

GEOPOLITICAL RISK ASSESSMENT IN AVIATION: MANAGERIAL STRATEGIES FOR AIRPORT RESILIENCE

Ahmed NAWZAD ^{a*}

^a *Erzincan Binali Yıldırım University, Department of Aviation Management, Turkey*

ABSTRACT

This study provides an analytical overview of key geopolitical risks affecting the operations of international airports. It highlights how armed conflicts, international sanctions, and cyber threats impact the resilience of the aviation industry in the context of global instability. The main focus is placed on risk management strategies that aim to improve adaptability and ensure the continuity of airport operations during crises. The research applies critical analysis of scientific literature, international case studies (including the experience of airports in Amsterdam, London, and Seoul), and a comparative approach to identify the most effective management solutions. Special attention is given to digital transformation, multi-stakeholder engagement, and strategic planning based on scenario modeling and vulnerability assessment. In conclusion, the paper justifies the need for an integrated geopolitical risk management system in aviation that enhances infrastructure resilience, organizational flexibility, and public trust. The findings can be useful for airport managers and regulatory bodies seeking to develop a stable and secure model for the future of civil aviation.

KEYWORDS: *airport resilience, aviation security, geopolitical risk, risk management, strategic planning.*

DOI: [10.24818/IMC/2025/01.09](https://doi.org/10.24818/IMC/2025/01.09)

1. INTRODUCTION

In the context of increasing global instability caused by political conflicts, sanctions, pandemics, and cyber threats, the aviation industry has become one of the most vulnerable components of infrastructure. Airports, serving as vital nodes in global logistics networks, not only facilitate the movement of people and goods but also shape the international image of regions. Their resilient functioning is of strategic importance in an era of geopolitical uncertainty (ICAO, 2023). Recent international developments have revealed the inadequacy of traditional risk management approaches in addressing today's multi-level challenges. For instance, the conflict in Ukraine led to the closure of airspace and disrupted global routes, while sanctions have restricted access to aviation technologies. Simultaneously, cyberattacks increasingly target flight control systems, underscoring a need for rethinking current strategies (UK Government, 2025; Bloch et al., 2021). This study seeks to explore the geopolitical risks that influence international airport operations and to identify managerial strategies that enhance their resilience. Specifically, it classifies key types of threats, investigates real-world responses from global aviation hubs, evaluates methodological approaches to risk management, and proposes integrated, adaptive models grounded in digital transformation and institutional cooperation. By approaching geopolitical risks through a comprehensive and systematic lens, this paper contributes to bridging the gap between isolated case

* Corresponding author. E-mail address: ahmadnawzad077@gmail.com

studies and the need for a unified strategy. The proposed framework offers practical insights applicable to airports of varying scales, reflecting both scientific relevance and real-world applicability.

2. LITERATURE REVIEW

The academic discourse on geopolitical risks in aviation has expanded significantly in recent years, reflecting the sector’s growing exposure to global instability. Scholars emphasize that airports, as critical nodes in international transport networks, are uniquely vulnerable to disruptions caused by political, economic, and digital turbulence.

2.1 Political Instability and Armed Conflicts

Research consistently identifies armed conflicts and political crises as primary disruptors of aviation safety and connectivity. Chernii (2024) highlights how international conflicts, particularly in Eastern Europe, have forced widespread airspace closures and rerouting, leading to increased operational costs and reduced efficiency. Bloch et al. (2021) further demonstrate that governance structures at European airports often lack the flexibility to adapt quickly to such geopolitical shocks, underscoring the need for more resilient institutional frameworks.

2.2 Economic Sanctions and Supply Chain Vulnerabilities

Economic sanctions represent another critical dimension of geopolitical risk. According to OECD (2020), sanctions not only restrict access to aviation technologies and spare parts but also delay modernization projects, thereby weakening long-term competitiveness. These findings align with broader studies on infrastructure dependency, which suggest that airports heavily reliant on foreign suppliers face heightened vulnerability during geopolitical disputes.

2.3 Cybersecurity Threats in Aviation

The digitalization of airport operations has introduced new layers of risk. IATA (2022) and Florido-Benítez (2024) document a sharp rise in cyberattacks targeting booking systems, flight management platforms, and passenger databases. Rossiter (2025) adds that “smart airports” are particularly exposed, as their reliance on interconnected systems increases the potential for cascading failures. ICAO (n.d.) emphasizes the urgent need for international standards in aviation cybersecurity, noting that fragmented approaches leave critical gaps in protection.

2.4 Regulatory Fragmentation and Post-Pandemic Challenges

The lack of harmonized international regulations has also been identified as a barrier to resilience. Studies show that inconsistent health protocols, visa policies, and certification requirements hinder recovery and erode trust among aviation partners (UK Government, 2025). This regulatory fragmentation complicates crisis management, particularly in the aftermath of global shocks such as the COVID-19 pandemic.

2.5 Environmental and Climatic Pressures

Recent scholarship has expanded the scope of geopolitical risk to include environmental and climate-related disruptions. Ren (2024) and Alam et al. (2024) argue that climate change not only exacerbates natural disasters affecting airports but also fuels geopolitical tensions through resource scarcity and policy disputes. These findings suggest that resilience strategies must integrate environmental sustainability with traditional security measures.

2.6 Human and Social Dimensions of Risk

Beyond technical vulnerabilities, scholars increasingly stress the importance of human factors. De Vynck (2024) demonstrates that crisis mismanagement often stems from psychological stress and communication failures rather than purely technical breakdowns. Lee et al. (2025) reinforce this perspective by showing how Incheon International Airport's governance model balances public safety with individual rights, offering insights into the role of institutional trust in resilience-building.

2.7 Synthesis and Research Gap

The literature collectively underscores that geopolitical risks in aviation are multidimensional, spanning political, economic, digital, environmental, and social domains. While existing studies provide valuable case-specific insights, there remains a gap in integrated frameworks that combine these dimensions into a unified resilience model. Most research addresses risks in isolation, whereas airports require holistic strategies that align digital transformation, international cooperation, and human capital development. This study seeks to bridge that gap by proposing a comprehensive model for airport resilience under geopolitical instability.

3. GEOPOLITICAL RISKS IN THE AVIATION SECTOR: CONCEPTUAL FRAMEWORK

Amid escalating global turbulence, the aviation industry stands as one of the most vulnerable sectors of critical infrastructure. Positioned at the intersection of political, economic, and digital processes, international airports become focal points for geopolitical risks. Their stable operation affects not only logistics and passenger mobility but also shapes regional reputation, national security, and investment attractiveness. The current international agenda demonstrates that the resilience of airports is directly linked to their capacity to adapt to volatile external conditions (ICAO, 2023).

3.1 Classification of Geopolitical Risks in the Aviation Sector

To respond effectively to emerging threats, it is essential to develop a systemic understanding of the structure of geopolitical risks. Based on recent case studies, reports from international organizations, and the latest analytical findings (OECD, 2020; IATA, 2022; UK Government, 2025), several key categories of risks can be identified.

3.1.1 Political Instability and Armed Conflicts.

Military confrontations, political crises, and growing international tensions often result in airspace closures, forced rerouting of flights, and increased operational costs. The ongoing conflict in Eastern Europe and escalating instability in the Middle East have led to significant disruptions in air traffic flows (Chernii, 2024).

3.1.2 Economic Sanctions and Restrictions.

Pressure from global institutions through sanction packages limits access to technology, investment, and spare parts. These restrictions slow down airport modernization and, in some cases, bring infrastructure projects to a complete halt (OECD, 2020).

3.1.3 Cyber Threats and Digital Attacks.

In the digital era, airport information systems are increasingly targeted by cyberattacks. According to IATA (2022), attacks on flight management systems, booking platforms, and security, databases have significantly increased in recent years with a notable spike record over the past two years a new spike was recorded, particularly in countries with weakened cybersecurity infrastructure (Rossiter, 2025; Florido-Benítez, 2024).

3.1.4 Regional Regulatory Barriers. Inconsistencies in health regulations, visa policies, and certification requirements between countries lead to delays, reduced international connectivity, and eroded trust among aviation partners. Research emphasizes that the lack of harmonized standards in the post-pandemic recovery phase has become a serious obstacle to restoring global mobility.

3.1.5 Environmental and Climatic Tensions.

Escalating climate policies and natural disasters have also emerged as drivers of geopolitical instability. Floods, heatwaves, droughts, and wildfires may disrupt airport operations indefinitely, particularly in regions with limited climate resilience (Ren, 2024; Alam et al., 2024).

Thus, risk classification serves not only as an academic exercise but as the foundation for practical, forward-looking management decisions. Only a multidisciplinary approach—one that incorporates digital transformation, strategic flexibility, and institutional coordination—can provide a sufficiently robust response to the multifaceted challenges facing airports in the 21st century. Yet the human dimension is no less critical. Geopolitical threats—especially those that escalate rapidly—inevitably trigger panic among passengers, disrupt logistical flows, undermine trust in air carriers, and destabilize the operational environment of airports. Studies show that periods of uncertainty provoke impulsive behavior fueled by the social contagion of anxiety. This highlights the need for airport managers not only to ensure technical readiness but also to foster emotional intelligence in their teams, strengthen transparency in communications, and implement protocols for managing crisis-related psychology. In this regard, geopolitical risks in aviation transcend mere infrastructure vulnerability, reaching into the domains of social resilience, public trust, and emotional safety—for both passengers and staff. Only by acknowledging these multilayered interdependencies can international airports develop truly adaptive and resilient governance models in the era of global uncertainty (de Vynck, 2024).

3.2 Strategies for Managing Geopolitical Risks in International Airports

Modern international airports are confronted not only with increasing operational volumes but also with the need for swift responses to an unstable global environment. Achieving sustainable development under such conditions requires more than just risk protection — it demands the creation of a proactive and flexible management system capable of addressing global threats while leveraging internal organizational resources. One of the key areas of focus is the implementation of forecasting and scenario modeling systems. These tools enable the analysis of potential shifts in the political and economic landscape and allow for the development of response mechanisms in advance (ICAO, 2025). For example, Incheon International Airport in South Korea has developed its own geopolitical monitoring platform, which informs real-time logistical and investment decisions. Digitalization and cyber resilience have moved to the forefront. Investment in secure digital infrastructure, the use of artificial intelligence for risk monitoring, and the development of protocols for the rapid containment of cyber threats have become fundamental elements of modern airport security systems. These measures are especially important in a context where cyberattacks are employed as tools of political pressure and destabilization. Operational flexibility also plays a critical role. Airports that can swiftly adapt their flight routes, resource distribution schemes, and staffing strategies tend to demonstrate higher levels of resilience. In this context, both technological and organizational readiness are essential — including the existence of crisis management plans, trained response teams, and continuous staff education (IATA, 2022). Furthermore, international airports are strengthening diplomatic and inter-institutional cooperation by participating in information-sharing networks. These platforms enable timely responses to cross-border threats and contribute to the creation of a unified regulatory and logistical environment, reducing the fragmentation of international aviation. A distinct priority in contemporary strategies is social and psychological resilience. As recent events have shown, managing panic and anxiety among passengers and staff is just as crucial as responding to technical disruptions. The implementation of

psychological support protocols, transparent communication practices, and trust-based engagement with the public establishes a new standard for humane and effective airport management. Thus, strategies for managing geopolitical risks in aviation are becoming increasingly complex and interdisciplinary, encompassing forecasting, digital security, operational flexibility, and the resilience of human capital. Only by integrating these components can international airports maintain their competitiveness and public trust amid global upheavals.

3.3 Resilience Assessment Methods for International Airports under Geopolitical Risks

In the face of intensifying geopolitical disruptions, accurate and comprehensive assessment of airport resilience is essential for strategic management. A fragmented view leads to reactive responses, while systematic diagnostics enable proactive adaptation. A key tool in this domain is the Aviation Resilience Index (ARI) which consolidates performance across four core pillars: infrastructure redundancy, risk governance, cyber defense, and human capital capacity (see Table 1). This index helps airports benchmark vulnerabilities and track resilience improvements over time. Complementing the ARI, scenario-based stress testing simulates targeted crises—such as cyberattacks or sanctions—to evaluate operational continuity under pressure. These simulations highlight latent weaknesses and inform contingency planning.

Table 1. Components of the Aviation Resilience Index (ARI)

| Dimension | Assessed Parameters | Weight (%) |
|------------------------|--|------------|
| Infrastructure | Backup power supply, redundant systems, alternative runways | 25% |
| Risk Management | Crisis protocols, scenario planning, emergency response training | 25% |
| Cybersecurity | Data protection, AI-based monitoring, response time to digital threats | 25% |
| Human Capital | Staff support programs, internal communication, adaptability and readiness | 25% |

Source: adapted by the author

To capture real-time efficiency, airports deploy Key Performance Indicators (KPIs) measuring metrics such as flight retention, response speed, passenger satisfaction, and recovery time (see Table 2). These metrics transform abstract risk into measurable performance thresholds. Critically, the human dimension is evaluated through structured perception audits, gauging psychological readiness, institutional trust, and crisis communication efficiency.

Table 2. Key Performance Indicators (KPI) For Geopolitical Resilience of Airports

| Indicator | Unit | Acceptable Threshold |
|--|--------------------|----------------------|
| Flight Retention During Crisis | Percentage (%) | $\geq 85\%$ |
| Response Time to Threat | Hours | ≤ 2 hours |
| Passenger Satisfaction During Crisis | Index (scale 1–10) | ≥ 7.5 |
| Recovery Time After Operational Failure | Days | ≤ 3 days |

Source: adapted by the author

These insights often reveal soft vulnerabilities that infrastructure-focused assessments may overlook. Together, these methods form an integrated framework for diagnosing, comparing, and strengthening resilience strategies across international hubs—anchoring long-term adaptability in a volatile geopolitical landscape.

4. DEVELOPMENT OF A STRATEGIC RESILIENCE MODEL FOR INTERNATIONAL AIRPORTS UNDER GEOPOLITICAL INSTABILITY

4.1 Model Components

The development of a strategic resilience model aims to ensure the uninterrupted operation of airports amid geopolitical and economic challenges. Unlike generic crisis management plans, this model considers the specific characteristics of the aviation sector, its high dependence on international partners, and the complexity of its infrastructure. The model comprises four interrelated components, each addressing a distinct set of tasks while collectively forming an integrated protection framework.

4.1.1 Preventive Monitoring - comprehensive set of measures for early threat detection. It involves continuous analysis of political and economic conditions, monitoring of news flows, the use of satellite data, and information exchange through international aviation networks. This approach minimizes the time between the emergence of a threat and its registration in the system.

4.1.2 Flexible Operational Management – the ability to rapidly restructure processes in response to changes in the external environment. This may include rerouting flights, using alternative air corridors, expediting agreements with partners, or reallocating resources between terminals. The effectiveness of this component depends on pre-developed response scenarios and the authority of managers to apply them swiftly.

4.1.3 Social and Human Resilience - preparing staff to operate under uncertainty. In addition to standard briefings, this involves simulation-based drills, psychological support, development of stress management skills, and fostering a culture of rapid adaptation. Such measures reduce the risk of errors and disorganization in critical situations.

4.1.4 International Integration - systematic collaboration with foreign airports, aviation alliances, and relevant organizations. It includes participation in joint exercises, signing mutual assistance agreements, and standardizing procedures. This cooperation format enables quick access to resources and information essential for sustaining operations during crises. All components operate in close interconnection: information obtained during monitoring directly informs management decisions; staff readiness enhances the effectiveness of flexible operations; international integration expands the range of response capabilities. To objectively assess the level of resilience, a set of criteria is applied, covering economic, infrastructural, and organizational parameters (Table 4).

Table 4. Criteria and Key Components of the Strategic Resilience Model

| Group Component | Evaluation Criterion | Example of Application |
|---|--|--|
| Economic | Cost-to-benefit ratio | Cost analysis and assessment of prevented losses |
| Infrastructural | Reserve capacity, technical condition | Availability of backup terminals, compliance with ICAO |
| Preventive Monitoring | Speed of threat detection and information flow | Satellite monitoring, data analytics |
| Flexible Management | Response time to external changes | Flight rerouting, activation of alternative routes |
| Social & Human Resource Resilience | Level of staff preparedness | Stress management, simulation-based training |
| International Integration | Depth of cooperation with partners | Joint drills, international agreements |

Source: adapted by the author

4.2 Practical Implementation of the Resilience Model and Its Limitations

Building on the strategic framework presented in Section 3, the proposed resilience model for airports operating under geopolitical risks transitions from a conceptual design to the realm of practical application. This shift from theory to implementation inevitably reveals both the strengths and vulnerabilities of the system. Recognizing these constraints during the planning stage is essential to ensure that the model remains viable not only under stable conditions but also during periods of acute crisis.

The following section presents an analysis of the model’s key limitations along with concrete managerial solutions to address them.

5. MANAGERIAL SOLUTIONS

5.1 Key Limitations and Managerial Solutions

5.1.1 High Implementation Costs

The introduction of predictive analytics, integrated digital platforms, and international coordination networks requires significant capital investment. For airports with moderate passenger flows, the return on investment may be delayed. **Solution:** Implement the model in phases, starting with the most critical modules—passenger flow forecasting and management. Funding can be secured through national transport security programs, ICAO grants, and joint projects with airlines and logistics operators.

5.1.2 Complexity of International Coordination

Political disagreements, regulatory differences, and infrastructural incompatibilities make it challenging to establish a fully functional global mutual assistance network. **Solution:** Begin with regional agreements between 3–5 strategically interconnected airports. Use existing ICAO standards as the foundation for interaction protocols to minimize delays in regulatory harmonization.

5.1.3 Increased Cybersecurity Risks

Greater digitalization of processes raises the risk of cyberattacks capable of disrupting airport operations. **Solution:** Divide IT infrastructure into isolated segments (operational systems and public services) so that an attack on one segment does not paralyze the rest. Establish long-term contracts with independent cybersecurity centers for annual penetration testing and system updates.

5.1.4 Dependence on External Suppliers

Reliance on foreign-made equipment and software creates vulnerability in the event of sanctions or supply chain restrictions. **Solution:** Choose solutions with open architecture (open API) to enable rapid integration of alternative suppliers. Maintain a strategic reserve of equipment and communication channels to ensure 6–12 months of autonomous operation.

5.1.5 Organizational Resistance

Staff may be reluctant to adopt new technologies and standards, particularly in the absence of visible short-term benefits. **Solution:** Implement a pilot project in one terminal with a team open to innovation, using the results as an internal case study. Introduce incentive programs—bonuses, career opportunities, and formal recognition—for employees actively engaged in the transformation process.

5.2 Integrated Approach: From Concept to Action

Phased implementation, regional cooperation, strengthened cybersecurity, diversified supply chains, and proactive change management transform the resilience model from a theoretical framework into

an operational tool. This ensures that, when faced with geopolitical instability, an airport can act not merely reactively but proactively maintaining passenger services, cargo flows, and strategic partnerships with minimal operational compromise.

6. CONCLUSIONS

The proposed strategic resilience model for airports operating under geopolitical risks integrates four essential management pillars — preventive monitoring, flexible operational control, social and human resilience, and international cooperation — into a cohesive system designed for both rapid response and long-term adaptation. The findings of this research highlight several notable contributions:

- the integration of advanced digital forecasting and traffic management tools enhances planning precision in volatile environments;
- the establishment of regional and international cooperation frameworks accelerates the exchange of critical information and resources during crises;
- targeted staff development programs and incentive-based engagement strategies increase organizational readiness for operational adjustments;
- diversified supply chains and segmented IT infrastructures reduce exposure to sanctions, cyber threats, and logistical disruptions.

Nevertheless, the model presents certain challenges, including substantial implementation costs, the complexity of cross-border coordination, dependency on external suppliers, and potential organizational resistance. The proposed mitigation strategies — phased implementation, leveraging regional alliances, adopting open technological standards, and deploying comprehensive cybersecurity measures — address these barriers and strengthen the feasibility of adoption.

Future research directions include:

- conducting quantitative assessments of the model’s economic and operational efficiency across various airport categories;
- refining international cooperation protocols with consideration of national regulatory frameworks;
- developing advanced simulation platforms for scenario-based resilience testing.

Overall, the model moves beyond a theoretical framework to offer a practical, scalable solution for enhancing the resilience of airports in the face of complex geopolitical challenges, ultimately safeguarding passenger services, cargo operations, and the stability of the global aviation network.

Table 3. Integrated Resilience Model for Airports

| Model Level | Components | Objective |
|--|---|---|
| Preventive Monitoring | Scenario planning, digital analytics, early warning systems | Early detection of emerging threats |
| Flexible Operational Management | Backup routes, autonomous processes, logistics diversification | Reducing dependency and increasing adaptability |
| Social and Human Resilience | Psychological preparedness, staff support, internal communication | Enhancing stress resistance and reducing panic responses |
| International Integration | Participation in global networks, standardization, data exchange | Strengthening collective security and reducing systemic fragmentation |

Source: adapted by the author



Figure 1. Implementation Pathway of the Integrated Resilience Model Strategic Model

Source: adapted by the author

REFERENCES

- Alam, M., A., Banna, H., Alam, A., W., Bhuiyan, M., B., U. & Moktar, N., B. (2024). *Climate change and geopolitical conflicts: The role of ESG readiness. Journal of Environmental Management, 353*, 120284. <https://doi.org/10.1016/j.jenvman.2024.120284>.
- Bloch, J., H., Janko, K., Thessen, T., Jensen, O., B. & Lassen, C. (2021). *Not all hubs are made equal: A case study of airport governance in Europe. European Urban and Regional Studies, 28*(3), 241–262. <https://doi.org/10.1177/0969776421998727>.
- Chernii, E., V. (2024). *International armed conflicts and their impact on aviation safety. Uzhhorod National University Herald. Series: Law, 4*(85), 351–355. <https://doi.org/10.24144/2307-3322.2024.85.4.52>.
- de Vynck, A. (2024). *The human aspect of crisis management: Evaluating human errors as reasons of technical failure for efficient prevention and resolution* (Master's thesis, Charles University, University of Glasgow, & Dublin City University). *DSpace at Charles University*. Retrieved from: <https://dspace.cuni.cz/bitstream/handle/20.500.11956/197750/120482781.pdf?sequence=1>.
- Florida-Benítez, L. (2024). *Identifying and classifying cyberattacks on airports. Cyber Security: A Peer-Reviewed Journal, 8*, 63–79. <https://doi.org/10.69554/TWHW5595>.
- IATA. (2022). *Cyber threats in aviation: A growing challenge*. Retrieved September 3, 2025, from <https://www.iata.org/en/programs/security/cyber-security/>.
- International Civil Aviation Organization. (n.d.). *Aviation cybersecurity. International Civil Aviation Organization*. Retrieved September 2, 2025, from <https://www.icao.int/aviation-cybersecurity>.

- International Civil Aviation Organization. (2025). *ICAO enhances global aviation safety and security framework*. Retrieved September 3, 2025, from <https://www.icao.int/news/icao-enhances-global-aviation-safety-and-security-framework>.
- International Civil Aviation Organization. (2023). *Annual report of the Council to the Assembly 2023*. Retrieved September 6, 2025, from <https://www.icao.int>.
- Lee, H., Kim, E. & Park, D., H. (2025). *Insights from the Incheon Airport case in South Korea: Balancing public safety and individual rights with global scalability analysis*. *Humanities and Social Sciences Communications*, 12, 1104. <https://doi.org/10.1057/s41599-025-05411-9>.
- OECD. (2020). *Economic sanctions and airport development*. Retrieved September 2, 2025, from: https://www.oecd.org/en/publications/oecd-economic-policy-papers_2226583x.html.
- Ren, Z. (2024). *Adaptation and mitigation measures for climate change in airport sustainability* (Bachelor's thesis, Haaga-Helia University of Applied Sciences). Theseus. Retrieved from <https://urn.fi/URN:NBN:fi:amk-202404126382>.
- 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>.
- UK Government. (2025). *National risk register 2025*. Retrieved September 5, 2025, from: https://assets.publishing.service.gov.uk/media/67b5f85732b2aab18314bbe4/National_Risk_Register_2025.pdf.