**Dr. Öğr. Üyesi**
**Kayser NASRAT**
*İbni Haldun Üniversitesi, Hukuk Fakültesi*
*Ibn Haldun University, Faculty of Law*
*İstanbul, TÜRKİYE*
*qaiser.nasrat@ihu.edu.tr*
*https://orcid.org/0000-0003-4676-8122*
*DOI: 10.70011/kahd.1826612*

# CYBERATTACKS ON AVIATION INFRASTRUCTURE: ANALYZING INCIDENTS AND ASSESSING FUTURE RISKS

*Havacılık Altyapısına Yönelik Siber Saldırılar: Olaylar ve Gelecekteki Riskler*

## Makale Bilgisi | Article Information

Makale Türü / Article Type:
Araştırma Makalesi / Researh Article
Geliş Tarihi / Date Received: 19/11/2025
Kabul Tarihi / Date Accepted: 13/01/2026
Yayın Tarihi / Date Published: 31/01/2026
Yayın Sezonu / Pub Date Season: Ocak / January
Cilt/Volume: 4
Sayı/Issue: 1

## Atıf | Citation

Nasrat, Kayser, "CyberAttacks on Aviation Infrastructure: Analyzing Incidents and Assessing Future Risks". *Karatekin Hukuk Dergisi* 4, sy. 1 (Ocak 2026): 46-61.

## Değerlendirme | Peer-Review

İki Dış Hakem / Çift Taraflı Körleme
*Double anonymized - Two External*

## İntihal | Plagiarism

Bu makale, Turnitin yazılımınca taranmıştır.
İntihal tespit edilmemiştir.
*This article has been scanned by Turnitin.*
*No plagiarism detected.*

## Etik Beyan | Ethical Statement

Bu çalışmanın hazırlanma sürecinde bilimsel ve etik ilkelere uyulduğu ve yararlanılan tüm çalışmaların kaynakçada belirtildiği beyan olunur.
*It is declared that scientific and ethical principles have been followed while carrying out and writing this study and that all the sources used have been properly cited (Kayser NASRAT).*



## Etik Bildirim | Complaints

kahd@karatekin.edu.tr

## Yayıncı | Published by

Çankırı Karatekin Üniversitesi Hukuk Fakültesi
*Çankırı Karatekin University Faculty of Law*

## Finansman | Grant Support

Bu araştırmayı desteklemek için dış fon kullanılmamıştır.
*The author(s) acknowledge that they received no external funding in support of this research.*

**Abstract**

The aviation industry's growing reliance on digital technologies has increasingly become the target of cyberattacks that can have devastating effects on safety and operational efficiency. Cybersecurity in aviation has become a top concern as regarding that cyber threats to aviation infrastructure. Cyberattacks can target operational systems of airlines, air traffic control, airport operations, data breaches, ransomware, denial-of-service (DoS) attacks, disrupt flight schedules, compromise passenger safety and expose sensitive data. A significant example of cybersecurity incident in the aviation sector is the DDoS attacks against Japan Airlines in 2024; these attacks resulted in serious disruptions to operational processes, and ticket sales and some flights had to be temporarily suspended. This recent incident highlights the fragility of aviation infrastructure and the potential for even more serious attacks in the future. Increasingly sophisticated attacks such as artificial intelligence and advanced persistent threats (APTs) require the aviation industry to adopt robust and dynamic cybersecurity strategies. These strategies should include real-time threat detection, proactive vulnerability management, and basic regulatory preparation, technical training, and international collaboration to protect global air transportation networks. This article provides an analysis of the current state of aviation cybersecurity, discusses various types of cyberattacks targeting aviation systems, analyzes major incidents, their impacts, and future risks posed by evolving cyber threats, and outlines key strategies to mitigate future risks to aviation infrastructure.

**Keywords:** Aviation Infrastructure, Aviation Safety, Cyber Attacks, Incident Analysis, Risk Assessment.

**Özet**

Havacılık altyapısına yönelik siber tehditler arttıkça havacılıkta siber güvenlik en önemli endişe haline gelmiştir. Siber saldırılar, uçuş programlarını bozmak, yolcu güvenliğini tehlikeye atmak ve hassas verileri ifşa etmek için veri ihlallerinden, fidye yazılımlarından ve hizmet reddi (DoS) saldırılarından havayollarının, hava trafik kontrolünün ve havalimanı operasyonlarının operasyonel sistemlerini hedef alabilmektedir. Havacılık sektöründeki siber saldırıların dikkate değer vaka çalışmaları arasında, önemli kesintilere neden olan ve bazı uçuşları ve bilet satışlarını geçici olarak askıya alan 2024'teki Japan Airlines'a yönelik DDoS saldırıları yer almaktadır. Bu son olay, havacılık altyapısının kırılganlığını ve gelecekte daha da ciddi saldırılar olasılığını vurgulamaktadır. Yapay zeka ve gelişmiş kalıcı tehditler (APT'ler) gibi giderek daha karmaşıklaşan saldırılar, havacılık sektörünün sağlam ve dinamik siber güvenlik stratejileri benimsemesini gerektiriyor. Bu stratejiler, gerçek zamanlı tehdit tespiti, proaktif güvenlik açığı yönetimi ve temel mevzuat hazırlığı, teknik eğitim ve küresel hava taşımacılığı ağlarını korumak için uluslararası iş birliğini içermelidir. Bu makale, havacılık siber güvenliğinin mevcut durumu, havacılık sistemlerini hedef alan çeşitli siber saldırı türleri, yaşanan olaylar, bunların etkileri ve gelişen siber tehditlerin oluşturduğu gelecekteki riskleri analiz eder ve havacılık altyapısına yönelik gelecekteki riskleri azaltmak için temel stratejileri ana hatlarıyla belirlemektedir.

**Anahtar Kelimeler:** Havacılık Altyapısı, Havacılık Emniyeti, Siber Saldırılar, Olay Analizi, Risk Değerlendirmesi.

## EXTENDED ABSTRACT

The aviation sector is an integral part of the global economy and ease of transportation, connecting people, goods, and services across vast distances. However, like many other sectors, aviation has become a major focus for policymakers, companies, and security experts, making it increasingly vulnerable to cyber threats. The aviation sector is a complex network of interconnected systems, ranging from air traffic control and flight management systems to airport operations, baggage handling, and passenger services. These systems work in a highly coordinated manner to ensure the safety, security, and efficiency of air travel. However, the rapid advancement of technology and the increasing reliance on digital systems have opened up new ways for malicious actors to target aviation infrastructure. Cybersecurity in aviation is not limited to preventing financial fraud or protecting passenger data; it is also important to ensure the physical safety of passengers, prevent disruptions to operations, and prevent threats such as cyber terrorism. The consequences of a cyberattack in this area can be catastrophic, leading not only to financial losses but also to potential loss of life, jeopardizing national security, and damaging the reputation of airlines, airports, and even entire countries. In practice, there are many cyberattacks targeting the aviation sector. One of the earliest known cyberattacks occurred in 2001, when a hacker successfully infiltrated the computer system of a major airline, disrupting flight schedules. However, as aviation infrastructure has become more digital and interconnected, the most notable cases have occurred in the last decade. For example, an incident occurred in 2015, when United Airlines' flight control system was breached, forcing the airline to temporarily ground its fleet. The cyberattack exploited vulnerabilities in the airline's system, highlighting the critical need for strong cybersecurity measures in flight operations. Another high-profile attack occurred in 2020, when cybercriminals targeted the airline industry with phishing scams, data breaches, and ransomware attacks, exposing the personal data of millions of passengers. These events highlighted the expanding threat landscape in the aviation industry and the increasing risk to data privacy. The increasing reliance on interconnected digital systems for navigation, communication, and control systems in aviation makes the industry particularly vulnerable to cyberattacks. ATC systems are critical to the safety of aircraft operations. These systems rely on satellite communications and radar, which, if compromised can lead to catastrophic consequences such as aircraft being rerouted or downed. Cyberattacks targeting ATC systems can cause significant delays or mid-air collisions and aircraft crashes. In addition, modern aircraft are equipped with complex avionics systems that include navigation, communication, and tracking functions. cyber offenders targeting these systems can manipulate critical flight parameters, creating security concerns. Airport infrastructure relies on interconnected systems for passenger management, baggage handling, check-in, and security. A cyberattack on airport infrastructure can disrupt operations, delay flights, and compromise passenger safety. The aviation supply chain includes manufacturers, maintenance providers, and third-party vendors. By targeting vulnerabilities in these systems, cyber offenders can introduce malware or sabotage aircraft components, leading to mechanical failures or other operational issues. Aviation companies also face insider threats, including employees with access to critical systems. Insider threats, combined with social engineering tactics, make the aviation industry an attractive target for cybercriminals looking to gain financial gain. In addition to these threats, as the aviation industry continues to evolve with the rise of artificial intelligence (AI), the Internet of Things (IoT), and 5G technologies, the future risks of cyberattacks are expected to increase in both scale and sophistication. Some of the risks that arise from these technological advances include: As AI systems become more integrated into aviation infrastructure, they will become targets for attackers looking to exploit vulnerabilities. AI-enabled attacks can automate large-scale cyberattacks and adapt in real time to bypass traditional security systems. As the aviation industry increasingly adopts IoT devices for real-time data sharing and monitoring, cyber attackers will have more entry points into aviation systems.

The multitude of connected devices across airports, airlines, and aircraft will rise the attack surface and open up new vulnerabilities. Aviation infrastructure, especially strategic airports and airline operations, is a high-value target for nation-state actors. Potential risk for cyberwarfare aimed at disrupting transportation systems or gaining geopolitical influence is a growing concern for national security. Cybercriminals are increasingly using ransomware to extort companies by disrupting operations and demanding financial compensation to return to normal. As seen in other industries, ransomware attacks in aviation can cause operational disruptions and financial losses. Attacks on the global aviation supply chain, from aircraft manufacturers to service providers, can have cascading effects across the industry. Given the interconnectedness of various actors, even a small breach in one part of the supply chain can disrupt operations on a global scale. To mitigate the growing risks of cyber threats, aviation stakeholders (governments, airlines, airports, manufacturers, and service providers) must take a proactive and collaborative approach.

## INTRODUCTION

In recent years, the aviation sector has been increasingly integrating digital technologies for global connectivity and economic growth. While this integration provides many advantages to the aviation sector, it is also exposed to cyber attack threats. These threats cover all services that involve air travel operations, from airports, air traffic control towers, airline communication networks and flight management systems, passenger check-in and information to airline reservations. Cybercriminals are developing various techniques to carry out cyber attacks by taking advantage of vulnerabilities in the interconnected systems of these aviation services. For example, Japan Airlines (JAL) was subject to various cyber attacks between 2019 and 2024. As a result of these attacks, the personal data of nearly 100 thousand passengers was compromised, advanced phishing techniques were used to access internal systems, and some domestic and international flights were delayed. Although these cyber attacks did not seriously affect flight operations, the incident raised serious concerns about the vulnerability of airline IT systems to social engineering attacks.[1] Additionally, the aviation sector may be exposed to various cyber threats such as malware and ransomware, phishing, Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks.

The increasing frequency and complexity of cyberattacks on aviation systems necessitate a closer examination of their future dangers and the serious risks they pose to public safety. In other words, while the aviation sector is being modernized through digital transformations such as the integration of Artificial Intelligence (AI), the Internet of Things (IoT) and automation, it is lacking and lagging behind in protecting against emerging cyber threats.

This study aims to answer the following fundamental research questions: how do cyberattacks targeting aviation infrastructure differ in terms of threat type, operational implications, and future risk potential? How can these risks be systematically categorized from a cybersecurity and aviation safety perspective?

Unlike the existing literature, which focuses solely on technical descriptions or individual event definitions, this article proposes a unique analytical risk classification framework by examining significant cyber incidents in the aviation sector using a qualitative and comparative

[1] "Major Cyber Attack Disrupts Holiday Season Flights at Japan Airlines," **Euro News**, December 26 2024, https://www.euronews.com/business/2024/12/26/major-cyber-attack-disrupts-holiday-season-flights-at-japan-airlines/, Date of Access: 10.04.2025.

case analysis method. The study aims to surpass descriptive narratives by systematically categorizing cyber threats based on attack vectors, targeted systems, and impact severity. In this respect, the research contributes to the literature by offering a structured risk assessment perspective for policymakers, regulators, and aviation safety stakeholders.

This study employs a qualitative analytical research design combining narrative literature review and comparative case study analysis. The methodology consists of three interconnected phases.

First, the study examines the major types of cyberattacks targeting aviation systems. Through a targeted literature review focusing on aviation cybersecurity, critical infrastructure protection, and cyber risk assessment, academic papers, international organization reports (including ICAO and Eurocontrol), and regulatory documents were analyzed. This phase provides insights into how significant cyberattacks disrupt aviation operations and highlights key lessons learned from past events.

Second, selected cyberattack incidents affecting aviation infrastructure are analyzed using a qualitative case study approach. These cases were selected based on their direct impacts on aviation operations or security, the public availability of reliable incident data, and their relevance to contemporary digital aviation systems. This phase specifically examines the consequences of cyberattacks, including operational disruption and financial loss, security concerns, reputational damage, and erosion of passenger confidence. Thirdly, the identified cyber threats were systematically categorized using a qualitative risk classification framework based on three dimensions: attack type, affected aviation subsystem, and the level of operational and security impact. At this stage, particular emphasis was placed on emerging threats posed by advanced technologies such as artificial intelligence and autonomous systems. Rather than presenting a quantitative risk score, the study offers a conceptual risk assessment, evaluates the effectiveness of existing policies and regulatory measures, and develops recommendations to enhance the resilience of aviation systems against future cyberattacks. This methodological approach goes beyond descriptive reporting, generating analytical insights into the evolving cybersecurity risks facing global aviation infrastructure.

## I. CYBER ATTACKS ON AVIATION INFRASTRUCTURE

Bir Cyberattack is defined as planned and coordinated attacks on the information and communication systems and critical infrastructures of targeted individuals, institutions, organizations and public institutions.[2] Another definition is that the concept of cyber threat is any type of cyber attack that will destroy the security of individual or institutional data in the cyberspace. According to this definition, the most fundamental feature that distinguishes cyber threats from other classical threats is that threats emerge in the cyberspace. It is extremely difficult to predict threats that emerge in the cyberspace and to take precautions against these attacks. Cyber attacks can be carried out anywhere and at any time. Thus, the fact that these threats do not

[2] Aslay, Fikret, "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi", **International Journal of Multidisciplinary Studies and Innovative Technologies,** v. 1, no. 1, 2017, p. 24-28.

have a central structure also brings uncertainties. In this sense, the source of the threat can be any individual, group, terrorist organization or state.[3]

There are three dimensions that lead to the emergence of cyber threats:[4]

1- Weaknesses in the design of the Internet (the addressing system, the fact that most of the systems that run the Internet are open and unencrypted, the ability to distribute malware, and the Internet being a large decentralized network),

2- Errors in hardware and software,

3- Online access to critical systems.

The low cost of cyberattacks makes them a very attractive option for attackers. However, they have devastating effects such as suppressing states, weakening authority, engaging in subversive activities, disclosing secret information of states, seizing systems such as electricity and transportation in the country, and stopping operations.[5]

One of the most important sectors targeted by cyber attacks is the aviation sector. The aviation sector consists of a large and complex network of systems including airlines, airports, flight operations, air traffic control, airport security systems, passenger data systems, aircraft manufacturers and regulators. While these systems increase operational efficiency, passenger comfort and general safety in aviation by integrating with technological advances today, they have also become the primary target of cyber attacks. Cyber attacks targeting the aviation sector can lead to flight delays, data theft, manipulation, flight cancellations and even serious accidents.

The Airport Managers Association has divided cyber threats into three groups:[6]

1- Renewable Information Technology systems,

2- Theft and fraud that cause direct financial losses for airlines, airports and passengers,

3- Terrorism.

The division of cyber threats into these three main groups allows for a more systematic assessment of the security risks of the aviation sector. Renewable information technology systems generally include threats that aim to access critical data by exploiting cybersecurity gaps. Such threats can damage airport management systems and flight information, thus causing operational disruptions and security breaches.

The second group, “theft and fraud that cause direct financial losses for airlines, airports, and passengers,” focuses more specifically on financial losses. Cybercriminals can steal sensitive

[3] Kurnaz, Salim and Önen, S. Mustafa, "Avrupa Birliği’ne Uyum Sürecinde Türkiye’nin Siber Güvenlik Stratejileri", **International Journal of Politics and Security**, v. 1, no. 2, 2019, p. 82-103.

[4] Aslay, Siber Saldırı Yöntemleri ve Türkiye’nin Siber Güvenlik Mevcut Durum Analizi, p. 24-28.

[5] Gürkaynak, Muharrem ve İREN, Adem Ali, "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, C. 16, S. 2, 2011, s. 263-279.

[6] Gramatica, M. D., Massacci, F., Shim, W., Tedeschi, A., and Williams, J., "IT Interdependence and the Economic Fairness of Cybersecurity Regulations for Civil Aviation," **IEEE Security & Privacy**, v. 13, no. 5, 2015, p. 52–61.

data from ticket sales to credit card information by attacking payment systems or passenger data. This can undermine trust in the industry and lead to serious economic losses.

The third group, "terrorism," aims to damage critical infrastructure, especially through cyberattacks. Since the aviation industry is a sector that can become a target for terrorists, such threats require the implementation of both physical and digital security measures. Each of these threats indicates that cybersecurity strategies in the industry must be constantly updated and strengthened.

Kagalwalla and Churi emphasized that the growing challenges in securing cybersecurity within aviation are linked to the widespread adoption of modern ICT technologies, such as IoT, machine learning, and cloud computing, each of which brings its own vulnerabilities.[7] Furthermore, Duchamp, Bayram, and Korhani pointed out that the rising number of travelers, the construction of new, advanced airports, and the increasing complexity of modern aircraft have all contributed to a surge in cyber-attacks within civil aviation.[8] ICAO notes that the growing dependence on the integrity and confidentiality of data to optimize daily operations has heightened the risk of cyber incidents. Additionally, the rise in automation—central to the development of next-generation systems—has expanded the attack surface, creating more opportunities for threat actors to exploit, aiming to disrupt business operations and steal information for both political and financial purposes.[9]

This section will examine the types of cyber attacks targeting the aviation sector and include some case studies that have occurred to date.

### A. TYPES OF CYBER ATTACKS TARGETING AVIATION

Types of cyberattacks specifically targeting aviation vary in complexity and purpose. This section examines the primary types of cyberattacks that pose a threat to the aviation sector, addressing the methods used, vulnerabilities exploited, and potential risks to the sector.

**Malware and Ransomware Attacks:** Ransomware is an advanced persistent threat that stealthily attacks the information system of the industry. This malware tends to encrypt essential files and/or lock users out of the system, bringing the operational activities of the organization to a standstill.[10] If an airline or airport's critical systems are attacked, essential services such as flight schedules, ground handling, and baggage handling, check-in and maintenance systems can be

---

[7] Kagalwalla, N. and Churi, P. P., "Cybersecurity in Aviation: An Intrinsic Review," **in Proceedings of the 2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA)**, Pune, India, 19–21 September 2019, p. 1–6.

[8] Duchamp, H., Bayram, I., and Korhani, R., "Cyber-Security, a New Challenge for the Aviation and Automotive Industries," **in Seminar in Information Systems: Applied Cybersecurity Strategy for Managers**, 2016, p. 1–4. https://blogs.harvard.edu/cybersecurity/files/2017/01/Cybersecurity-aviation-strategic-report.pdf/, Date of Access: 12.03.2025.

[9] Security and Facilitation Strategic Objective: Aviation Cybersecurity Strategy, **International Civil Aviation Organization (ICAO)**, 2019, https://www.icao.int/cybersecurity/Documents/AVIATIONCYBERSECURITYSTRATEGY.EN.pdf/, Date of Access: 06.03.2025.

[10] Mukhopadhyay, A. and Jaın, S., "A Framework for Cyber-Risk Insurance Against Ransomware: A Mixed-Method Approach," **International Journal of Information Management**, v. 74, 2024, p. 102724, https://doi.org/10.1016/j.ijinfomgt.2023.102724/, Date of Access: 01.15.2025.

disrupted. Swissport, the world's largest airport ground handling and cargo handling company, was targeted by ransomware hackers in 2022.[11]

**Phishing and Social Engineering:** Phishing is a form of deception technique that attackers use to fraudulently obtain sensitive information, usually about individuals and organizations.[12] In the aviation sector, phishing can target both airline employees and passengers sensitive information such as usernames, passwords, and financial details by masquerading as legitimate communications.

**Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS):** (DoS) and (DDoS) attacks are among the most common and devastating types of cyber threats faced by the aviation industry. These attacks are an attack that disrupts a website, operations or services as a result of saturating the server with a large amount of traffic.[13] In 2023, the websites of seven German airports were hit by several DDoS attacks, and these occurred one day after a major IT incident in which Lufthansa grounded its flights.[14]

### B. CASE STUDIES OF NOTABLE CYBER ATTACKS

Cyberattacks on the aviation industry are not new. In 1997, a Bell Atlantic control system[15] used for air traffic communications at Worcester Airport in Massachusetts, U.S. was breached, knocking out the telephone system at the airport for six hours, shutting down telephone services to the control tower, airport security, airport fire service, weather service, and aircraft operators. The attack also disabled the tower's main radio transmitter, a transmitter controlling the runway lights, and a printer used by controllers to track flight progress. Telephone services to 600 nearby homes were also cut off.[16]

In 2013, a significant malware attack targeted the passport control systems at Istanbul Ataturk and Sabiha Gokcen airports in Istanbul (Türkiye). The attack led to a shutdown of these systems at the departure terminals, disrupting normal airport operations. As a result, numerous flights were delayed, causing frustration for passengers and affecting the overall efficiency of

[11] "Swiss-Based Airport Services Firm Suffers Ransomware Attack," **Swissinfo**, February 4 2022, https://www.swissinfo.ch/eng/sci-tech/swiss-based-airport-services-firm-suffers-ransomware-attack/47321738/, Date of Access: 05.01.2025.

[12] Varshney, G., Kumawat, R., Varadharajan, V., Tupakula, U., and Gupta, C., "Anti-Phishing: A Comprehensive Perspective", **Expert Systems with Applications,** v. 238, 2024, p. 122199, https://doi.org/10.1016/j.eswa.2023.122199/, Date of Access: 12.03.2025.

[13] Teichmann, F. M. J., Sergi, B. S., and Wittmann, C., "The Compliance Implications of a Cyberattack: A Distributed Denial of Service (DDoS) Attack Explored", **International Cyber Law Review**, v. 4, 2023, p. 291–298, https://doi.org/10.1365/s43439-023-00090-1/, Date of Access: 12.03.2025.

[14] J. L. Hardcastle, "'Russian Hacktivists' Brag of Flooding German Airport Sites," *The Register*, February 17, 2023, https://www.theregister.com/2023/02/17/german_airport_websites_ddos/, Date of Access: 12.12.2024.

[15] Rindskopf, A., "Juvenile Computer Hacker Cuts Off FAA Tower", **Irational.org**, March 1998, http://www.irational.org/APD/CCIPS/juvenilepld.htm/, Date of Access: 12.12.2024.

[16] "Air Traffic Management: A Cybersecurity Challenge," *Eurocontrol,* 2021, https://www.eurocontrol.int/sites/default/files/2021-12/eurocontrol-atm-cybersecurity-report.pdf, 20.03.2025.

airport services.[17] The malware's impact on essential systems raised concerns about the vulnerability of critical infrastructure in the aviation sector and highlighted the growing threat of cyberattacks on air travel, prompting increased security measures and awareness in the aviation industry to prevent similar incidents in the future.

In 2018, an agency that conducted mandatory security checks on airport personnel on behalf of the Australian Government was hacked,[18] this breach resulted in the exposure of sensitive personal information of hundreds of aviation workers. This raised concerns about the breach of employee privacy, the potential misuse of information by criminals, and the vulnerability of the aviation system.[19]

In 2020, British Airways (BA) was fined £20 million for failing to protect the personal and financial information of over 400,000 customers after a cyberattack resulted in the failure to adequately secure its systems. The fine was imposed as a result of a breach of the General Data Protection Regulation (GDPR), that requires organisations to protect the personal data of everyone in the EU and uphold their privacy rights.[20]

Singapore Airlines was hit by a cyberattack that exposed the personal information of over 1.5 million passengers. Hackers gained access to customer data stored in the airline's database, including frequent flyer information, contact details and travel history. Even though no financial data was breached, passengers were compromised and were at risk of phishing attacks and identity theft. The airline had to notify affected customers and take steps to mitigate the damage.

In 2021, a software error occurred in the IT system in Birmingham, United Kingdom, which failed to detect significant discrepancies between the loadsheet and the flight plan. As a result, the aircraft's take-off mass exceeded the required weight by 1606 kg.[21]

A Distributed Denial of Service (DDoS) attack targeted JAL's network, causing delays and cancellations of multiple domestic flights during the year-end holiday season. The airline was forced to temporarily suspend same-day flight ticket sales. Customer data was not compromised and flight security was not affected in any way. However, passengers experienced significant

[17] Paganini, P., "Istanbul Ataturk International Airport Targeted by a Cyber-Attack," **Security Affairs**, 2013, https://securityaffairs.co/wordpress/16721/hacking/istanbul-ataturk-international-airport-targeted-by-cyber-attack.html/, Date of Access: 14.12.2024.

[18] Pash, C., "Cyber Security Is Being Tightened at Australian Airports After an Identity Card Data Hack", **Business Insider Australia**, July 2018, https://www.businessinsider.com.au/identity-card-data-hack-data-breach-australian-airports-2018-7/, Date of Access: 18.01.2025.

[19] Eurocontrol, Air Traffic Management A Cybersecurity Challenge.

[20] "ICO fines British Airways £20m for data breach affecting more than 400,000 customers", **Information Commissioner's Office**, October 2020, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[21] Claburn, T., "Airline Software Super-Bug: Flight Loads Miscalculated Because Women Using 'Miss' Were Treated as Children", **The Register**, April 8, 2021, https://www.theregister.com/2021/04/08/tuisoftwaremistake/, Date of Access: 03.03.2025.

confusion and inconvenience due to multiple flight cancellations and multiple minutes of delay during the busy travel period.[22]

These incidents underscore the critical need for robust cybersecurity measures across all sectors of the aviation industry. Implementing comprehensive security protocols, conducting regular vulnerability assessments, and creating a culture of cybersecurity awareness are essential to reduce the risks associated with cyberattacks.

## II. ASSESSING FUTURE RISKS AND STRATEGIES

The purpose of cybersecurity risk assessment is to evaluate risk levels by identifying potential cyber threats that have a negative impact on aviation systems, determining their probability of occurrence, and their potential impact on aviation operations, infrastructure, and other impacts.[23] The increasing complexity of cyber risks to aviation infrastructure due to the development of digital technologies has made combating these threats a critical necessity.

The concept of "smartness" in the civil aviation sector is based on concrete examples of digitalization, including the integration of IoT-enabled devices and sensors into physical systems, the use of blockchain, artificial intelligence, cloud technology and big data to maintain service quality. The aim of the aviation is to provide enhanced customer experience and optimum services in a reliable and sustainable manner by ensuring growth, operational efficiency, security and safety optimization.[24] This situation is escalating the threat of cyberattacks, exposing the aviation industry to numerous risks.

Among the primary future risks, the emergence of technologies such as IoT and AI in aviation creates new vulnerabilities. IoT devices integrated into various operational systems can be exploited by cyber attackers to gain access to critical infrastructure. In addition, AI systems used for flight optimization and maintenance can be misused to cause outages. Koroniotis et al. argue that the developments in the integration of IoT devices in infrastructures in the aviation sector are leading to the emergence of smart airports. The aim of these developments is to provide an excellent customer experience by increasing the efficiency of daily operations and to strengthen the reliability and control of services.[25] In addition, Zamorano et al. have highlighted technologies such as Radio Frequency Identification (RFID), geolocation, immersive realities, biometric systems and robotics as important components in the next generation smart airport environments.[26]

---

[22] "Japan Airlines Systems Back to Normal After Cyberattack Delayed Flights", **Reuters**, December 26 2024, https://www.reuters.com/technology/cybersecurity/japan-airlines-systems-hit-by-cyberattack-ntv-says-2024-12-26/, Date of Access: 12.01.2025.

[23] Elmarady, Ahmed Abdelwahab and RAHOUMA, Kamel, "Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment", **Digital Object Identifier,** v. 9, 2021.

[24] Lykou, Anagnostopoulou and Gritzalis, Smart airport cybersecurity: Threat mitigation and cyber resilience controls, 19.

[25] Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., and Janicke, H., "A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports", **IEEE Access**, v. 8, 2020, p. 209802–209834.

[26] Zamorano, M., Fernández-Laso, M. C., and Curiel, J. de Esteban, "Smart Airports: Acceptance of Technology by Passengers", **Cuadernos de Turismo,** v. 45, 2020, p. 567–570.

Koroniotis et al. suggest that IoT systems and devices are prone to APT-led attacks due to hardware limitations, software bugs, or misconfigurations. Machine learning-based and AI-enabled techniques are proposed as a potential solution to deal with the challenges of IoT-based cyberattacks. A strong cyber defense framework in smart airports is critical to ensure the reliability of services, prevent disruptions and cancellations, and loss of sensitive data.[27]

According to Wolf et al., IoT, electronic data interchange and digital networking play a critical role in improving the efficiency of the industry's in-flight operations. It is therefore important to conduct a review of the role and potential of digitally enabled devices in the development of digital networking and electronic data interchange in future e-enabled aircraft, as well as their associated vulnerabilities, attack surfaces, and possible preventive measures.[28]

Mitigating and eliminating these future risks requires a multi-faceted approach. Therefore, strengthening the resilience of aviation infrastructure is critical. This starts with upgrading and replacing legacy systems in the aviation sector with modern systems. It is essential to re-equip airports and airlines with updated security protocols and provide regular software updates. Additionally, adopting cybersecurity frameworks such as the NIST Cybersecurity Framework will help aviation stakeholders establish a robust risk management approach.

Additionally, strengthening public-private collaboration is essential. Governments should work closely with the aviation industry to develop and implement cybersecurity regulations and standards. International collaboration plays a critical role in combating cross-border cyber threats, as cybercriminals often operate in regions with less stringent laws. Establishing global norms for aviation cybersecurity and ensuring compliance will help create a safer environment for all stakeholders.

Another important way to reduce future risks is to improve threat detection and defense capabilities. The aviation industry needs to invest in advanced cybersecurity technologies such as intrusion detection systems (IDS), as well as anomaly detection and real-time threat intelligence sharing. Systems must be continuously monitored for anomalous activity using artificial intelligence, and potential cyber threats must be detected and responded to in a timely manner.

In addition, human factors are also extremely important. Human error is considered one of the weakest links in cybersecurity. Therefore, education and awareness programs should be a key element of any strategy to combat cyber threats. Airline and airport personnel, from ground crew to managers, should be trained on cybersecurity best practices, such as recognizing phishing attacks, managing passwords securely, and understanding the importance of system updates. Additionally, organizations should conduct regular cybersecurity drills and simulations to ensure that personnel can effectively respond to cyber incidents.

In conclusion, the risks related to cyber attacks on aviation infrastructure are serious, but not impossible to overcome with the right strategies. Investment in advanced and smart technologies, national and international legislation, encouragement of international cooperation,

---

[27] Koroniotis, Moustafa, Schiliro, Gauravaram and Janicke, Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports, 8.

[28] Wolf, M., Minzlaff, M. and Moser, M., "Information Technology Security Threats to Modern E-Enabled Aircraft: A Cautionary Note", **Journal of Aerospace Information Systems**, v. 11, 2014, p. 447–457.

and human resources training can create a durable defense against future cyber threats to the aviation sector.

## CONCLUSION

The aviation sector has also been affected by the technological developments in recent years. While it has positive effects such as travel comfort and economic growth, it has also become the primary target of cyber attacks. In other words, while continuing to witness advances in technology, the aviation sector's dependence on interconnected digital systems makes it vulnerable to exploitation by malicious actors. These attacks, which can range from data breaches to large-scale disruptions of operations, pose a significant threat to the security, safety and operational continuity of aviation systems worldwide. In addition, aviation infrastructure, including flight control systems, ticketing and passenger information systems, baggage handling and air traffic management, are increasingly becoming the target of cyber attacks. Cyber attacks can disrupt any of these critical systems and lead to serious consequences such as flight delays, data theft, loss of operational control, reputational damage to airlines and airports, major financial losses, route changes and even aircraft collisions and crashes in the air.

Cyber attacks on aviation infrastructure in recent years have also highlighted the vulnerability of this sector. The 2015 cyberattack on United Airlines is an example of how vulnerabilities in the airline’s flight management systems could have allowed hackers to access sensitive data and systems onboard. Similarly, a major cyberattack was carried out on Japanese Airlines in 2024. The attack disrupted the airline’s operations and caused serious delays in flight schedules.

The aviation industry’s increasing reliance on artificial intelligence and IoT systems, in particular, presents new challenges. In addition, future risks include APTs that remain undetected for long periods of time, sophisticated state-sponsored cyberattacks, and vulnerabilities originating from third-party vendors protecting key systems. A multi-layered cybersecurity strategy is essential to mitigate these risks. First, cooperation between governments and private sector organizations should be strengthened to take effective measures against cyberattacks. Also, the aviation industry should adopt a proactive rather than reactive approach to cyber defense by adopting advanced encryption, continuous monitoring, and regular cybersecurity audits. Cybersecurity training should be provided to personnel working in the aviation sector. Comprehensive national and international legal regulations should be developed for the aviation sector. Integrating AI and blockchain technologies into aviation security systems can play a role in detecting anomalies, suspicious activities, and improving the security of data processing.

The findings of this study parallel the existing literatüre, arguing that aviation systems have become more vulnerable to cyber threats due to increasing digital interdependence. However, unlike previous studies that focused solely on technical vulnerabilities or isolated incidents, this paper highlights the systemic nature of aviation cyber risk by identifying the level of institutional preparedness and the fragmented structure of the regulatory framework as key risk-increasing factors. In this context, the proposed qualitative risk classification framework bridges the gap between descriptive incident reporting and analytical risk assessment by enabling cross-case comparison and prospective risk identification.

The research results also predict that future aviation cybersecurity risks will be shaped by APTs, supply chain vulnerabilities, and the integration of AI-driven systems. This not only confirms concerns voiced by international organizations such as ICAO but also expands upon them by examining them through a structured analytical lens. From a policy perspective, these

findings underscore the need for the creation of harmonized international cybersecurity standards, the introduction of mandatory risk controls for aviation stakeholders, and the strengthening of public-private sector cooperation. Future research could further enhance the cyber resilience strategies of aviation infrastructure by enriching this framework with quantitative risk modeling or sector-specific simulations.

## REFERENCES


"Air Traffic Management: A Cybersecurity Challenge", **Eurocontrol**, 2021, https://www.eurocontrol.int/sites/default/files/2021-12/eurocontrol-atm-cybersecurity-report.pdf, 20.03.2025.

Aslay, Fikret, "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi", **International Journal of Multidisciplinary Studies and Innovative Technologies,** v. 1, no. 1, 2017, p. 24-28.

Claburn, T., "Airline Software Super-Bug: Flight Loads Miscalculated Because Women Using 'Miss' Were Treated as Children", **The Register**, April 8, 2021, https://www.theregister.com/2021/04/08/tuisoftwaremistake/, Date of Access: 03.03.2025.

Duchamp, H. / Bayram, I. / Korhani, R., "Cyber-Security, a New Challenge for the Aviation and Automotive Industries," **in Seminar in Information Systems: Applied Cybersecurity Strategy for Managers**, 2016, p. 1–4. https://blogs.harvard.edu/cybersecurity/files/2017/01/Cybersecurity-aviation-strategic-report.pdf/, Date of Access: 12.03.2025.

Elmarady, Ahmed Abdelwahab / Rahouma, Kamel, "Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment", **Digital Object Identifier,** v. 9, 2021.

Haass, J. / Sampigethaya, R. / Capezzuto, V., "Aviation and Cybersecurity: Opportunities for Applied Research", **TR News**, v. 304, 2016, p. 39.

Freiherr, G., "Will Your Airliner Get Hacked?", **Smithsonian Magazine**, 2021, https://www.smithsonianmag.com/air-space-magazine/will-your-airliner-get-hacked-180976752/, Date of Access: 15.03.2025.

Gramatica, M. D. / Massacci, F. / Shim, W. / Tedeschi, A. / Williams, J., "It Interdependence and the Economic Fairness of Cybersecurity Regulations for Civil Aviation," **IEEE Security & Privacy**, v. 13, no. 5, 2015, p. 52–61.

Gürkaynak, Muharrem / İren, Adem Ali, "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, C. 16, S. 2, 2011, s. 263-279.

Hardcastle, J. L., "'Russian Hacktivists' Brag of Flooding German Airport Sites", **The Register**, February 17, 2023, https://www.theregister.com/2023/02/17/german_airport_websites_ddos/, Date of Access: 12.12.2024.

"ICO fines British Airways £20m for data breach affecting more than 400,000 customers", **Information Commissioner's Office**, October 2020, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/.

Kagalwalla, N. / Churi, P. P., "Cybersecurity in Aviation: An Intrinsic Review," **in Proceedings of the 2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA)**, Pune, India, 19–21 September 2019, p. 1–6.

Koroniotis, N. / Moustafa, N. / Schılıro, F. / Gauravaram, P. / Janicke, H., "A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports", **IEEE Access**, v. 8, 2020, p. 209802–209834.

Kurnaz, Salim / Önen, S. Mustafa, "Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri", **International Journal of Politics and Security**, v. 1, no. 2, 2019, p. 82-103.

"Japan Airlines Systems Back to Normal After Cyberattack Delayed Flights", **Reuters**, December 26 2024, https://www.reuters.com/technology/cybersecurity/japan-airlines-systems-hit-by-cyberattack-ntv-says-2024-12-26/, Date of Access: 12.01.2025.

Lykou, G. / Anagnostopoulou, A. / Grıtzalıs, D., "Implementing Cyber-Security Measures in Airports to Improve Cyber-Resilience", **in Proceedings of the 2018 Global Internet of Things Summit (GIoTS)**, Bilbao, Spain, 4–7 June 2018, p. 1–6.

"Major Cyber Attack Disrupts Holiday Season Flights at Japan Airlines," **Euro News**, December 26 2024, https://www.euronews.com/business/2024/12/26/major-cyber-attack-disrupts-holiday-season-flights-at-japan-airlines/, Date of Access: 10.04.2025.

Mukhopadhyay, A. / Jaın, S., "A Framework for Cyber-Risk Insurance Against Ransomware: A Mixed-Method Approach," **International Journal of Information Management**, v. 74, 2024, p. 102724, https://doi.org/10.1016/j.ijinfomgt.2023.102724/, Date of Access: 01.15.2025.

Paganini, P., "Cyber Threats Against the Aviation Industry", **InfoSec Institute**, 2014, https://resources.infosecinstitute.com/topic/cyber-threats/, Date of Access: 19.09. 2024.

Paganini, P., "Istanbul Ataturk International Airport Targeted by a Cyber-Attack," **Security Affairs**, 2013, https://securityaffairs.co/wordpress/16721/hacking/istanbul-ataturk-international-airport-targeted-by-cyber-attack.html/, Date of Access: 14.12.2024.

Pash, C., "Cyber Security Is Being Tightened at Australian Airports After an Identity Card Data Hack", **Business Insider Australia**, July 2018, https://www.businessinsider.com.au/identity-card-data-hack-data-breach-australian-airports-2018-7/, Date of Access: 18.01.2025.

Rindskopf, A., "Juvenile Computer Hacker Cuts Off FAA Tower", **Irational.org**, March 1998, http://www.irational.org/APD/CCIPS/juvenilepld.htm/, Date of Access: 12.12.2024.

Security and Facilitation Strategic Objective: Aviation Cybersecurity Strategy, **International Civil Aviation Organization (ICAO)**, 2019, https://www.icao.int/cybersecurity/Documents/AVIATIONCYBERSECURITYSTRATEGY.EN.pdf/, Date of Access: 06.03.2025.

"Swiss-Based Airport Services Firm Suffers Ransomware Attack," **Swissinfo**, February 4 2022, https://www.swissinfo.ch/eng/sci-tech/swiss-based-airport-services-firm-suffers-ransomware-attack/47321738/, Date of Access: 05.01.2025.

Teichmann, F. M. J. / Sergi, B. S., / Wittmann, C., "The Compliance Implications of a Cyberattack: A Distributed Denial of Service (DDoS) Attack Explored", **International Cyber Law Review**, v. 4, 2023, p. 291–298, https://doi.org/10.1365/s43439-023-00090-1/, Date of Access: 12.03.2025.

Varshney, G. / Kumawat, R. / Varadharajan, V. /Tupakula, U., /Gupta, C., "Anti-Phishing: A Comprehensive Perspective", **Expert Systems with Applications,** v. 238, 2024, p. 122199, https://doi.org/10.1016/j.eswa.2023.122199/, Date of Access: 12.03.2025.

Wolf, M. / Mınzlaff, M. / Moser, M., "Information Technology Security Threats to Modern E-Enabled Aircraft: A Cautionary Note", **Journal of Aerospace Information Systems**, v. 11, 2014, p. 447–457.

Zamorano, M. / Fernández-Laso, M. C., / Curiel, J. de Esteban, "Smart Airports: Acceptance of Technology by Passengers", **Cuadernos de Turismo,** v. 45, 2020, p. 567–570.

Zetter, K., "Feds Say that Banned Researcher Commandeered a Plane", **Wired**, May 2015, https://www.wired.com/2015/05/, Date of Access: 15.01.2025.