IDEA STUDIES Journal
Open Access Refereed E-Journal & Indexed & Puplishing

Subject Area
Management and Strategy
Article Type
Research Article

e-ISSN:2587-2168
Year: 2022
Vol: 8 Issue: 47
pp 742-752

Article ID
65891
Arrival
23 September 2022
Published
30 November 2022

DOİ NUMBER
http://dx.doi.org/10.29228/ideas.65891

How to Cite This Article
Kızılcan, S. & Mızrak, K.C. (2022). "Cyber Attacks In Civil Aviation And The Concept Of Cyber Security", International Journal of Disciplines Economics & Administrative Sciences Studies, (e-ISSN:2587-2168), Vol:8, Issue:47; pp: 742-752

Cyber Attacks In Civil Aviation And The Concept Of Cyber Security

Serdar KIZILCAN [1] Kağan Cenk MIZRAK [2]

[1] Lecturer, Uşak University, Civil Aviation Vocational School, Department Of Transportation Services, Uşak, Turkey
[2] Assistant Prof.Dr., Uşak University, Vocational School of Civil Aviation, Department of Transportation Services, Uşak, Turkey

ABSTRACT

Although civil aviation has an effective technology to increase the efficiency and safety of air transport, the interconnectedness of systems and dependence on information-communication technology cause new risks to emerge. The use of extensive computer-based and interconnected technologies in airport ground systems, air navigation systems, flight information systems, in-flight control systems and security scanning has brought along new dangers as well as gains.

The concept of cyber security has become one of the most important agenda items of institutions, international organizations and states in the aviation sector, where information and communication technologies are rapidly developing. It is important to recognize the multifaceted and disciplined nature of cyber security and not to overlook the fact that cyber attacks are a rapidly spreading threat. In this sense, international civil aviation organizations are constantly updating their work in order to keep the aviation industry safe against cyber attacks. Studies are not only limited to aviation organizations, but are also carefully carried out by governments.

The aim of this article is to draw attention to the negative effects of cyber attacks, which are increasingly important in civil aviation, to the aviation industry. Cyber attacks on civil aviation cause great losses in the world economy in general. For this reason, aviation organizations and governments, as well as aircraft manufacturers, airline companies and airport management staff, need to use existing and developing technologies well and develop systems that can guarantee operational safety in order to increase sectoral efficiency and meet the expectations of customers.

In this study, firstly, information about cyber space, cyber security, cyber threat and cyber attack is given, and cyber attacks against civil aviation from past to present are stated in chronological order. Then, the studies carried out by civil aviation authorities within the scope of national and international fight against cyber threats were discussed, and finally, a general evaluation was made and various suggestions were made.

Key Words: Civil Aviation, Cyber Attack, Cyber-Terrorism, Cyber Security, Aviation Security.

1. INTRODUCTION

The aviation industry is one of the fast-moving and classics worldwide. With this departure, flight operations become dependent on the computer systems of the passengers' facilities, passengers' boarding-and-departure plan, air control control, and flight control system. In this case, you will be able to create it safely from a security point of view.

Although adequate security measures are taken by governments and organizations, the aviation industry, which has critical infrastructure and rapidly digitizes, needs to reevaluate its standards. As a matter of fact, in order to achieve their ultimate goals, the attackers seek new ways of civil aviation operations and try to infiltrate the systems of airline companies, airports and aircraft manufacturers. The collapse of a critical system such as air traffic control can crowd air traffic and cause accidents. Infiltrating passenger information systems and obtaining personal and credit card information of all passengers can lead to large-scale robberies.

Perhaps the most important challenge posed by cyberattacks is that the digital environment that allows us to create and share information creates a vast opportunity for cybercrime to be committed. Informatics experts state that the vast majority of companies in the industry are exposed to cyber attacks, the aviation industry suffers financially every year due to these attacks, and therefore it is imperative for companies to develop a comprehensive strategy and share information on cyber attacks (Abeyratne, 2020).

A cyberattack could potentially impact hundreds of companies, just like a natural disaster. In case of insufficient intervention, there is a loss of reputation and damage to customer perception. Cyber attacks are not only in the aviation sector; Considering that it also has an impact on the wider economy, it has become an operational requirement for organizations operating in the aviation industry to understand cybersecurity well, adopt a proactive approach, and effectively manage the technology used to deliver services. However, while fulfilling

this requirement, it should be kept in mind that there is no single solution for cyber security and that all stakeholders must act jointly in aviation, which is a global sector.

2. CONCEPTUAL FRAME

2.1. Cyber Space

Cyberspace is the digital environment created by the information systems and related networks in the world and in space or in independent information systems. Accordingly, all kinds of electronic devices, computers and technological devices that can be connected to the internet are defined as a part of cyberspace. Cyber security, on the other hand, is to protect information from attacks in cyberspace, to ensure the confidentiality, integrity and accessibility of data in the information system, to detect attacks and cyber security incidents, to activate the related mechanisms and to return the systems to the pre-cyber attack. (UDHB, 2013).

Another definition of cyberspace is made by the US Department of Defense. Accordingly, cyberspace is a global space in the information environment consisting of interconnected networks, consisting of information technology infrastructures, including internet communication networks, embedded processors and control units. Although cyberspace is thought of as a concept related to the internet, it means much more than the internet. Because even a transaction that does not occur in the real world is capable of occurring in cyberspace. For example; Even computing on a simple chip is a cyberspace event, which requires no internet connection (Ceylan, 2014).

Until recently, issues related to cyberspace were treated as a “low politics” issue. But it has now been understood that cyberspace is the source of the vulnerability that poses a potential threat to national security and disruption of the usual international order. Significant cybersecurity events have played a persuasive role in the importance of cybersecurity and have made cyberspace-related issues increasingly a "high policy" issue (Sertçelik, 2015).

2.2. Cyber Security

Along with the developments in information and communication technology, the opportunities and conveniences provided by the cyber environment make life more dependent on itself day by day, while this environment causes threats, attacks, harm to life and property, etc. The great damage suffered by individuals, societies and countries as a result of its use for various purposes has led to great changes in the understanding of security (Şenol, 2016).

Cyber security is defined as all the activities carried out to ensure the confidentiality, integrity and accessibility of cyber life. Confidentiality means that the information system and its data can only be accessed by authorized systems or individuals. Integrity means that information systems can only be changed by authorized systems or individuals. Accessibility, on the other hand, means that authorized persons can access information and information systems when needed and of quality (Kara, 2013).

The digitization of aviation services and devices simplifies many aspects of our lives and opens up new possibilities. However, such positive developments are never without risk. Malicious persons or groups may try to steal passengers' information, manipulate or interrupt services for economic or political reasons. The increasing digitization of aviation systems and the interdependence of services required for flight require aviation stakeholders to be resilient to cyberattacks (Ishtiaq, 2022).

While technologies in aviation are designed to provide fast and efficient communication, they also cause aircraft to not operate as closed systems and increase the possibility of cyber threats or risks. Because these technologies are also used during flight, a vulnerability can lead to disaster. In addition, a cyber attack on the airline's network structure can cause great damage to the entire airline. The increase in the use of technology therefore means that more efforts must be made to make it safe (Kagalwalla & Prathamesh, 2019).

The biggest challenges facing cybersecurity in aviation are lack of resources, budgetary constraints and lack of knowledge in cybersecurity. Lack of resources is a major barrier to the implementation of cybersecurity and affects 78% of organizations. Investments in cyber security by airline companies and airports are increasing and are expected to total 3.9 billion dollars (Shahbazian & Rogova, 2016).

Infrastructure for hiring experts and training staff is another challenge faced by managers. Continually educating staff in cybersecurity is not easy and requires staff highly experienced in Cybersecurity, as well as resources to replicate the threat scenario (De Cerchio & Riley, 2011).

In aviation, the company's top management and, if any, the board of directors are responsible for ensuring cyber security within the company. The business management is obliged to show the necessary determination in taking cyber security measures regarding information and operational systems and to allocate sufficient resources for the activities to be carried out. Within the scope of this responsibility, the management of the enterprise carries out the following activities (SHGM Talimat, 2022):

- ✓ Establishing an effective asset assessment process and ensuring that this process is kept up-to-date,
- ✓ Conducting regular cyber security risk and threat assessment studies for business assets,
- ✓ Establishing and operating the process of testing, auditing and monitoring and reporting the results of controls and established structures in terms of cyber security for providing cyber security,
- ✓ Following up-to-date security vulnerabilities for business assets and performing necessary updates and patches,
- ✓ Carrying out studies to increase cyber security awareness for all stakeholders of the company, such as all business employees, external service providers and customers, including senior management.

2.3. Cyber Threat and Cyber Security Vulnerability in Civil Aviation

The concept of cyber threat is any kind of cyber attack that will destroy the security of individual or corporate data in the cyber space. With this definition, the main feature that distinguishes cyber threats from classical threats is the emergence of threats in cyberspace. It is extremely difficult to predict and take precautions against emerging threats in cyberspace. An attack in the cyber space can be carried out anywhere and at any time. On the other hand, the fact that these threats do not have a central structure increases the uncertainty. In this sense, the source of the threat can be a single individual, groups of individuals, terrorist organizations or states (Kurnaz & Önen, 2019).

There are three dimensions that lead to the emergence of cyber threats (Aslay, 2017):

- ✓ Weaknesses in the design of the Internet (the addressing system, the fact that most of the systems that make the Internet work are open and unencrypted, the ability to distribute malicious software, and the Internet is a large decentralized network),
- ✓ Errors in hardware and software,
- ✓ Online access to critical systems.

Table 1. Cyber Security Threats, Actors and Purposes

Level of Threat	Actor	Purpose
Threats to National Security	Knowledge Warrior (Cyber Soldier)	Restricting a state's ability to make decisions, creating an atmosphere of chaos and psychological terror in the country.
	National Intelligence Officer (Cyber Spy)	Leaking information in order to gain political, economic and military superiority.
Common Threats Faced by Governments and the Private Sector	Cyber Terrorist	Making their actions visible to the masses; creating political changes.
	Industrial Espionage	To gain a competitive advantage.
	Organized Crime	Acting with the impulse of revenge, gaining financial gain; making institutional/political changes.
Local Threats	Corporate Hackers	To provide financial gain; excitement / challenge; promote and gain prestige.
	Recreational Hackers	excitement, challenge.

Source: Karasoy, 2021: 23, as cited in İrdem & Çobanoğlu, 2022

When Table 1 is examined, threats to national security are at the top of the threat level. The second level is the common threat areas faced by states and private sector organizations, and the third level is local threats with less threat level compared to the other two. Although the level and purpose of threats have some differences, cyber attacks by states or other non-state actors can have devastating results and transform the traditional concept of war and attack. (İrdem &Çobanoğlu, 2022).

The Airport Managers Association has divided cyber threats into three groups (Gramatica, 2015):

- ✓ Defeatable Information Technology systems,
- ✓ Theft and fraud that cause direct financial losses for airline companies, airports and passengers,

✓ Terrorism.

Cybersecurity vulnerability in aviation means that errors in flight-related computer-based systems or affected systems compromise network and information security. The vulnerability provides an entry point or gateway to exploit a system and therefore poses potentially serious security risks. Any system connected to the Internet, or more generally not physically isolated, is likely to be attacked by "hackers". Therefore, it is extremely important for an organization to manage the risk of cyber attacks. First, it is necessary to understand the potential impact and the probability of its occurrence. Then checks should be implemented for safety purposes. In general, the higher the potential impact of controls, the lower the probability of an attack. Therefore, the implementation of controls should be given priority (Abeyratne, 2011).

Manufacturers (COTS-Commercial Off The Shelf) use ready-made commercial software and hardware in aircraft to reduce costs. According to some sources, this situation poses a safety risk. Aircraft manufacturers have also developed systems that allow routine aviation commands between air traffic control and aircraft to use new technology. These systems are used in commercial services and are validated by the pilot for safety purposes. This, in turn, causes security weakness by intensifying radio traffic (Kovalchuk, 2019).

The ATC industry is vulnerable to a range of cyber threats, including threats to data integrity and privacy, malicious code, physical attacks (drones, lasers, etc.), GPS/frequency jamming, and UHF/VHF transmitters. Therefore, it is difficult to create a robust cyber security system (Silva, 2021).

According to the 2013-2023 Transportation Industry Control Systems Cyber Security Standards Strategy prepared by the National Cyber Security Department of the US Department of National Security, there are currently no cyber security standards for airports in existing systems. To give an example of how open airports can be to cyber threats; The IT infrastructure of Terminal 5 at Heathrow Airport consists of 1500 closed circuit camera systems (CCTV), 1100 secure access control points, a wireless LAN network with 750 ports and a telephone infrastructure built using 2800 hybrid technology, all of which are open to cyber attacks (Gopalakrishnan, 2013).

Thanks to the "Electronic flight bag" system, the information needed during the flight and stored on paper can be kept electronically. This system is a system that allows documents created during flight to be transferred to electronic media. It is claimed that this system, which provides automatic calculations such as pre-flight performance analysis and includes purpose-built sub-applications, can cause serious damages if hacked. The in-flight entertainment system may not seem like a possible candidate for a cyberattack, but upon closer inspection, it appears to have a number of vulnerabilities. The entertainment system includes a USB port under the passenger seats. This system is also connected to a number of other devices. In 2013, the Boeing company applied to amend the type certificate to address this type of issue, demonstrating that unauthorized access is possible. This system uses well-known technologies such as Ethernet and Android. This means that information is readily available to attack these systems. Similar applications are available for other aircraft models (Zalewski, 2019).

The U.S. Government Accountability Office's report states that the FAA has not fully addressed the cybersecurity issues of aviation technology systems against hackers since 2015. For example; According to the report, the FAA failed to adequately encrypt sensitive data and identify security weaknesses in a timely manner. However, the FAA stated that comprehensive updates in information security are necessary to ensure cybersecurity of the interconnected IP-based air traffic control system (Fox, 2016).

Teso, a German security researcher, presented a scenario where cybercriminals could have the ability to compromise a protocol used to send data to commercial aircraft. Teso focused on Aircraft Combat Addressing and Reporting System (ACARS) for three years. During this time, he reverse-engineered the flight navigation software and sent his own commands to the flight computer system. The researcher has developed an Android app that allows a user to redirect a virtual plane using the map app on their Samsung Galaxy smartphone. The simplicity of infiltrating a network and taking control of an aircraft using a smartphone clearly demonstrates the current vulnerability of cyber attack (Schmidt, 2016).

In 2018, cybercriminals accessed around 9.8 million passenger data, including passport numbers and credit card information. After the investigation, it was revealed that the airline had many security vulnerabilities such as unprotected backups and outdated software. Earlier that same year, British Airways' website was hacked that exposed the data of thousands of passengers. Air Canada experienced a similar breach through its app. The attacks also targeted airports (Berger, 2022).

2.4. Cyber Attack Methods and Attacks on Civil Aviation

Cyber Attack is defined as planned and coordinated attacks on information and transmission systems and critical infrastructures of targeted individuals, companies, institutions, organizations and government (Aslay, 2017).

Cyber attacks are among the preferred actions as they do not affect the attackers in terms of cost. All actions such as suppressing the states, undermining the authority, engaging in destructive activities, revealing the secret information of the states, seizing the systems such as electricity and transportation in the country and stopping the operation are all among the cyber attack activities (Gürkaynak & İren, 2011).

One of the methods of cyber attack on aviation is attacks on aircraft networks. Airplanes use radio signals to communicate. Therefore, cybercriminals can interfere with these networks and divert flights from the route. As aircraft include more IoT technology, attackers gain more potential gateways to infiltrate aircraft control or communication systems. Air traffic control and airline reservation systems, which process large amounts of data on a daily basis, are also possible targets. Cyber attackers can infiltrate airport networks to steal personal and financial information of passengers (Filinovych, 2021).

In addition to cyber attacks on aircraft networks, deflecting and destroying GPS signals, and causing accidents by deflecting unmanned aerial vehicles and aircraft from their routes are among the other examples of cyber attacks. Not only through the computer system; It is also possible to take actions that endanger flight safety over radio frequencies. Therefore, cyber attack should not be considered as a type of attack that takes place only through a computer over the internet network. An attack carried out over any communication network or targeting information or communication systems can have the characteristics of a cyber attack. Current cyber security practices in civil aviation date back more than 60 years (Oster, 2013).

Oster et al. (2013) stated that the methods and tools used by terrorists should be based on in terms of developing cyber defenses, raising awareness and preventing future threats. Statistics confirm an alarming increase in 38% of cyber web-based attacks recorded in the EU and worldwide in 2015. Although these are not specifically related to cyber terrorism, they still show that the threat level against it is increasing (Fox, 2016).

In Table 2, cyber attacks against civil aviation around the world between 2003 and 2021 are shown chronologically.

Table 2. Cyber-Attacks in Civil Aviation Industry

Year	Incident	Location	Description
2003	Slammer Worm attack	USA	One of the FAA's administrative server was compromised through a slammer worm attack. This attack shut down Internet service in some parts of Asia and slowed connections worldwide
2006	Cyber attack	Alaska, USA	Two separate attacks on US Federal Aviation Administration (FAA) internet services that forced it to shut down some of its air traffic control systems.
2008	Malicious hacking attack	Oklahoma, USA	Hackers stole administrative password of FAA's interconnected networks when they took control of their system.
2009	Malicious hacking attack	USA	A malicious hacking attack on FAA's computer, which gave them access to personal information on 48,000 current and former FAA employees.
2013	Malware attack	İstanbul, Türkiye	Shutting down of passport control system at the departure terminals of Istanbul Atatürk and Sabiha Gökçen airports due to malware attack, leading to the delay of many flights.
2013	Hacking and Phishing attacks	USA	Malicious hacking and phishing attacks that targeted about 75 airports.
2015	DDoS attack	Poland	A Distributed Denial of Service (DDoS) IT Network attack by cyber-criminals that affected LOT Polish Airlines flight-plan systems at the Warsaw Chopin airport. The attack made LOT's system computers unable to send flight plans to the aircraft, thus grounding at least 10 flights, leaving about 1,400 passengers stranded.
2016	Hacking an Phishing attacks	Vietnam	The defacement of website belonging to Vietnam airlines and flight information screens at Ho Chi Minh City and the capital, Hanoi, displaying messages of supportive China's maritime claims in the South China Sea by Pro-Beijing hackers.
2016	Cyber attack	Boryspil, Ukraine	A malware attack was detected in a computer in the IT network of Kiev's main airport, which includes the airport's air traffic control system.
2017	Human error	United Kingdom	British flag-carrier computer systems failure caused by disconnecting and reconnection of the data-center power supply by a contracted engineer. This accident left about 75,000 passengers

			of British Airways stranded.
2018	Data breach	Hong Kong	Cathay Pacific Airways data breach of about 9.4 million customers' personal identifiable information
2018	Data breach	United Kingdom	British Airways Data breach of about 380,000 Customers' personal identifiable information.
2018	Data breach	USA	Delta Air Lines Inc. and Sears Departmental stores reported a data breach of about 100,000 customers' payment information through third party
2018	Ransomware attack	Bristol Airport, UK	An attack on electronic flight information screens at Bristol Airport. This resulted to the screen being taken offline and replaced with whiteboard information.
2018	Mobile app data breach	Air Canada, Canada	Air Canada reported a mobile app data breach affecting the personal data of 20,000 people.
2018	Data breach	Washington DC, USA	Data breach on NASA server that led to possible compromise of stored personally identifiable information (PII) of employees on October, 23, 2018.
2018	Ransomware attack	Chicago, USA	Boeing was hit by the WannaCry computer virus. The attack was reported to have minimal damage to the company's internal systems.
2018	Cyber attack	Sweden	Cyber-attack launched by Russian APT group that jammed Sweden's air traffic control capabilities, grounding hundreds of flights over a 5-day period.
2019	Bot attacks	Ben Gurion Airport, Israel	About 3 million bots attacks were blocked in a day by Israel's airport authority as they attempted to breach airport systems.
2019	Cyber incident	Toulouse, France	A cyber incident that resulted to an unauthorised access to Airbus "Commercial Aircraft business" information systems.
2019	Ransomware attack	Albany, USA	Albany International Airport experienced a ransomware attack on Christmas of 2019. The attackers successfully encrypted the entire database of the airport forcing the authorities to pay a ransom in exchange of the decryption key to a threat actor.
2019	Crypto mining Malware infection	Europe	A discovery through Cyberbit's Endpoint Detection and Response (EDR) by Cyberbit researchers that showed an installation of crypto mining software infection that infected more than 50% of the European airport workstations.
2019	Phishing attack	New Zealand	A phishing attack targeted at Air New Zealand Airpoints customers. This attack compromised the personal information of approximately 112,000 customers, with names, details and Airpoints numbers among the data exposed.
2020	Ransomware attack	Denver, USA	A cyber-incident that involved the attacker accessing and stealing company data. The stolen data were later leaked online.
2020	Ransomware attack	San Antonio, USA	ST Engineering's aerospace subsidiary in the USA suffered a data breach, which involved Maze Cyber-criminal gaining unauthorised access to its IT network and thus launched a ransomware attack.
2021	Human Error	Birmingham, United Kingdom	A flaw in the IT system used by the operator to produce the load sheet, meant that an incorrect takeoff weight was passed to the flight crew.

Source: Ukwandu et al., 2021

As can be seen in Table 2, cyber attacks occurred as malicious hacking attack, malware attack, data breach, ransomware attack, mobile app data breach, cyber incident, crypto mining Malware infection, phishing attack and human error.

2.5. Cyber Security Studies of National and International Civil Aviation Organizations

2.5.1. Civil Aviation General Directorate - Sivil Havacılık Genel Müdürlüğü (SHGM)

DGCA, the measures that civil aviation enterprises should take against cyber threats and the place of the Corporate Cyber Incidents Response Team, which they should establish, in the business organization, capacity planning, qualifications of the personnel, the training they should take, the work that the enterprises should do before, during and after the cyber incident, the internal and issued an instruction to determine the procedures and principles regarding communication with external stakeholders (SHGM Talimat, 2022).

In September 2022, Aviation Sector Cyber Security Workshop was held with the participation of cyber security managers of 28 companies operating in the aviation sector. In the said workshop, cyber security activities in the aviation sector, which was determined as a critical infrastructure sector within the scope of the National Cyber Security Strategy and Action Plan, increasing cyber threats to the sector and cyber security structuring within

the scope of the Aviation Sector Institutional Transformation Project were discussed. On the other hand, the necessary steps to increase the current activities of the aviation industry in the field of cyber security were consulted with industry stakeholders (SHGM, 2022).

2.5.2. International Civil Aviation Organization (ICAO)

ICAO organizes international events to exchange information and discuss cybersecurity between governments, international organizations and industry. At the 40th session of the ICAO Assembly, the parliamentary decision on "Dealing with Cyber Security in Civil Aviation" was adopted. With this decision, the importance and urgency of protecting the critical infrastructure systems and data of civil aviation against cyber threats has been confirmed. ICAO organized the Cyber Security and Resilience Symposium in Amman, Jordan, between 15-17 October 2019, in order to take measures to reduce the abuse of critical information systems and promote a culture of cybersecurity (ICAO, 2022).

2.5.3. International Air Transport Association (IATA)

While IATA recognizes that aviation security is the responsibility of governments and that relevant authorities must respond to the needs of the aviation industry when faced with an urgent security threat, IATA believes that governments should be an active partner of the industry. IATA is developing the "Aviation Cyber Security Strategy and Risk Management Program" to systematically reduce the risk of cyber threats around the world. Thus, IATA takes an active leadership role in this challenge by engaging with members, industry leaders and stakeholders (IATA, 2022).

2.5.4. Federal Aviation Administration (FAA)

The FAA organizes an annual Cyber Security Awareness Symposium to promote cybersecurity awareness, collaboration, and partnerships among inter-agency stakeholders, industry and academia. The symposium provides an opportunity to discuss current security challenges as well as interact with colleagues and leading industry experts (FAA, 2022).

2.5.5. European Organisation for the Safety of Air Navigation (EUROCONTROL)

EUROCONTROL raises awareness to promote cybersecurity and cyber resilience and helps stakeholders develop the ability to defend against cyber threats. It also conducts threat and risk assessments while supporting the implementation of a harmonized security approach at the European and global level. It does this by collecting, generating and distributing relevant cyber intelligence, coordinating pan-European responses to cybersecurity alerts and incidents, and supporting national emergency response teams (EUROCONTROL, 2022).

2.5.6. European Civil Aviation Conference (ECAC)

The Cybersecurity in Civil Aviation Working Group (CYBER), formed by ECAC, develops best practices by providing guidance to ECAC member countries on cybersecurity. It also aims to increase awareness of cyber threats in ECAC member countries. The working group keeps the relevant ECAC recommendations and supplements updated. At CYBER's meeting in April 2022, topics discussed include competency-based cybersecurity training, risk management for the supply chain, cybersecurity standards for scanning equipment, and cyber surveillance models (ECAC, 2022).

2.5.7. European Union Aviation Safety Agency (EASA)

EASA has developed a Cybersecurity Roadmap that was approved by the Board of Directors in November 2015. EASA has since been working on its implementation and has launched a number of initiatives that increase flexibility and support embedded security to better understand and address cybersecurity threats in the aviation industry. In addition to its institutional rule-making activity, EASA works to increase international cooperation on the subject and to promote knowledge sharing among sectoral stakeholders.

Creating an aviation system that is resistant to cyber threats and incorporating cyber security into the current safety concept depends on the coordinated effort of aviation stakeholders. That's why EASA chairs the European Strategic Coordination Platform, which includes representatives of member states, European Union institutions and key industry stakeholders. This collaboration contributed to the alignment of aviation stakeholders' goals, making it possible to develop the first joint strategy for cybersecurity in aviation. Relevant stakeholders are also in the process of determining a common roadmap to implement this strategy. Finally, EASA supports the creation of the European Center for Cybersecurity in Aviation (ECCSA) to promote voluntary knowledge sharing and expert collaboration (Easa, 2022).

The main activities of EASA regarding cyber security are:

- ✓ 2nd High Level Conference on European Union Cyber Security Strategy (28.05.2015),
- ✓ 1st Meeting of Member States' Aviation Cyber Security Representatives (26.05.2016),
- ✓ Workshop on the Roles and Activities of the European Cyber Security Center in Aviation (13.07.2016),
- ✓ Cyber Security High Level Meeting in Civil Aviation (08.11.2016),
- ✓ Aviation Cyber Security Workshop (31.05.2017),
- ✓ 1st Transport Cyber Security Conference (23.01.2019),
- ✓ Inviting Eligible Organizations to Participate in the European Center for Cybersecurity in Aviation (24.07.2019).

2.6. Cyber Security Studies of Aircraft Manufacturers

2.6.1. Cyber Security Studies of Boeing Company

Boeing, together with the aviation and information security industry, is developing a holistic cybersecurity that addresses aircraft and ground systems and has a threat management component. Aviation security includes identifying emerging threats, guiding incident response, and conducting forensic analysis. These response and analysis services are provided through CAS Professional Services. Boeing strives to develop a unified cyber strategy and deliver cybersecurity solutions to airlines around the world to enhance industry collaboration. Boeing has established the Cyber Technical Center to develop these solutions and will provide the following services through this center (Boeing, 2022):

- ✓ Making cyber threat and vulnerability assessments of airborne systems,
- ✓ Designing cyber protection for Boeing commercial aircraft,
- ✓ Development of industry standards for aviation safety,
- ✓ Monitoring and detecting cyber incidents.

2.6.2. Cyber Security Studies of Airbus Company

The presence of nearly 1000 security experts, experienced in the field, within the company called "Airbus Cybersecurity", which Airbus established for cyber security, shows how much importance is given to cyber security. Hyperconnected systems are more vulnerable to cyber attacks. In the case of critical infrastructures such as production facilities, power grids and nuclear power plants, such attacks can seriously affect both operational continuity and human safety. Airbus is innovating to protect organizations against this possibility. On the other hand, Airbus trains its cyber analysts to work seamlessly with AI by creating next-generation AI-powered cyber defense tools.

- ✓ The scope of Airbus' innovation projects includes (Airbus, 2022):
- ✓ Security/security risk analysis,
- ✓ Cyber-physical security and situational awareness,
- ✓ The cyber-resilient factory of the future,
- ✓ Security of collaborative smart industrial assets,
- ✓ Security of air transport infrastructure,
- ✓ Security of unmanned aircraft systems,
- ✓ Enemy artificial intelligence,
- ✓ Cyber security simulation and training.

3. CONCLUSION AND RECOMMENDATIONS

Cyber attacks pose a growing threat to the aviation industry. Aviation institutions are increasingly relying on electronic systems for critical operations as well as routine operations. It has become a necessity to protect electronic systems from cyber attacks and maintain the level of security. For this purpose, all organizations and units operating in civil aviation have to implement the necessary measures.

Airlines must encrypt customer data on their websites, apps, and other systems. Passengers entrust their personal information, credit card and passport information to airline companies. If airlines do not encrypt this data, their passengers' identities and/or financial information can be stolen or leaked. Given that so many people's data is at stake, it's inevitable that encryption needs to be comprehensive. On the other hand, it is almost impossible to regain the trust of passengers when passenger information is stolen or leaked. Therefore, being equipped with security measures is an important part of maintaining reputation in the business world.

It is important to strengthen information technology departments in airline companies and airports. Professionals are needed who can think like a hacker and anticipate the next steps. Organizations that include well-trained and expert employees should benefit from the knowledge of these personnel and prepare the ground for transferring their experiences to other employees. On the other hand, one of the issues that employees should pay attention to is to be careful against suspicious messages and e-mails. In case of doubt, the personnel should report the message or e-mail to the relevant unit of the company.

The large number of devices in aircraft and air traffic control systems can make it difficult to detect the vulnerability. For this reason, control systems can be put to the test by means of inspection at certain intervals. These tests will reveal whether the aircraft and air traffic control systems have glaring vulnerabilities and, if so, how the vulnerabilities can be remedied. At the same time, these tests will help organizations stay up-to-date on attack trends.

Governments around the world are taking action to take cybersecurity measures for both commercial and military aviation. For example; The US government allocated $14 billion in 2016 to improve cybersecurity systems and prevent cyberattacks by organized crime gangs. That same year, the U.S. government allocated $160 million to the Department of Energy's National Nuclear Security Administration for cyber-protection of weapons programs (Jabil, 2022).

In general, although governments take adequate precautions, providing cyber security should not be left to governments alone. In this sense, all aviation stakeholders, including the public, private sector and non-governmental organizations, need to evaluate their physical and digital security strategies and determine how they will respond to increasing threats. In addition, organizations need to communicate with industry players in order to be aware of developments and innovations in the industry.

In order to effectively manage cyber risks in terms of aviation management:

- ✓ Predetermination of cyber risks (Proactive approach),
- ✓ Developing the cyber security workforce,
- ✓ Renewal of old systems,
- ✓ Having an educated and skilled workforce in cyber security,
- ✓ Increasing cyber security awareness (Governments and international authorities fulfill their responsibilities),
- ✓ National and international civil aviation organizations to cooperate and share information about cyber threats and cyber attacks,
- ✓ Relevant public institutions must ensure that new technologies are tested and certified.

REFERENCES

1. Abeyratne, R. (2011). Cyber Terrorism and Aviation-National and International Responses, Journal of Transportation Security, 4 (4), 337-349.
2. Abeyratne, R. (2020). Aviation and Cybersecurity in the Digital World, Aviation in the Digital Age, 173–211.
3. Airbus, (2022). https://www.cyber.airbus.com/innovation/
4. Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi, International Journal of Multidisciplinary Studies and Innovative Technologies, 1 (1), 24-28.
5. Berger, D. (2022). https://www.tripwire.com/state-of-security/ics-security/defending-aircraft-networks-against-cybersecurity-breaches/
6. Boeing, (2022). https://www.boeing.com/commercial/aeromagazine/articles/2012_q3/5/

7. De Cerchio, R. & Riley, C. (2011). Aircraft Systems Cyber Security, In 2011 IEEE/AIAA 30th Digital Avionics Systems Conference (pp. 1C3-1), Seattle, USA.
8. EASA, (2022). European Union Aviation Safety Agency, https://www.easa.europa.eu/en/domains/cyber-security/main-easa-activities
9. ECAC, (2022). European Civil Aviation Conference, https://www.ecac-ceac.org/activities/security/study-group-on-cyber-security-in-civil-aviation-cyber
10. EUROCONTROL, (2022). European Organisation for the Safety of Air Navigation, https://www.eurocontrol.int/cybersecurity
11. FAA, (2022). Federal Aviation Administration, https://www.faa.gov/air_traffic/technology/cas
12. Filinovych, V. & Zhengbing, H. (2021). Aviation and the Cybersecurity Threats, Advances in Economics, Business and Management Research, vol. 188, 120-126.
13. Fox, S. J. (2016). Flying Challenges for the Future: Aviation Preparedness – in The Face of Cyber-Terrorism, Journal of Transportation Security vol. 9, 191-218.
14. Gopalakrishnan, K., Govindarasu, M., Jacobson, D.W. & Phares, B.M. (2013). Cyber Security for Airports, International Journal for Traffic and Transport Engineering, 3 (4), 365-376.
15. Gramatica, M. D., Massacci, F., Shim, W., Tedeschi, A. & Williams, J. (2015). IT Interdependence and the Economic Fairness of Cybersecurity Regulations for Civil Aviation, IEEE Security & Privacy, 13 (5), 52 – 61.
16. Gürkaynak M., & İren A. A. (2011). Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 16 (2), 263-279.
17. IATA, (2022). International Air Transport Association, https://www.iata.org/en/programs/security/
18. ICAO, (2022). International Civil Aviation Organization, https://www.icao.int/Search/pages/results.aspx?k=cyber%20security
19. Ishtiaq, S. & Rahman, N. A. (2022). Cybersecurity Vulnerabilities and Defence Techniques in Aviation Industry, Atlantis Highlights in Computer Sciences, vol. 4, 559-567.
20. İrdem, İ. ve Çobanoğlu, S. (2022). Yapay Zekanın İç Güvenlik Yönetimi Üzerine Yansımaları: Siber Güvenlik, Kamu Yönetimi ve Teknoloji Dergisi, 3 (2), 175-202.
21. Jabil, (2022). https://www.jabil.com/blog/defense-and-aerospace-security.html
22. Kagalwalla, N. & Prathamesh, P. C. (2019). Cybersecurity in Aviation : An Intrinsic Review, 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA), 1-6, Pune, India.
23. Karasoy, H. A. (2021). Kamu Güvenliğinde Yeni Paradigmalar: Hibrit Savaş Asimetrik Savaş Vekâlet Savaşı İstihbarat ve Terörle Mücadele, Nobel Yayıncılık, Ankara.
24. Kovalchuk, T. I., Korystin, O.Y. & Sviridyuk, N.P. (2019). Hybrid Threats in the Civil Security Sector in Ukraine, Problems of Legality, vol. 147, 163-175.
25. Kurnaz, S. ve Önen, S. M. (2019). Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri. International Journal of Politics and Security, 1 (2), 82-103.
26. Oster, C. J., Strong, J. & Zorn, C. (2013). Analyzing Aviation Safety: Problems, Challenges, Opportunities. Research in Transportation Economics, 43 (1), 148–164.
27. Schmidt, A.V. (2016). Cyberterrorism: Combating the Aviation Industry's Vulnerability to Cyberattack, Suffolk Transnational Law Review, 39 (1), 169-181.
28. Sertçelik, A. (2015). Siber Olaylar Ekseninde Siber Güvenliği Anlamak, Medeniyet Araştırmaları Dergisi, 2 (3), 25-42.
29. Shahbazian, E. & Rogova, G. (2016). Critical Aviation Information Systems Cyber-Security, In Meeting Security Challenges Through Data Analytics and Decision Support, Vol. 47, p. 308, IOS Press.

30. SHGM Talimat, (2022). Sivil Havacılık Genel Müdürlüğü, https://web.shgm.gov.tr/documents/sivilhavacilik/files/mevzuat/sektorel/talimatlar/2022/SHT-Siber.pdf

31. SHGM, (2022). Sivil Havacılık Genel Müdürlüğü, https://web.shgm.gov.tr/tr/s/6955-havacilik-sektoru-siber-guvenlik-calistayi-sona-erdi

32. Silva, S. J. da & Silva, J. M. R. (2021). Cyber Risks in the Aviation Ecosystem: An Approach Through a Trust Framework, Integrated Communications Navigation and Surveillance Conference, ICNS, 1-12, USA.

33. Şenol, M. (2016). Siber Güçle Caydırıcılık Ama Nasıl? Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 2 (2), 10-17.

34. UDHB, (2013). Ulaştırma Denizcilik ve Haberleşme Bakanlığı, "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf

35. Ukwandu, E., Farah, M.A.B., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C. & Bellekens, X. (2021). Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends, https://doi.org/10.48550/arXiv.2107.04910

36. Zalewski, J. & Kornecki, A. (2019). Trends and Challenges in the Aviation Systems Safety and Cybersecurıty, Task Quarterly, 23 (2), 159-175.