Hanna Dzido
Dr
Uniwersytet Morski w Gdyni
Wydział Nawigacyjny
Katedra Transportu i Logistyki
h.dzido@wn.umg.edu.pl

DOI: 10.35117/A_ENG_23_05_03

Cybersecurity threats to aviation infrastructure

Abstract: Aviation is an example of a highly interconnected and complex sector, with a high level of media exposure and a key role in the socio-economic development of countries. Aviation infrastructure (line and point) constitutes elements of critical infrastructure, which is why it is subject to special protection. In view of the ongoing changes, digitization of many processes in the functioning of airports, airlines, passenger service, data transfer directly related to the nature of aviation, IT systems used by aviation market entities, including: airports, airlines, maintenance organizations, airport services. The article presents the issues of cyber security in civil aviation and the main directions of activities of the civil aviation supervision authorities of the global ICAO and the European EASA. The author presents the leading documents and actions taken so far to ensure cyber security in the field of data protection of all participants of the aviation market, developed at the international level. The author points to ICAO and EASA initiatives relating to cyberspace, the need to coordinate national regulations with relevant regulations on data security and protection management, and to include cybersecurity in state aviation safety and security oversight systems as part of a comprehensive risk management framework. The article also presents examples of cyber incidents in the aviation industry in the context of events monitored by Eurocontrol and recommendations for improving the ability to predict, detect, respond and mitigate cyber threats in civil aviation.

Keywords: Cybersecurity; Aviation cybersecurity; Civil aviation; Cyberattack; Digital infrastructure; Critical infrastructure

The global digital infrastructure currently forms the foundation of almost every aspect of economic and social life, thereby leading to a paradigm shift in information exchange. The uniqueness of this change is manifested not only by rapid technological development but also by an unprecedented level of global interconnectivity among systems and networks. All of this brings consequences in the form of a constant increase in cyberattacks. Aviation serves as an example of a sector with extensive interconnections and complexity, a high level of media exposure, and a key role in the socio-economic development of countries. Aviation infrastructure (both linear and point) constitutes elements of critical infrastructure, and therefore is subject to special protection. In the face of ongoing changes, the digitization of many processes in the operation of airports, airlines, passenger services, and data transfer directly related to the nature of aviation, the components of aviation infrastructure also include the IT systems used by entities in the aviation market, including, among others: airports, airlines, service organizations, and airport services. Due to its global nature, the aviation sector, like the interactions of systems and the accompanying data flows that go beyond national borders and individual organizations, is subject to a high potential risk of cyberattacks. Over the years, in line with the constant increase in demand for efficient mobility of people and goods, the civil aviation sector has undergone several digital transformations aimed at leveraging the power of technology to increase the industry's

productivity and efficiency. This has allowed maintaining a rapid growth rate while ensuring safety. At the same time, the consequence of digital progress has been the exposure of all stakeholders in the sector to cybersecurity threats. Successful cyberattacks can have (have) a negative impact on the continuity and safety of service provision, the reputation of aviation entities, financial efficiency, the safety of people, aircraft, aviation infrastructure facilities, or equipment used in passenger services. Therefore, the approach to cybersecurity and threats to civil aviation must adopt a comprehensive nature based on global frameworks, implying cooperation between countries and all interested parties (aviation regulatory authorities, services, aviation market entities, travelers).

Both the International Civil Aviation Organization (ICAO) and the European Union Aviation Safety Agency (EASA) provide forums for developing international cooperation for the cybersecurity of civil aviation. ICAO's work on aviation cybersecurity has evolved alongside the increasing dependence of civil aviation on technology. The scope and authority of both institutions ensure consistency, harmonization, compliance with international civil aviation priorities for the international air transport community, along with ensuring oversight of all areas of civil aviation.

ICAO's Actions on Cybersecurity Issues

ICAO's work on aviation cybersecurity is comprehensive and complex. It includes:

- Developing Standards and Recommended Practices (SARPs) (Standard 4.9.1 and Recommended Practice 4.9.2 in Annex 17 – Protection against Acts of Unlawful Interference [8] to the Convention on International Civil Aviation (Chicago Convention));
- Developing procedures and supporting materials;
- Ensuring that the framework of international aviation law is adequate to combat cyberattacks on civil aviation;
- Raising awareness about the importance of cybersecurity measures in civil aviation;
- Supporting discussions on aviation cybersecurity at national, regional, and global levels;
- Developing initiatives that support the creation and implementation of aviation cybersecurity capabilities for states and the broader aviation community.

The importance of cybersecurity efforts in civil aviation was further emphasized by the adoption of three ICAO Assembly resolutions:

1. Resolution A39-19 – Addressing Cybersecurity in Civil Aviation from 2016 (replaced in 2019 by Resolution No. 2)
2. A40-10 – Addressing Cybersecurity in Civil Aviation (replaced in 2022 by Resolution No. 3)
3. A41-19 – Solving the Cybersecurity Problem in Civil Aviation.

These resolutions contain important clauses that, among other things, recognize the interconnections between cybersecurity and the safety, protection, and efficiency of aviation. The agenda at ICAO Assemblies regarding cybersecurity includes ensuring a cross-sectional, holistic approach to aviation cybersecurity at both national and international levels. During the 41st ICAO Assembly, states were called upon to adopt and implement the 2010 Beijing Convention (Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation [6]) and the 2010 Beijing Protocol (Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft [7]) as a way to address cyberattacks on civil aviation.

EASA's Actions on Cybersecurity Issues

EASA developed the Strategy for Cybersecurity in Aviation [2], which was approved by the board in November 2015. Since then, EASA has been working on its implementation. A series of initiatives have been undertaken to better counter cyber threats in aviation, improve resilience, and support built-in security measures. In addition to its institutional regulatory activities, EASA is working on improving international cooperation in this field, as well as promoting information sharing among stakeholders in the aviation industry. Achieving a cyber-resilient aviation system and incorporating cybersecurity into the current concept of safety requires coordinated efforts from aviation system stakeholders. In this regard, EASA participates in and chairs the European Strategic Coordination Platform (ESCP), which includes representatives from key stakeholders in the industry, member states, and EU institutions. This cooperation contributes to harmonizing the objectives of aviation stakeholders and has enabled the development of the first joint aviation cybersecurity strategy. Engaged stakeholders are also in the process of defining a joint action plan to implement this strategy. To promote voluntary information sharing and expert cooperation, EASA supports the creation of the European Cybersecurity Centre for Aviation (ECCSA) and provides initial operational capabilities in collaboration with the EU CERT.

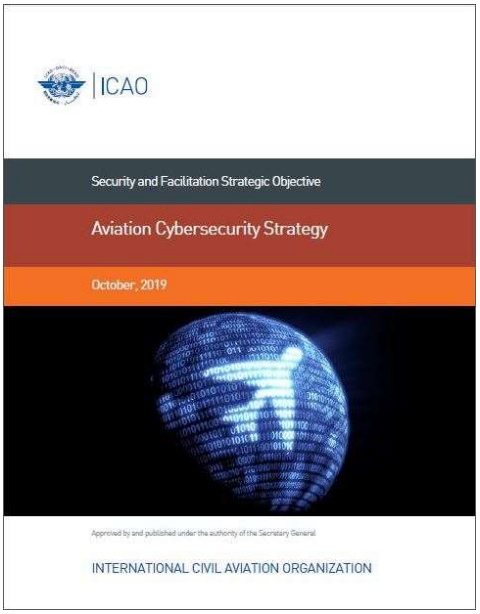
1. Components of the aviation critical infrastructure cybersecurity system
Source: own study

Cybersecurity Strategy in Civil Aviation According to ICAO

The foundation of ICAO's cybersecurity vision is the Aviation Cybersecurity Strategy, which aims for the global civil aviation sector to be resilient against cyberattacks, safe, and protected, while still maintaining the ability to innovate and develop. Recognizing the multifaceted and multidisciplinary nature of cybersecurity and noting that cyberattacks can simultaneously impact multiple areas and spread rapidly, a common vision and the definition of a global cybersecurity strategy are essential. The strategy has been adapted to other ICAO initiatives related to cyberspace and coordinated with appropriate regulations concerning safety management and protection.

The strategy establishes a framework based on seven pillars:

1. International Cooperation.
2. Governance.
3. Effectiveness of Legislation and Regulations.
4. Cybersecurity Policy.
5. Information Sharing.
6. Incident Management and Contingency Planning.
7. Building Capacity, Training, and Cybersecurity Culture.



2. ICAO Publication titled Aviation Cybersecurity Strategy
Source: https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx

Aspect of International Cooperation

The aspect of international cooperation arises from the cross-border nature of both cybersecurity and aviation. Both require collaboration at national and international levels, as well as mutual recognition of efforts to develop, maintain, and enhance cybersecurity to protect the civil aviation sector from all cyber threats to safety and protection. The ability to promote global consistency and ensure full interoperability of protective measures and risk management systems necessitates harmonized actions at the global, regional, and national levels. ICAO member states, in accordance with the Aviation Cybersecurity Strategy, must formulate and implement appropriate legislative and executive regulations in compliance with ICAO provisions before deploying national cybersecurity policies in civil aviation.

3. Components of the Aviation Ecosystem
Source: own study

Cybersecurity Strategy in Civil Aviation According to ICAO

Cybersecurity is to be integrated into national aviation safety and protection oversight systems as part of comprehensive risk management frameworks. In the meantime, states are encouraged to ratify ICAO instruments, including the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Beijing Convention) and the Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing Protocol).

Due to the existence of various risk assessment methodologies, priority should be given to revising and potentially developing new guidelines related to threat and risk assessments for cybersecurity to achieve comparability of assessment results.

Throughout the civil aviation sector, cybersecurity policies can encompass the full lifecycle of aviation systems and include elements such as:

- Cybersecurity Culture
- Promoting Security from the Design Phase
- Security of the Software and Hardware Supply Chain
- Data Integrity and Appropriate Access Control
- Proactive Vulnerability Management
- Improving the Efficiency of Security Updates Without Compromising Safety
- Incorporating Systems and Processes for Monitoring Cybersecurity-Related Data

4. Aviation Ecosystem – Interoperability of Information Sharing Among Users
Source: Informal Briefing to the ICAO Council, Update on Cybersecurity The Trust Framework, https://www.icao.int/SAM/Documents/2018-GREPECAS18/GRP18_P03.pdf

Cyberattacks can easily spread and have a global impact. The goal of information sharing is to enable the prevention, early detection, and mitigation of significant cybersecurity-related events before they lead to broader consequences for aviation safety or protection. Appropriate mechanisms, along with a culture of information sharing, will

significantly reduce systemic cyber risk across the entire aviation sector, whose value has already been proven in terms of aviation safety and protection. Sharing information on aspects such as vulnerabilities, threats, incidents, and best practices through established and trusted relationships can lessen the impact of ongoing attacks.

Incident Management and Contingency Planning According to ICAO's Approach

In the context of incident management and contingency planning, ICAO's approach necessitates having appropriate and scalable plans to ensure the continuity of air transport during cyber incidents. ICAO recommends that states and the aviation sector utilize existing contingency plans that have already been developed and modify them to incorporate cybersecurity regulations. Cybersecurity exercises are highly recommended as a useful tool for testing existing cyber resilience and identifying improvements. Such exercises can take various formats, for example: tabletop exercises, simulations, or real-time drills, and can vary in scale: international, national, or organizational.

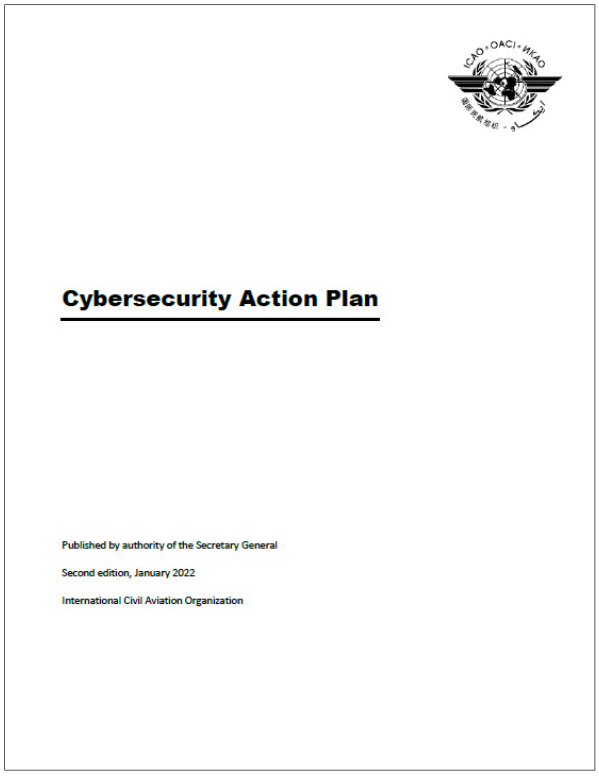
However, the human element remains fundamental to cybersecurity. The civil aviation sector must take concrete and effective steps to increase the number of qualified personnel possessing knowledge in both aviation and cybersecurity. This goal can be achieved through raising awareness, as well as education and training. Cybersecurity-related curricula and aviation cybersecurity programs at all levels should be integrated into national educational frameworks, as well as into relevant international training programs. Aviation should strive for innovative ways to combine and intersect traditional information technologies with career paths in cyberspace. Supporting and stimulating the development of skills in the current and new workforce should lead to fostering innovations in cybersecurity and relevant research and design of solutions dedicated to the aviation industry and its collaborating sectors.

Civil aviation has achieved commendable results in safety (safety and security), which are based on a proactive safety culture (just culture) that is created and upheld by everyone. The principles of this safety culture are to be applied to develop and maintain a cybersecurity culture across the entire aviation sector.

ICAO Assembly Resolution A40-10

ICAO Assembly Resolution A40-10 called upon ICAO to develop a Cybersecurity Action Plan (CyAP) to support states and the industry in adopting the aviation cybersecurity strategy. The first edition of CyAP was published in November 2020, and the second edition in January 2022.

CyAP provides a foundation for collaboration between ICAO, states, and stakeholders and proposes a range of principles, measures, and actions to achieve the goals of the seven pillars of the aviation security strategy. To this end, CyAP develops the strategy's pillars into 32 priority actions, which are then divided into 51 tasks to be implemented by ICAO, states, and interested parties.



5. ICAO Publication Titled Cybersecurity Action Plan
Source: https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx

ICAO Continues Developing Guidelines to Further Support States and Stakeholders in Civil Aviation Cybersecurity and Implementing Their Obligations Defined in ICAO Standards and Recommended Practices Related to Aviation Cybersecurity.

To date, ICAO has published the following guidelines:

1. Chapter 18 in the ICAO Aviation Protection Manual (Doc 8973 – Restricted)
   This chapter provides guidelines for states on implementing their obligations related to Standard 4.9.1 in Annex 17 – Protection against Acts of Unlawful Interference.
2. Material in the Air Traffic Management (ATM) Protection Management Manual (Doc 9985 – Limited)
   The ATM Security Manual offers a comprehensive approach to security within the ATM environment, combining guidelines for both physical security and cybersecurity elements.
3. Guidelines on the Traffic Light Protocol (TLP)
   This document provides guidelines for using the Traffic Light Protocol (TLP) to facilitate the exchange of cybersecurity information. TLP ensures a simple and intuitive way for the information source to specify restrictions on the further sharing of that information by recipients, thereby minimizing human error in inadvertently sharing confidential information beyond intended recipients.
4. Guidelines on Cybersecurity Policy
   These guidelines address the protection and resilience of international civil aviation critical infrastructure against cyber threats and the requirement for multilateral cooperation in civil aviation, as well as with external bodies such as the military, cybersecurity authorities, and national security agencies. Additionally, the material includes a template to support the development of national aviation cybersecurity policies.
5. Cybersecurity Culture in Civil Aviation

The guidelines are based on civil aviation's experiences in implementing successful and effective aviation safety and protection cultures. They combine relevant elements from both cultures and supplement them with aspects specific to aviation cybersecurity to support the design and implementation of a robust organizational cybersecurity culture in civil aviation.

As part of efforts to establish international aviation trust frameworks in 2019, guided by Recommendation 13 of the Air Navigation Conference, ICAO began work on ensuring the security and resilience of the Air Navigation System against cyberattacks. This activity also encompassed the storage, processing, and exchange of data and information meeting confidentiality, integrity, and availability requirements. Ongoing work includes the development of principles, policies, and guidelines related to the International Aviation Trust Framework (IATF). The work also involves defining performance requirements for the processing, exchange, and storage of information in networked applications, including the development of technical requirements needed to meet the current and future needs of aviation.

Cybersecurity Strategy in Civil Aviation According to EASA

The Strategy for Cybersecurity in Aviation document was adopted by the European Strategic Coordination Platform (ESCP) shortly before the 40th Session of the ICAO General Assembly. The ESCP recognizes the importance of reviewing the strategic document with the Assembly's outcomes and ensuring consistency and updating the language related to the ICAO Assembly resolutions on cybersecurity. EASA's strategy envisions a future aviation system characterized by two main enhancements. The future aviation system aims to:

- Create a Trusted and Reliable Environment: This allows aviation stakeholders to rely on services and information provided by others to achieve their operational goals.
- Develop an Adaptive System of Systems: This system is capable of adapting and thus countering new threats without significant disruptions. It is to be developed through a systemic approach to aviation cybersecurity, utilizing both current and legacy systems.

Achieving the desired enhancement requires aviation sector stakeholders to undertake a collective effort focused on two directions:

1. Making Aviation an Evolutionary System Resilient to Cyberattacks: Such a system can maintain its core functions even in the event of an attack.
2. Self-Strengthening Aviation through an "Embedded Security" Approach: This approach considers the security objectives that need to be achieved from the inception of systems, alongside traditional operational and safety goals.

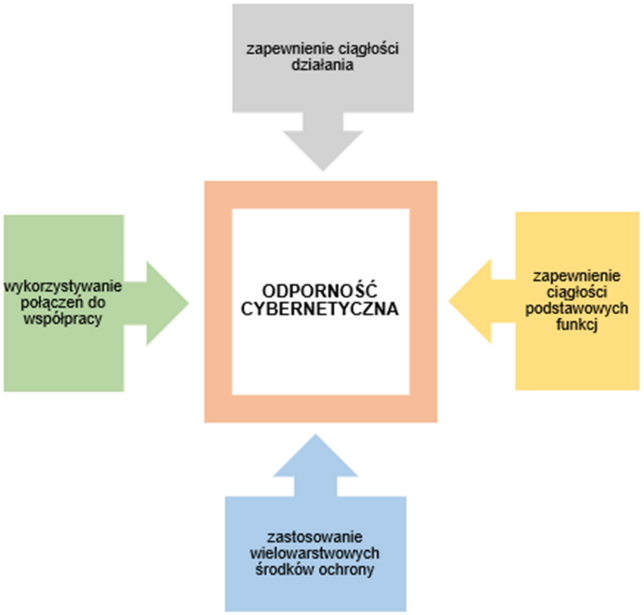
EASA has established four measurable objectives to improve cybersecurity resilience:

1. Ensuring Continuity of Operations: Through protective measures deployed along functional chains (adequate to the level of risk).
2. Ensuring Continuity of Core Functions of Operational Systems.
3. Applying Multi-layered Protective Measures Within Operational Systems: These measures make the progression of an attack more difficult.
4. Leveraging Existing Relationships and Connections Within the Transorganizational Nature of the System.

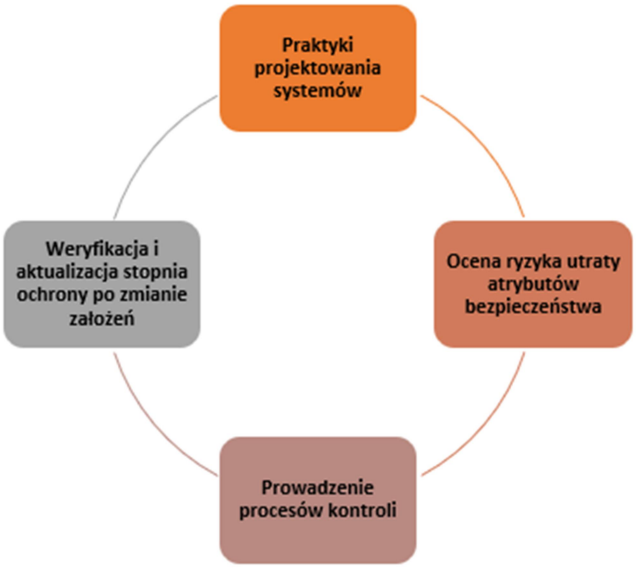
Additionally, EASA has set four measurable objectives for a self-strengthening aviation system implementing an embedded security approach:

1. System Design Practices: Aimed at avoiding the unintended use of functions available to users.
2. Risk Assessment of Security Attribute Loss and Implementation of Protective Measures: Including adaptive solutions.

3. Conducting Control Processes: These allow for the effectiveness of system security throughout the lifecycle.
4. Verification and Updating of Protection Levels After Changes to Original Assumptions.



6. EASA's Measurable Objectives for Improving Cyber Resilience
Source: own study



7. Objectives of a Self-Strengthening Aviation System Implementing an Embedded Security Approach
Source: own study

The Most Significant Cyber Threats to the Aviation Industry

The aviation industry, encompassing a wide range of stakeholders, including airlines, airports, airspace management services, technology suppliers, etc., constitutes one of the most critical infrastructures along with its entire network, resources, and systems. Additionally, it collaborates with various fundamental infrastructure sectors, including defense and national security, transportation, communication, banking, and energy. As a result, any disruption to the functioning of the aviation industry has negative consequences for the establishment of social order and the provision of public services.

The aviation industry operates on an international scale, encompassing numerous subsectors such as tourism and foreign trade. To meet the needs of this complex structure, it must utilize technological solutions. In this context, the sector has gradually undergone a digitization process, increasingly adopting innovative technologies. The COVID-19 pandemic, like other economic sectors, forced the aviation industry to implement additional solutions and further shift operations online. The consequence of such extensive digitization has been increased (heightened) vulnerability to cyberattacks. Due to the nature of the aviation industry, cybercriminals are motivated by access to sensitive data, such as passports and high-value credit card information.

Actors Posing Cybersecurity Threats to Aviation:

- **State-Sponsored Attack Organizations:** These groups conduct attacks to steal intellectual property and intelligence information to weaken the aviation capabilities of other countries, enhance local aviation capabilities, and develop preventive technologies against the capabilities of other nations [3].
- **Cybercriminals:** Possessing the necessary knowledge and skills, these individuals focus on causing the greatest possible damage through their attacks.
- **Cyberterrorists:** Driven by political, religious, ideological, and social factors, their actions aim to threaten national security, cause mass casualties, harm the economy of the targeted state, disrupt public order, and undermine trust in aviation systems.
- **Cyber Spies:** Targeting the aviation industry, which is one of the most critical infrastructures, their objectives include financial, industrial, political, and diplomatic espionage.
- **Insiders:** This term refers to dissatisfied employees, former employees, or business partners. Their motivation for cyberattacks may be financial gain or revenge.
- **Activists:** Not driven by financial or political considerations, they attack to gain greater influence, develop skills, and earn recognition among cybercriminals.
- **Passive Observers:** Operating with the intent to gather information, they obtain real-time views of air traffic and communication from public and private websites and mobile applications that display air traffic, utilizing the open nature of air traffic protocols.

Attacks and Security Vulnerabilities

The use of complex and interconnected IT systems in the aviation industry is increasing daily. From Wi-Fi connections and in-flight entertainment systems for passengers to software used at airports and airlines for managing security control and reservations, sophisticated IT solutions are employed throughout the industry's supply chain. These modern technologies have a significant positive impact on aircraft control systems, enhancing the quality of aviation operations and increasing flight safety and performance. However, they power an ecosystem where data flows between numerous stakeholders and internal/external systems, thereby expanding the attack surface. The fundamental technologies used in the aviation industry can be categorized as:

- Intelligent Systems,

- Internet of Things (IoT) Devices,
- Cloud Infrastructures,
- Big Data,
- Blockchain.

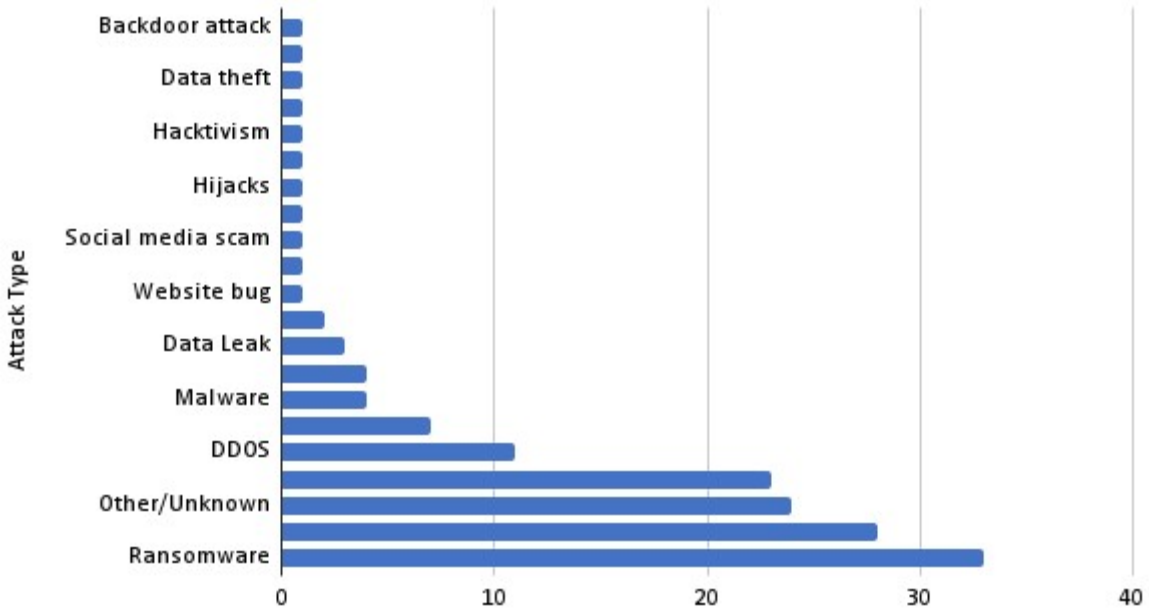
Attackers primarily target remotely accessible intelligent systems (biometric systems, robotic systems, etc.), IoT devices (sensors, actuators, etc.), and cloud systems. The main systems often exposed to cyber threats in the aviation industry include:

- In-Flight IP Networks,
- Digital Air Traffic Control (ATC) and Traffic Management Systems,
- Flight By Wire Systems,
- In-Flight Interface Devices,
- Flight History Servers,
- Fleet and Route Planning Systems,
- Passenger Reservation Systems and Loyalty Programs,
- Ticket Reservation Portals,
- Cargo Handling and Shipping Systems,
- Access Control, Departure, and Passport Systems,
- Crew Member Devices,
- Internal Threats.

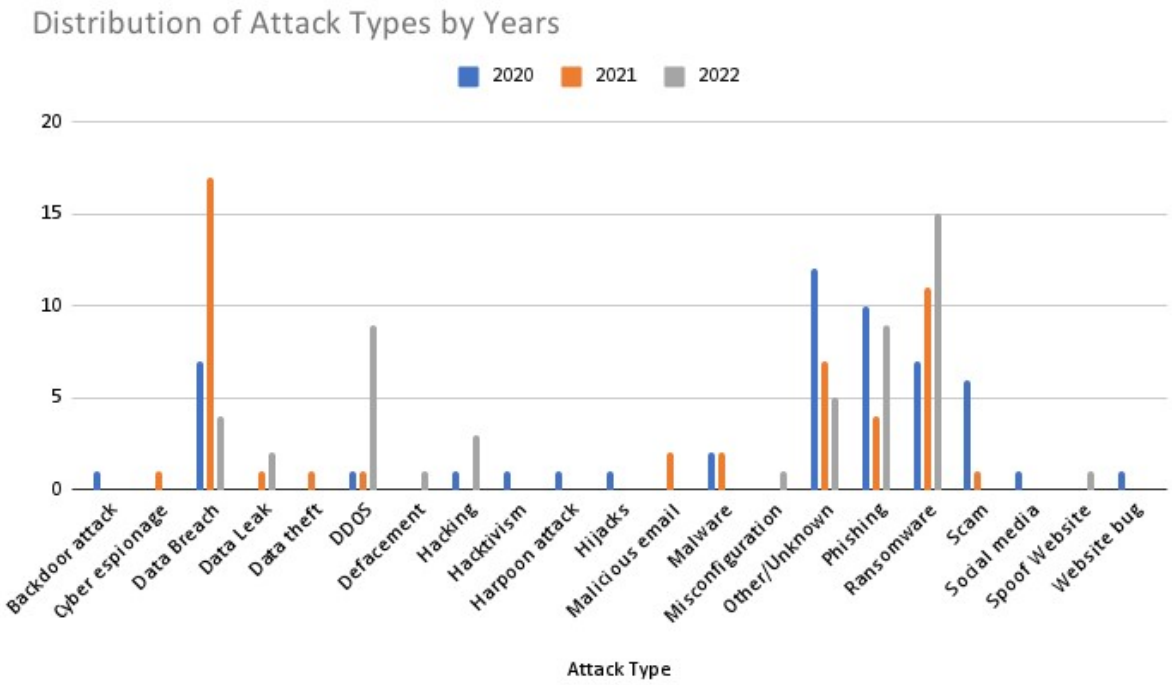
Cyberattacks on the Aviation Industry in Recent Years

In recent years, cyber incidents in the aviation industry have been reviewed in the context of events monitored by Eurocontrol. Eurocontrol (the pan-European civil-military organization supporting European aviation) publishes the EATM-CERT (European Air Traffic Management Computer Emergency Response Team) Aviation Cyber Event Map. Data on this map have led to the following findings and charts:

- In 2020, 52 attacks were reported, in 2021 – 48, and by the end of August 2022 – 50 attacks. Thus, cyber incidents in 2022 reached the average of 2020 and 2021 in just eight months.
- The most frequently observed types of attacks over the past three years (2020, 2021, and 2022) are ransomware (22%), data breaches (18.6%), phishing (15.3%), and DDoS (7.3%). Other/Unknown types of attacks accounted for 16%.
- In addition to civil aviation attacks, eight military incidents were reported. Some of these attacks aimed at cyber espionage and data theft. Two of these attacks were conducted using ransomware software, two using malware, and one using a backdoor. The methods used in three of them are unknown.



8. Types of Attacks Targeted at the Aviation Industry from 2000 to 2022
Source: https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/



9. Distribution of attack types by year
Source: https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/

Only in August 2022, seven attacks took place. Three of them were classified as high, and four as medium. Information published on this topic indicates a security breach (threat) that generates or could generate far-reaching consequences [3]. Among the exemplary cyberattacks, the following can be mentioned:

- Cyberattack on the Portuguese airline (TAP Air Portugal), after which the airline stated in an issued statement that its security mechanisms were immediately activated and unauthorized access was blocked.

- Leak of some passenger databases from airlines in Malaysia and the United Arab Emirates due to hacker activities.
- Security breach of personal data of passengers of the Indian airline (Akasa Air), exposed through a cyberattack.
- Disclosure of personal data of users of the Canadian airline's application (WestJet).
- Cyberattack on American Airlines Group Inc (AAL.O). The company reported a data breach on the email accounts of a small number of its team members. Addresses, phone numbers, driver's license numbers, passport numbers, and/or medical information may have been accessed by unauthorized cybercriminals.
- Cyberattack on Philippine Airlines. The cybersecurity breach affected an external IT provider as part of a program for frequent travelers. Among the compromised information were members' names, dates of birth, nationality, gender, date of joining, level, and point balances. The airline recommended that members immediately change their passwords.
- Ransomware LockBit attacked the Air Navigation Safety Bureau in Africa and Madagascar (ASECNA). During this very serious incident, data from 18 member countries of the agency were encrypted, and the agency threatened to disclose the breached data on the dark web unless a ransom of $25,000 USD was paid.

In the aviation industry, similar to many other industries, digital evolution affects all stakeholders in the aviation ecosystem. It concerns both systems and people, and changes in one area are felt by all. Cybercriminals are driven by financial and political goals as well as the desire to obtain confidential information. In addition to the risk of financial losses or loss of reputation, successful attacks in the aviation sector can cause disruptions in air traffic, accidents, and even loss of life. The aviation industry, utilizing numerous technological solutions to provide its customers with the best possible user experiences, must demonstrate the same sensitivity in detecting and responding to cyber threats.

In this context, the following recommendations can be presented for the aviation industry to improve its ability to predict, detect, respond to, and mitigate cyber threats:

- Educate employees in cybersecurity and equip them with necessary high-capacity tools.
- Identify supply chain risk points.
- Ensure the security of data transmission between ground and aircraft.
- Implement access security for network devices and systems.
- Protect end devices.
- Build robust identity and access management systems from both the aviation entity's and the customer's (passenger's) perspectives.
- Encrypt all data transmitted, stored, and processed in environments end-to-end.

Assessing all aviation systems for security gaps, determining risk assessments, and establishing priorities should include several elements. Essential components include defining the attack surface and the ability to protect all digital resources, estimating the potential use of information in terms of cyber threats, as well as determining possible threats and proactively responding, which is crucial.

Source materials

[1] European Strategic Coordination Platform
[2] European Strategic Coordination Platform, Strategy for Cybersecurity in Aviation, First Issue – September 10th, 2019
[3] https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/
[4] https://www.easa.europa.eu/en/domains/cyber-security/main-easa-activities#group-easa
[5] https://www.icao.int/aviationcybersecurity/Pages/default.aspx

[6] https://www.icao.int/secretariat/legal/Docs/beijing_convention_multi.pdf
[7] https://www.icao.int/secretariat/legal/Docs/beijing_protocol_multi.pdf
[8] https://www.ulc.gov.pl/_download/prawo/prawo_miedzynarodowe/konwencje/Zalacznik_17.pdf
[9] Podręcznik ochrony zarządzania ruchem lotniczym (ICAO Doc 9985)
[10] Rezolucja A39-19 – Zajęcie się cyberbezpieczeństwem w lotnictwie cywilnym z 2016 r.,
[11] Rezolucja A40-10 – Zajęcie się bezpieczeństwem cybernetycznym w lotnictwie cywilnym
[12] Rezolucja A41-19 – Rozwiązanie problemu cyberbezpieczeństwa w lotnictwie cywilnym
[13] Strategy for Cybersecurity in Aviation – Analysis and Objectives