

Safeguarding National Interests

Evaluating the Risks of Defence–Civilian Airport Proximity

Harsh Diwakar** and *Kritika Jain**

This article examines the risks posed by the proximity of military facilities to civilian airports, particularly in the context of the Indian Air Force (IAF) as well as Indian Naval Air Station sites adjacent to commercial hubs. It highlights concerns regarding unauthorised access to sensitive information, infrastructure and potential terrorist threats. The article advocates for relocating civil installations away from military airports to bolster national security. Given the rapid expansion of both civilian and military aviation, the current joint-use model will become increasingly strained, leading to operational inefficiencies and heightened security risks. Implementing advanced monitoring, enhanced cybersecurity protocols, and stronger coordination between civilian and military authorities is essential in the short-term. However, relying solely on security enhancements within existing limitations offers only a partial solution, as the continued growth of air traffic will exacerbate congestion and security concerns.

A phased transition towards dedicated civilian and military airport infrastructure remains the most viable long-term approach to safeguarding national security while ensuring sustainable aviation growth. This article underscores the importance of balancing immediate security needs with

* Mr Harsh Diwakar is pursuing BA.LLB (Hons), 3rd year at India International University for Legal Education and Research, Goa, India.

** Ms Kritika Jain is pursuing BA.LLB (Hons), 3rd year at India International University for Legal Education and Research, Goa, India.

long-term infrastructure planning to address the evolving challenges of the aviation sector. There is a need for stringent security measures, including enhanced monitoring and cybersecurity protocols, and cooperation between civilian and military authorities. This article also addresses technological vulnerabilities such as electronic eavesdropping and GPS spoofing, thereby urging the development of strategies to mitigate these risks.

Keywords: *Military–Civilian interface, National security, Airport proximity risks, Cybersecurity protocols, Technological vulnerabilities*

INTRODUCTION

The presence of Indian Air Force (IAF) facilities beside commercial airports has surfaced as a serious problem, sparking discussion and concerns about national security. This topic has gained relevance due to the high exposure of Air Force activities to both local and international tourists, heightening concerns about potential security breaches. The closeness of defence planes, neatly aligned beside bustling commercial runways, creates a perilous situation filled with security risks.¹ This juxtaposition unintentionally exposes sensitive military activities, crucial infrastructure and secret material to the prying eyes of unauthorised persons, jeopardizing the integrity of the national security processes.

At the heart of this issue is a delicate balance between operational challenges and security imperatives. While the cohabitation of IAF facilities and commercial airports may expedite logistical operations, to a certain extent, it concurrently accentuates the risks associated with espionage, sabotage and terrorist activities. Incursions generate security issues because unauthorised persons or vehicles approaching active runways may jeopardise the protection of military facilities or critical equipment.

The presence of civilian personnel, passengers and commercial operations near military installations significantly increases the risk of unauthorised access, espionage and intelligence leaks. Commercial employees, either unintentionally or deliberately, may expose sensitive military information, compromising national defence strategies. The attack on the Pathankot Air Force Station in 2016 serves as a stark reminder of the vulnerability of military installations to infiltration, demonstrating how unchecked access can lead to catastrophic security breaches. The integration of military and civilian infrastructure without stringent access controls creates an environment ripe for potential terrorist activities, sabotage and surveillance by adversaries. Therefore, securing the aircraft maneuvering area and limiting access to

only authorised personnel are imperative to safeguarding national security and preventing threats to both civilian and military operations. The seamless integration of defence assets with civilian aviation infrastructure unwittingly creates a veritable goldmine for potential threats, endangering not only the security of military installations but also the safety of civilian populations.²

Against this backdrop, it becomes imperative to delve deeper into the multifaceted implications of such arrangements and chart out a path towards mitigating security risks while upholding national interests. This article endeavours to understand circumstances which led to joint user Aerodrum policy, the complexities surrounding the proximity of IAF bases to commercial airports, meticulously examining the underlying security threats and operational challenges, highlighting the need for relocation of commercial airports from military airports. Furthermore, it advocates for a paradigm shift in defence infrastructure planning, advocating for the relocation of commercial airports away from Military airforce bases as a proactive measure to safeguard national security and fortify the nation's defence apparatus.

Separating military and civilian airports is essential for national security, as joint-use facilities pose intelligence and operational risks. While immediate relocation is impractical, a phased transition ensures a smooth shift without disrupting aviation operations. Several Indian cities have successfully implemented this model, such as Goa's shift from Dabolim (*INS Hansa*) to Manohar International Airport, Hyderabad's transition from Begumpet to Rajiv Gandhi International Airport, and Bangalore's move from HAL Airport to Kempegowda International Airport. Globally, cities like Washington, D.C. and Beijing have also adopted this approach.

Military airports face security threats, including espionage, cyberattacks and unauthorised access, due to their visibility and civilian proximity. A structured plan over a period of 5–20 years can mitigate these risks by introducing restricted zones, dedicated airspace and legal reforms. In the short term, stricter security at joint-use airports is necessary. Mid-term measures should include reassignment of dual-use airports, legal restrictions on civilian expansion and enhanced cybersecurity. Long-term plans should mandate separate infrastructure and legislation for dedicated military and civilian airports. Though economic concerns exist, separation improves defence readiness and commercial aviation growth. India must recognise phased military–civilian airport separation as a necessary security measure and invest in its structured implementation.

In elucidating these concerns and proposing alternative strategies, this article seeks to stimulate discourse, foster informed decision-making, and

catalyse concerted action towards fortifying India's defence infrastructure and preserving its sovereignty in an increasingly volatile geopolitical landscape. One of the most important key aspect is the security risk that it poses. While joint-use airports provide logistical and operational benefits, they also pose unique security issues such as operational concerns, technical threats, public security hazards, civilian–military integration and coordination challenges, infrastructural constraints and so on.

WHAT LED TO CIVIL–MILITARY AIRPORT PROXIMITY?

In India, defence airfields were established prior to civilian airports, initially for military purposes during World Wars I and II under British rule. Notable examples include Ambala Air Force Station (established in 1919) and Chakeri Air Force Station in Kanpur. The first civilian airport, Juhu Aerodrome in Mumbai, commenced operations in 1928.

Post-independence, the scarcity of dedicated civilian airports led to the dual-use of military airfields for both 'defence' and commercial aviation. During the 1950s and 1960s, numerous military airbases began accommodating civilian flights. This practice was formalised through the 1997 Joint User Aerodrome Policy, which outlined the terms for shared use of defence airbases. Currently, airports such as Goa's Dabolim, Pune's Lohegaon and Srinagar function as joint civil–military facilities, wherein the Airports Authority of India (AAI) manages civil operations, and defence authorities retain control over military operations. The 1997 Joint User Aerodrome Policy, while facilitating the shared use of military airbases for civilian flights, presents significant security risks to military bases. The policy's shortcomings include increased exposure of sensitive military infrastructure to unauthorised access, espionage and potential terrorist threats. Civilian presence at these airbases raises the risk of security breaches, as contractors, employees or passengers may inadvertently or deliberately leak classified information. Additionally, the dual use of airspace complicates military operations, restricting operational flexibility and potentially delaying critical defence missions. The policy also fails to address cybersecurity risks, such as hacking or GPS spoofing, which could compromise military readiness. The coexistence of military and civilian aviation at shared airports, though initially a logistical necessity, has now become a strategic liability, necessitating urgent policy revisions and potential relocation of commercial operations to mitigate security vulnerabilities.

Risks of Joint Military–Civilian Airports in Today’s Context

While the Joint User Aerodrome Policy has been useful in the past, modern challenges pose significant risks that must be taken into consideration:³

Security Risks: The biggest concern with joint military–civilian airports is that civilian access to military airbases increases the risk of sensitive defence infrastructure being exposed. Civilians, commercial employees and contractors may unintentionally or maliciously leak information regarding military operations, aircraft or defence equipment.

Operational Disruption: Military operations often require high levels of secrecy and flexibility, which can be compromised by civilian air traffic. The need to accommodate commercial flights may interfere with urgent defence missions or readiness.

Air Traffic Control Issues: Managing both civilian and military flights at a joint airport can create air traffic control complexities, leading to potential miscommunication or operational delays. Military aircraft typically operate under different protocols compared to civilian flights, adding to the risk of accidents or mismanagement.

Infrastructure Overlap: Many military bases are not designed for the heavy volume of commercial traffic seen in today’s aviation industry. This can lead to wear and tear on runways, hangars and other critical infrastructure. The overlap of civil and military operations may lead to congestion and inefficiency. The infrastructural constraints is often seen in terms of joint usage since both use the same airport infrastructure.

Cybersecurity Risks: With the increasing digitalisation of both military and civil aviation operations, there are heightened concerns over cybersecurity. A breach in the civilian segment of a joint airport could allow hackers to access sensitive military data or infrastructure.

For instance, in 2016, a major security breach at the Pathankot Air Force Station (though not due to commercial flights) demonstrated how vulnerable defence installations could be to infiltration. Terrorists gained access to the base, leading to a deadly attack. This incident heightened concerns about the proximity of civilians to sensitive military areas.

Security Concerns Case Study

Analysing various case studies related to security concerns involving joint airport usage is essential for gaining insights into the strategies, techniques, and methods employed by terrorist organisations or other hostile actors targeting such airports. These case studies illuminate potential scenarios and vulnerabilities that may have previously gone unexamined.

Fort Drum, USA (2019): In August 2019, two Chinese nationals were apprehended and charged with taking photographs and videos of a US Navy station near Fort Drum in upstate New York. These individuals were observed attempting to capture images of infrastructure and critical military equipment while trespassing near the base's perimeter.⁴ This incident raised significant concerns about espionage and unauthorised access to military installations.

Joint Base Andrews, USA (November 2016): In November 2016, a man breached the security checkpoint at Joint Base Andrews, a major US military base located in Maryland.⁵ After crashing his vehicle into a security barrier, the intruder was apprehended by security personnel. Although the incident was ultimately determined to be the result of a personal dispute rather than an act of terrorism, it underscored the vulnerabilities of military sites to unauthorised entry and potential security breaches.

By examining these past incidents and their implications, policymakers can develop strategies to address emerging threats and respond to evolving security concerns. Such analysis is crucial for enhancing preparedness, improving response capabilities, and building resilience against terrorist threats and other security challenges, including unanticipated operations, all of which are matters of national security.

SECURITY RISKS

The proximity of IAF bases to commercial airports presents significant national security risks by exposing critical defence assets to increased surveillance and reconnaissance by potential adversaries. This closeness allows foreign visitors and individuals with malicious intent to potentially gather intelligence on military operations, infrastructure and personnel, thereby creating a serious security threat. Moreover, the shared use of airspace by defence aircraft and commercial flights raises the risk of sabotage, espionage and terrorist activities.⁶ The risks of shared airspace outweigh its benefits, particularly in terms of national security, operational efficiency and safety. Additionally, civilian air traffic can disrupt urgent defence missions, compromise secrecy and create logistical bottlenecks for military readiness. These risks compromise national security and threaten strategic interests, making it imperative to address the vulnerabilities associated with such proximity.

A thorough analysis of the national security implications stemming from the proximity of military bases to commercial airports highlights the urgency

of implementing measures to safeguard defence assets, protect classified information, and enhance overall security preparedness. The following concerns underscore the security risks associated with the joint usage of airports:

Operational Security Concerns: Conducting operations and training exercises near commercial airports increases the risk of exposing sensitive tactics, techniques and procedures (TTPs) to adversaries, potentially compromising mission effectiveness and strategic advantage.⁷

Technological Vulnerabilities: Defence aircraft stationed near commercial runways are vulnerable to technological threats such as electronic eavesdropping, cyberattacks and GPS spoofing. Adversaries could exploit these vulnerabilities to gather intelligence, disrupt operations or hijack aircraft, posing a severe threat to national security,⁸ undermining national sovereignty.⁹

Civil–Military Integration Challenges: Differing operational requirements, airspace management issues and conflicting priorities between civil and military authorities can hinder effective collaboration and compromise national security preparedness and response capabilities.

Public Safety Risks: The presence of defence aircraft near commercial runways raises concerns about public safety and the potential for accidents or incidents involving military aircraft. Inadequate safety protocols, airspace congestion or other hazards pose a threat to civilian air traffic and infrastructure, necessitating measures to ensure the safety and security of all airspace users.¹⁰

These risks are exacerbated by the complexities of managing multiple entities within a shared environment, which may result in gaps in security standards, coordination challenges between civilian and defence personnel, and increased exposure to security breaches. The convergence of civilian and military operations within the same airspace could create security vulnerabilities that malicious actors may exploit for nefarious purposes. Additionally, the interconnected nature of various aviation stakeholders within shared-use frameworks may inadvertently facilitate the infiltration of terrorist networks or the transit of illegal goods.

Case Study: The mid-air collision between American Airlines Flight 5342 and a US Army UH-60 Black Hawk helicopter near Washington, D.C. on 29 January 2025, underscores the dangers of civilian–military airspace integration. The accident, caused partly by the lack of ADS-B signals on the military aircraft, highlights the risks of shared airspace, operational inefficiencies and security vulnerabilities, similar to concerns raised in

India's joint-use airports. The crash, which resulted in 67 deaths, reinforces the argument that military and civilian aviation must operate separately to avoid air traffic conflicts, espionage risks and operational delays. This article's emphasis on relocating civilian flights away from military-controlled airports aligns with the FAA and Pentagon's response to the crash, which called for stricter air traffic regulations and enhanced surveillance technology. This case should be integrated into the Security Concerns Case Study Section, the Risks of Joint Military–Civilian Airports Section, and the Recommendations & Conclusion to strengthen the argument for separate infrastructure and airspace for civilian and military aviation.

Impact on National Security

The integration of civilian and military operations within shared aviation infrastructure at joint-use airports compromise not only the safety of passengers, crew and critical equipment, but also the security of defence airports and military operations. The proximity of defence and civilian airports heightens the risk of terrorism in several ways:

Disruption of Military Operations: Terrorist attacks on defence facilities near civilian airports and vice versa can severely disrupt military operations, undermining strategic readiness and response capabilities. The destruction or loss of critical assets and infrastructure could weaken the nation's defence posture and impair its ability to respond to emerging threats.

Civilian Casualties and Infrastructure Damage: Attacks targeting civilian airports in close proximity to defence installations may result in significant civilian casualties and extensive infrastructure damage. Such incidents can lead to societal unrest and economic disruption, further destabilising the security environment and amplifying the impact of terrorism on national security.

The close proximity of defence and civilian airports poses significant challenges in safeguarding national interests against the threat of terrorism.¹¹ The diverse nature of terrorism, encompassing conventional attacks, cyberterrorism and biological warfare, underscores the complexity of the security landscape. Addressing these challenges requires comprehensive strategies that prioritise protection of critical installations, enhance security measures, and promote inter-agency cooperation to effectively mitigate the risks posed by terrorism.

By thoroughly assessing the implications of defence–civilian airport proximity on national security¹² and implementing necessary improvements to existing policies, laws and arrangements, policymakers can suggest proactive

measures to counter emerging threats and ensure the resilience of the nation's defence infrastructure.

Types of Terrorism

The convergence of civilian and military operations within the same airspace may result in security vulnerabilities that could be exploited by malevolent actors for nefarious purposes. Additionally, the interconnectedness of various aviation stakeholders within shared-use frameworks may inadvertently facilitate the infiltration of terrorist networks or the transit of illegal commodities.

Malicious actors may attempt to blend in with civilian populations or exploit employment opportunities within airport facilities to gain access to restricted areas or sensitive information. Such methods of infiltration could enable reconnaissance, sabotage, or direct attacks on defence assets, thereby compromising national security and defence capabilities. The psychological impact of terrorism on military personnel and their families further exacerbates concerns regarding the safety of deployed forces and the efficacy of defence efforts. Various forms of terrorist activities may arise under these circumstances, including:

Conventional Terrorism: Traditional acts of terrorism, such as bombings or armed assaults, could target defence installations or civilian airports to inflict casualties, cause destruction and instill fear.¹³ Terrorist groups may exploit the accessibility of civilian airports to launch coordinated attacks on defence assets, thereby compromising national security.

For example, on 2 January 2016, heavily armed terrorists, suspected to be from the Pakistan-based group Jaish-e-Mohammed, infiltrated the Pathankot Air Force Station in Punjab, India. The attackers engaged in a prolonged gun battle with security forces, leading to the deaths of seven Indian security personnel and six terrorists. The attackers exploited the base's proximity to civilian areas to gain access, highlighting vulnerabilities in the security of military–civilian infrastructure. The incident underscored the risks of unrestricted access near defence installations and reinforced the need for enhanced perimeter security, intelligence coordination and stricter civilian–military separation at high-risk locations.

Cyberterrorism: In an era dominated by technology, cyberterrorism presents a significant threat. Malicious actors may target critical infrastructure systems, including air traffic control and communication networks, to disrupt operations and compromise security. The interconnectedness of defence and civilian aviation infrastructure heightens the risk of cyberattacks, posing

substantial challenges to national security.¹⁴ Airport security faces additional threats from drones, cyberattacks, dirty bombs, suicide bombers, vehicle assaults and other vulnerabilities, as demonstrated by incidents such as the terrorist attack at Brussels Airport in Belgium. Failures in security measures, such as inadequate background checks and poor perimeter security, further contribute to risks such as hijackings. Moreover, the lack of Crime Prevention Through Environmental Design (CPTED) and vulnerabilities in automated systems due to hacking are critical concerns.

Insurgency and Guerrilla Warfare: Insurgent groups may exploit the proximity of defence facilities to civilian airports to conduct guerrilla-style attacks, thereby disrupting military operations and causing widespread chaos. Such attacks could undermine national security by eroding public confidence in the government's ability to protect vital installations.

For example, on 1 October 2001, terrorists belonging to the Jaish-e-Mohammed (JeM) group launched a fidayeen (suicide) attack near the Srinagar Airport, which also serves as an Indian Air Force (IAF) base. The militants infiltrated the airport perimeter and stormed the complex, targeting the entrance gate with grenades and gunfire, intending to breach the military section. The attack resulted in the deaths of four security personnel, three civilians and six terrorists, while also injuring several others. This attack highlights the vulnerability of joint-use airports, where military installations are exposed to insurgent attacks due to their shared infrastructure with civilian operations. The proximity of commercial traffic, civilian access and lack of strict perimeter security controls provided insurgents an opportunity to exploit these gaps. The attack underscored the urgent need for enhanced security measures, stricter access control, and potential relocation of military operations away from civilian airports to prevent similar guerrilla-style threats in the future.

Biological and Chemical Terrorism: The convergence of defence and civilian infrastructure increases the risk of biological or chemical attacks. Terrorist groups may seek to deploy hazardous substances to cause mass casualties and chaos. The accessibility of civilian airports could facilitate the transportation and dissemination of such agents, posing serious threats to national security and public safety.

The close proximity of civilian and defence operations necessitates strict coordination and collaboration among relevant entities to effectively safeguard national security interests. Failure to adequately address these issues could compromise the integrity and functionality of defence installations, thereby weakening their essential role in protecting the

nation's sovereignty and defence preparedness. A balanced approach that prioritises security while maximising the benefits of shared airport use is crucial to protecting national interests and mitigating the vulnerabilities associated with terrorist threats. These concerns can be better understood through a thorough analysis of various global incidents and their associated security implications.

Existing Security Arrangements

Access to existing provisions and security arrangements in India for joint use of airports is essential for a comprehensive understanding of the current frameworks governing airport security, legal and regulatory compliance, risk assessment, mitigation measures, technological capabilities and infrastructure readiness.

The Security of Information Act (SOIA) is particularly relevant when assessing the risks associated with the proximity of defence and civilian airports. Enacted to protect sensitive government information, SOIA ensures that crucial data related to national security, defence and intelligence are safeguarded against unauthorised access, disclosure, or espionage. In the context of defence–civilian airport proximity, SOIA's significance lies in its provisions for maintaining the confidentiality and integrity of defence-related information. The increasing integration of military facilities with civilian infrastructure, such as airports, heightens the need to secure sensitive defence information from potential risks, including espionage, sabotage, or unauthorised access by hostile entities seeking to exploit vulnerabilities in airport security. SOIA plays a pivotal role in preventing breaches that could compromise national interests.

Specifically, Section 4 of SOIA¹⁵ addresses the protection of information related to defence and international relations. This section covers a broad spectrum of data, including military plans, operations, capabilities and infrastructure. The discussion on the proximity of defence and civilian airports directly falls under this section, as it involves evaluating the risks posed by the closeness of civilian installations to military airports.

The current security protocols in India for shared airport usage demonstrate a commendable level of collaboration and vigilance, aimed at preserving the safety and integrity of aviation operations. However, there remains room for improvement and adaptation in response to evolving security dynamics and technological advancements. Continuous review, innovation and collaboration are necessary to strengthen India's airport security landscape and to maintain the highest levels of safety for travellers,

defence personnel and aviation staff. Further examination of current, real-world examples will assist in a deeper evaluation of potential reforms in this sector.

CASE STUDY: DABOLIM AIRPORT, GOA

Dabolim Airport in Goa exemplifies the complex challenges that arise from the concurrent operation of military and civilian aviation infrastructure. The airport's proximity to *INS Hansa*, a naval airbase operated by the Indian Navy, results in the frequent presence of military aircraft that is visible to both civilians and tourists. This coexistence presents multifaceted concerns, particularly regarding the security and integrity of military assets and the potential compromise of national security. The visibility of defence aircraft to the public raises concerns about the vulnerability of military installations to unauthorised access, as such visibility may inadvertently reveal sensitive information about military operations and infrastructure, thereby posing a significant risk to national security.

Furthermore, the close proximity of civilian and military operations necessitates the implementation of stringent measures to prevent inadvertent breaches and to ensure the safety of both military personnel and civilians. Managing the interface between civilian and military aviation at Dabolim Airport requires a careful balance between operational requirements, security imperatives and the facilitation of civilian air traffic. Effective coordination and communication between civilian and military authorities are crucial to addressing these challenges successfully. This includes the implementation of robust security protocols, the regular conduct of joint exercises, and the promotion of a collaborative approach to safeguarding both civilian and military interests.

In conclusion, the situation at Dabolim Airport highlights the inherent complexities of the coexistence of military and civilian aviation infrastructure. Addressing these challenges requires a comprehensive approach that prioritises security while accommodating the needs of civilian air travel.

Suggestions

To effectively address these security concerns, relocation of commercial airport bases away from military bases through a Gradual Phased Approach, needs to be considered. It would reduce the exposure of defence assets to unauthorised individuals, further strengthen defence capabilities and mitigate the risk of security breaches.¹⁶

A practical example of this approach can be seen in Goa, where the Manohar International Airport was established in 2022 as a separate facility dedicated solely for commercial flights. This development presents a valuable precedent for addressing similar concerns elsewhere. Following this model, it would be advisable to stop all commercial operations at Dabolim International Airport, which currently shares its airspace with military operations, and shift them entirely to the Mopa Airport. It would not only lead to more secure defence operations, but also allow for more streamlined military activities at Dabolim.

Several airports in India currently exemplify the coexistence of military and civilian aviation infrastructure,¹⁷ which underscores the urgency of this issue:

Indira Gandhi International Airport, Delhi (DEL): Indira Gandhi International Airport in Delhi is situated adjacent to the Indian Air Force's Palam Air Force Station.¹⁸ This proximity raises significant security concerns and potential vulnerabilities related to unauthorised access.

Chhatrapati Shivaji Maharaj International Airport, Mumbai (BOM): Mumbai's international airport, commonly known as Mumbai Airport, is located near the Indian Air Force's Santacruz Air Force Station. The close proximity of these facilities presents challenges in terms of security and coordination between military and civilian authorities.

Netaji Subhas Chandra Bose International Airport, Kolkata (CCU): Kolkata's international airport shares its premises with the Indian Air Force Station at Kolkata. The proximity of military and civilian aviation infrastructure at this location similarly raises concerns about security and the risk of unauthorised access.

Rajiv Gandhi International Airport, Hyderabad (HYD): Hyderabad's international airport is located near the Indian Air Force's Begumpet Airport. Although commercial operations are primarily concentrated at Rajiv Gandhi International Airport, the presence of a nearby military airfield adds complexity to the security arrangements.

These examples show the widespread issue of military and civilian aviation infrastructure coexisting in India, highlighting the need for comprehensive strategies to address security risks and protect national interests.

CASE STUDY: SECURITY CHALLENGES IN LAKSHADWEEP AIRSPACE

Lakshadweep, a cluster of islands in the Arabian Sea, presents unique security challenges due to its strategic location. Similar to Dabolim Airport in Goa,

Lakshadweep hosts a civilian airport in close proximity to defence installations, including an Indian Air Force (IAF) base.¹⁹ This juxtaposition creates several complexities and security concerns that necessitate careful examination of the risks involved and the implementation of effective mitigation strategies.

Geopolitical Significance

Located along critical sea lanes and near international maritime boundaries, Lakshadweep holds significant geopolitical importance. Its strategic position underscores the need for robust security measures to safeguard national interests and maritime sovereignty. The joint usage of airports in Lakshadweep presents several pressing security and operational challenges. Given its strategic location near critical sea lanes, the proximity of civilian aviation infrastructure to defence installations heightens the risk of espionage, unauthorised surveillance and potential terrorist threats.

Operational Challenges

The coexistence of civilian and military aviation infrastructure in Lakshadweep presents operational challenges for the Indian Air Force. Conducting training exercises and operational sorties in close proximity to civilian air traffic requires meticulous planning and coordination to avoid inadvertent breaches and ensure the safety of all involved. The coexistence of military and civilian aviation in this region complicates airspace management, making it difficult to ensure the safety and confidentiality of defence operations.

Foreign Influence and Diplomatic Implications

The visibility of defence activities in Lakshadweep to foreign visitors raises diplomatic concerns. The presence of foreign visitors and diplomatic personnel further increases concerns about intelligence leaks and diplomatic complications. Unauthorised access to defence installations by foreign nationals or diplomatic personnel could strain international relations, compromise bilateral agreements and challenge India's sovereignty in the region.

Mitigation Strategies

Addressing these security challenges requires a multifaceted approach. Relocating the Indian Air Force base away from the civilian airport would reduce exposure to unauthorised individuals and enhance security. This relocation should be complemented by enhanced surveillance, cybersecurity measures and strict access controls to effectively safeguard defence assets.

Closure

The case of Lakshadweep highlights the delicate balance between operational requirements, security imperatives and geopolitical considerations in managing civilian and military aviation infrastructure. By thoroughly assessing security risks and implementing proactive mitigation strategies, India can strengthen its defence posture in the region, protect national interests and preserve maritime sovereignty in this critical domain.²⁰

Examining the case studies of the Lakshadweep and Dabolim airports provides valuable insights for evaluating measures aimed at enhancing joint use of airports. These cases underscore the importance of addressing security concerns, geopolitical significance, operational challenges and technological vulnerabilities. By analysing the strategies employed and the lessons learned from these incidents, policymakers can better anticipate potential risks and suggest measures for appropriate mitigation.

Adopting a comprehensive approach that incorporates lessons from the Lakshadweep and Dabolim airports can significantly improve reforms at other airports, fostering safer, more resilient and integrated aviation ecosystems. As the concept of joint-use of airports gains traction, there is an urgent need to ensure not only the smooth integration of civilian and defence activities, but also the implementation of effective security measures to protect against potential threats. The successful implementation of shared airport usage hinges on a holistic approach that addresses a wide range of challenges, from ensuring civilian safety to enhancing defence capabilities and countering terrorist activities.

BALANCING MILITARY AND CIVILIAN AIR TRAFFIC: NAVY'S PUSHBACK ON INCREASED CIVILIAN SLOTS AT VISAKHAPATNAM AIRPORT

In 2022, at a time when stakeholders were advocating for more slots for civilian flights at Visakhapatnam Airport, which is operated by the Indian Navy, the Navy has pushed back on these demands. According to Vice Admiral Biswajit Dasgupta, Flag Officer Commanding-in-Chief of the Eastern Naval Command, the commercial airlines have not been fully utilising the slots already allotted to them at *INS Dega*.²¹

Vice Admiral Dasgupta emphasises that the Visakhapatnam Airport, primarily a military airbase, later allowed commercial operations. He pointed out that sufficient slots have already been allocated for civilian flights, and with the expected increase in military air traffic, it would be challenging to accommodate more commercial flights. The Admiral also highlighted that

the future military use of *INS Dega* will increase significantly, especially with the upcoming stationing of the *INS Vikrant*, India's aircraft carrier, in Visakhapatnam. Once *INS Vikrant* is based there, *INS Dega* will need to support the carrier's main fighter squadron, the MiG-29K, leading to even higher demands on the airbase's capacity.

In view of this, the Andhra Pradesh government is planning to build a new international airport near Bhogapuram in the Vizianagaram district, whose construction would be completed by 2026. This new airport is seen as a solution to accommodate civilian air traffic, as military operations at *INS Dega* are expected to grow substantially in the coming years.

The situation at Visakhapatnam Airport underscores the pressing need for the relocation of commercial flights from defence-operated airports due to infrastructural constraints and the increasing demands of military operations. With the Indian Navy prioritising defence needs, including the anticipated stationing of the *INS Vikrant* and its associated fighter squadron at *INS Dega*, the airbase's capacity for accommodating additional civilian flights is becoming severely limited. Despite the availability of allocated slots, underutilisation by commercial airlines highlights inefficiencies in the current dual-use model. The underutilisation of existing facilities by commercial airlines at joint-use airports stems largely from operational inefficiencies, security constraints and airspace limitations imposed by military priorities. For example, at Visakhapatnam Airport (*INS Dega*), despite the allocation of civilian slots, commercial airlines failed to fully utilise them, as confirmed by the Indian Navy. This inefficiency is exacerbated by the need to prioritise defence operations, especially with increasing military activity like the deployment of the *INS Vikrant* and its MiG-29K squadron. Such operational overlaps lead to congested infrastructure, delayed flights and restricted flexibility for commercial airlines.²² These inefficiencies, alongside heightened security risks, highlight the impracticality of shared use and justify the segregation of civil airports from military bases. The planned shift of commercial flights from Dabolim (*INS Hansa*) to the new Manohar International Airport in Goa exemplifies a successful model, ensuring optimised usage of both civil and military infrastructure while minimising interference and security threats. This demonstrates that dedicated facilities not only enhance efficiency but also protect national security, thus validating the need for structural separation of military and civilian aviation operations. As military operations expand, balancing defence and civilian aviation needs at shared facilities becomes increasingly unsustainable. The development of a dedicated civilian airport

at Bhogapuram offers a timely solution, providing the much-needed relief for civilian air traffic and ensuring that both defence and commercial sectors can operate without compromising operational efficiency. Given the growing complexity of military requirements, transitioning commercial aviation to independent airports is essential to avoid long-term operational bottlenecks and ensure optimal infrastructure usage.

Recommendations for Mitigation

As India continues to emerge as a dynamic economic and strategic hub, optimising the use of its aviation infrastructure becomes increasingly critical. To effectively address the multifaceted challenges associated with the shared usage of airports across India, particularly in the context of both civilian and defence operations, a comprehensive approach is necessary. This approach should encompass the following measures.

Relocation of commercial airports: The need to relocate commercial airports away from military airbases is increasingly urgent due to India's evolving economic capacity, growing civil aviation sector and heightened security concerns. While joint user aerodromes were once a practical solution, India's economic growth now makes it feasible to invest in dedicated civilian airports. Initiatives like the UDAN scheme have already led to the development of regional airports, reducing the need for military bases to accommodate civilian flights. Overcrowded joint-use airports, such as Goa's Dabolim, have faced operational bottlenecks, straining both military readiness and infrastructure.

Security concerns strongly emphasise the need to separate civilian and military operations. As geopolitical tensions rise and technological threats, such as drone espionage, become more sophisticated, safeguarding defence airbases is more crucial than ever. The presence of civilian activity near military installations increases the risk of unauthorised surveillance, intelligence leaks and potential security breaches.

Dedicated military bases with no civilian access would significantly enhance operational security, ensuring that sensitive defence activities remain protected from external threats. Restricting civilian presence would minimise the chances of espionage and prevent potential data leaks that could be exploited by terrorist organisations or hostile entities.

Historical incidents have demonstrated the risks posed by such proximity. While the 2008 Mumbai attacks were not directly related to airport security, they highlighted how vulnerabilities in critical infrastructure could be exploited for large-scale attacks. In volatile regions like Srinagar,

where security threats are even more pronounced, the presence of civilians near defence airports creates additional risks that must be addressed.

Given these factors, relocating commercial airports away from military airbases is not just a matter of convenience but a strategic necessity. A well-planned separation would strengthen national defence, enhance operational efficiency, and secure India's air transport infrastructure for the long term.

Strengthening the Practicality of Relocation: A Gradual Phased Approach, while relocation is ideal, would be more realistic. The government can expand on a 5–20 year structured transition plan, prioritising high-risk joint-use airports like Pune, Goa (Dabolim) and Srinagar. Addressing the financial burden of relocation, potential public–private partnerships (PPP) or government-backed infrastructure funding can be used as was done for the Manohar International Airport in Goa.

Implementation of Robust Security Protocols: It is imperative to implement stringent security protocols, including enhanced surveillance systems, advanced cybersecurity measures and strict access controls, to safeguard both civilian and defence infrastructures from security breaches and unauthorised access.

Enhanced Coordination and Communication: Strengthening coordination and communication between civilian and military authorities is crucial to addressing operational challenges effectively and ensuring seamless execution of defence missions. This includes regular joint exercises and the establishment of clear communication channels to facilitate collaboration.

Deployment of Advanced Technological Safeguards: The deployment of advanced technological safeguards is necessary to protect defence infrastructure from cyber threats and other technological vulnerabilities. This includes measures to prevent electronic eavesdropping, GPS spoofing and cyberattacks that could compromise national security. Strengthen references to the Security of Information Act (SOIA) by proposing amendments to criminalise unauthorised drone surveillance near military–civilian airports.

By adopting this comprehensive approach, India can effectively enhance the security and operational coordination of its aviation infrastructure, thereby mitigating the risks associated with terrorist activities and preserving national security interests.

CONCLUSION

The proximity of Indian Air Force (IAF) and Indian Navy (IN) installations to civilian airports presents significant security risks, including unauthorised

access to critical military operations, infrastructure and confidential information. This situation increases the likelihood of espionage, sabotage and terrorist threats. To mitigate these risks, it is essential to relocate IAF and IN facilities away from commercial airports, implement stringent security measures, and foster effective coordination between civilian and military authorities.

The integration of military and civilian airports also has political implications and may impact international relations. The integration of military and civilian airports can strain diplomatic relations by raising concerns about national security, sovereignty and intelligence vulnerabilities. Countries with shared military–civilian airports may face diplomatic tensions if foreign governments perceive such arrangements as security risks. For example, China’s expansion of dual-use airstrips in the South China Sea has provoked strong diplomatic opposition from neighbouring countries like the Philippines and Vietnam, as well as the United States, which view these facilities as potential military threats rather than purely civilian infrastructure. Similarly, India’s joint-use airport policy has drawn scrutiny from foreign entities concerned about military operations being conducted in proximity to civilian aviation. In cases where international airlines operate at such airports, foreign governments may demand transparency in military activities, creating conflicts over classified defence strategies. Moreover, the presence of foreign nationals in civilian airports adjacent to military installations increases the risk of espionage, as seen in incidents where unauthorised personnel attempted to photograph or infiltrate defence bases. The dual-use nature of these airports can also trigger disputes over airspace management, particularly when military exercises disrupt civilian air traffic, causing diplomatic friction with countries whose airlines are affected. As global aviation regulations emphasise strict separation between military and civilian operations, joint-use airports can lead to diplomatic rifts, forcing governments to justify their policies in international forums. Additionally, runway incursions at joint-use airports pose complex challenges for defence authorities, necessitating proactive measures to enhance safety, improve cooperation and ensure the security of all stakeholders.

Neglecting these security concerns could compromise the integrity and functionality of defence airports, thereby undermining their critical role in protecting national sovereignty and ensuring defence preparedness. While the Joint User Aerodrome Policy was appropriate during a period of economic constraint, India’s evolving economic strength and strategic priorities now necessitate a reconsideration of this approach. Establishing

separate military and civilian airports would reduce security risks, prevent operational disruption and allow the military to operate more efficiently without interference from civil aviation.²³ The development of more civilian airports and their relocation away from the current joint-use model with military airports would ease the burden on defence infrastructure. This transition would establish a well-balanced system that prioritises security while maximising the efficiency and benefits of civilian aviation.

Furthermore, the Security of Information Act (SOIA)²⁴ provides legal mechanisms for penalising individuals or entities responsible for compromising national security through unauthorised access to sensitive materials. This legal framework serves as a deterrent against espionage and other detrimental activities that could threaten the safety and security of defence–civilian infrastructure.

Adopting a comprehensive strategy that incorporates lessons learned from the Lakshadweep and Dabolim airports can significantly enhance security reforms at other airports, leading to safer, more resilient and integrated aviation systems. In summary, a proactive approach is necessary to maintain national security while ensuring efficient operation of civilian air traffic.

NOTES

1. Georgia Lykou, Argiro Anagnostopoulou and Dimitris Gritzalis, 'Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls', *National Library of Medicine*, Vol. 1, No. 19, 2018, pp. 1–2.
2. Bill Frain, 'The Evolution of Airport Security and the Threats that Drive it', *Security Magazine*, 16 September 2022, available at <https://www.securitymagazine.com/articles/98346-the-evolution-of-airport-security-and-the-threats-that-drive-it>, accessed on 19 March 2024.
3. 'Joint Civilian/Military(Joint-use) Airports', Federal Aviation Administration, Department of Transportation, United States of America, available at https://www.faa.gov/airports/planning_capacity/joint_use_airports, accessed on 24 September 2024.
4. 'Chinese Nationals Arrested for Trespassing at Navy Base in Key West', *CBS News*, 16 September 2019, available at <https://www.cbsnews.com/news/chinese-nationals-arrested-for-trespassing-at-navy-base-in-key-west/>, accessed on 10 March 2024.
5. Michael Levenson, 'Intruder Boards a Military Plane at Joint Base Andrews', *The New York Times*, 5 February 2021, available at <https://www.nytimes.com/2021/02/05/us/air-force-base-security-breach.html#:~:text=An%20unarmed%20man%20gained%20access%20to%20Joint%20Base%20Andrews%20in,Force%20bases%20worldwide%2C%20officials%20said>, accessed on 27 March 2024.

6. 'Risks Posed to Civil Aviation Operations Over or Near Conflict Zones', ICAO, available at <https://www.icao.int/safety/ConflictZones/Pages/default.aspx>, accessed on 19 March 2024.
7. Ibid.
8. Ibid.
9. Mihir Mishra, 'International Flights from India's Military-owned Airport May Stop After December', *The Economic Times*, 5 October 2021, available at https://m.economictimes.com/industry/transportation/airlines/-aviation/international-flights-from-indias-military-owned-airports-may-stop-after-december/amp_articleshow/86743208.cms, accessed on 18 March 2024.
10. 'Active Shooter Reported at Wright Patterson Air Force Base in Ohio', *The Florida Times Union*, 2 August 2018, available at <https://www.jacksonville.com/story/news/2018/08/02/active-shooter-reported-at-wright-patterson-air-force-base-in-ohio/11170784007/>, accessed on 26 March 2024.
11. Jane Garvey, 'What Was the Nation's Aviation Security Posture as of September 11, 2001?', National Commission on Terrorist Attacks Upon the United States, 22 May 2003, available at https://9-11commission.gov/hearings/hearing2/witness_garvey.htm, accessed on 25 March 2024.
12. Madhupriya Dhanwate, 'Pune Airport Expansion Proposal by Sudhir Mehta Advocates Relocation of IAF Base Lohegaon and Yerawada Central Jail', *Pune Times Mirror*, 6 January 2024, available at <https://punemirror.com/pune/others/pune-airport-expansion-proposal-by-sudhir-mehta-advocates-relocation-of-iaf-base-lohegaon-and-yerawada-central-jail/cid1704531188.htm>, accessed on 26 March 2024.
13. Paul Kirby, 'Brussels Bombers Found Guilty After Long Murder Trial', *BBC News*, 26 July 2023, available at <https://www.bbc.com/news/world-europe-66299186>, accessed on 27 March 2024.
14. Stanislaw Zajas, 'Countering Air Terrorism', *The Quarterly Journal*, Vol. 8, No. 4, 2009, pp. 1–10.
15. Security of Information Act, 2001, § 4.
16. Prachi Bari, 'Dedicated Civilian Airport in Pune Need of the Hour', *Hindustan Times*, 24 October 2021, available at <https://www.hindustantimes.com/cities/pune-news/your-space-dedicated-civilian-airport-in-pune-need-of-the-hour-101635072180208.html>, accessed on 26 March 2024.
17. Ajay Shukla, '7 More Military Airports to Increase Assistance to Civil Airlines', *Business Standard*, 4 June 2022, available at https://www.business-standard.com/article/current-affairs/7-more-military-airports-to-increase-assistance-to-civil-airlines-122060400046_1.html, accessed on 20 March 2024.
18. Airports Authority of India, March 2024, available at <https://www.aai.aero/en/airports/delhi/indira-gandhi-international-airport>, accessed on 22 March 2024.
19. 'India Plans New Airport for Both Military, Civilian Aircraft Operations in Lakshadweep's Minicoy', *The Economic Times*, 9 January 2024, available at <https://>

economictimes.indiatimes.com/industry/transportation/airlinesaviation/india-plans-new-airport-for-both-military-civilian-aircraft-operations-in-lakshadweeps-minicoy/articleshow/106663513.cms, accessed on 22 March 2024.

20. 'Active Shooter Reported at Wright Patterson Air Force Base in Ohio', n. 10.
21. Nalla Babu, 'No More Flight Slots at Vizag Airport: Navy', *The Times of India*, 20 December 2022, available at <https://timesofindia.indiatimes.com/city/visakhapatnam/no-more-flight-slots-at-vizag-airport-navy/articleshow/96363453.cms>, accessed on 24 September 2024.
22. Ibid.
23. Ibid.
24. Security of Information Act, 2001.