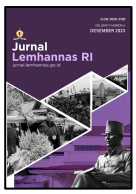

Jurnal Lemhannas RI (JLRI)
E-ISSN : 2830-5728
Vol. 13 No. 4, December 2025: 606-623
DOI: 10.55960/jlri.v13i4.1240
https://jurnal.lemhannas.go.id/index.php/jkl

National Resilience and Terrorism Risk Mitigation in Hajj Air Transport Services after the Kualanamu Airport Bomb Threat Incident

Agus Purwo Wicaksono[1]* , Cynthia Rahmawati[2]
[1]Management Study Program, Faculty of Economics and Business, Marsekal Suryadarma Aerospace University, Indonesia
[2]Aeronautical Engineering Study Program, Faculty of Aerospace and Industrial Engineering, Marsekal Suryadarma Aerospace University, Indonesia

Corresponding Author: aguspurwo.lhn@gmail.com

Article Info:

Keywords:
National Resilience, Terrorism Risk Mitigation, Aviation Security, Cyber-Physical SystemVulnerability, Multi-Agency Coordination

Article History:
Received: 12-09-2025
Revised : 19-10-2025
Accepted: 30-12-2025

Article DOI :
10.55960/jlri.v13i4.1240

Abstract

Purpose: This study analyses the application of the National Resilience Concept in mitigating terrorism risks in Hajj air transport services after the Kualanamu Airport bomb threat incident. It focuses on SOP adaptability, inter-agency coordination, cyber-physical protection, regulatory responsiveness, and human-centred security culture.

Study Design/Methodology/Approach: This study used a qualitative descriptive design based on documentary analysis and literature-based inquiry. Data were drawn from institutional documents, policy reports, academic publications, and reputable public records related to aviation security, terrorism risk mitigation, Hajj transport governance, airport resilience, and crisis coordination. The data were analysed through thematic coding and interpretative gap analysis.

Findings: The findings indicate that the implementation of National Resilience in Hajj aviation security remains partial and uneven. The main gaps concern limited SOP adaptability, fragmented coordination and information sharing, and unresolved regulatory, technological, and human-resource challenges. These gaps may constrain preventive capability, response coordination, and recovery capacity during aviation security incidents.

Originality/Value: This article contributes to aviation security and resilience studies by linking National Resilience with Hajj air transport as a high-density and high-symbolism mobility system. It highlights the need for adaptive SOP reform, integrated response coordination, stronger cyber-physical security, risk-based training, and a pilgrim-centred resilience approach.

How to cite : Wicaksono, A. P., & Rahmawati, C. (2025). National resilience and terrorism risk mitigation in Hajj air transport services after the Kualanamu Airport bomb threat incident. *Jurnal Lemhannas RI, 13* (4), 606-623. https://doi.org/10.55960/jlri.v13i4.1240

E-ISSN: 2830-5728

INTRODUCTION

The recent emergency landings of several Hajj chartered aircraft at Kualanamu International Airport following bomb threats have exposed serious weaknesses in Indonesia's national aviation security system, particularly in air transport operations that are strategically sensitive and symbolically important. These incidents disrupted civil aviation operations and, more importantly, tested Indonesia's National Resilience framework in relation to security assurance, preparedness, and citizen protection. In aviation security studies, threats to civil aviation are no longer understood only as direct acts of terrorism, but also as risks that emerge from layered system failure, human-mediated error, regulatory rigidity, and the reactive evolution of aviation security measures (Klenka, 2019; McFarlane, 2020; Zeballos et al., 2023). Although the Indonesian government has long designated the National Resilience Concept as a fundamental framework for defence and security management, its application within the Standard Operating Procedures (SOPs) for terrorism risk mitigation in Hajj air transport still requires critical examination. This concern is consistent with studies showing that aviation security systems remain vulnerable when formal procedures are not accompanied by adaptive risk assessment, proactive security design, and organisational learning (McFarlane, 2020; Callander, 2022; Zeballos et al., 2023).

Over the past decade, scholars have increasingly examined aviation security governance, airport resilience, cyber-physical vulnerability, and inter-agency crisis coordination. Resilience engineering emphasises that complex socio-technical systems must be able to cope with complexity, adapt to unexpected disruption, and maintain safe performance under pressure (Patriarca et al., 2018; Vert et al., 2021). In the airport context, resilience refers to the capacity of airport systems and stakeholders to maintain essential functions during disruptive events and restore operations within an acceptable period (Janić, 2022). Recent studies on airport resilience further show that disruptions affecting airport operations cannot be addressed only through recovery procedures, but also require anticipatory planning, robustness, adaptive capacity, and coordinated decision-making among stakeholders (Janić, 2022; Zapola et al., 2024). These perspectives are relevant to Hajj aviation because bomb threats, hoaxes, drone-related disruption, and cyber risks may affect not only airport operations, but also passenger confidence, crowd movement, and public trust in state protection.

The digital transformation of airports has also expanded the threat landscape. Smart airport systems increasingly rely on digital platforms, IoT devices, passenger processing systems, access control, communication networks, surveillance technologies, and operational technologies. While these systems improve efficiency and situational awareness, they also introduce new cyber-security vulnerabilities when physical operations are connected to digital infrastructures (Lykou et al., 2019; Koroniotis et al., 2020). Aviation security scholarship has also noted that cyber innovations have changed the aviation threat picture and pushed security governance to adapt to new forms of technological disruption (Callander, 2022). In addition, the increasing use of unmanned aircraft systems around airport environments has created regulatory and operational challenges for aviation security, especially when drone activities intersect with protected airspace and critical airport operations (Huttunen, 2019). Therefore, terrorism risk

DOI: 10.55960/jlri.v13i4.1240

E-ISSN: 2830-5728

mitigation in Hajj aviation cannot rely solely on conventional screening procedures, but must also include cyber-physical protection, drone-risk preparedness, adaptive regulation, and intelligence-informed coordination.

Inter-agency coordination is another crucial dimension. Emergency management research shows that effective crisis response depends on collaborative networks, shared information, pre-established relationships, and coordinated decision-making among organisations with different mandates (Kapucu & Hu, 2016; Parker et al., 2020). Crisis management should also be understood as a learning system in which institutions adapt and transform between crises rather than merely repeat formal procedures (Eriksson & Hallberg, 2022). In the context of Hajj aviation, this means that aviation security actors, airport operators, airlines, relevant security authorities, Hajj service authorities, and other government stakeholders need to operate through clear communication channels and integrated response mechanisms. Weak coordination may reduce the effectiveness of threat assessment, operational decision-making, evacuation planning, and recovery after disruption.

The Hajj context gives this issue additional significance. Hajj is widely discussed in the literature as one of the world's largest religious mass gatherings, involving complex crowd movement, risk communication, emergency planning, and multi-actor governance (Owaidah et al., 2019; Taibah et al., 2020). Studies on Hajj crowd modelling and risk communication show that pilgrim safety requires not only logistical management, but also effective communication, anticipation of crowd dynamics, and preparedness for emergency situations (Owaidah et al., 2019; Taibah et al., 2020). For Indonesia, Hajj air transport therefore cannot be treated merely as a routine aviation service. It is a high-density and high-symbolism mobility system in which aviation security, religious service governance, citizen protection, public communication, and national resilience intersect.

Despite these theoretical and empirical developments, three gaps remain relevant to the Kualanamu case. First, rigid procedural frameworks may limit the capacity of SOPs to address hybrid threats such as bomb hoaxes, cyber-enabled disruption, drone-related risks, and information-based threats. Second, fragmented inter-agency coordination may weaken the operational use of intelligence, delay response, and create ambiguity in command arrangements. Third, limited risk-based security culture among personnel may reduce the effectiveness of technology and regulation in practice. These gaps are consistent with studies showing that aviation security failures often emerge from the interaction between technical vulnerabilities, organisational routines, human error, and incomplete coordination (McFarlane, 2020; Lykou et al., 2019; Koroniotis et al., 2020; Kapucu & Hu, 2016).

Given these challenges, this study examines the implementation of the National Resilience Concept in terrorism risk mitigation for Indonesian Hajj air transport after the Kualanamu Airport bomb threat incident. This study aims to: (1) identify the extent to which National Resilience is reflected in SOPs and operational practices; (2) assess the effectiveness of inter-agency coordination mechanisms; and (3) propose regulatory, technological, and cultural policy recommendations to strengthen aviation security governance for Hajj operations. Employing a qualitative approach with documentary

E-ISSN: 2830-5728

analysis and literature-based triangulation, this study places Hajj aviation security as a critical case for understanding how National Resilience can be translated into adaptive SOPs, integrated command structures, cyber-physical protection, and human-centred security practices. The study contributes to aviation security and resilience studies by linking airport resilience with the specific characteristics of Hajj air transport, namely religious mobility, mass passenger movement, state responsibility for citizen protection, and the need for coordinated multi-agency governance.

The remainder of this article is structured as follows. Section 2 elaborates the conceptual and theoretical foundation underpinning National Resilience and aviation security systems. Section 3 describes the research methodology and data analysis procedures. Section 4 presents and discusses the findings in relation to resilience theories, inter-agency coordination, cyber-physical vulnerability, and security culture. Section 5 concludes with policy recommendations for enhancing Indonesia's integrated aviation security governance.

LITERATURE REVIEW

Theoretical Studies

This study uses National Resilience as the main theoretical lens for analysing terrorism risk mitigation in Hajj aviation services. In this context, terrorism against Hajj air transport is not only viewed as an aviation security problem, but also as a non-traditional threat to state responsibility, public safety, religious mobility, and citizen protection. National Resilience is therefore used to examine how defence, security governance, institutional coordination, infrastructure protection, and human preparedness are integrated in the management of aviation terrorism risks.

Three supporting theoretical clusters are used in this study. The first cluster concerns airspace resilience and threat dynamics. Resilience engineering explains that complex socio-technical systems need the capacity to anticipate, absorb, adapt to, and recover from disruption, particularly when normal procedures are challenged by unexpected events (Patriarca et al., 2018; Vert et al., 2021). In the airport context, resilience refers to the ability of airport systems and stakeholders to maintain essential functions during disruptive events and restore operational performance within an acceptable period (Janić, 2022). Recent airport resilience studies also show that passenger terminals and airport systems require tailored resilience metrics because disruption in one operational component may affect wider airport performance and passenger movement (Zapola et al., 2024). This perspective is relevant to bomb threats, drone risks, cyber-enabled hoaxes, information-based disruption, and other hybrid threats affecting Hajj flight operations.

The second cluster concerns governance, coordination, and crisis management. Terrorism risk mitigation in Hajj aviation requires more than sectoral security procedures because it involves multiple actors with different mandates, including aviation security actors, airport authorities, airlines, security authorities, intelligence-related institutions, and Hajj service authorities. Recent studies on collaborative emergency management

DOI: 10.55960/jlri.v13i4.1240

E-ISSN: 2830-5728

show that crisis response depends on sustainable inter-organisational networks, shared information, pre-established relationships, and decision-making arrangements that can function under urgency and uncertainty (Kapucu & Hu, 2016; Parker et al., 2020). Crisis management should also be treated as a learning system in which institutions adapt between crises, not merely repeat established procedures (Eriksson & Hallberg, 2022). This cluster supports the use of Multi-Agency Resilience, Holistic Aviation Security, and the Integrated Intelligence Cycle as analytical perspectives for assessing command structures, communication channels, intelligence sharing, and joint operational readiness.

The third cluster concerns infrastructure, regulation, and security culture. Airports increasingly depend on cyber-physical systems, including passenger processing platforms, baggage handling systems, access control, surveillance technologies, communication networks, and operational technologies. Studies on smart airport cyber-security show that digital integration can improve efficiency and situational awareness, but it also creates new vulnerabilities when cyber-resilience controls and risk governance are not adequately implemented (Lykou et al., 2019; Koroniotis et al., 2020; Rossiter, 2025). In addition, drone-related risks have become an important aviation security issue because unmanned aircraft systems may affect protected airspace, airport operations, and crisis response arrangements (Huttunen, 2019). These developments justify the use of Cyber-Physical System Vulnerability and Adaptive Regulatory Framework perspectives in analysing whether existing SOPs and regulations are sufficiently responsive to emerging aviation security risks.

The fourth theoretical concern is human-centred security culture. Aviation security is not determined only by technology, formal procedures, or regulatory design. It also depends on human judgement, organisational routines, training quality, risk awareness, and frontline behaviour. McFarlane (2020) explains that aviation security failures may emerge from human-mediated errors and organisational weaknesses, not only from technical failure. Recent studies on aviation security practice also emphasise the need for proactive, risk-based, and less predictable security arrangements in order to reduce routine-based vulnerability (Zeballos et al., 2023). In Hajj aviation, this human-centred perspective is particularly important because frontline personnel interact directly with pilgrims, manage passenger movement, support public communication, and assist operational response during disruption.

Based on these theoretical foundations, National Resilience is treated not as an abstract doctrine, but as an operational framework for assessing whether SOPs, command structures, intelligence flows, cyber-physical protection, regulatory responsiveness, and human-resource readiness are sufficiently adaptive to terrorism risks in Hajj air transport. The theoretical framework is also linked to the specific characteristics of Hajj as a large-scale religious mobility system. Studies on Hajj crowd modelling and disaster risk communication show that pilgrimage safety depends on crowd management, communication, emergency planning, and multi-actor coordination under dense mobility conditions (Owaidah et al., 2019; Taibah et al., 2020). Therefore, Hajj aviation security should be examined not only as airport security, but also as a citizen-protection system involving aviation safety, security governance, religious service management, and public trust.

E-ISSN: 2830-5728

Empirical Studies

The theoretical relationships used in this study are summarised in Table 1.

Table 1. Theoretical Framework for Hajj Aviation Terrorism Mitigation

Theory group	Core focus	Relevance to Hajj aviation terrorism mitigation
Airspace Resilience Theory	Continuity of airport and airspace functions during disruption	Supports early warning, coordinated airspace monitoring, and rapid operational recovery during bomb threats or other intentional disruptions.
All-Azimuth Threat Perspective	Multi-directional and hybrid threat vectors	Frames terrorism, drone incursions, cyber-enabled hoaxes, and information-based threats as risks that may affect both pilgrims and airport operations.
Integration of Non-Traditional Threats	Non-military threats within defence and security policy	Justifies treating threats against Hajj flights as strategic security issues requiring whole-of-government responses.
Multi-Agency Resilience Theory	Inter-agency coordination and shared decision-making	Explains the need for joint structures, clear communication channels, and coordinated SOPs among aviation security actors, airport authorities, airlines, security authorities, intelligence-related institutions, and Hajj service authorities.
Holistic Aviation Security	Integrated view of aviation security as an ecosystem	Highlights the need to connect procedures, technology, intelligence, personnel, passengers, and institutional responsibilities.
Integrated Intelligence Cycle	Timely intelligence collection, analysis, sharing, and operational use	Underpins the need for real-time threat assessment and information sharing among relevant operational and security stakeholders.
Cyber-Physical System Vulnerability	Risks arising from digital and physical airport infrastructure	Identifies vulnerabilities in navigation support, baggage handling, passenger processing, access control, communication systems, and airport operational technologies.
Adaptive Regulatory Framework	Flexible and responsive regulatory adjustment	Supports faster updates to SOPs and regulations in response to drones, hoax bomb threats, cyber incidents, and hybrid terrorism risks.
Human-Centred Security Culture	Values, behaviour, awareness, reporting, and risk-based mindset	Guides scenario-based training and proactive security behaviour among frontline personnel involved in Hajj aviation operations.

In this configuration, National Resilience acts as the integrating lens through which operational SOPs, inter-agency structures, cyber-physical vulnerabilities, regulatory responsiveness, and security culture are analysed. The framework is directly connected to the results of this study, which identify three main problems: partial implementation of National Resilience in SOPs, inconsistent inter-agency coordination, and regulatory, technological, and human-resource challenges in Hajj aviation security.

Empirical studies on aviation security and airport resilience over the last decade have highlighted four relevant strands. First, studies on airport resilience show that airports must be assessed in terms of robustness, vulnerability, recoverability, and continuity of function during disruptive events (Janić, 2022; Zapola et al., 2024). These studies support the argument that airport security should not be evaluated only by the existence of formal procedures, but also by whether those procedures can maintain

DOI: 10.55960/jlri.v13i4.1240

E-ISSN: 2830-5728

essential functions during disruption. For Hajj aviation, this is important because bomb threats or hoaxes may affect not only aircraft operations, but also pilgrim movement, crowd confidence, and the continuity of embarkation services.

Second, research on aviation cyber-security and smart airports shows that the integration of digital and physical airport systems increases exposure to cyber and hybrid threats. Smart airport infrastructures depend on interconnected technologies, IoT-enabled services, surveillance systems, access control, passenger processing, and communication networks. These systems can improve operational efficiency, but also expand the attack surface when cyber-security controls are weak or fragmented (Lykou et al., 2019; Koroniotis et al., 2020; Rossiter, 2025). This empirical strand supports the use of Cyber-Physical System Vulnerability as a key analytical category in this study.

Third, studies on drone risks and aviation security regulation demonstrate that unmanned aircraft systems create new challenges for airport security governance. Drone-related incidents may affect protected airspace and require clearer coordination between airport operators, aviation authorities, security actors, and regulatory institutions (Huttunen, 2019). This supports the need for an adaptive regulatory approach in Hajj aviation security, especially because bomb threats, hoaxes, drone possibilities, and cyber-enabled disruption may occur simultaneously or interact with one another.

Fourth, emergency management and collaborative crisis governance studies show that fragmented communication, unclear authority, and weak inter-organisational coordination can reduce response effectiveness and delay recovery. Kapucu and Hu (2016) show that collaborative emergency response depends on sustainable networks and pre-existing relationships among institutions. Parker et al. (2020) further demonstrate that collaborative crisis management requires coordination under urgency, threat, and uncertainty. Eriksson and Hallberg (2022) add that crisis management systems must learn and adapt between crises rather than treat emergency response as a static procedure. These studies support the argument that Hajj aviation security requires integrated command, shared situational awareness, and operational intelligence sharing across relevant stakeholders.

Finally, empirical studies on aviation security culture and Hajj mass gathering management show that human factors remain decisive. Aviation security failures may emerge when human-mediated errors, organisational routines, and limited risk awareness are not addressed through training and institutional learning (McFarlane, 2020). At the same time, Hajj-related studies show that pilgrim safety requires careful crowd modelling, risk communication, emergency preparedness, and behavioural understanding during dense religious mobility (Owaidah et al., 2019; Taibah et al., 2020). These studies reinforce the argument that Hajj aviation security should adopt a human-centred and pilgrim-centred resilience approach, rather than relying only on technology or formal SOPs.

These empirical strands are relevant to the Kualanamu bomb threat case because the central issue is not merely whether formal SOPs exist, but whether those SOPs are adaptive enough to address hybrid threats; whether institutions can coordinate decisions in real time; whether airport cyber-physical systems are protected; and whether frontline

E-ISSN: 2830-5728

personnel have a proactive security culture. Building on these studies, this article positions Hajj aviation security as a critical case for examining the practical application of National Resilience in a high-density and high-symbolism transport setting.

METHODS

This study employs a qualitative descriptive design grounded in documentary and literature-based inquiry to examine the implementation of the National Resilience Concept in terrorism risk mitigation for Hajj air transport after the Kualanamu Airport bomb threat incident. A qualitative descriptive design was selected because the study aims to provide a clear and context-sensitive interpretation of policy, institutional, and operational issues rather than to develop a grounded theory, test causal relationships, or measure variables statistically. This approach is suitable when the research seeks to describe and interpret a phenomenon based on available textual and contextual evidence (Kim et al., 2017; Doyle et al., 2020). The study therefore analyses institutional documents, policy reports, academic literature, and public records rather than primary data from interviews, surveys, or field observation.

The research combines document analysis and literature-based inquiry. Document analysis was used to examine written materials as sources of evidence, particularly because official documents, policy reports, and public records can reveal how institutions define problems, formulate procedures, and construct responsibilities in security governance. This procedure is consistent with the READ approach to document analysis, which emphasises preparing materials, extracting relevant data, analysing the data, and distilling findings into a coherent interpretation (Dalglish et al., 2020). Literature-based inquiry was used to organise and interpret scholarly debates on aviation security, airport resilience, cyber-physical vulnerability, inter-agency coordination, emergency management, and security culture. The use of literature review as a research methodology requires transparent searching, screening, evaluation, and synthesis of relevant studies in order to strengthen analytical rigour (Snyder, 2019; Xiao & Watson, 2019).

The data consisted of secondary sources drawn from official state documents, including audit reports, parliamentary reports, ministerial or agency reports, and documents related to aviation security, counter-terrorism, Hajj transport governance, and crisis management. These sources were complemented by peer-reviewed academic publications on National Resilience, aviation security, airport resilience, cyber-physical vulnerability, multi-agency coordination, emergency management, and security culture, as well as reputable media reports related to the Kualanamu bomb threat incident. Documents were included when they addressed at least one of the following themes: terrorism risk, Hajj air transport, aviation security, SOP implementation, inter-agency coordination, intelligence sharing, airport cyber-security, regulatory adaptation, drone or hoax threats, recovery capacity, or security culture. Documents were excluded when they lacked clear relevance to the Indonesian Hajj aviation context, could not be verified, or discussed terrorism and resilience only in a general manner.

Data analysis was conducted through systematic reading, screening, classification, coding, and interpretation of the selected documents. The analysis followed three stages.

DOI: 10.55960/jlri.v13i4.1240

E-ISSN: 2830-5728

First, the documents were mapped according to three research foci: the implementation of National Resilience in SOPs and operational practice, the effectiveness of inter-agency coordination, and the regulatory, technological, and human-resource challenges affecting Hajj aviation security. Second, relevant findings were coded using the theoretical framework of National Resilience, Multi-Agency Resilience, Holistic Aviation Security, the Integrated Intelligence Cycle, Cyber-Physical System Vulnerability, the Adaptive Regulatory Framework, and Human-Centred Security Culture. Third, the coded findings were compared with the ideal requirements of adaptive and integrated aviation security governance in order to identify gaps in implementation, coordination, technology, regulation, and security culture. This procedure follows the logic of thematic analysis, in which data are coded, grouped into themes, reviewed, and interpreted to produce an analytically coherent explanation (Nowell et al., 2017; Naeem et al., 2023).

Gap analysis was applied to compare the ideal conditions prescribed by the National Resilience framework with the documented condition of Hajj aviation security governance. The comparison used document-based indicators, including SOP adaptability, unified command, real-time intelligence sharing, inter-agency coordination, cyber-physical system protection, regulatory responsiveness, recovery capacity, and risk-based training. These indicators were used as interpretative references rather than statistical variables. Therefore, any visualisation of implementation gaps in the results section should be understood as a conceptual assessment derived from documentary analysis, not as a numerical measurement based on primary quantitative data.

Trustworthiness was strengthened through triangulation across official documents, scholarly literature, and reputable media reports. Triangulation was used to compare patterns across different types of sources and to reduce dependence on a single institutional or textual perspective. Credibility was further supported by consistency checks in coding and interpretation, ensuring that each finding remained aligned with the research objectives, theoretical framework, and documentary evidence. This approach is consistent with qualitative trustworthiness criteria, particularly credibility, dependability, confirmability, and transparency in the analytical process (Nowell et al., 2017; Korstjens & Moser, 2018).

RESULT AND DISCUSSION

Implementation of National Resilience in SOPs and Operational Practice

Documentary evidence indicates that the implementation of the National Resilience Concept in security and preparedness remains partial and uneven within SOPs and day-to-day mitigation practices for Hajj air transport after the Kualanamu bomb threat incident. Reviewed parliamentary, audit, policy, and academic documents suggest that the main weaknesses are related to SOP adaptability, inter-agency command, intelligence sharing, and technological readiness. Intelligence products from relevant security institutions are not always integrated with Avsec, airport operators, and airline systems in a timely operational format. This condition constrains proactive and preventive responses, especially when threat information must be translated rapidly into airport-level security decisions.

E-ISSN: 2830-5728

The documentary analysis also indicates a deficit in unified field command. During airport security incidents, overlapping authority among airport authorities, the Police, the Military, and other relevant institutions may create uncertainty in decision-making. This finding is consistent with the principle that effective emergency management requires clear authority, reliable communication, and coordinated institutional action Kapucu & Hu (2016); Parker et al. (2020). In the context of Hajj aviation, the problem is more sensitive because security operations do not only involve aircraft and airport infrastructure, but also the protection of pilgrims as citizens participating in a high-density religious mobility process.

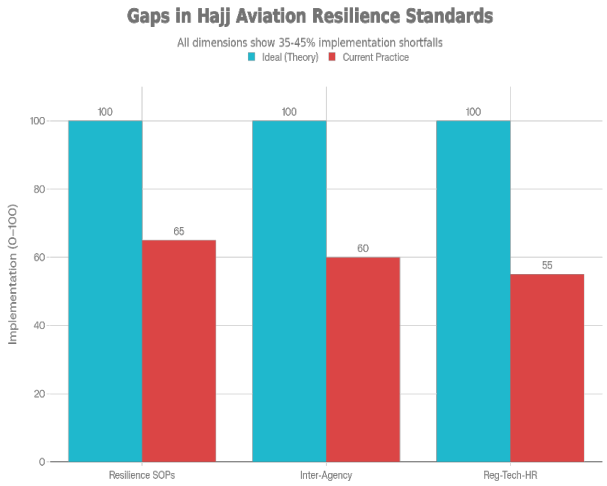

Figure 1. Provides A Conceptual Visualisation of the Relative Gap Between Ideal National Resilience Standards

Figure 1 should therefore be understood as a conceptual visualisation of the implementation gap, not as a statistical measurement. The figure maps the relative distance between the ideal requirements of National Resilience and the documented condition of Hajj aviation security governance across several key dimensions. The gap is visible in four areas: SOPs that remain largely procedural, limited integration of cyber and drone-related threats, weak real-time intelligence flow, and insufficient operational linkage between aviation security and pilgrim protection. From the perspective of resilience engineering, a security system should not only recover after disruption, but also anticipate and adapt when unexpected disturbances challenge normal operations (Patriarca et al. 2018; Vert et al. 2021). In this regard, the implementation of National Resilience in Hajj aviation remains more normative than fully operational.

Table 2 presents the document-based indicators used to interpret the implementation gap. These indicators are not treated as statistical variables, but as analytical references derived from the qualitative document review.

Table 2. Document-based indicators of implementation gaps in Hajj aviation security

DOI: 10.55960/jlri.v13i4.1240

E-ISSN: 2830-5728

Analytical indicator	Ideal condition	Documentary finding	Implementation gap
SOP adaptability	SOPs are adaptive to bomb threats, cyber threats, drone risks, and hoaxes	SOPs remain more procedural and physically oriented	Limited adaptation to hybrid and non-traditional threats
Unified command	Clear single command structure during airport security incidents	Authority may overlap among airport authorities, Police, Military, and related agencies	Command deficit and possible delay in decision-making
Intelligence sharing	Real-time threat information is shared with operational actors	Intelligence flow is not always integrated with Avsec and airport operators	Weak operational use of intelligence
Cyber-physical protection	Airport digital and physical systems are protected as integrated infrastructure	Cyber risks to passenger processing, baggage systems, access control, and communication systems remain a concern	Incomplete cyber-physical resilience
Security culture	Personnel are trained through risk-based and scenario-based programmes	Training remains more periodic and procedural	Reactive rather than proactive security culture

Effectiveness of Inter-Agency Coordination and Synergy

The effectiveness of coordination among Avsec, airport authorities, the Police, the Military, intelligence agencies, airlines, and the Ministry of Religious Affairs is assessed as limited and inconsistent across prevention, response, and recovery phases. The reviewed documents indicate that tactical threat information is not always transmitted quickly and clearly to the operational units responsible for airport security and passenger handling. This weakness reflects a break in the Integrated Intelligence Cycle because intelligence is not fully transformed into shared situational awareness and coordinated action.

This finding is consistent with studies on emergency governance, which show that crisis response depends on inter-agency communication, boundary-spanning actors, and shared decision-making under uncertainty (Kapucu & Hu, 2016). Parker et al. (2020) also emphasise that effective emergency management requires institutional arrangements that can reduce fragmentation and clarify responsibility during disruptive events. In the Kualanamu case, the lack of consistent single command and the limited involvement of all relevant actors in simulation and response planning indicate that Hajj aviation security has not fully reflected the requirements of Multi-Agency Resilience and Holistic Aviation Security.

The role of the Ministry of Religious Affairs is particularly important because Hajj aviation security is not merely an airport security issue. It also concerns pilgrim movement, public communication, evacuation planning, psychological assurance, and citizen protection. When religious authorities are only partially involved in crisis simulations, the security ecosystem becomes incomplete. This gap explains why formal improvements in aviation security governance may not automatically produce stronger

E-ISSN: 2830-5728

resilience if inter-agency coordination remains fragmented and if pilgrim-related human factors are treated as secondary issues.

Regulatory, Technological, and Human-Resource Challenges

The results identify three interrelated clusters of challenges: regulatory rigidity, cyber-physical vulnerability, and limited human-resource readiness. On the regulatory side, SOPs remain slow to incorporate procedures for non-traditional threats such as drone incursions, cyber-enabled disruption, and hoax bomb threats. This indicates a gap between formal security procedures and the changing character of aviation threats. An adaptive regulatory approach is needed because aviation security threats increasingly combine physical, digital, informational, and psychological dimensions.

From a technological perspective, Hajj embarkation airports depend on cyber-physical systems, including passenger processing platforms, baggage handling, access control, communication networks, and operational technologies. Studies on smart airport cyber-security show that digital integration can improve operational efficiency, but it also creates new vulnerabilities if cyber resilience controls are not adequately implemented (Lykou et al., 2019). Similar concerns are found in aviation communication and surveillance systems, where insecure digital protocols may expose aviation infrastructure to manipulation, disruption, or information integrity risks (Koroniotis et al. 2020; Rossiter, 2025). This supports the finding that terrorism risk mitigation in Hajj aviation cannot rely only on physical screening, but must also include cyber-physical protection.

The third challenge concerns human-resource readiness and security culture. Aviation security is not determined only by technology and regulation, but also by the behaviour, judgement, and risk awareness of personnel. McFarlane (2020) shows that human-mediated errors may become exploitable weaknesses in aviation security systems when organisational routines and security awareness are inadequate. In the Hajj aviation context, this means that non-security staff, frontline service personnel, and personnel involved in pilgrim handling must also be included in risk-based training. Routine training is not sufficient if it does not include scenario-based exercises for bomb threats, hoaxes, drone risks, evacuation, crowd movement, public communication, and coordination with religious authorities.

Discussion

The discussion of this study centres on three issues: the extent to which the National Resilience Concept has been operationalised in Hajj aviation terrorism mitigation, the effectiveness of inter-agency coordination after the Kualanamu bomb threat incident, and the structural challenges that continue to weaken aviation security resilience. These issues correspond directly to the three research foci described in the methodology, namely SOP implementation, inter-agency coordination, and regulatory, technological, and human-resource challenges. The discussion therefore interprets the results by comparing documentary findings with relevant studies on resilience engineering, airport resilience, collaborative crisis management, cyber-physical vulnerability, aviation security culture, and Hajj mass-gathering risk management.

DOI: 10.55960/jlri.v13i4.1240

E-ISSN: 2830-5728

First, the findings show that National Resilience has not yet been fully translated into adaptive aviation security practice. The existence of formal SOPs is important, but it does not automatically guarantee resilience. Resilience engineering literature emphasises that complex socio-technical systems require the capacity to anticipate disruption, adapt under pressure, and maintain essential functions when normal procedures are challenged (Patriarca et al., 2018; Vert et al., 2021). In the airport context, resilience also involves robustness, vulnerability reduction, and the ability to restore operational performance after disruption (Janić, 2022). The Kualanamu bomb threat case indicates that the central problem is not merely the absence of formal rules, but the limited ability of existing SOPs to respond to hybrid threats involving hoaxes, cyber risks, drone-related disruption, and mass passenger sensitivity. This confirms that National Resilience in Hajj aviation remains stronger as a policy doctrine than as a practical operational mechanism.

Second, the findings on inter-agency coordination confirm the importance of communication, command clarity, shared situational awareness, and pre-established collaborative networks in emergency response. Kapucu and Hu (2016) show that sustainable collaborative emergency response depends on inter-organisational networks and relationships that are built before a crisis occurs. Parker et al. (2020) further explain that collaborative crisis management is particularly important under conditions of urgency, threat, and uncertainty. In this study, fragmented information flow, delayed operational use of threat information, and inconsistent response coordination may reduce the effectiveness of terrorism risk mitigation in Hajj aviation. This is particularly important because Hajj flights involve multiple stakeholders, including aviation security actors, airport operators, airlines, relevant security authorities, intelligence-related institutions, Hajj service authorities, and other government actors. If these actors do not operate within a coordinated response structure, preventive capability and recovery capacity may remain limited.

Third, the findings also show that aviation security governance needs to be treated as a learning system. Eriksson and Hallberg (2022) argue that crisis management should not be understood only as a response mechanism during emergencies, but also as a system that learns, adapts, and transforms between crises. This insight is important for the Kualanamu case because bomb threats, cyber-enabled disruption, drone risks, and public anxiety cannot be managed only through static procedures. SOPs need to be periodically reviewed through lessons learned, simulation, scenario-based exercises, and cross-institutional evaluation. In this sense, National Resilience should be operationalised not only through written regulations, but also through institutional learning that improves preparedness before future incidents occur.

Fourth, the regulatory and technological findings are consistent with the literature on cyber-physical vulnerabilities in modern airports. Lykou et al. (2019) show that smart airport systems face cyber-security threats linked to IoT, digital infrastructure, and operational technologies. Koroniotis et al. (2020) also explain that smart airports rely on interconnected systems that may expand the cyber-attack surface if cybersecurity and reliability controls are not adequately integrated. In the present study, these insights are relevant because terrorism risk mitigation in Hajj aviation requires protection of both physical and digital infrastructures, including passenger processing systems, baggage

E-ISSN: 2830-5728

handling, access control, communication networks, surveillance technologies, and operational platforms. The continued emphasis on conventional physical screening is therefore insufficient when airport operations increasingly depend on cyber-physical systems.

Fifth, the findings on drone-related and hybrid threats indicate the need for a more adaptive regulatory framework. Huttunen (2019) shows that civil unmanned aircraft systems create security challenges for aviation because they may affect protected airspace, airport operations, and regulatory authority. In the Hajj aviation context, drone risks should not be treated as a separate technical issue, but as part of a wider hybrid threat environment that includes bomb hoaxes, information-based disruption, cyber vulnerabilities, and crowd anxiety. This supports the argument that aviation security SOPs must be updated through adaptive regulation that can respond to emerging risks without creating ambiguity in operational authority.

Sixth, the human-resource findings indicate that security culture remains a critical component of National Resilience. McFarlane (2020) argues that aviation security failures may emerge from human-mediated errors and organisational weaknesses, not only from technical failures. Zeballos et al. (2023) also show that unpredictability in aviation security can be used as a proactive approach to address risks from both external threats and insider vulnerabilities. These studies support the finding that Hajj aviation security requires a broader human-centred security culture involving both security and non-security personnel. Personnel who interact directly with pilgrims need to understand threat indicators, reporting mechanisms, evacuation procedures, crowd behaviour, and communication protocols. Without such preparedness, advanced technology and formal regulation may not translate into effective prevention and response.

Seventh, the Hajj context gives the discussion a specific contribution that is not fully addressed in general aviation security studies. Hajj is widely recognised as a major religious mass-gathering event that requires crowd modelling, emergency planning, and effective risk communication (Owaidah et al., 2019; Taibah et al., 2020). For this reason, Hajj aviation security cannot be understood only as airport infrastructure protection. It also involves pilgrim movement, public communication, psychological reassurance, evacuation planning, and citizen protection. The findings of this study therefore extend airport resilience and aviation security literature by showing that Hajj air transport requires a pilgrim-centred resilience approach. Such an approach integrates aviation safety, terrorism risk mitigation, crowd management, religious service governance, and state responsibility for protecting citizens.

These findings also need to be read in relation to the empirical studies and theoretical perspectives discussed in the literature review. The incomplete translation of National Resilience into adaptive SOPs supports the argument that resilience requires anticipatory capacity, operational flexibility, and adaptive learning rather than reliance on formal procedures alone (Patriarca et al., 2018; Vert et al., 2021; Eriksson & Hallberg, 2022). The finding on fragmented coordination is consistent with studies showing that crisis response depends on collaborative networks, shared information, and coordinated decision-making among actors operating under uncertainty (Kapucu & Hu, 2016; Parker

DOI: 10.55960/jlri.v13i4.1240

E-ISSN: 2830-5728

et al., 2020). Similarly, the technological findings correspond to studies showing that smart airports require cyber-resilience controls because digital integration can create new points of vulnerability (Lykou et al., 2019; Koroniotis et al., 2020). Finally, the weakness of risk-based training confirms the argument that aviation security is shaped by human behaviour, organisational routines, and the ability of personnel to act proactively in uncertain situations (McFarlane, 2020; Zeballos et al., 2023).

Taken together, the findings support a more operational understanding of National Resilience in aviation security. First, National Resilience should be viewed as a tri-layered construct consisting of legal and doctrinal alignment, cyber-physical and procedural adaptation, and socio-cultural internalisation among frontline actors. These three layers are interdependent. Legal frameworks and SOPs provide authority, cyber-physical protection strengthens operational resilience, and security culture ensures that personnel can recognise and respond to threats. Second, Hajj aviation security requires a pilgrim-centred resilience approach because the protected object is not only airport infrastructure, but also pilgrims as citizens engaged in religious mobility. This approach extends Holistic Aviation Security by integrating aviation safety, terrorism mitigation, crowd management, religious service governance, and citizen protection.

In addressing the research problem, the discussion confirms that the implementation of the National Resilience Concept in Indonesian Hajj aviation remains partial and uneven. Inter-agency synergy has been formally recognised, but it still requires stronger operational mechanisms for integrated command, intelligence-informed coordination, and cross-institutional learning. Regulatory inertia, cyber-physical vulnerability, and weak security culture also continue to produce a resilience gap that cannot be solved by technological investment alone. Therefore, the policy direction should prioritise adaptive SOP reform, clearer response coordination, improved information sharing, cyber-physical security investment, and risk-based multi-agency training involving aviation, security, Hajj service, and other relevant government stakeholders.

CONCLUSION

This study examined the implementation of the National Resilience Concept in mitigating aviation security risks related to Hajj air transport after the Kualanamu Airport bomb threat incident. Based on documentary analysis and literature-based inquiry, the findings indicate that the application of National Resilience in Hajj aviation security remains partial and uneven. Formal SOPs and institutional mandates already provide an important basis for aviation security governance, but their operationalisation appears to require further strengthening in responding to hybrid and non-traditional threats such as bomb hoaxes, cyber risks, drone-related disruption, and mass passenger sensitivity. This suggests that National Resilience in Hajj aviation should not be understood only as a policy doctrine, but also as an operational capacity that requires adaptive procedures, coordinated response mechanisms, intelligence-informed decision-making, cyber-physical protection, and proactive security culture.

The study also indicates that inter-agency coordination remains an important factor in strengthening aviation security for Hajj operations. The involvement of multiple

E-ISSN: 2830-5728

stakeholders, including aviation security actors, airport operators, airlines, relevant security authorities, Hajj service authorities, and other government institutions, requires clearer communication channels and a more integrated response structure. The findings suggest that information flow, operational coordination, and command arrangements need to be continuously improved in order to strengthen preventive capability and recovery capacity during aviation security incidents. In this context, Hajj service authorities should not be positioned only as administrative actors, but also as important stakeholders in pilgrim protection, evacuation planning, risk communication, and crisis simulation.

The regulatory, technological, and human-resource dimensions also require careful attention. Existing procedures need to become more responsive to emerging aviation security threats, particularly those involving cyber-physical systems, airport digital infrastructure, drone risks, and information-based disruption. However, technological investment alone is unlikely to be sufficient without human-resource preparedness and institutional coordination. The findings suggest that risk-based and scenario-based training should be strengthened, not only for aviation security personnel but also for frontline staff who interact directly with pilgrims. Such training may help build a human-centred security culture in which personnel are better prepared to recognise threat indicators, report anomalies, support evacuation procedures, and coordinate responses across institutional boundaries.

In practical terms, this study supports a policy agenda that prioritises adaptive SOP reform, clearer response coordination, improved information sharing, stronger cyber-physical security, and risk-based multi-agency training for Hajj aviation operations. Theoretically, the study suggests that National Resilience in aviation security can be further developed as a tri-layered framework consisting of legal and doctrinal alignment, cyber-physical and procedural adaptation, and socio-cultural internalisation among frontline actors. It also points to the need for a pilgrim-centred resilience approach that integrates aviation safety, security risk mitigation, crowd management, religious service governance, and citizen protection. Since this study relies on secondary documents and literature-based analysis, future research should test these findings through interviews, field observation, operational data, and comparative studies across Hajj embarkation airports or other high-density transport systems.

REFERENCE

Callander, B. (2022). Technological innovation in aviation security: From industries as policy entrepreneurs. *Politeja, 19*(4/79), 55–71. https://doi.org/10.12797/Politeja.19.2022.79.04

Dalglish, S. L., Khalid, H., & McMahon, S. A. (2020). Document analysis in health policy research: The READ approach. *Health Policy and Planning, 35*(10), 1424–1431. https://doi.org/10.1093/heapol/czaa064

Doyle, L., McCabe, C., Keogh, B., Brady, A., & McCann, M. (2020). An overview of the qualitative descriptive design within nursing research. *Journal of Research in Nursing, 25*(5), 443–455. https://doi.org/10.1177/1744987119880234

Eriksson, P., & Hallberg, N. (2022). Crisis management as a learning system:

 DOI: 10.55960/jlri.v13i4.1240

Understanding the dynamics of adaptation and transformation in-between crises. *Safety Science, 151*, 105735. https://doi.org/10.1016/j.ssci.2022.105735

Huttunen, M. T. (2019). Civil unmanned aircraft systems and security: The European approach. *Journal of Transportation Security, 12*(3–4), 83–101. https://doi.org/10.1007/s12198-019-00203-0

Janić, M. (2022). Analysis and modelling of airport resilience, robustness, and vulnerability: Impact of COVID-19 pandemic disease. *The Aeronautical Journal, 126*(1305), 1924–1953. https://doi.org/10.1017/aer.2022.25

Kapucu, N., & Hu, Q. (2016). Understanding multiplexity of collaborative emergency management networks. *The American Review of Public Administration, 46*(4), 399–417. https://doi.org/10.1177/0275074014555645

Kim, H., Sefcik, J. S., & Bradway, C. (2017). Characteristics of qualitative descriptive studies: A systematic review. *Research in Nursing & Health, 40*(1), 23–42. https://doi.org/10.1002/nur.21768

Klenka, M. (2019). Major incidents that shaped aviation security. *Journal of Transportation Security, 12*(1), 39–56. https://doi.org/10.1007/s12198-019-00201-2

Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., & Janicke, H. (2020). A holistic review of cybersecurity and reliability perspectives in smart airports. *IEEE Access, 8*, 209802–209834. https://doi.org/10.1109/ACCESS.2020.3036728

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice, 24*(1), 120–124. https://doi.org/10.1080/13814788.2017.1375092

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2019). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. *Sensors, 19*(1), 19. https://doi.org/10.3390/s19010019

McFarlane, P. (2020). Linking aviation security failures to human-mediated error: A review of the related literatures with directions for policy and research. *Journal of Transportation Security, 13*, 33–51. https://doi.org/10.1007/s12198-020-00209-z

Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A step-by-step process of thematic analysis to develop a conceptual model in qualitative research. *International Journal of Qualitative Methods, 22*, 1–18. https://doi.org/10.1177/16094069231205789

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*(1), 1–13. https://doi.org/10.1177/1609406917733847

Owaidah, A. A., Olaru, D., Bennamoun, M., Sohel, F., & Khan, N. (2019). Review of modelling and simulating crowds at mass gathering events: Hajj as a case study. *Journal of Artificial Societies and Social Simulation, 22*(2), 9. https://doi.org/10.18564/jasss.3997

Parker, C. F., Nohrstedt, D., Baird, J., Hermansson, H., Rubin, O., & Baekkeskov, E. (2020). Collaborative crisis management: A plausibility probe of core assumptions. *Policy and Society, 39*(4), 510–529. https://doi.org/10.1080/14494035.2020.1767337

Patriarca, R., Bergström, J., Di Gravio, G., & Costantino, F. (2018). Resilience engineering: Current status of the research and future challenges. *Safety Science, 102*, 79–100. https://doi.org/10.1016/j.ssci.2017.10.005

Rossiter, A. (2025). Smart airports and the evolving cyber threat. *Journal of Transportation Security, 18*, 26. https://doi.org/10.1007/s12198-025-00311-0

Snyder, H. (2019). Literature review as a research methodology: An overview and

E-ISSN: 2830-5728

guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Taibah, H., Arlikatti, S., Andrew, S. A., Maghelal, P., & DelGrosso, B. (2020). Health information, attitudes and actions at religious venues: Evidence from Hajj pilgrims. *International Journal of Disaster Risk Reduction, 51*, 101886. https://doi.org/10.1016/j.ijdrr.2020.101886

Vert, M., Sharpanskykh, A., & Curran, R. (2021). Adaptive resilience of complex safety-critical sociotechnical systems: Toward a unified conceptual framework and its formalisation. *Sustainability, 13*(24), 13915. https://doi.org/10.3390/su132413915

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research, 39*(1), 93–112. https://doi.org/10.1177/0739456X17723971

Zapola, G. S., Silva, E. J., Alves, C. J., & Müller, C. (2024). Towards a resilience assessment framework for the airport passenger terminal operations. *Journal of Air Transport Management, 114*, 102508. https://doi.org/10.1016/j.jairtraman.2023.102508

Zeballos, M., Fumagalli, C. S., Ghelfi-Wächter, S. M., & Schwaninger, A. (2023). Why and how unpredictability is implemented in aviation security: A first qualitative study. *Heliyon, 9*(3), e13822. https://doi.org/10.1016/j.heliyon.2023.e13822.

DOI: 10.55960/jlri.v13i4.1240