CYBER RESILIENCE IN PAKISTAN'S AVIATION INFRASTRUCTURE: THREAT MODELLING, RISK MITIGATION AND POLICY DEVELOPMENT

Samreen Shahbaz

Centre for Aerospace and Security Studies (CASS), Lahore

August 2025

ABSTARCT

The rapid evolution of cyberspace has led to a significant increase in cyber threats, with the aviation sector being one of the most vulnerable among other industries. Given the global interconnectedness of air transport, any cyber-related incident within the aviation domain could have catastrophic consequences, affecting national security with global repercussions. In the context of Pakistan, ensuring cyber resilience within the aviation infrastructure has become increasingly critical to proactively address and mitigate these threats. This study conducts a qualitative investigation by conducting interview and using existing literature to identify the key cyber vulnerabilities present in the aviation system. Additionally, the paper provides different case studies that draw lessons on cyber resilience and provide risk mitigation strategies. Finally, the study offers a series of recommendations for strengthening Pakistan's aviation infrastructure against cyber risks. By discussing these critical aspects, this research aims to contribute to the development of a robust and secure aviation sector in Pakistan, ensuring that the nation can effectively safeguard its airspace and maintain trust in its aviation services amidst an increasingly complex cyber threat landscape.

Keywords: *Cyber Resilience, Aviation Infrastructure, Cyber Threats, Pakistan, Risk Mitigation, Policy Development.*

TABLE OF CONTENTS

List of Tables

List of Figures

INTRODUCTION

The growing digitalisation of the aviation sector has made air travel one of the most technologically incumbent industries globally. While, this incorporation of digital systems has improved efficiency, connectivity and passenger services, it has also brought unprecedented vulnerabilities simultaneously. Such dangers are acute in aviation, and the infrastructure is vulnerable to growing cyber threats which requires the development of strong cyber resilience.

Nevertheless, it is important to differentiate cyber-security and cyber-resilience first. Cyber-security is concerned with constructing defences against attacks, whereas cyber-resilience is more inclusive of preparing organisations to counter the existence of breaches and recover normal operations in the shortest possible time.[1] Cyber-security lays the foundation of the perimeter, but cyber-resilience keeps it going and recovers the perimeter upon breach. The difference underlines the reason why cyber-resilience is a requirement to protect today's complex, advanced threats to aviation infrastructure.[2]

The aviation industry is pregnable because of its high integration internationally. The airlines, airports, air traffic control and the third-party vendors work in interconnected systems, which translates to a cyber-incident in one sector to rampage throughout the whole network.[3] These risks are complicated by ageing infrastructure, old systems and

[1] Snehal Antani, “Attack Yourself First: The Logic Behind Offensive Security,” TechRadar, August 12, 2025, https://www.techradar.com/pro/attack-yourself-first-the-logic-behind-offensive-security.

[2] Jake Olcott, “Cyber Resilience Vs. Cybersecurity: What’s the Difference and How to Build a Plan for Both,” *Bitsight* (blog), August 22, 2024, https://www.bitsight.com/blog/cyber-resilience-vs-cybersecurity.

[3] Nahla Davies, “Cybersecurity in Aviation: Rising Threats and Modernization Efforts,” *SecureWorld*, June 9 2025.

older software. Moreover, aviation relies heavily on critical technologies such as the Traffic Alert and Collision Avoidance System (TCAS) and Global Positioning System (GPS) navigation.[4] Thus, attacks such as GPS spoofing, jamming, or TCAS interference may cause flights to be misdirected, operations to be interrupted, and lives to be at risk, which is why the resistance against attacks should be a priority.[5]

New risks are also involved in the new technologies, even though they enhance the capabilities of aviation. The use of Artificial Intelligence (AI) has opened up prospects of automation and efficiency in the system, but, at the same time, expose aviation systems to the threats of algorithmic manipulation, data poisoning, and automated exploitation.[6] These vulnerabilities associated with AI[7] will become an even more significant threat unless resilience measures are in place.

Given that, cyber resilience is not only important but indispensable for long-term sustainability of aviation sector. Significant cyber-attacks, either an information theft, system compromise, or a massive surge in service failure, may trigger catastrophic consequences, encompassing safety lapses, critical economic consequences and reputational concerns, and government distrust.[8] The paper thus analyses the cyber

[4] David Jones, "Aviation Sector Faces Heightened Cyber Risks Due to Vulnerable Software, Aging Tech," *Cybersecurity Dive*, April 14, 2025, https://www.cybersecuritydive.com/news/aviation-cyber-risks-aging-tech/745273/.

[5] Jeff Wise, "Exploding Cargo. Hacked GPS Devices. Spoofed Coordinates. Inside New Security Threats in the Skies," *Vanity Fair*, April 24, 2025, https://www.vanityfair.com/news/story/inside-new-security-threats-in-the-skies.

[6] Dua Shahid, "Silent Threats: Cyber Vulnerabilities in Aviation Industry," Modern Diplomacy, July 26, 2025, https://moderndiplomacy.eu/2025/07/26/silent-threats-cyber-vulnerabilities-in-aviation-industry/.

[7] Dua Shahid, "Silent Threats: Cyber Vulnerabilities in Aviation Industry," Modern Diplomacy, July 26, 2025, https://moderndiplomacy.eu/2025/07/26/silent-threats-cyber-vulnerabilities-in-aviation-industry

[8] "Cybersecurity in Aviation: Building a Resilient Future," World Economic Forum, June 3, 2025, https://www.weforum.org/impact/cybersecurity-in-aviation/.

threats that the aviation infrastructure in Pakistan can experience. It also examines the risk management and formulation of policy that elaborates the framework of enhancing cyber resilience in the aviation sector in Pakistan.

This paper assumes a qualitative facet to determine and develop cyber resilience in the aviation industry in Pakistan. The approach taken to give a complete and well-balanced analysis is the fusion of interview, literature review, and case studies. An interview with one of the aviation instructors of SAPS Aviation College has been carried out to interrogate information of interest to this research. However, the limited number of interviews is due to security restrictions and time constraint. Moreover, a comprehensive review of the available literature, policy documents, and international standards to comprehend the situation of aviation cyber-security and resilience initiatives has been conducted. Case studies of various global best practices in aviation cyber resilience have also been analysed to extract lessons for Pakistan. This multi-method approach ensures a holistic understanding of the cyber resilience landscape in Pakistan's aviation sector and provides a solid foundation for the recommendations presented in this study.

In this study, there are seven sections. The introduction provides the background information and relevance of cyber resilience in aviation and explains the importance of considering it within the framework of the aviation industry in Pakistan. The second section introduces the summary of the cyber threats and resilience actions that are currently undertaken in the Pakistan's aviation industry. Section three is dedicated to the model of cyber threats and risk landscape, which deals with the study of the different cyber threats to which the aviation infrastructure is exposed. Part four explores the global best practices in aviation cyber resilience and provides insights from international

organisations that can serve as examples for Pakistan to boost its aviation industry. In section five, the paper discusses risk mitigation strategies, with a focus on how the Safety Management System (SMS) can be leveraged to mitigate cyber risks across technical, operational, regulatory, and forward-looking dimensions. Section six gives a set of recommendations to enhance aviation cyber resilience in Pakistan. Lastly, the research ends with a synthesis of major findings and the provision of a comprehensive perspective needed to improve cyber resilience in the Pakistan's aviation sector.

2. CYBER THREATS AND RESILIENCE EFFORTS IN PAKISTAN'S AVIATION SECTOR

The aviation industry in Pakistan has not been hit hard by major cyber-attacks, still there are a few cases that have occurred in the past few years which highlight the vulnerability of the industry. An incident took place in July of 2022,[9] when the Pakistan Air Force (PAF) fell victim to a spear-phishing malware attack. The attackers tried to install the malicious programmes and steal important files. This attack underscored the fact that aviation-related organisations especially with national security ties, are appealing targets for adversaries.

In another case, Pakistan International Airlines (PIA) experienced cyber attack when its official website crashed in April 2023 and showed a Cloudflare Error 1020.[10] This seemed to be the outcome of a distributed denial-of-service (DDoS) or other

[9] "Significant Cyber Incidents | CSIS," n.d., https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[10] Ashish Khaitan, "Pakistan Cyber Attack: Hackers Take Down PIA Website," *The Cyber Express*, April 4, 2023, https://thecyberexpress.com/pakistan-cyber-attack-international-airlines.

computer attack which was admitted by Indian hacker group Team UCC. Although the event attracted the attention of people, the airline did not issue official data concerning the magnitude of the incident, the consequences of its operations, and the process of recovery.[11] Consequently, the omission of disclosure provided loopholes in the realisation of cyber risks in the sector.

Now Pakistan has started enhancing its cyber defence at policy level. One of the significant action is the formation of the National Cyber Emergency Response Team (PKCERT) in March 2024. PKCERT becomes a federal coordinator of the response to cybersecurity incidents among public institutions. Its establishment has been viewed as a significant institutional change; it indicates that the country acknowledged the fact that the cyber threat is critical matter that has to be tackled systemically and proactively.

Simultaneously, the Pakistan Civil Aviation Authority (PCAA) has showcased the capability to align with the standards of international aviation security. The authority has been subjected to intensive international supervision, such as passing International Civil Aviation Organisation (ICAO) audits in December 2021 and a validation mission in June 2024.[12] Such tests certify PCAA determination to be compliant and resilient, making Pakistan standing closer to the world standards in terms of aviation safety and security.

In parallel, PCAA manages another safety programme known as the State Safety Programme (SSP) that also helps to integrate safety regulations and activities to provide an acceptable level of safety in aviation services and products. SSP was put in place in

[11] Ashish Khaitan, “Pakistan Cyber Attack: Hackers Take Down PIA Website,” *The Cyber Express*, April 4, 2023, https://thecyberexpress.com/pakistan-cyber-attack-international-airlines/.

[12] Interview, August 1, 2025.

2011 in line with ICAO Annex 19 and Doc 9859, focusing on the proactive management of safety.[13] Moreover, Pakistan has developed the National Civil Aviation Security Programme (NCASP) that gives a systematic framework to ascertain the safety of civil aviation operations. [14]

Briefly, these developments indicate that cyber incidents have not been widespread and extensive till now but growing threats signal limitations of existing infrastructure. However, the institutional response of Pakistan, including the establishment of PKCERT, the evidence of the PCAA's compliance with the ICAO standards, and the introduction of the SSP and NCASP, suggest increasing awareness and willingness to fight against emerging cyber threats. Nonetheless, creating an extensive cyber resilience against this risk requires a more targeted approach focusing on threat modelling, mitigation of risk, and the development of the policy with a reference to the aviation infrastructure in Pakistan.

3. CYBER THREAT MODELLING AND RISK LANDSCAPE IN AVIATION

The aviation infrastructure is exposed to a range of cyber threats globally. General terminology normally like hacking, data breaches or system failures are not the threats but are the effects of the underlying factors. These root causes are malware and ransomware, social engineering and phishing, insider threats, supply chain

[13] “State Safety Programme | Pakistan Civil Aviation Authority,” Civil Aviation Authority Pakistan, n.d., https://pcaa.gov.pk/functions/state-safety-programme.

[14] Civil Aviation Authority of Pakistan. "National Programmes." Accessed August 18, 2025. https://caapakistan.com.pk/security/sec-np.aspx.

vulnerabilities, GPS spoofing or jamming, and advanced persistent threats (APTs). All of these threats can destabilise the safety, continuation, and performance of aviation activities, and a combination of them forms an extremely challenging risk environment.

Every aspect such as airline IT infrastructure, flight management systems, airport operations and passenger services, is vulnerable to cyber-attacks, and attackers take advantage of vulnerabilities of insecure networks and human error. Cases in point comprise malware and ransomware attacks on airline IT frameworks, phishing attacks on aviation employees, insider threats by workers or contractors, GPS spoofing disrupting aircraft navigation, and unauthorised entrance to onboard systems by use of insecure Wi-Fi or maintenance interfaces.[15]

The risk can be better understood by the following explanation of threats bellow:

3.1. Malware and Ransomware

Malicious software designed to disrupt systems, ex-filtrate sensitive information, or take control of technologies. Ransomware, a specific subset, encrypts files or systems and demands payment to restore access. [16]

[15] Nahla Davies, “Cybersecurity in Aviation: Rising Threats and Modernization Efforts,” *SecureWorld*, June 9 2025.

[16] Ömer Aslan et al., “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions,” *Electronics* 12, no. 6 (March 11, 2023): 1333, https://doi.org/10.3390/electronics12061333.

3.2. Insider Threats

Risks posed by trusted individuals within the organisation, such as employees, contractors, or former staff, who misuse legitimate access to steal information, damage systems, or cause operational harm.

3.3. Phishing and Social Engineering

Deceptive tactics, often through emails, messages, or fake websites, trick individuals into revealing credentials or installing malware. These remain among the most common cybercrimes targeting aviation.

3.4. GPS Spoofing and Jamming

Spoofing involves broadcasting false GPS signals to mislead navigation systems, while jamming disrupts signals altogether. Both can have serious consequences for aircraft safety and flight operations. [17]

3.5. Unauthorised Access to Aircraft Systems

It involves exploitation of insecure access points, such as onboard Wi-Fi or maintenance interfaces, enabling attackers to infiltrate sensitive aircraft systems.

Current tendencies prove the intensification of these threats. In the aviation sector, ransomware attacks rapidly increased by 600 percent in 2023 alone,[18] with significant disruptions to the operations of various airlines operating in various regions. Also, there

[17] Aircraft Performance Group, “GPS Spoofing in Aviation: Threats, Detection, and Mitigation Strategies,” *APG Aviation Blog*, June 30, 2025.

[18] Anna Ribeiro, “New CSC 2.0 Report Outlines Roadmap to Strengthen Aviation Cyber Defenses Amid Growing Threat Landscape,” Industrial Cyber, April 11, 2025, https://industrialcyber.co/transport/new-csc-2-0-report-outlines-roadmap-to-strengthen-aviation-cyber-defenses-amid-growing-threat-landscape/.

has always been a high prevalence of phishing and social engineering attacks, frequently involving professional organisations like help desk operations such as Scattered Spider, a hacking group based in the UK and the US[19], is one such organisation that uses the vulnerability in the operation of help desks to install ransomware and break into the systems of airlines. [20]

Attacks on air traffic control and aircraft systems are also other areas of critical concern, which may compromise flight safety,[21] and DDoS attacks targeting airports or airline IT systems, leading to outages and stolen data[22]. The vulnerability of supply chains also exacerbates the risks because third-party traders use the vulnerability in the supply chain to intrude into the aviation networks.[23] Meanwhile, advanced persistent threats (APTs), often state-sponsored and stealthy, pose long-term risks by infiltrating systems over extended periods to gather intelligence or conduct sabotage.

These patterns indicate that aviation cyber threats are multi-layered, evolving, and deeply interconnected**.** They affect not only direct airline and airport operations but also extend across supply chains, critical communication systems, and even state security dimensions. In the case of Pakistan, incidents recorded in recent years align with these

---

[19] Alanna Nason, "Who Is Scattered Spider? | Coro Cybersecurity," *Coro Cybersecurity* (blog), May 1, 2024, https://www.coro.net/blog/who-is-scattered-spider.

[20] Lauren Edmonds, "A Notorious Hacker Group Is Now Targeting the Aviation Industry, the FBI Says," Business Insider, June 28, 2025, https://www.businessinsider.com/airlines-hacked-scattered-spider-cybersecurity-2025-6.

[21] Michael Levin, "The Top Five Cybersecurity Threats to the Aviation Industry," Center for Information Security Awareness, March 23, 2025, https://cfisa.com/top-five-cybersecurity-threats-to-the-aviation-industry/.

[22] Aircraft Performance Group, "GPS Spoofing in Aviation: Threats, Detection, and Mitigation Strategies," *APG Aviation Blog*, June 30, 2025.

[23] Sarah Lee, "Aviation Cybersecurity Threats," n.d., https://www.numberanalytics.com/blog/ultimate-guide-cyber-threats-aviation-infrastructure.

global patterns, suggesting that the country's aviation sector is exposed to the same underlying threat landscape that challenges the wider industry.

4. GLOBAL PRACTICES IN AVIATION CYBER RESILIENCE: LESSONS AND INSIGHTS

Cyber resilience in international aviation can used an example in strengthening aviation industry of Pakistan against evolving threats. Other aviation agencies and industry players have shown remarkable achievements regarding the inculcation of resilience in their respective structures, which Pakistan can emulate to fit in its own aviation industry. [24]

4.1. International Air Transport Association (IATA)

The International Air Transport Association (IATA), which was founded in 1945, is a trade association, which makes the representation of approximately 300 airlines, or more than 80 percent of world air traffic. [25] It has been at the forefront of constant cyber-security awareness and training in the airline industry. IATA has strived through campaigns like aviation cyber-security training and the creation of groups like the Cybersecurity and Resilience Management Working Group (CRMWG) to create a spirit of alertness, cooperation, and information exchange. This practice has helped to increase resilience not only in the process of airline operations but also in the entire supply chain of aviation. [26]

[24] Interview, August 1, 2025.
[25] International Air Transport Association. https://www.iata.org/en/about/.
[26] "Aviation Cybersecurity," n.d., https://www.iata.org/en/programs/security/cyber-security.

4.2. Federal Aviation Authority (FAA)

The Federal Aviation Administration (FAA) of the US Department of Transportation oversees all civil aviation in the US. The FAA has incorporated cyber resilience in the regulation and operational systems through resilience exercises, red teaming, and a prototype programme.[27] It is also worth noting that it performs tests regarding GPS/GNSS vulnerability and provides resilience-based funding via its Airport Improvement Programmes. The latest roadmap of the "Zero Trust" [28] is implemented into the wider National Airspace System security, ensuring not only operational preparedness, but also systemic defence. [29]

4.3. National Aeronautics and Space Administration (NASA)

The National Aeronautics and Space Administration (NASA) works with the FAA in the domain of advanced cyber resilience. It has made one such contribution in the form of the cyber-security protocol of the extensible traffic management (XTM) that is used to predict threats in the unmanned and autonomous airspace ecosystems.[30] It can be viewed as indicative of the increased significance of planning the future of aviation, in which drones and autonomous aircraft will be steadily involved in the controlled airspace.[31]

---

[27] "Agencies - Federal Aviation Administration," Federal Register, n.d., https://www.federalregister.gov/agencies/federal-aviation-administration.

[28] Interview, August 1, 2025.

[29] Federal Aviation Administration, *FAA Response to REDAC Recommendations for FY 2026 Research and Development (R&D) Portfolio* (August 8 2024).

[30] Terrence D. Lewis, Hassan Ali, and Kenneth Freeman, "Developing a Cybersecurity Architecture for Extensible Traffic Management (xTM)," conference paper presented at the AIAA SciTech Forum and Exposition (Orlando, FL, January 6–10, 2025), NASA Ames Research Center, Document ID 20240015311.

[31] Interview, August 1, 2025.

4.4. European Aviation Safety Network (EASA)

The European Aviation Safety Agency (EASA) is the regulatory body on safety and environmental standards in European civil aviation. The frameworks of EASA have the concept of security by design, in which manufacturers and Air Navigation Service Providers (ANSPs) must implement cyber-security during the initial phases of system design.[32] EASA collaborates with the FAA to impose compulsory compliance requirements, such as special requirements covering the protection of aircraft systems against electronic interference and ensures structural requirements of resilience instead of being a retrofit.

4.5. Common Pillars of Global Aviation Cyber Resilience

Three key pillars stand out across the international examples:

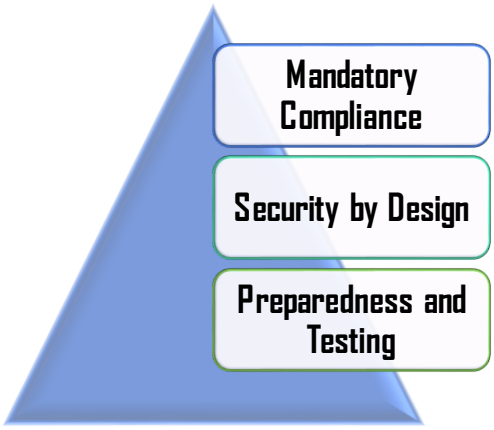

Figure 1 Common Pillars of Global Aviation Cyber Resilience[33]

[32] Interview, August 1, 2025.
[33] Interview, August 1, 2025

1. **Mandatory Compliance**; aviation service providers and manufacturers are required to meet rigorous cyber security standards as part of certification and operational approval. [34]
2. **Security by Design**; cyber resilience measures are integrated into systems from the earliest stages of design and development.
3. **Preparedness and Testing**; adversarial testing, simulations, and resilience exercises ensure systems are continuously evaluated and strengthened.

These approaches demonstrate that aviation cyber resilience is achievable when regulatory authority, industry collaboration, and technological adaptation operate in tandem.

Authority/Body	Core Role	Key Cyber Resilience Measures	Distinctive Features
IATA	Trade association for airlines	Cyber security training, CRMWG for industry-wide awareness	Focus on training, collaboration, and supply chain resilience
FAA	US aviation regulator	Resilience exercises, GPS/GNSS testing, Zero Trust roadmap	Integrates funding, testing, and systemic resilience planning
NASA	Research & development agency	Cyber protocols for XTM (unmanned/autonomous airspace)	Anticipates threats in future autonomous and drone operations

[34] "What a Tangled Web: Aviation Prosperity, Cybersecurity Risk," Federal Aviation Administration, May 11, 2023, https://www.faa.gov/speeches/what-tangled-web-aviation-prosperity-cybersecurity-risk.

EASA	EU aviation regulator	Mandatory compliance and certification standards[35]	Strong emphasis on “security by design” in aircraft systems

Table 1 Global Examples of Aviation Cyber Resilience[36]

4.6. Lessons for Pakistan

Global examples highlight that cyber resilience in aviation is not a one-off achievement but a continuous journey of adaptation, testing, and collaboration. [37] The World Economic Forum (WEF), in partnership with ICAO, EASA, IATA, and other stakeholders, has also stressed that industry-wide coordination is essential to counter globalised cyber risks. Aviation systems demand flexible, evolving responses rather than siloed or static defences. [38] In the context of Pakistan, the emergence of institutions such as PKCERT along with a strong pool of local aviation and technology professionals, showcases a readiness to engage with these international practices. The comparative insights from IATA, FAA, NASA, and EASA including continuous training, regulatory

[35] “European Union Aviation Safety Agency | European Union,” European Union, n.d., https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-aviation-safety-agency-easa_en.

[36] Made by Author

[37] National Business Aviation Association, “Aviation Cybersecurity: Risks and Mitigations | NBAA - National Business Aviation Association,” NBAA - National Business Aviation Association, September 2, 2023, https://nbaa.org/news/business-aviation-insider/2023-07/aviation-cybersecurity-risks-and-mitigations

[38] “Cybersecurity in Aviation: Building a Resilient Future,” World Economic Forum, June 3, 2025, https://www.weforum.org/impact/cybersecurity-in-aviation.

alignment, and proactive testing are the hallmarks of resilience in civil aviation[39] that Pakistan can also work on in its aviation sector.

5. RISK MITIGATION STRATEGIES THROUGH SAFETY MANAGEMENT SYSTEMS (SMS) IN AVIATION

The persistence of cyber threats in aviation highlights the importance of structured frameworks for safety and security management. In this regard, the Safety Management System (SMS) [40] functions as a systematic and proactive model for identifying hazards, evaluating risks, and embedding controls that reduce exposure to disruptions. Originally conceived to address safety risks, SMS is increasingly relevant in understanding how cyber resilience can be structured within aviation infrastructure of any country including Pakistan.

An SMS is built on four interrelated components

i. **Safety Policy** It defines the organisation's safety objectives and expresses its commitment to achieving them.
ii. **Safety Risk Management** It identifies hazards, evaluates risks, and applies controls to mitigate them.

[39] eMudhra Limited, "Aviation Cyber Resilience Strategies for Combating Threats," *eMudhra* (blog), July 21, 2025, https://emudhra.com/en/blog/aviation-cyber-resilience-strategies-against-threats.

[40] Jcox, "The Importance of Safety Management Systems (SMS) in Aviation: A Timely Perspective," *AvSafetyCompliance* (blog), October 17, 2024, https://www.avsafetycompliance.com/post/the-importance-of-safety-management-systems-sms-in-aviation-a-timely-perspective

iii. **Safety Assurance** It monitors and evaluates performance to ensure continuous improvement.

iv. **Safety Promotion** It encourages a culture of safety through training, communication, and shared responsibility. [41]

When considered within the cyber domain, SMS can serve not only as a compliance tool but also as a framework that captures the layered and evolving nature of Pakistan's aviation exposure to digital threats.

5.1. Technical Dimension

Resilience in SMS-related frameworks has been noted by technical measures like segmenting or micro-segmenting of networks that protect aircraft systems by separating them from the ground networks.[42] The integrity and privacy of data are ensured by encrypting communication channels, such as ACARS (Aircraft Communications Addressing and Reporting System) or CPDLC (Controller-Pilot Data Link Communications). Additional security mechanisms, such as intrusion detection systems in avionics, such as hardware-based anomaly detection of ARINC 429 data buses, [43] offer further security by detecting abnormal signals at the physical and protocol levels.

[41] Jcox, "The Importance of Safety Management Systems (SMS) in Aviation: A Timely Perspective," *AvSafetyCompliance* (blog), October 17, 2024, https://www.avsafetycompliance.com/post/the-importance-of-safety-management-systems-sms-in-aviation-a-timely-perspective.

[42] Elochukwu Ukwandu et al., "Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends," *Information* 13, no. 3 (March 10, 2022): 146, https://doi.org/10.3390/info13030146.

[43] Connor Trask et al., "ARINC 429 Cyber-vulnerabilities and Voltage Data in a Hardware-in-the-Loop Simulator," arXiv.org, August 29, 2024, https://arxiv.org/abs/2408.16714

Authenticated firmware updates also represent another security method, which eliminates the risks of intrusion of faulty or malicious code in avionics. [44]

5.2. Operational Dimension

At the functional level, cyber resilience in the SMS is divulged in training, preparedness, and organised responses. Training programmes for pilots, air traffic controllers, and maintenance crews reinforce awareness of potential cyber incidents, consistent with the emphasis on safety promotion in ICAO Annex 19. [45] To complement this, structured incident response planning involves pre-determined mechanisms of managing and containing disruptions. Red teaming and penetration testing, i.e., simulated phishing campaigns or network probing, have also been utilised as diagnostic tools to reveal vulnerabilities before engendering any threat. [46]

5.3. Regulatory and Compliance Dimension

Regulatory and compliance structures also constitute an important risk mitigation layer. The international standards and recommended practices (ICAO Standards and Recommended Practices, SARPs), especially the Safety Management Manual (Doc 9859), offer the international standard of integrating SMS into the aviation systems. In Europe, one of the tools, like the EASA Management System Assessment Tool (MSAT), helps organisations to assess the maturity and the depth of the framework of SMS,

[44] U.S. Government Accountability Office, *Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks*, GAO-21-86 (Washington, DC: U.S. Government Accountability Office, October 9 2020).

[45] Sybert Stroeve, Job Smeltink, and Barry Kirwan, “Assessing and Advancing Safety Management in Aviation,” *Safety* 8, no. 2 (March 22, 2022): 20, https://doi.org/10.3390/safety8020020.

[46] International Civil Aviation Organization, *Session 3: Overview of ICAO Policy Work on Aviation Cybersecurity*, CYSEC Seminar (12 March 2025).

including the cyber resilience. Those mechanisms show how regulation and assessment are used as necessary tools in maintaining consistency throughout jurisdictions. [47]

5.4. Forward-Looking Dimension

An anticipatory outlook is also observed to exhibit predictive and data-driven practices in SMS. By monitoring the safety indicators and analysing the risk intelligence, as well as real-time detection of anomalies, the potential disruptions can be recognised before they manifest themselves. This proactive factor showcases the transition of SMS from an unchanging mode of risk management to a more dynamic system, one that recognises the evolving nature of aviation's exposure to cyber threats. [48]

Dimension	Key Measures in Aviation Cyber Resilience
Technical	Network segmentation/micro-segmentation; encryption of ACARS & CPDLC communications; IDS for avionics (e.g., ARINC 429 anomaly detection); authenticated firmware updates.
Operational	Cyber security training for pilots, ATC staff, and maintenance crews; incident response planning; red teaming and penetration testing; phishing simulations.

[47] "Management System Assessment Tool | EASA," EASA, September 1, 2023, https://www.easa.europa.eu/en/document-library/general-publications/management-system-assessment-tool.

[48] K. Ellis et al., *An In-Time Aviation Safety Management System Concept of Operations and Modernization of the National Airspace System*, conference paper, AIAA SciTech Forum and Exposition, Orlando, FL, January 6–10, 2025.

Regulatory & Compliance	Alignment with ICAO SARPs (Annex 19, Doc 9859); EASA Management System Assessment Tool (MSAT); certification and audit mechanisms for assessing SMS maturity.
Forward-Looking	Real-time anomaly detection; monitoring safety indicators; predictive analytics; integration of risk intelligence for anticipatory threat recognition.

Table 2 Dimensions of Risk Mitigation within SMS Framework[49]

Taken together, these dimensions illustrate how the principles of SMS extend beyond conventional safety management into the cyber domain. This structure framework entailing technical, operational, regulatory, and predictive measures within SMS collectively can contribute to mitigating cyber risks and enhancing cyber resilience in Pakistan's aviation sector, ensuring continued safety and operational integrity.

6. RECOMMENDATIONS

To fortify cyber-resilience in aviation sector of Pakistan, it is crucial to adopt a structured approach in which each component complements rather than overlaps. The following measures are the most important to consider as for future strides vis-à-vis cyber resilience in Pakistan's aviation infrastructure.

6.1. Conform to ICAO SMS Frameworks and National Cyber Standards

The PCAA ought to uphold the incorporation of cyber resilience within the Safety Management Systems (SMS) and must comply with ICAO Annex 19 and Doc 9859. This

[49] Made by the Author on the basis of the interview conducted

alignment will guarantee the systematic identification, evaluation, and mitigation of cyber-risks as part of the overall safety management procedures.[50] Additionally, cyber resilience should be introduced as one of the key pillars of NCASP. This needs to be harmonised with international standards that all Aircraft Operator Security Programmes (AOSPs) conform to standards and interoperate across the borders.[51]

6.2. Institutionalise Continuous Audits, Training and Incident Reporting

Internal and external structured audits should be undertaken regularly to determine vulnerabilities in aviation infrastructure to effectively address cyber threats. At the same time, role-specific cyber-security training needs to be implemented among various personnel such as pilots, air traffic controllers, maintenance crews, and IT staff to minimise the risks of human errors.[52] Besides, a dual mechanism of both mandatory and voluntary incident reporting should be established. This will enhance transparency, promote organisational learning and facilitate information-sharing among aviation entities in line with ICAO cyber strategy. [53]

[50] "ICAO Safety Management Manual Doc 9859," SKYbrary Aviation Safety, July 12, 2024, https://skybrary.aero/articles/icao-safety-management-manual-doc-9859.

[51] International Air Transport Association, *Aviation Security Trust Framework: Enhancing Aviation Security through Open Verifiable Credential Standards* (white paper, January 2025).

[52] International Civil Aviation Organization, *Session 4.04: Risk Management in Aviation Cybersecurity*, presentation at the CYSEC Seminar (Bangkok, March 12 2025)

[53] Interview, August 1, 2025.

6.3. Investment in Preventive Technology and Empower PKCERT

To keep up with cyber threats, Pakistan should invest in predictive technologies like anomaly detection systems and digital twin technologies.[54] These tools will facilitate the aviation authorities to simulate cyber-attacks and enhance readiness in real-time. In addition to that, PKCERT must be commissioned to spearhead aviation-related cyber incident response, support early warning systems and integrate sectorial intelligence into national cyber resilience actions. [55]

6.4. Strengthen Governance, Oversight, and Multi-Stakeholder Collaboration

The PCAA ought to set standards on performance, establish check on compliance and ensure cooperation with international aviation security agencies. This will certify convergence with international standards and address the operational provision peculiar to Pakistan's aviation.[56] Furthermore, airlines, airports, ANSPs and regulators should work in a multi-stakeholder environment to increase effectiveness. This will help these entities to exchange data and intelligence easily. Lastly, joint red-teaming exercises and simulations needs to be institutionalised to boost defences and enhance resilience of aviation systems.[57]

---

[54] Dua Shahid, "Silent Threats: Cyber Vulnerabilities in Aviation Industry," Modern Diplomacy, July 26, 2025, https://moderndiplomacy.eu/2025/07/26/silent-threats-cyber-vulnerabilities-in-aviation-industry.

[55] Interview, August 1, 2025.

[56] "ICAO Safety Management Manual Doc 9859," SKYbrary Aviation Safety, July 12, 2024, https://skybrary.aero/articles/icao-safety-management-manual-doc-9859.

[57] "ICAO Safety Management Manual Doc 9859," SKYbrary Aviation Safety, July 12, 2024, https://skybrary.aero/articles/icao-safety-management-manual-doc-9859.

CONCLUSION

Pakistan has strong groundwork; PCAA's alignment with ICAO programmes, the emergence of PKCERT, and rising institutional awareness, all these efforts signal towards readiness of the country. Nonetheless, cyberspace is transforming and AI threats, supply chain risks, and digital infrastructure expansion requires that vigilance and readiness must follow the pace. Emerging strategies, like digital twin technology for simulation-driven monitoring, layered supply chain audits, and modernisation of legacy systems, offer promising paths forward. If Pakistan continues to invest in regulatory alignment, workforce training, regional coordination, and forward-looking technology, it can not only keep pace with global trends but also become a leader in aviation cyber resilience. The key is to remain proactive, collaborative, and innovative; since challenges evolve daily, so must defences of Pakistan.

BIBLIOGRAPGHY

Aircraft Performance Group. “GPS Spoofing in Aviation: Threats, Detection, and Mitigation Strategies.” APG Aviation Blog, June 30, 2025.

Antani, Snehal. “Attack Yourself First: The Logic Behind Offensive Security.” TechRadar, August 12, 2025. https://www.techradar.com/pro/attack-yourself-first-the-logic-behind-offensive-security.

Aviation Cybersecurity. “Aviation Cybersecurity,” n.d. https://www.iata.org/en/programs/security/cyber-security.

Bentley, Steven. “Understanding the 12 Elements of the ICAO SMS Framework - SasSofia.” SasSofia (blog), June 10, 2025. https://sassofia.com/blog/understanding-the-12-elements-of-the-icao-sms-framework/.

Civil Aviation Authority of Pakistan. "National Programmes." Accessed August 18, 2025. https://caapakistan.com.pk/security/sec-np.aspx.

Civil Aviation Authority Pakistan. “State Safety Programme | Pakistan Civil Aviation Authority,” n.d. https://pcaa.gov.pk/functions/state-safety-programme.

Comply365new. “Ensuring Aviation Safety & Cybersecurity Compliance in 2025: What You Need to Know.” Comply365, February 7, 2025. https://comply365.com/ensuring-aviation-safety-and-cybersecurity-compliance-2025/.

Davies, Nahla. “Cybersecurity in Aviation: Rising Threats and Modernization Efforts.” SecureWorld, June 9, 2025. https://www.secureworld.io/industry-news/aviation-cybersecurity-threats.

Edmonds, Lauren. “A Notorious Hacker Group Is Now Targeting the Aviation Industry, the FBI Says.” Business Insider, June 28, 2025. https://www.businessinsider.com/airlines-hacked-scattered-spider-cybersecurity-2025-6.

Ellis, K., L. Prinzel, M. Vincent, P. Krois, J. Ackerson, S. Infeld, S. Brandt, W. Okolo, J. Coughlan, M. Davies, R. Mah, N. Oza, C. Stephens, and A. Glenn-Chase. "An In-Time Aviation Safety Management System Concept of Operations and Modernization of the National Airspace System." Conference paper, AIAA SciTech Forum and Exposition, Orlando, FL, January 6-10, 2025.

European Union. “European Union Aviation Safety Agency | European Union,” n.d. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-aviation-safety-agency-easa_en.

Federal Aviation Administration. “FAA Response to REDAC Recommendations for FY 2026 Research and Development (R&D) Portfolio.” August 8, 2024.

Federal Aviation Administration. “Safety Management,” July 17, 2025. https://www.faa.gov/about/initiatives/sms/international.

Federal Aviation Administration. “What a Tangled Web: Aviation Prosperity, Cybersecurity Risk,” May 11, 2023. https://www.faa.gov/speeches/what-tangled-web-aviation-prosperity-cybersecurity-risk.

Federal Register. “Agencies - Federal Aviation Administration,” n.d. https://www.federalregister.gov/agencies/federal-aviation-administration.

International Air Transport Association. Aviation Security Trust Framework: Enhancing Aviation Security through Open Verifiable Credential Standards. White paper, January 2025.

International Air Transport Association. https://www.iata.org/en/about/.

International Civil Aviation Organization. Session 3: “Overview of ICAO Policy Work on Aviation Cybersecurity,” CYSEC Seminar, 12 March 2025.

International Civil Aviation Organization. Session 4.04: “Risk Management in Aviation Cybersecurity.” Presentation at the CYSEC Seminar, Bangkok, March 12, 2025.

Jcox. “The Importance of Safety Management Systems (SMS) in Aviation: A Timely Perspective.” AvSafetyCompliance (blog), October 17, 2024. https://www.avsafetycompliance.com/post/the-importance-of-safety-management-systems-sms-in-aviation-a-timely-perspective.

Jones, David. “Aviation Sector Faces Heightened Cyber Risks Due to Vulnerable Software, Aging Tech.” Cybersecurity Dive, April 14, 2025. https://www.cybersecuritydive.com/news/aviation-cyber-risks-aging-tech/745273/.

Johnson, Michael. “The Top Five Cybersecurity Threats to the Aviation Industry.” Center for Information Security Awareness, March 23, 2025. https://cfisa.com/top-five-cybersecurity-threats-to-the-aviation-industry/.

Lee, Sarah. “Aviation Cybersecurity Threats,” n.d. https://www.numberanalytics.com/blog/ultimate-guide-cyber-threats-aviation-infrastructure.

Levin, Michael. “The Top Five Cybersecurity Threats to the Aviation Industry.” Center for Information Security Awareness, March 23, 2025. https://cfisa.com/top-five-cybersecurity-threats-to-the-aviation-industry/.

Nason, Alanna. “Who Is Scattered Spider? | Coro Cybersecurity.” Coro Cybersecurity (blog), May 1, 2024. https://www.coro.net/blog/who-is-scattered-spider.

Olcott, Jake. “Cyber Resilience Vs. Cybersecurity: What’s the Difference and How to Build a Plan for Both.” Bitsight (blog), August 22, 2024. https://www.bitsight.com/blog/cyber-resilience-vs-cybersecurity.

Ribeiro, Anna. “New CSC 2.0 Report Outlines Roadmap to Strengthen Aviation Cyber Defenses Amid Growing Threat Landscape.” Industrial Cyber, April 11, 2025. https://industrialcyber.co/transport/new-csc-2-0-report-outlines-roadmap-to-strengthen-aviation-cyber-defenses-amid-growing-threat-landscape/.

Shahid, Dua. “Silent Threats: Cyber Vulnerabilities in Aviation Industry.” Modern Diplomacy, July 26, 2025. https://moderndiplomacy.eu/2025/07/26/silent-threats-cyber-vulnerabilities-in-aviation-industry/.

SKYbrary Aviation Safety. “ICAO Safety Management Manual Doc 9859,” July 12, 2024. https://skybrary.aero/articles/icao-safety-management-manual-doc-9859.

Stroeve, Sybert, Job Smeltink, and Barry Kirwan. “Assessing and Advancing Safety Management in Aviation.” Safety 8, no. 2 (March 22, 2022): 20. https://doi.org/10.3390/safety8020020.

Trask, Connor, Steve Movit, Justace Clutter, Rosene Clark, Mark Herrera, and Kelly Tran. “ARINC 429 Cyber-vulnerabilities and Voltage Data in a Hardware-in-the-Loop Simulator.” arXiv.org, August 29, 2024. https://arxiv.org/abs/2408.16714.

Ukwandu, Elochukwu, Mohamed Amine Ben-Farah, Hanan Hindy, Miroslav Bures, Robert Atkinson, Christos Tachtatzis, Ivan Andonovic, and Xavier Bellekens. “Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends.” Information 13, no. 3 (March 10, 2022): 146. https://doi.org/10.3390/info13030146.

U.S. Government Accountability Office. Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks. GAO 21 86. Washington, DC: U.S. Government Accountability Office, October 9, 2020.

Wise, Jeff. “Exploding Cargo. Hacked GPS Devices. Spoofed Coordinates. Inside New Security Threats in the Skies.” Vanity Fair, April 24, 2025. https://www.vanityfair.com/news/story/inside-new-security-threats-in-the-skies.

World Economic Forum. “Cybersecurity in Aviation: Building a Resilient Future,” June 3, 2025. https://www.weforum.org/impact/cybersecurity-in-aviation/.

APPENDICES

QUESTIONAIRE

1. Introduction

- What is your definition of cyber resilience, and why should it be considered significant in the aviation industry?
- What is your opinion of the critical priorities in the provision of cyber resilience in the aviation infrastructures in Pakistan?
- What are, in your experience/knowledge, the possible hypotheses about the current situation of cyber resiliency in aviation of Pakistan?

2. Aviation Infrastructure Cyber Resilience in Pakistan.

- What do you consider to be the greatest cyber threats affecting the aviation industry in Pakistan?
- Do you remember any particular instance when the infrastructure of Pakistan aviation has been targeted by cyber-attacks? Please expound on the response and the impact.
- Do you feel that the aviation industry in Pakistan is ready to profile a possible cyber threat? What do you believe are the most important threats to the aviation sector?
- What types of threats do you believe aviation infrastructure in Pakistan is most vulnerable to? (e.g., hacking, data breaches, system failures, etc.)

3. Risk Mitigation

- What are some of the strategies/best practices that you have observed that can be successfully utilised to mitigate cyber resilience in aviation infrastructure?
- What are some examples of organisations or aviation bodies that were able to effectively implement cyber resilience measures? What were the key steps or practices that contributed to their success?
- So, what would you suggest the aviation infrastructure in Pakistan do better in preparation to face a cyber-threat in the future?

4. Recommendations

- What are some of the policies or practices that you would suggest would enhance cyber resiliency in the aviation infrastructure in Pakistan?
- What role do you think governmental bodies and regulatory agencies should play in strengthening cyber resilience within the aviation sector?
- How could the cooperation of aviation players (airlines, airports, government) be increased to make sure that they all have a single approach towards cyber risk management?

5. Conclusion

- To what extent do you consider it important to invest in cyber resilience to create long-term sustainability of the aviation sector in Pakistan?
- What are the key takeaways or lessons that Pakistan can learn from international case studies on cyber resilience in aviation?
- How do you evaluate the future of cyber resilience in the Pakistan aviation infrastructure in relation to the current trends and challenges?