, re-examined the aviation security procedures from the popular base to the top level to identify the loopholes and formulate new security mechanisms. The primary concern is safeguarding individuals and preventing unwanted events, such as hijacking, sabotaging aircraft, airport infrastructure, etc. Many airports currently undertake a three-tier security course of action in international and domestic terminals to prevent unwanted events and detect illegal substances. With innovative threats in the security environment, aviation security is emerging as a significant spot for terror attacks and sabotage activities. The protection of passengers, aircraft and the prevention

Dr **Ingudam Yaipharemba Singh** is Assistant Professor at the Department of National Security Studies, Manipur University.

of destruction from hijacking is a considerable apprehension for the authorities to deal with. The study intends to highlight the security paradigm of India's aviation sector in the 21st century acknowledging its increasing importance and dependency.

Aviation security systems are multilayered systems that employ a variety of approaches and combat various aviation threats. A robust, multilayered approach is a necessary component of a properly designed attack-resistant design.[1] Aviation security is, by definition, a collection of materials and human resources, a countermeasure designed to combat unlawful interference with aviation. Its goal is to keep passengers, flight attendants, airport staff, airline staff and the public safe from criminals. Aviation security is primarily regulated by international and national regulations and industry bodies, including the International Civil Aviation Organization (ICAO), the International Air Transport Association (IATA), and the Civil Aviation Security Regulations. Annex XVII of the ICAO Chicago Convention serves as the basis for all aviation security rules and regulations.

Aircraft are the economic lifeline of global commerce. Today's society relies heavily on aviation to execute transactions. Aviation security experts understood that a combination of activities could have overall effectiveness against an attack, preventing catastrophic events. As a result, all levels of protection are expected to reach their full potential, resulting in the highest level of deterrence available when used in conjunction with other layers of protection. As a result, the primary goal of aviation security is for security personnel at every level to strive for maximum efficiency within the scope of their responsibilities. To approve a plan, it is important to understand everyone who is attacking. If the target is sufficiently valuable, the readiness is developing new strategies to achieve the target, especially by designing systems with interim complementary capabilities to detect and defend against system failures or terrorist threats. Various screening steps are in place to identify weapons and other dangerous goods carried by individuals, for example, hijacking aircraft or damaging airport infrastructure. A security

1. Bartholomew Elais, *Airport and Aviation Security: U.S. Policy and Strategy in the Age of Global Terrorism* (Boca Raton, FL: CRC Press, 2009).

system is a complex system, but it is fundamentally a human system. Humans design systems to defend against threats that other humans have. As a result, the performance of individuals in various roles, including security screeners and aviation marshal intelligence analytics, pilots and flight attendants, is critical. The multiple layers of embedded systems that make up the entire aviation security system aim to deter attacks against complementary aerial targets.[2] In addition to the human side, individuals who perform and manage security operations contribute significantly to system vulnerabilities. Understanding human variables such as performance, errors, and organisational issues that affect system performance is essential for building a robust security system.

The aviation industry and governments are taking steps to ensure passenger safety, and commerce is currently providing information to other corporate sectors of the economy. As a result, the primary task of aviation professionals is to achieve security while protecting the vitality of the industry and the rights of people.[3] The basics and practical strategies of airport security are easy to understand. Despite the latest knowledge and security procedures, airports are vulnerable to terrorist attacks, and perpetrators are constantly looking for new ways to bypass security measures.

### *Aviation Security in India*

In India, after the Kandahar hijacking, aviation security is taken as a priority to speed up technological advancement and equipment. As a result, a more stringent but passenger-friendly security check-up was adopted without compromising the ease of the passengers. Thus, India also introduced an anti-hijacking policy to fight any episode of aircraft hijacking.

The Bureau of Civil Aviation Security (BCAS) is the single entity in charge of policy concerns in aviation security. The Central Industrial Security Force is responsible for airport security (CISF).[4] The Government of India has also provided $7.62 million to the Civil

2. Ibid., p. 19.
3. Jeffery Price, *Practical Aviation Security: Predicting and Preventing Future Threats* (USA: Butterworth-Heinemann, 2012).
4. Manju V., "Airport operators give security a pass, allow entry in crucial areas", June 9, 2010, at http://timesofindia.indiatimes.com/. Accessed on May 15, 2021.

Aviation Safety Authority to meet the expenditures of the Coalition Budget for the fiscal year 2019.

India has stringent measures to ensure that international aviation laws governing cargo and passenger security are obeyed in letter and spirit. Baggage and persons are thoroughly checked to detect and identify dangers. The primary threat in the aviation industry is improvised explosive devices, hijacking, and sabotage; but, given the rising complexity of the aviation industry, cybersecurity, car bombs, errant drones, and soft perimeters must also be considered. Surveillance equipment, perimeter security equipment, X-ray screening systems for cargo, explosive trace detector systems for explosives in cargo and baggage, and CISF canine explosive detection teams and human intelligence are currently used in aviation security in India. Security personnel also include equipment, such as explosion-proof cargo containers, stricter boundary intrusion detection and evaluation systems, computed tomography scanners, and neutron-based technology scanners, the same new sophistication as liquid explosives detectors and IED jammers. Consider an X-ray scanner that has been used.[5] Also, in India, the human intelligence element of aviation security is crucial to solving all problems. CISF staff at airports across the country have realised that several initiatives have provided complete evidence of efficiency against all threats and prevent unwanted events. Therefore, all levels of protection are highly valued for achieving maximum efficiency and maximum deterrence in harmony with other protective measures.

The hijacking of aircraft has happened 12 times in India to date. On December 24, 1999, the last hijack occurred when an Indian Airlines flight IC-814 was seized back to Delhi from Kathmandu via Amritsar and Lahore.[6] It took the Indian government five years after the incident to establish an anti-hijacking policy. The policy, adopted by the Cabinet Committee on Security (CCS), says that foreign-registered aircraft hijacked in Indian airspace are not allowed to land. Instead, the aircraft must escape safely and quickly from Indian territory. Air

5. National Academy of Sciences, National Institute for Advanced Studies, *India-United States Cooperation on Science and Technology for Countering Terrorism* (New Delhi, India: National Academies Press, 2014).
6. Maya Sharma, *The hijacking of Indian Airlines flight IC-814*, August 30, 2009, at http://www.ndtv.com/. Accessed on May 15, 2021.

Force jets accompanying the aircraft ensure that the airspace of the hijacked plane is cleared between 25 nautical miles. However, this strategy complied with international obligations by allowing planes to land when fuel was running out. If a registered aircraft is hijacked in India, the protocol is to land at an Indian airport. CCS's ruling clearly shows the need to take all measures to prevent hijacked jets from taking off again after landing at Indian airports. Airport staff try to secure the aircraft and not take off under such circumstances. Upon receipt of a hijacking alert, the Air Traffic Control (ATC) Watch Surveillance Supervisor (WSO) should contact the Joint Control and Analysis Centre (JCAC), where Indian Air Force (IAF) officers are stationed. JCAC will investigate the issue with support from ATC, and the IAF will be notified immediately.[7] Efficient decision-making requires adherence to the chain of command at any cost. The WSO summons the Central Committee and is led by the Director of Civil Aviation (DGCA) after the aircraft has been designated 'Rogue'. This triggers various processes to act as the Committee of Secretaries on Air Hijacking (COSAH) Crisis Management Group and the CCS as the final decision-making body. COSAH and CCS, in cooperation with the appropriate ministries, are expected to implement directives to the decision-making bodies of the Central Committee.[8]

It must first determine if the hijacked aircraft will hit a strategic target, according to rules set for direct action against an aircraft. For this evaluation, a three-stage categorisation procedure has been developed: First, a *Doubtful Aircraft* occurs when an aircraft deviates from its assigned path, fails to comply with ATC orders, and its transponder fails to react. Second, a *Rogue Aircraft* disregards Air Traffic Control and continues to deviate. It turns off its transponder and does not respond to radio communication. Third, *Threat Aircraft* arises when a rogue aircraft ignores ATC warnings or fighter aircraft and whose flight route intersects with critical objectives, such as high-profile governmental buildings, installations, and so on.[9] When a plane is designated as a "Threat Aircraft", the decision is to fire active countermeasures. The CCS is in charge of carrying out such a decision.

7. See "Report of the committee on a road map for the civil aviation sector", Government of India: Ministry of Civil Aviation, October 2004.
8. Ibid.
9. Samantha, Pranab Dhal.

However, there are instances when a jet may turn a danger during landing or taking off, leaving the Indian Air Force with extremely little reaction time; in such cases, the Indian Air Force chooses.[10] Air Headquarters chooses to label a 'Rogue' aircraft a threat. However, the doctrine states that the pilot of the trailing fighter aircraft will not make independent judgments. While executing an interception operation, fighters must maintain a distance of more than 500 feet from the hijacked aeroplane.[11]

Large aircraft are an essential asset of civil aviation. Today's threats are increasing and are spreading to all airports operated by large airliners. Recently, threats have increased in the development of missile technology. Complete for non-technical crews, explaining threat technologies, detection systems and methods to address the potential for future developments, such as today's SAM (Surface-to-Air Missile) technology and armed drones. It is imperative to provide good guides and referrals for technicians. Countermeasures will be revealed not only tactically but also scientifically. Evaluations should be made due to the increased risk of MANPAD (Man-Portable Air Defence System), UAV (Armed Drones or Unmanned Aerial Vehicle), infrared technology, and the necessary response procedures to be implemented on private platforms as well. In particular, it is essential to explain the issues of flight platform robustness and viability during take-off and access landings. The goal is to support the operation of large aircraft that can meet the new requirements of formal civilian operations of traditional and non-traditional threats.

***Strengthening Airport Security***

Aviation exists as a choice target to cause substantial loss of life, disrupt connectivity between countries, regions, cities, etc., and cause economic damage and successful countermeasures. However, there remain vulnerabilities and loopholes that terror groups continue to exploit; among the key concerns, they can sneak improvised explosive devices into airports and onto aircraft. Cybersecurity is also a significant concern as airport systems and infrastructure. Aviation

10. Gautam Sen, *Conceptualizing Security for India in the 21st Century* (New Delhi: Atlantic Publishers, 2007).
11. Ibid., p. 71.

infrastructures are increasingly reliant on computers and information technology that increase their exposure to cyber threats. The concerns over terror threats don't just extend to safety and security; they also can hit the economy. For example, some 50 per cent of international tourism occurs through the aviation industry, and it accounts for 35 per cent of the value of international trade. Countermeasures are in place to address threats, but much focus has been on the air side in recent years. ICAO and its partners are looking to address the dangers on the land side more intensely, so airport security is the focal point. There are measures underway to bring in law enforcement agencies, security forces and the airport authority, and airport vendors to implement countermeasures. Other areas include better information sharing, better coordination among countries and their aviation authorities, and better passenger data collection to prevent or limit the movement of suspected individuals.

Active countermeasures are being developed in the aviation sector to analyse current threat scenarios, covering various aspects to strengthen airport security infrastructure from threats. Regulations target airport perimeter fences and access control points. This is an example of a physical security countermeasure used to restrict and control access to security-critical areas. Monitoring systems focus on terminal areas surrounding aircraft, the airport, and other critical areas and monitor activity throughout the airport premises. Identity and access control systems are used to verify the entitlement information of individuals authorised to access the airport's property and facility areas and sensitive locations. Finally, services such as background checks that evaluate individuals needing access to restricted areas of airports and aircraft against terrorist watchlists and criminal databases of individuals requiring access to airports and aircraft restricted areas, etc.[12]

Other features to which Passenger Name Record (PNR) data contribute significantly include expediting customs and immigration processing at airports, facilitating passenger flow, and preserving passengers' legal rights.[13] PNR data is an essential

12. Bartholomew Elais, n. 1.
13. Ruwantissa Abeyratne, *Aviation Security Law* (USA: Springer Science & Business Media, 2010).

instrument in assuring aviation security, which is why it is required to be submitted in advance. In addition, the data is essential for the threat assessment values derived from the analysis of PNR data in the fight against terrorism and the possibility of unlawful interference.[14] The data primarily helps security officers identify potentially high-risk passengers through PNR data analysis, improve aviation security, and prevent international crime, including militants and other border-like crimes and organised crime.[15] Aviation experts also support the use of more biometrics in security systems. Biometrics is a method for identifying people who have evaluated some unique biological properties. All unique identifiers are fingerprints, hand measurements, earlobe measurements, retina and iris patterns, voice waves, DNA and hand signatures.[16] These identities may give the essential information, and biometrics' technical application to improve aviation security is accurate and straightforward.

The biometrics/biostatistics approach also applies to aeroplane pilots who have comparable identical equipment. The pilot must validate the biometric identification procedure to ensure the validity of personal identity and to eliminate duplication. Similarly, passengers might perform the technique during screening before approaching the gate and boarding the aircraft. The authentication process permits accurate passengers in real-time and allows airline personnel to figure out who has checked in but not boarded the plane. A related feature of this system allowed airline personnel to match passengers with their respective luggage. Possibly, the bags for an un-boarded passenger can be identified and removed before flight. Finally, it can extend the use of biometrics or biostatistics to facial recognition. Facial biometrics can scan individuals in a crowd as they pass through a security checkpoint. The system can compare a scanned face instantaneously with an already stored database of suspected criminals within a matter of seconds.[17]

14. Ibid.
15. Ibid.
16. Margaret Rose (n. d.), *Biometric verification*, at http://searchsecurity.techtarget.com/. Accessed on May 18, 2021.
17. Sarosh R. Khan, Cletus C. Coughlin and Jeffrey P. Cohen (eds.), *Aviation Security and Terrorism: A Review of the Economic Issues* (St. Louis: Federal Reserve Bank Press, 2002), pp. 6-7.

The use of sophisticated technology is not merely a technology issue but also a matter of cost. In assessing the costs and benefits of using new technology, various non-technical questions can influence whether one should employ a particular technology. First, health issues arise because using a technology implanted in a machine, particularly one that releases radiation, might harm some individuals. Even the perception that the technology may be hazardous could create undesirable financial effects for the industry. Second, the use of technology needs concerns about official and privacy issues. For example, the technology can violate an individual's guarantee against complex searches. Although the security search is legal, it might deter potential travellers from uncomfortable feelings about personal information. Also, many are concerned about physical scans that produce images. Finally, the function of equipment increases space problems of their volume and the lines of passengers. In some instances, the technology can support airline personnel in meeting their timetables and increase passenger handiness. So far, it shows that the greater the threat, the greater the patience and inconvenience travellers have to endure.[18]

Another proactive approach is arming the pilot of the aircraft. However, various issues need to be solved before such transformation could take place. Like qualifications and training, the pilots need to carry weapons, control and supervise pilots' carriage of firearms, types of small armed weapons have to be selected, and how the gun needs to be kept, concealed, and transported, modifications to the aircraft required, and the cost to arm the pilots. Each issue has to be dissected and studied for the full potential of the arming procedures. Also, a range of questions emerges, whether pilots' involvement would be entirely voluntary or should store the firearm between flights. Nevertheless, these attempts generally maximise the effectiveness of any programme to arm the pilot while minimising its risk to safety and security.[19]

The Communications, Navigation and Surveillance (CNS) system provides data to air traffic controllers to ensure aircraft removal and

18. Ibid., pp. 7-8.
19. Jennifer Zella, *Aviation Security: Current Issues and Developments* (New York: Nova Science Publishers Inc., 2003).

actual airspace operation, supporting the crew for safe operation. Air Traffic Management (ATM), especially radar systems that enable Air Traffic Control (ATC), must be fully operational, especially when providing ATC services in low altitude, remote or maritime areas. When service cannot be provided from sea and remote locations, in bad weather, limited-service limits the supply of replacement parts to keep the system running, and there are no restrictions on surveillance systems, such as old equipment. Make sure that. Aircraft surveillance systems, especially air traffic management, are essential in the aviation industry.

**CONCLUSION**

Today's aviation security is a reaction mechanism to developing threats and detected assaults. The necessity of keeping hazardous people and substances from boarding an aeroplane cannot be overstated. A similar approach may result in dangerous dissemination to the most vulnerable elements of the air transportation system. Since the beginning of the 21st century, aviation has been changing drastically. New technologies and fresh means are transforming the industry, which requires adjusting the latest security system. The concept of layered security is a defining characteristic of aviation security. Using interwoven and multiple layers build in redundancy. If one layer fails, another one comes into play. The layered security model explains how various layers complement and reinforce each other, preventing any disastrous failure if a threat can cross any one of the layers. Today's aviation security system needs enhancement with further layers capable of addressing emerging concerns and facilitating a holistic end-to-end security concept. Real-time airport security systems continuously provide the security levels required by airport infrastructures while making the passenger experience comfortable and fluid in transit from public to boarding gates. The systems integrate the security procedures at the airport, ensuring fluid passenger experiences at the checkpoints. A blend of operational, technical, and management measures will form a flexible set of layers to prevent and respond to new attack methods. Intelligent and adaptive measures are required to meet the challenges of changing threats and emerging vulnerabilities while strengthening the flexibility of the

air transportation system. The critical element in aviation security is protecting and safeguarding human life, either in the air or on the ground. Besides, traditional aviation security revolves around the preventive airport and aircraft security measures in the physical domain. As a response to the new challenges to the current system, aviation security needs to expand into the cyber realm. The growing use of information technology throughout the aviation industry will make the cyber domain a priority for aviation security.

The aviation security systems are complex and require constant attention and focus on staying one step ahead of the next attack. All aviation staff must be prepared to respond to new threats and prevent future disasters. Aviation security systems are covered, from critical historical events to regulators and policymakers, to the significant terrorist or criminal activities that have impacted the systems today, to the cutting-edge technologies that define the future. This investigation is linked to airport security procedures and threat situations, data that can be used to create effective security programmes and accountability for protecting facilities of all sizes that meet international standards. Threats, threat detection and response systems and global security concerns are all possible scenarios. Security coverage should establish a safety foundation for protecting the future of world travel and trade with a focus on security rules and guidelines. Aviation expertise is applied to predict and prevent attacks.