International Journal of
Technology and
Systems
(IJTS)

Cybersecurity Challenges in Aviation: Safeguarding Airline Operations against Emerging Threats

Journal of Technology and Systems
ISSN: 2788-6344 (Online)
Vol. 7, Issue No. 5, pp 1 – 13, 2025
www.carijournals.org

Cybersecurity Challenges in Aviation: Safeguarding Airline Operations against Emerging Threats

Rukayat Omobolanle Ojo-Oba

https://orcid.org/0009-0000-0600-4756

Accepted: 27th June, 2025, Received in Revised Form: 14th July, 2025, Published: 23rd July, 2025

Abstract

Purpose: This research examines the impacts of cyber-security challenges on airline operations and devising ways of mitigating them.

Methodology: This research adopted an interpretivist approach, enabling consideration of cyber-security from a subjective human meaning, experiences and interpretations. As such, qualitative data was collected through document analysis from Google Scholar, Research Gate, JSTOR, Federal Aviation Administration and EUROCONTROL. 24 peer reviewed articles and journals that were published between 2010 and 2025 were used in analysis through thematic analysis.

Findings: This research found ransomware attacks, DDos, breach of confidential data, attacks due to of in-flight systems and GPS spoofing to be the most prevalent cyber-security challenges facing airlines. Although airlines have been collaborating with IT vendors and government agencies, there have been numerous instances of uncoordinated response to cybersecurity attacks. This is despite the increased ability of early detection of threats through technological advancements. This research suggests adoption of multidisciplinary response towards cyber-security issues, involving all stakeholders and focusing on addressing both the technical and the social aspects of cybersecurity.

Unique Contribution to Theory, Policy and Practice: This study has advanced the application of the socio-technical systems theory and the CIA triad in aviation cybersecurity. This demonstrated the interplay of social and technical factors in aviation cybersecurity, as well as the value of confidentiality, integrity and availability in integration of technological advancements in aviation infrastructure. The study also identified the rising nature of cybersecurity risk in aviation, raising awareness to airlines' risk management strategies. Part of the research also contributes towards the development of policies that foster collaborative efforts among stakeholders towards improving cybersecurity in aviation.

Keywords: *Cybersecurity, Aviation, Airline Operations*

1.0 Introduction

Technological advancements have led into an increase in the integration of mechanical devices with information communication technology (ICT) tools in aviation. Although this has brought about significant benefits such as streamlined and automatic operations (Haass et al., 2016), it has raised cybersecurity concerns. The effectiveness of cyber-security frameworks is becoming a challenge in aviation as e-enabled aircraft infrastructure and smart airports are increasingly being adopted. An example that depicts the nature of impacts caused by cyber-attacks is the faulty updates that were distributed to Falcon sensor software by CrowdStrike in July 2024, resulting in the crash of 8.5 million Windows systems and marking the largest outage in information technology (IT) (Moncrieff, 2025). This resulted in aviation losses, such as the up to US$550 million recorded by Delta Airlines (Amorim et al., 2025). The increased threat of cyber-attacks was also cited in a report by Eurocontrol in 2024 which concluded that there is a rise in the quantity and quality cyber-security threats in aviation (Eleimat and Őszi, 2025). The report found the main impact of cyber-attacks to be financial operations of airlines, with an estimation of losses worth billions of Euros every year (Eleimat and Őszi, 2025). Cyber-attacks are a major threat to safety and business continuity in aviation as ICT and mechanical operations continue to integrate. They can vary from high profile attacks that attract media attention, those that lead to litigious claims, or involve multiple jurisdictions. This study examines this threat of cyber-security in aviation, focusing on the safety of airline operations. It starts by examining existing literature and theories, then conducts a document analysis to develop findings and implications for theory and practice.

2.0 Purpose

The purpose of this study is to evaluate the nature and severity of cyber-security challenges in aviation, and develop mitigation strategies that can safeguard airline operations. The aviation industry plays a significant role in the global economy, acting as a gateway among countries. The integrity of the infrastructure that supports it is therefore vital, and errors can result in dire global consequences such as fatalities, theft of intelligence and intellectual property, exposure of customer information, among others (Duchamp et al., 2016; Ukwandu et al., 2022). It is evident that as the aviation industry integrates technological advancements and ICT the threat of cyber-attacks is also rising in scale and sophistication (Eleimat and Őszi, 2025). The aviation industry is rapidly adopting digital tools such as air traffic control (ATC) automation systems, in-flight entertainment networks (IFE), satellite communication systems (SATCOM), and electronic flight bags (EFBs) (Dave et al., 2022). These systems bring about efficiency in airline operations, but expose them to cyber-security vulnerabilities. For instance, IFE systems are normally connected to the internal networks of aircrafts and if there are weak integrations they can be used by attackers to gain access to more sensitive systems (Fox, 2016). Similarly, ATC systems have been targeted by denial-of-service (DDoS) attacks such as in the case of Boryspil International Airport in 2017 (Cooper et al., 2019). The need for safety in aviation is paramount and since the nature of digital integrations is evolving, there is a need for continued research on the threat of cyber-security in

aviation. This study fills this gap by contributing towards an understanding of the impacts of cyber-security challenges in aviation and identifying ways of safeguarding airline operations and mitigating threats.

3.0 Literature review

3.1 Cyber-Security Challenges in Aviation

The aviation industry has been a target of cyber-attacks over the decades, and this has only grown worse in recent times. For instance, Jeppesen (a unit of Boeing) was attacked in 2022 by a cyber-threat that wanted to access to operational planning and flight navigation tools (Greig, 2023). In 2024 another cyber-attack that lasted for days halted operations in the Port Seattle Tacoma International Airport due to disruptions of check-in, ticketing and other services (Jones, 2024). These are just but a few of the cyber-attacks that have been witnessed in aviation. These and more attacks have led to the classification of cyber-attacks into three kinds that are discussed below.

3.1.1 Operations Disruptions

The aviation industry has also been experiencing operational outages mostly due to its sophisticated IT systems (George, 2024). An example is the previously mentioned faulty software update by CrowdStrike which resulted in global disruptions like cancellation and delays of flights (Moncrieff, 2025). This shows that cyber-attacks that result in operational disruptions have a domino effect on airline operations. In the case of Delta Airlines, the faulty system update affected more than 3 million passengers and resulted in more than 7,000 flight cancellations (Amorim et al., 2025).

3.1.2 Malware and Ransomware Attacks

Malware refers to any form of malicious software that is developed to harm systems or computers. The most common type of malware attack in aviation is ransomware which locks out users and demands payment from the user to regain access, which has been reported to have up to 600% increase (*Together against threats: Advancing aviation cybersecurity through collective action*. 2025). The aforementioned Seattle Tacoma International Airport attack was a ransomware by Rhysida ransomware group (Jones, 2024). Another example is the data breach that took place in American Airlines in 2024 resulting in access of sensitive customer data (Black and Rubenov, 2025).

3.1.3 GPS Spoofing and Navigation System Attacks

GPS spoofing and navigation system attacks are normally in the form of deception to the aircraft navigation system which diverts the aircrafts' course (Simmons, 2017). These kind of attacks have been reported to have about 400% increase in the past decade and have also been used to tamper with encrypted communication systems often grounding aircrafts (Stastny and Stoica, 2022). An average of about 1500 flights were affected by GPS spoofing daily in 2024, from an average of 300 flights in 2023 (*Spirent*. 2025). These incidents mostly impacted regions like Asia, Black Sea

and Eastern Mediterranean (Eleimat and Őszi, 2025). In addition, GPS spoofing was associated with the crash of Azerbaijan Airlines Flight 8243 in 2024 (*Official Report: Foreign objects caused Azerbaijan Airlines crash*. 2025).

3.2 Theoretical Framework

3.2.1 The Confidentiality, Integrity and Availability (CIA) Triad

The CIA triad is core to the formulation of policies regarding information security in organizations. It stipulates the foundational principles in protection of electronic data; confidentiality, integrity and availability (Osazuwa et al., 2023; Samonas and Coss, 2014). The CIA triad is key in understanding the aspects of cyber-security that the aviation industry must fulfill. In this context, confidentiality entails protection of sensitive data from unauthorized access (Samonas and Coss, 2014). Integrity is concerned with maintaining the trustworthiness, accuracy and consistency of data throughout airline operations (Yee and Zolkipli, 2021). Availability involves proper maintenance of technical and hardware infrastructure systems to ensure that information is availed consistently to authorized parties (Osazuwa et al., 2023). The triad framework has been used in this study to guide the development of cyber-security policies and procedures to safeguard airline operations.

3.2.2 The Socio-Technical Systems (STS) Theory

The STS theory views organizations as comprising of interdependent sub-systems (Appelbaum, 1997). When applied in the aviation industry, this theory helps to understand the interdependence that exists between technical systems (such as ATC systems, avionics and flight management systems) and personnel (such as IT staff, engineers and pilots) which is key to the success of airline operations. The STS theory holds that the success of any organization can only be achieved if the technical and social aspects work in sync and viewed as being interdependent (Majchrzak and Borys, 2001). Thus, as the aviation sector embraces technological advancements and integrate ICT into its operations, it needs to consider the impact of social actors (such as hackers) on its operations. The failure to consider the interdependence between technical factors and social actors in aviation can introduce cyber vulnerabilities resulting from faulty interface design, human errors or organizational structure (Dave et al., 2022; Yurtseven and Buchanan, 2013). The STS is key in understanding how changes in technical aspects of airline operations can affect the entire operations in airlines.

4.0 Methodology

4.1 Research Design

This research adopted an interpretivist philosophy, which enabled the researcher to consider the research phenomenon from a subjective human meaning, experiences and interpretations (Melnikovas, 2018). As such, this research collected qualitative data which helped in documenting the nature of cyber-security threats in aviation, citing the interdependence nature of the relationship

between technical and social factors in aviation. This would not have been achieved through a positivism approach which would have required quantification of data (Houseman et al., 2004). This research also adopted an inductive approach. It started by collecting data and then moved to analyze it and develop concepts as suggested by McManners (2016).

4.2 Data Collection

The data used in this research was collected through document analysis. Document analysis entails systematic review of electronic or printed documents for interpretation in order to gain insights on a research topic (Rice et al., 2017). It was adopted due to its flexibility, cost-effectiveness and the availability of documents on cyber-security online.

The research process started with a literature review. This review gave the researcher an understanding of the research context, which led to the development of a research aim and objectives. The aim of this research was to understand the challenges of cyber-security in aviation and develop strategies that can safeguard airline operations. The following objectives were developed in order to guide the processes of data collection and interpretation:

1) To understand the most prevalent cybersecurity challenges in aviation
2) To evaluate the effectiveness of the collaborations between government agencies, airlines and IT vendors in dealing with cyber-security
3) To examine the role of emerging technologies such as blockchain and artificial intelligence (AI) in enhancing cybersecurity in the aviation industry
4) To identify measures that can enhance cyber-security in aviation

The process of document analysis started identification of databases that would be used to access peer reviewed journals on cybersecurity in Aviation. The following databases were used: Google Scholar, Research Gate and JSTOR. Other industry sources that provided valuable materials include Federal Aviation Administration and EUROCONTROL. The following search terms were used to search for materials online: “cyber-security in aviation”, “cyber-threats in aviation” and “cyber-security challenges in aviation”, “emerging technologies, cyber-security in aviation” and “stakeholder role in cyber-security in aviation”. The initial search resulted in a total of 214 potential sources. Once possible sources were identified through an online search, the researcher used an inclusion/exclusion criterion to choose the most viable ones. This started with elimination of duplicates. Secondly, the researcher only included articles that were published between 2010 and 2025 in order to gather relevant data. Thirdly, the researcher chose to use sources that were published for public use in order to maintain integrity (Wiggins and Stevens, 2016). The screening of articles resulted in identification of 24 sources which were used for data collection.

4.3 Data Analysis

The collected data was analyzed through thematic analysis, which was adopted due to its relative ease of application and deeper understanding of data (Houseman et al., 2004). The researcher

started thematic analysis by familiarizing with the data by reading through all the sources manually. The next step involved a second reading of the sources while identifying codes such as "effects of cyber-insecurity on airline operations" and "sources of cyber-insecurity in aviation". The researcher then used the codes to develop themes that aligned with the four research objectives, which guided the reporting of findings.

5.0 Findings and Discussion

5.1 The Most Prevalent Cyber-Security Threats in Aviation

This study found that cyber-security threats in aviation are on the rise are occur in various forms. To begin with, DDos are common, whereby airline systems are normally interrupted hindering operations such as check-in and ticketing (Shah et al., 2024). For instance, Vitenam Airlines experienced DDoS in 2016 which made its systems unusable and confidential customer data was shared (Kagalwalla and Churi, 2019). In addition, the aviation sector has been facing increasing ransomware attacks. According to Zalewski and Kornecki (2019), ransomware attacks often cripple airline operations including baggage handling, ticketing and air traffic control systems. Another prevalent cyber-security challenge in aviation is airline data breach. This happens when confidential data such as customer passport numbers, credit card details and names are accessed by unauthorized parties. Such breaches are prime for attackers, like in the case of British Airways whereby more than 400,000 passenger data was accessed in 2018 resulting in a £20 million fine (*British Airways fined £20M over Data Breach*. 2020). Further, the aviation industry is facing significant incidents of GPS spoofing (Alrefaei et al., 2021). Such attacks are often aimed at causing flight collisions or changing flight paths. Lastly, there are significant attacks due to vulnerabilities of in-flight systems. According to Sabillon and Bermejo (2023), cyber-attackers are increasingly targeting unpatched interconnected avionics and digital cockpits. These threats are expected to continue increasing in severity and sophistication, raising the need for industry-wide address of cyber-security (Lykou et al., 2019; Zalewski and Kornecki, 2019).

5.2 The Effectiveness of Collaboration between Government Agencies, Airlines and IT Vendors in Managing Aviation Cybersecurity

There has been an improvement in the efforts of collaborations among stakeholders in the aviation industry in their efforts against cyber-insecurity, which crucial due to the need for the social and technical systems to work together in line with STS theory (Lehto, 2020 Majchrzak and Borys, 2001). A major improvement has been the emergence of collaboration between public and private stakeholders. This is led by the view of cyber-security as a public safety issue, which has steered the collaborative efforts of both the private and the public sectors (Bergamasco et al., 2020). With formation of bodies such as the Aviation Information Sharing and Analysis Center (Aviation ISAC) which coordinates the sharing of data between government entities like the FAA, manufacturers, and airlines, there has been real-time sharing of crucial intelligence among involved parties (Faye et al., 2024).

There has also been evidence of coordinated crisis response among governments and airlines in response to cyber-attacks. For instance, the European Union Aviation Safety Agency (EASA) has developed uniform protocols that are followed by EU members through its Cybersecurity Action Plan 2021 (Jaber et al., 2024). It has been collaborating with IT vendors and governments to share best practices and conduct risk assessments. Another example of a coordinated crisis response was between the British Airways and UK authorities like the National Cyber Security Centre (NCSC) and the Information Commissioner's Office (ICO) in response to the data breach that accessed customer data (*British Airways fined £20M over Data Breach*. 2020). NCSC was pivotal in mitigating the breach, while ICO facilitated responses after the breach including imposing a fine to encourage enhanced security measures on BA (*British Airways fined £20M over Data Breach*. 2020).

Although collaboration is improving, it is worth noting that the effectiveness of these collaborations vary from one region to the other. While there have been successful collaborations, there have also been cases of failures or limited collaborations among governments, airlines and IT vendors. For instance, when SITA (IT services provider) was hacked in 2021 the response of affected airlines was fragmented (Faye et al., 2024). The attack affected airlines such as Singapore Airlines, Air India, Lufthansa, among others, and while these were supposed to collaborate in addressing the breach, some failed to act and even informed their customers months after the attack (Faye et al., 2024; Freeman et al., 2024). Despite the global nature of the SITA breach, there was no industry-wide intervention.

5.3 The Role of Emerging Technologies in Addressing Cyber-Security in Aviation

As the aviation industry continues to adopt emerging technologies, this research found that it can utilize these technologies to enhance its ability to predict and detect cyber-security threats early, and secure systems (Klenka, 2021). One of the most valuable technologies is AI, whereby through machine learning the aviation industry can predict threats, detect anomalies and execute automated responses (Svanadze, 2020). An example of such application is by an organization named Darktrace which is collaborating with UK airlines and stakeholders implement AI-powered systems that detect cyber-threats and enact automated responses (*Ai cybersecurity: A new approach to AI in Cybersecurity*. 2025). Blockchain technology can also be used to develop decentralized and tamper proof ledgers thus giving airlines an edge in their security by having traceable logs (Elmarady and Rahouma, 2021). Airlines can also invest in quantam cryptography which encrypts data to ensure detection in case of breach. Other emerging technologies that can enhance cyber-security in airlines include digital twins for risk simulations and cloud based cyber-security platforms (Klenka, 2021). The application of these technologies need to be done in a way that respects confidentiality, integrity and availability of information to all parties as stipulated by the CIA triad (Osazuwa et al., 2023).

5.4 Measures that can Ensure Cyber-Security in Airlines

The final aim of this research was to identify best practices that can be adopted to enhance cyber-security in aviation. Since airlines and other organizations in the aviation industry operate as systems (STS theory), they should adopt multi-layered interventions that combine preventative, detective and responsive measures which involve all their technical and social aspects (Svanadze, 2020; Żmigrodzka, 2020). There is a need to enact a zero-trust architecture, whereby all the systems should assume that no one should be trusted without verification in order to meet the confidentiality aspect of the CIA triad. It is also necessary to have regular cyber-security training to all personnel since technical improvements may be useless if the social actors are not trained (Ukwandu et al., 2022). Finally, the aviation industry needs to develop clear and applicable policies that encourage intelligence sharing among relevant participants in order to prevent widespread attacks (Svanadze, 2020).

6.0 Unique Contributions to Theory, Practice and Policy

The findings of this study are of significant value to theory, policy and practice. To begin with, this research has advanced the application of existing theories to the concept of cyber-security in aviation. It has applied the STS theory, demonstrating how cyber-security relies on the simultaneous advancement of both technical and social aspects of aviation (Yurtseven and Buchanan, 2013). The STS theory confirms the need for the industry to consider the interdependence of social and technical aspects of organizational systems in enhancing cyber-security. It is also worth noting the value of the CIA triad in the understanding of cyber-security. This research has advanced the application of confidentiality, integrity and availability in enhancing cyber-security in aviation (Osazuwa et al., 2023). It has advanced the application of CIA triad in the development of measures that ensure real-time communication and emphasizes operational continuity while working towards enhancing cyber-security. For instance, the "availability" principle requires airlines to avail intelligence to all the necessary parties which contributed towards the suggestion for improved government's, airlines' and IT vendors' collaboration.

This research has significant input to practice in the aviation sector. It confirmed the rising risk of cyber-insecurity in the aviation industry, with some forms like malware and ransomware increasing by more than 600% (*Together against threats: Advancing aviation cybersecurity through collective action*. 2025). This understanding raises the need for the development of strategic risk management strategies which are outlined under section 4.4 of this study. It depicts the value in adoption of a zero-trust architecture, whereby systems should be designed to not trust anyone by default but only after verification (Ukwandu et al., 2022). In addition, this study contributes towards the understanding of the interconnected nature of social and technical aspects in aviation, resulting in the suggestion of a human- and technical-centered approach towards cyber-security. Neither the technical nor the human aspect of cyber-security is more valuable, hence the

need for the development of a multilayered approach (Yee and Zolkipli, 2021). This research has therefore suggested the value of training all staff on cyber-security while at the same time using emerging technologies such as AI to foster automated prediction, detection and responses to cyber-security threats in aviation (*Ai cybersecurity: A new approach to AI in Cybersecurity*. 2025; Ukwandu et al., 2022).

It is important to note that this study is valuable to policy development in the aviation sector. Part of the research objectives examined the effectiveness of collaborative efforts by stakeholders towards enhancing cyber-security. This research found that although these collaborations are improving, their effectiveness varies from region to region, with some incidences of cyber-security that had global impacts receiving minimal attention from involved parties like in the case of SITA breach (Faye et al., 2024). Such evidence-based insights can inform policy making in the industry, informing bodies governments, airlines and IT vendors on the synergy that is brought about by collaborations. Policy frameworks pertaining to cyber-security should integrate collaborations of public and private sectors, regulations and enforcement (Żmigrodzka, 2020).

7.0 Conclusion

This study was aimed at examining cyber-security challenges in the aviation industry and develop strategies that can be used to safeguard airline operations. It has fulfilled its objectives by collecting secondary qualitative data that addresses four key areas. Firstly, the study found that the most prevalent cyber-security challenges in aviation include: DDos, ransomware attacks, breach of confidential data, GPS spoofing and attacks due to of in-flight systems. In addition, this study found that although collaborations between airlines, governments and IT vendors have been improving over time, there have been instances of uncoordinated responses to cyber-attacks that have global impacts (Faye et al., 2024). Moreover, emerging technologies can enhance early detection, prevention and response to cyber-attacks. This study also found the need for a collaborative response to cyber-security which will involve both social and technical aspects of the aviation industry (Osazuwa et al., 2023).

This research has advanced the application of the CIA triad and STS theory, depicting the value of multi-layered interventions that combine preventative, detective and responsive measures which involve all their technical and social aspects (Svanadze, 2020; Żmigrodzka, 2020). It has also identified the need for development of policies that will enhance collaborative efforts from IT vendors, airlines and governments while predicting, detecting and responding to cyber-security issues (Svanadze, 2020). Although advancements in technologies and their integration into aviation are resulting in cyber-security vulnerabilities, this research has found them to be a necessary evil thus recommending continued improvement of cyber-security measures in aviation.

This study might have been limited by time constraints and its cross-sectional nature (Wiggins and Stevens, 2016). It is necessary for future studies to consider a longitudinal approach that examines the changes in nature and severity of cyber-security challenges over time. It is also important to

examine the unique nature of cyber-security challenges that arise due to adoption of specific technologies such as ATC, SATCOM, IFE, among others.

References

Ai cybersecurity: A new approach to AI in Cybersecurity (2025) *Darktrace*. Available at: https://www.darktrace.com/cyberai#:~:text=Darktrace's%20Self%2DLearning%20AI%20is,cyber%20risk%20in%20your%20organization. (Accessed: 27 May 2025).

Alrefaei, F., Alzahrani, A., Song, H., Zohdy, M. and Alrefaei, S., 2021, April. Cyber physical systems, a new challenge and security issue for the aviation. In *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)* (pp. 1-5). IEEE.

Amorim, V., Fernandes, A. and Filipe, V., 2025. Analyzing the Impact of the CrowdStrike Tech Outage on Airport Operations and Future Resilience Strategies. *Procedia Computer Science*, *256*, pp.633-640.

Appelbaum, S.H., 1997. Socio-technical systems theory: an intervention strategy for organizational development. *Management decision*, *35*(6), pp.452-463.

Bergamasco, F., Cassar, R. and Popova, R., 2020. *Cybersecurity: key legal considerations for the aviation and space sectors*. Kluwer Law International BV.

Black, J. and Rubenov, E. (2025) *Why are airlines a prime target for cyberattacks? | Akamai*. Available at: https://www.akamai.com/blog/security/why-are-airlines-prime-target-for-cyberattacks (Accessed: 27 May 2025).

British Airways fined £20M over Data Breach (2020) *BBC News*. Available at: https://www.bbc.com/news/technology-54568784 (Accessed: 27 May 2025).

Cooper, P., Handler, S. and Shahwan, S., 2019. *Aviation cybersecurity: Scoping the challenge*. Atlantic Council, Scowcroft Center for Strategy and Security.

Dave, G., Choudhary, G., Sihag, V., You, I. and Choo, K.K.R., 2022. Cyber security challenges in aviation communication, navigation, and surveillance. *Computers & Security*, *112*, p.102516.

Duchamp, H., Bayram, I. and Korhani, R., 2016, June. Cyber-Security, a new challenge for the aviation and automotive industries. In *Seminar in information systems: applied cybersecurity strategy for managers* (pp. 1-4).

Eleimat, M. and Őszi, A., 2025. Cybersecurity in Aviation: Exploring the Significance, Applications, and Challenges of Cybersecurity in the Aviation Sector. *Periodica Polytechnica Transportation Engineering*.

Elmarady, A.A. and Rahouma, K., 2021. Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment. *IEEE access*, *9*, pp.143997-144016.

Faye, S., Abdulrahman, J., Talb, R.A. and Martin, R.J., 2024. Cybersecurity in Aviation: A Case-Based Approach to Preparedness. *Int'l J. Info. Sec. & Cybercrime*, *13*, p.33.

Fox, S.J., 2016. Flying challenges for the future: Aviation preparedness–in the face of cyber-terrorism. *Journal of transportation security*, *9*, pp.191-218.

Freeman, K., Lewis, T.D. and Ali, H., 2024, August. Aviation Cybersecurity Challenges. In *CNS & Security Workshop*.

George, A.S., 2024. When trust fails: Examining systemic risk in the digital economy from the 2024 crowdstrike outage. *Partners Universal Multidisciplinary Research Journal*, *1*(2), pp.134-152.

Greig, J. (2023) *Boeing says cyber incident affects parts and distribution business*, *Cyber Security News | The Record*. Available at: https://therecord.media/boeing-cyberattack-parts-distribution-business (Accessed: 27 May 2025).

Haass, J., Sampigethaya, R. and Capezzuto, V., 2016. Aviation and cybersecurity: opportunities for applied research. *Tr News*, (304), p.39.

Houseman, O., Tiwari, A. and Roy, R., 2004. A methodology for the selection of new technologies in the aviation industry.

Jaber, E.M., Haitam, A. and Abderrahim, A., 2024, May. Cybersecurity Challenges in the Global Aviation Network. In *International Conference on Connected Objects and Artificial Intelligence* (pp. 165-171). Cham: Springer Nature Switzerland.

Jones, T., 2024. *Investigating the Opportunities and Limitations of Artificial Intelligence and Cybersecurity in Aviation* (Master's thesis, Eastern Michigan University).

Kagalwalla, N. and Churi, P.P., 2019, September. Cybersecurity in aviation: An intrinsic review. In *2019 5th international conference on computing, communication, control and automation (ICCUBEA)* (pp. 1-6). IEEE.

Klenka, M., 2021. Aviation cyber security: legal aspects of cyber threats. *Journal of transportation security*, *14*(3), pp.177-195.

Lehto, M., 2020. Cyber security in aviation, maritime and automotive. *Computation and Big Data for Transport: Digital Innovations in Surface and Air Transport Systems*, pp.19-32.

Lykou, G., Iakovakis, G. and Gritzalis, D., 2019. Aviation cybersecurity and cyber-resilience: assessing risk in air traffic management. *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies*, pp.245-260.

Majchrzak, A. and Borys, B., 2001. Generating testable socio-technical systems theory. *Journal of Engineering and Technology Management*, *18*(3-4), pp.219-240.

McManners, P., 2016. The action research case study approach: A methodology for complex challenges such as sustainability in aviation. *Action Research*, *14*(2), pp.201-216.

Melnikovas, A., 2018. Towards an Explicit Research Methodology: Adapting Research Onion Model for Futures Studies. *Journal of futures Studies*, *23*(2).

Moncrieff, S. (2025) *What caused the crowdstrike outage: A detailed breakdown*, *Messageware*. Available at: https://www.messageware.com/what-caused-the-crowdstrike-outage-a-detailedbreakdown/#:~:text=On%20July%2019%2C%202024%2C%20CrowdStrike,Screen%20of%20Death%20(BSoD). (Accessed: 26 May 2025).

Official Report: Foreign objects caused Azerbaijan Airlines crash (2025) *euronews*.

Osazuwa, O.M.C., Mitchell, O. and Osazuwa, C., 2023. Confidentiality; Integrity, and Availability in Network Systems: A Review of Related Literature. *International Journal of Innovative Science and Research Technology*, *8*(12), pp.1946-1953.

Rice, S., Winter, S.R., Doherty, S. and Milner, M., 2017. Advantages and disadvantages of using internet-based survey methods in aviation-related research. *Journal of Aviation Technology and Engineering*, *7*(1), p.5.

Sabillon, R. and Bermejo Higuera, J.R., 2023, July. The importance of cybersecurity awareness training in the aviation industry for early detection of Cyberthreats and vulnerabilities. In *International Conference on Human-Computer Interaction* (pp. 461-479). Cham: Springer Nature Switzerland.

Samonas, S. and Coss, D., 2014. The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3).

Shah, I.A., Jhanjhi, N.Z. and Brohi, S., 2024. Cybersecurity issues and challenges in civil aviation security. *Cybersecurity in the Transportation Industry*, pp.1-23.

Simmons, H.O., 2017. Cybersecurity in Aviation: Constant Vigilance Required. *J. Air L. & Com.*, *82*, p.771.

Spirent (2025). Available at: https://www.spirent.com/blogs/gps-spoofing-and-egpws-the-risks-for-the-commercial-aviation-industry (Accessed: 27 May 2025).

Stastny, P. and Stoica, A.M., 2022, February. Protecting aviation safety against cybersecurity threats. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1226, No. 1, p. 012025). IOP Publishing.

Svanadze, V., 2020. Cybersecurity in the civil aviation and existing challenges. *Legal Bulletin. Aviation and Space Law*. (4), pp.27-33.

Together against threats: Advancing aviation cybersecurity through collective action (2025) *Technology Advancement Center*. Available at: https://thetac.tech/together-against-threats-advancing-aviation-cybersecurity-through-collective-action/ (Accessed: 27 May 2025).

Ukwandu, E., Ben-Farah, M.A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I. and Bellekens, X., 2022. Cyber-security challenges in aviation industry: A review of current and future trends. *Information*, *13*(3), p.146.

Wiggins, M.W. and Stevens, C., 2016. *Aviation social science: Research methods in practice*. Routledge.

Yee, C.K. and Zolkipli, M.F., 2021. Review on confidentiality, integrity and availability in information security. *Journal of ICT in Education*, *8*(2), pp.34-42.

Yurtseven, M.K. and Buchanan, W.W., 2013, March. Socio-technical system design: a general systems theory perspective. In *VIII International Conference on Engineering and Computer Education (COPEC), Luanda, Angola*.

Zalewski, J. and Kornecki, A., 2019. Trends and challenges in the aviation systems safety and cybersecurity. *TASK Quarterly: scientific bulletin of Academic Computer Centre in Gdansk*, *23*.

Żmigrodzka, M., 2020. Cybersecurity–One of the Greatest Challenges for Civil Aviation in the 21st Century. *Safety & Defense*, *6*(2), pp.33-41.