bildiri 21.05.2023

Yazar Rafet Ertekin

Gönderim Tarihi: 21-May-2023 09:02AM (UTC+0300)
Gönderim Numarası: 2098131888
Dosya adı: TRY_S_CYBERSECURITY_THREATS_AND_FUTURE_TRENDS_Rafet_Ertekin.docx (264.81K)
Kelime sayısı: 5369
Karakter sayısı: 36573

AVIATION INDUSTRY'S CYBERSECURITY: THREATS AND FUTURE TRENDS

Rafet Ertekin[1] Vildan Durmaz[2]

ABSTRACT

The aviation industry is a complex system of computer systems and networks that rely on reliable operation. Therefore, ensuring the security of these systems and networks is crucial for the safety of passengers, crew, and aircraft, as well as for the protection of sensitive information and data. The aviation sector is faced with a wide range of cyber threats, including attacks on computer systems, networks, and other critical infrastructure, from various sources such as nation-states, criminal organizations, and individual hackers. Aviation companies also perform regular security assessments to identify vulnerabilities in their systems and networks, and provide their employees with training and awareness programs to detect and respond to potential cyber threats. Overall, cybersecurity is a critical issue for the aviation industry, requiring constant attention and proactive measures to protect against cyber threats. In this study, cyberattacks against the aviation industry worldwide are examined, and potential cyber attack scenarios are presented from the perspective of the Civil Aviation Cybersecurity Instructions. The current level of preparedness of the Turkish civil aviation industry is emphasized, along with the measures that need to be taken in the face of future cyber attack trends and expected challenges.

Keywords: Aviation Cyber Security, Cyber Attacks and Threats, Cyber Security Ecosystem

1. Introduction

International Telecommunication Union (ITU) cybersecurity; It defines the cyber environment as a collection of tools, policies, security concepts, security measures, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the organization and the user's assets. This includes the assets of the organization and the user, the information processing devices connected to them, the personnel, the infrastructure, the applications, the services, the telecommunications systems, and all the information transmitted and/or stored in the cyber environment (Von Solms, R., & Van Niekerk, J, 2013). Cybersecurity can be defined as technologies and processes developed to protect computers and their hardware, software, networks and data from unauthorized access, vulnerabilities created over the Internet by cybercriminals, terrorist groups, and hackers (Goutam, R. K. 2015).

Aviation industry, airlines, airports, technology providers etc. It covers a wide network of stakeholders and interacts with various sectors, especially defense and national security, transportation, communication, banking and energy. The aviation industry, which operates in the international arena and has direct and indirect activities with many sub-sectors such as tourism and foreign trade, has to benefit from technological solutions in order to meet the needs of this complex structure and to provide safety and security. In this context, with the increase in the use of innovative technology, it is seen that the sector is gradually becoming digital. Within the scope of the above-mentioned issues, cyber attacks against the aviation industry have increased even more recently. When the said attacks disrupt the functioning of the sector, negative consequences arise in the establishment of social order and the provision of public services, and economic losses arise due to cancellations and delays.

[1] Öğr. Gör., İstanbul Okan Üniversitesi, TÜRKİYE, e-mail: rafet.ertekin@okan.edu.tr, rafetertekin1@gmail.com
ORCID: https://orcid.org/0000-0001-7781-4852
[2] Doç. Dr., Eskişehir Teknik Üniversitesi, TÜRKİYE, e-mail: vkorul@eskisehir.edu.tr
ORCID: https://orcid.org/0000-0003-3649-1780

1.1. RESEARCH OBJECTIVE AND METHODOLOGY

In this study, it is aimed to improve and update the cyber security regulations, standards and principles of the sector within the current legal framework, considering the importance of cyber technologies for the operational integrity of the aviation industry. It is aimed to make a situation analysis regarding potential cyber threats and to determine the precautions to be taken. The research method used in this study is qualitative and based on document analysis. In the "Conceptual Framework" section, which is the first part of the study, the concepts of cyber security, cyber space and critical infrastructure are explained. The second part covers topics such as the Attack Surface and Vulnerabilities, threat actors, their motivations, and an examination of past cyberattacks faced by the aviation industry. The study examines threats, attack types and predicts future cyber attack trends based on potential attack scenarios. In the third part, the study analyzes the preparedness and future strategy of the Turkish civil aviation sector against cyber threats within the legal framework of SHT-SİBER (Civil Aviation Cyber Security Institution). It offers solutions and future vision in line with the ICAO Global Aviation Security Plan (GASeP), IATA Aviation Security Strategy and Objectives.

1.2. CONCEPTUAL FRAMEWORK

1.2.1. Cybersecurity

The first studies and definitions of cyber security emerged with the increasing prevalence of computers and the expansion of the internet. One of the first studies in this area, Robert Morris Sr. tried the program called Morris worm on Harvard University computers in 1988 and was recorded as the first person to be penalized within the framework of the Computer Fraud and Abuse Law (Güner, 2015). In the 1990s, the concept of cyber security gained even more importance with the rapid spread of the internet. In this period, cyber security studies and definitions were further developed and diversified. Today, cybersecurity is an interdisciplinary field made up of many different disciplines and includes a set of technologies, policies and processes designed to protect computer systems, networks and data from malicious attacks.

Cyber security in the 2020-2023 Türkiye National Cyber Security Strategy and Action Plan; It is a series that covers the protection of the information systems that make up the cyber space from attacks, ensuring the confidentiality, integrity and accessibility of the information and data processed in this environment, activating the reaction mechanisms against these detections. Cyber security experts work to prevent cyber attacks and ensure cyber security by performing these activities. In addition, cyber security measures, detection of cyber incidents and the development of effective response mechanisms are also a part of cyber security.

According to the International Telecommunication Union (ITU), cyber security; It is defined as "the collection of methods, policies, concepts, guidelines, risk management approaches, activities, training, best practice experiences and technologies used to protect the information assets of institutions, organizations and users".

In recent years, cyber attacks in the aviation industry are considered as a hybrid threat. One of the most important issues of such attacks is the scenario of crashing the aircraft during flight. Damages caused by malicious cyber attacks on air traffic control systems are a general concern worldwide (Bachmann, 2011). These attacks can be carried out by state or non-state actors, as well as by highly specialized groups and firms. In recent years, the concept of "hacktivism", formed by combining the words "hacker" and "activism", refers to activists who use the Internet for various purposes. They continue their propaganda activities for specific purposes, especially by hacking for political or ideological reasons (Chertoff, 2011).

1.2.2. Cyberspace

Cyberspace is a term also known as "cyber domain" or "cyber world". As defined in the national strategy documents, it defines a digital environment consisting of interconnected information systems distributed around the world and located in a digital environment extending into space (Sagiroglu, 2018, p.25). This digital environment includes data, software, hardware and communication infrastructures as well as technological devices such as the internet, computers, mobile devices and other electronic devices. The importance of cyber space is increasing and it needs to be protected against cyber attacks by cyber security experts.

The definition of cyberspace may differ among researchers focusing on different technological features. While some think that this term is only suitable for the internet environment, in fact, cyberspace is a universe that encompasses all information systems and their users. In the most general sense, it is an intangible space where people interact and communicate with other people or entities through interconnected information systems (Bıçakçı, 2014: 106). At the NATO Lisbon summit held in 2011, cyberspace was accepted as a part of the defensive reflexes in the Strategic Concept (Herzog, 2011).

1.2.3. Critical Infrastructure

Critical infrastructure is infrastructure that is vital for a country's daily life and can cause serious social, economic and even national security risks if damaged. These infrastructures often include sectors such as energy, transportation, communications, water supply, healthcare, financial services and utilities. Critical infrastructure includes the infrastructure, including information systems, that can cause significant damage when the confidentiality, integrity or accessibility of the processed information/data is compromised (Transport, T. C., & Ministry, A. 2020). There are many critical infrastructures, applications and systems in the cyber environment. These include many infrastructures and applications such as online shopping systems, banking systems, electricity generation and distribution facilities, smart grids, mobile network operators, SCADA systems, communication systems, natural gas control and transmission systems, air traffic control centers, computer and communication systems (Sagiroglu, 2018, p.37).

Europe's critical infrastructure protection program is an initiative of the European Union. This program aims to protect critical infrastructures in Europe from cyber attacks, natural disasters, man-made events and other threats. According to the program, critical infrastructure is defined as physical and information technology facilities, networks, services and assets that will have a serious impact on the health, safety, economic well-being of citizens or the effective functioning of governments in EU countries (EU, 2006).

2. Attack Surface and Security Vulnerabilities.

The aviation industry manages its operations using complex information technology solutions such as software used on aircraft and airports, Wi-Fi connections, and in-flight entertainment systems. These modern technologies increase the effectiveness of aircraft control systems and improve flight safety and performance. However, the situation where data flows between multiple stakeholders and internal/external systems in this ecosystem widens the attack surface. The basic technologies used in the aviation industry can be classified as smart systems, IoT devices, cloud infrastructures, big data and blockchain. Especially remotely accessible smart systems (for example, biometric systems, robotic

systems), IoT devices (sensors, actuators, etc.) and cloud systems have become the target of cyber attacks.

2.1. Threat Actors and Their Motivations

The aviation industry is frequently targeted by threat actors due to access to sensitive data. This sensitive data includes information such as passport details and high-value credit card information. The most common threat actors and their motivations in the aviation industry are outlined below.

Table 1: Threat Actors and Their Motivations

Threat Actor	Motivation
Hacktivists	Political or ideological reasons, activism
Cybercriminals	Financial gain, stealing personal information
Nation-state actors	Espionage, political influence, national security interests
Competitors	Gaining a competitive advantage
Insiders	Revenge, personal gain, sabotage
Terrorist organizations	Disrupting transportation systems, instilling fear

Source: Adapted from https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/#

2.2. Cyber Attacks Occurring in the Aviation Industry

The aviation industry is a target for cyber attacks due to its involvement in critical activities such as international travel and cargo transportation. Therefore, ensuring security in the aviation industry is of paramount importance. Cyber attacks pose serious threats to data security, flight safety, and customer information within the aviation industry. Airlines and airports are vulnerable to cyber attacks, with many attacks being carried out through ransomware attacks, phishing, malware attacks, and exploiting security vulnerabilities. Such attacks can have significant consequences in the aviation industry. For example, an attack on an air traffic control system can lead to flight delays or cancellations. Another area that becomes a target of cyber attacks is the systems related to air transportation. These systems perform critical functions such as flight planning and management, cargo transportation, customer reservations, ticket sales, and baggage management. Therefore, a cyber attack on these systems can cause a major disruption in the aviation industry. The table below provides examples of cyber threats and attacks that have occurred in the aviation sector.

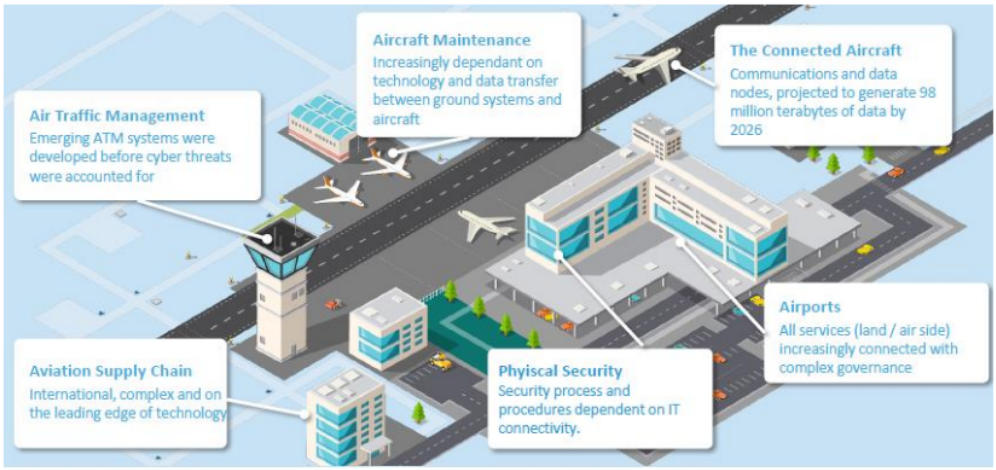
Table 2: Major Cyber Threats and Attacks in the Aviation Industry

Year	Company/Organization	Description
2001	American Airlines	American Airlines' reservation system was targeted in a cyber attack after the September 11 attacks, leading to the cancellation of thousands of flights [1].
2003	Naval Air Weapons Station	Naval Air Weapons Station was infiltrated and national security information was accessed by Chinese hackers.
2005	Lockheed Martin and Boeing	NASA networks managed by Lockheed Martin and Boeing were hacked to gain access to information about the Space Shuttle Reconnaissance program.
2006	NASA	NASA had to block email attachments as a precautionary measure before shuttle launches due to potential cyber attacks.

2008	Air Traffic Control	More than 800 unresolved cyber incident alerts reported at air traffic control facilities [2].
2009	FAA	FAA's computer systems were hacked and commercial air traffic was disrupted.
2010	Iranian Nuclear Program	A computer virus named Stuxnet has been detected, targeting Iran's nuclear program. [3].
2012	Turkish Airlines	THY website experienced a cyber attack, resulting in restricted access to the website [4].
2013	Iranian Hacker Group Attack	Iranian hackers targeted airlines, energy companies, and transportation organizations to steal user credentials and passwords [5].
2014	Warsaw Chopin Airport	The flight planning system at Warsaw's Chopin Airport was locked for approximately five hours [6]. Malaysia Airlines' website was hacked [7].
2015	LOT	Polish airline LOT's passenger information system was compromised, leading to flight cancellations [8]. US and European aviation companies also had turbofan engine-related secrets stolen. United Airlines' flight planning system and pilots' flight information system were blocked, and customer data was leaked.
2017	Boryspil Airport	Ukraine's Boryspil Airport experienced a cyber attack, affecting flight operations and leading to flight cancellations [9]. British Airways' website and mobile app were targeted, resulting in the theft of personal and financial information of 380,000 customers [10].
2018	Ben Gurion Airport	An attempted cyber attack aimed to take control of Israel's airport computer systems, potentially causing flight cancellations [11]. Singapore Airlines disclosed the theft of customers' credit card information in a cyber attack.
2020	EasyJet	The travel records of nine million EasyJet customers were accessed.
	Travelex	Travelex, a financial institution providing foreign exchange services at airports, was affected by ransomware attack [12].
	Garmin	Garmin, a GPS technology provider, was targeted in a ransomware attack [14].
	SITA	SITA, an IT provider for the air transport industry, experienced a cyber attack resulting in the theft of customer information [15].
	Air India	Air India. suffered a cyber attack, leading to the theft of customer information [16].
2022	BAE [17] / BECU	Boeing Employees' Credit Union reported a data breach [18].
	DJI	DJI's airspace monitoring devices had a database leak, exposing over 80,000 drone identities [19].
2023	Air France-KLM	Air France and KLM warned customers about the hacking of their loyalty program accounts [20]. DDoS attacks targeted airports in Nepal and Poland [21]. Eurocontrol, reported an attack claimed by pro-Russian hackers.

Source: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230404_Significant_Cyber_Events.pdf?VersionId=3UxjuqXLPluSCUtSXhGM1ZecgewJ4wPI

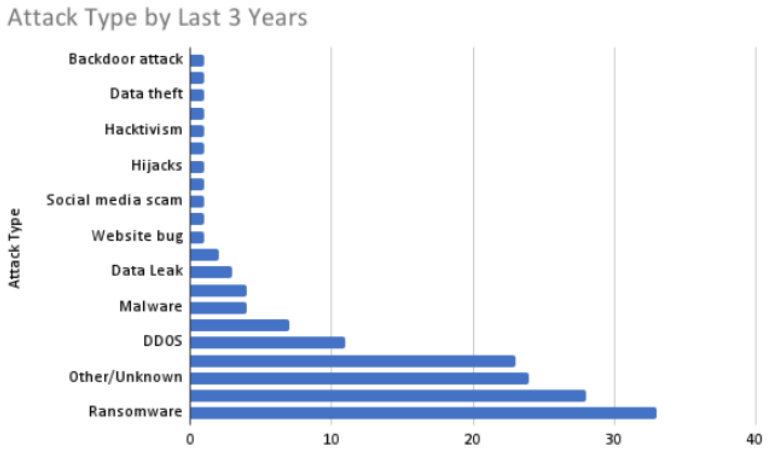
Airports are increasingly digitizing and interconnected to provide services. However, many of these services are delivered through remote or wireless connections. This includes access control, maintenance, baggage handling systems, and high-speed wireless connections between the airside systems and aircraft docking gates. All these digitized services operate within the complex framework of airport management and accountability, which expands the attack surface. Therefore, airport operators need to develop security policies, processes, and technologies to identify and mitigate security vulnerabilities, thereby strengthening the defense of airport systems. This way, airports can become more resilient against cyber attacks and ensure the safety and comfort of passengers (Atlantic Council, 2019).



Source:(ICAO,2019)

In recent years, cyber incidents in the aviation sector have been evaluated within the scope of events monitored by Eurocontrol. Eurocontro publishes the Aviation Cyber Incident Map[3] through EATM-CERT (European Air Traffic Management Computer Emergency Response Team). The findings and graphs based on the data from this map are as follows: In 2020, 52 attacks were reported, followed by 48 attacks in 2021, and as of the end of August 2022, 50 attacks have been reported, indicating that only in this period of 2022, the eight-month average of the past two years has been reached. The most common attack types in the past three years are as follows: 16% are categorized as other/unknown, ransomware (22%), data breaches (18.6%), phishing (15.3%), and DDoS (7.3%). In addition to attacks on civil aviation, eight incidents related to military-linked cyber espionage and data theft have been reported.

Chart 1: Types of Cyber Attacks in the Last 3 Years (2020-21-22)



[3]https://www.google.com/maps/d/embed?mid=1ptVIma0CZqoPiNzsomzbRVQDRS7BXGk&ll=58.511497552256955%2C-105.7431945&z=8

Source: https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/#

2.3. Possible Cyber Attack Scenarios in Aviation Infrastructure Security

The NextGen project, launched in the USA in 2005, and the SESAR project in Europe, made significant contributions to the modernization of aviation infrastructure. These studies created a more efficient structure by automating the operations in various subsystems, but also led to the emergence of interdependent systems. This dependency has led to the emergence of different security vulnerabilities. Studies focusing on these issues are of great importance for the safety, reliability and sustainability of aviation systems. When the security of aviation infrastructure is examined, the table presents attack scenarios for five different subsystems (Sağıroğlu, 2022).

Table 5: Vulnerabilities of Aviation System Subcomponents in Navigation and Attack Scenarios

Component	Vulnerabilities
Networks	Use of internet protocol addresses for air traffic management (ATM)
Electronic subsystems	Sensors supporting power supply and engine control
Software subsystem	Integrated Modular Avionics (IMA)
Analytical subsystems	GPS
Communication subsystem	Navigation signals necessary for coordinating flights
Data	Collision avoidance real-time support (System Wide Information Management - SWIM) feature
Electronic Flight Bag (EFB):	
Code execution attack	The attacker gains full access to the bad critical system on the server.
Privilege escalation attack	The attacker escalates privileges from standard user to admin/root user.
Authentication bypass attack	An attacker may try to connect to the critical system with an unauthorized device or use stolen credentials.
Denial-of-Service (DoS) attack	An attacker occupies the remote access protocol, preventing real users from connecting to the system.
Spoofing attack	Modifies the commands the user performs.
Aircraft Communications Addressing and Reporting System (ACARS):	
Lack of authentication in data .transfer	Attackers can modify and manipulate about 99% of the plaintext traffic transmitted, potentially causing harm
Interference with ACARS communications	Attackers can interfere with unprotected ACARS communications and send incorrect or false messages to aircraft
Automatic Dependent Surveillance Broadcast (ADS-B):	
Passive attacks	Limited to listening to the transmitted data without making changes to it
Active attacks	Manipulating radar images of aircraft to create ghost planes or disrupt services
- Ghost Plane Insertion	Adding fake messages to the ADS-B communication channel to create ghost planes
- Ghost Plane Raid	Simultaneously adding multiple aircraft to the system, causing denial of service to surveillance systems
- Ground Station Raid	Attack on ground station systems, potentially causing disruptions to ATC systems that use ADS-B
- Virtual Orbit Change	Aims to change the trajectory of an aircraft by manipulating its position reports
- Aircraft Disappearance	Erasing all messages of a target aircraft from ADS-B broadcasts, preventing the aircraft from being detected
Instrument Landing System (ILS):	
Spoofing attack	Using carefully prepared fake signals with higher signal power to disrupt genuine ILS signals and mislead the pilot
Single-tone attack	Poses a significant danger, particularly for pilots flying under low visibility conditions
Spoofing attack	Blocking genuine signals and sending fake signals to receivers, potentially leading to incorrect speed and position information
Signal jamming attack	Suppressing satellite signals by emitting high-power interference signals

Source: (Akleylek, N. Ç. S., 2018)

The aviation sector, due to its global and interconnected nature, presents challenging cybersecurity risks in terms of scale and complexity. Therefore, understanding, prioritizing, and taking action on cybersecurity risks can be difficult for organizations. Additionally, cybersecurity incidents in the aviation sector are considered to have the potential to rapidly escalate and have international implications. This highlights the necessity of addressing and managing cybersecurity risks on a global scale. However, inconsistencies and inadequacies persist in identifying, managing, and communicating cybersecurity vulnerabilities in the aviation sector. This leads to a weak visibility of the actual cybersecurity risk. Therefore, better collaboration and coordination among all stakeholders in the aviation sector are necessary (ICAO, 2019).

Table 6: Cybersecurity Threats to Aviation Security

Subsystem	Threats
Central Maintenance System (CMS)	Data issues causing operational disruptions
Electronic Flight Bag (EFB)	Advanced threats due to program launches on onboard systems
Flight Management System (FMS)	Data corruption or upward attacks affecting various flight systems
Avionics	Vulnerable to similar threats as FMS due to constant connections and integration with flight controls
Electronic Logbook	There is the potential for operations to be interrupted due to a cyberattack on the aircraft.
On-Board Server	Potential weak point for multiple cyber attacks
Navigation Systems	Potential vulnerabilities due to increased use of data communications, such as ADS-B
Aircraft Management Systems	Electronic cabin management offers new opportunities for cyber attacks
Central Maintenance System (CMS)	Data issues causing operational disruptions
Catering/In-Flight Services	Unauthorized catering or materials loaded onto the aircraft, counterfeit documents
Access Control	Unauthorized access granted, doors left open
Access Control	Unauthorized access to airport access cards
Background Checks	Counterfeit information
CCTV/Intrusion Detection Systems	System compromise, undetected threats, and unauthorized access
Reservation System	(Dos) attacks
Passenger Name Registration (PNR) and Customer Relationship Management (CRM)	(Dos) attacks Passengers data preaches.
Departure Control Systems (DCS)	Denial of Service (DoS) and Spoofing; Advanced Passenger Information response, Watchlist response. Unauthorized boarding of the aircraft.
Airline Mobile Applications	Fraud attacks and data privacy concerns.
Frequent Flyer Programs	Financial fraud, airline's financial liability
Flight Planning	Impact on overall aircraft operations
Baggage Discrepancy	Unauthorized or uncontrolled baggage loading
Crew Planning	Complex logistics, limited backup personnel
Back Office Management	Email and office application vulnerabilities, Trojan attacks, identity theft
Cargo	For carriers that provide cargo, airlines are vulnerable to spoofing and upstream attacks. Cargo reservations, E-Airline Invoices or E-Delivery Security Statements may be fraudulent; Unauthorized or uncontrolled cargo may be loaded onto the aircraft.
Supply Chain Intervention	Unauthorized products entering restricted areas or loaded onto aircraft,
Passenger Screening	Algorithms in scanning equipment (WTMD, FBS, ETD, X-RAY) can be manipulated so that they do not detect threats.
Baggage/Cargo Screening	Manipulation of algorithms in screening equipment (ETD, X-ray) to evade threat detection, automatic cleaning or bypass mode settings for X-ray systems
Communication	Interference or complete shutdown of communication systems, negative impact on security incident response

Source: (ICAO, 2019)

3. CYBERSECURITY REGULATIONS AND LEGAL FRAMEWORK IN AVIATION AUTHORITIES

3.1. ICAO Global Aviation Security Plan (GASeP)

The Cybersecurity Strategy published by ICAO provides a vision for the global industry of civil aviation. This vision aims for the sector to remain resilient against cyber attacks and to maintain global security and trust while continuing to innovate. To achieve this, it is essential for all aviation stakeholders, including governments, international organizations, regulators, manufacturers, and service providers, to collaborate. This requires understanding and managing cybersecurity risks in aviation, implementing rapid, globally harmonized, and effective changes. As stated in ICAO Assembly Resolutions A40-10, support for this strategy addressing cybersecurity in aviation is necessary (Atlantic Council 2019).

In 2014, hackers of the global aviation system were identified by the International Civil Aviation Organization (ICAO), Airports Council International (ACI), the Civil Aviation Navigation Services Organization (CANSO), the International Air Transport Association (IATA) and the Aviation Industry Associations International Coordinating Council (ICCAIA). An agreement has been signed for a joint fight against cyber threats, fearing that it may be vulnerable to attacks by other These five aviation organizations have declared that they form a front against cyber threats and will take measures against attacks that may be carried out with malicious purposes such as information theft and loss of people. In addition, these organizations have committed to share information on threat identification, risk assessment and cybersecurity measures. Its aim is to create a safe cyber culture and develop useful strategies for civil aviation (ICAO, 2014).

At the 39th Assembly of ICAO held in 2016, GASeP (Global Aviation Security Plan) was created to identify cyber security threats to the critical infrastructure, data and information communication technology systems of civil aviation. This plan aims to improve aviation security through internationally recognized priority actions, missions and objectives that are fully aligned with the Global Air Navigation Plan (GANP) and the Global Aviation Safety Plan (GASP). GASeP is designed to facilitate collaboration among all industry stakeholders and improve overall aviation safety. The plan addresses five key priorities: increasing risk awareness and response, developing a culture of safety and human capacity, advancing technological resources and innovation, strengthening oversight and quality assurance, and increasing collaboration and support. This plan replaces ICAO's Comprehensive Aviation Security Strategy.

As part of its broader initiative in Aviation Cybersecurity, IATA organized the first Aviation Cybersecurity Roundtable Meeting (ACSR) in 2019 at its Regional Office in Singapore. The participants included representatives from various sectors such as airports, airlines, Air Traffic Management (ATM), regulators, Original Equipment Manufacturers (OEMs), and cybersecurity service providers. The objective of the ACSR was to better understand and manage cybersecurity risks in civil aviation by promoting interdisciplinary collaboration, sharing experiences and knowledge, and developing concrete actions that could assist the aviation industry. The meeting highlighted the increasing complexity of cybersecurity risks in the aviation sector due to the growing digitization and connectivity, emphasizing the need for proactive measures (IATA, 2019).

According to the "Finding Lift, Minimizing Drag" report published by the Atlantic Council in 2017, the aviation sector faces a significant cybersecurity challenge, and the nature of this problem,

along with different perspectives, can hinder concrete progress. While the aviation industry is globally resilient, even attacks on non-critical systems can undermine stakeholder confidence and perceptions. Therefore, it is crucial for stakeholders to come together and collaborate. Enhancing the level of security through risk management, technological innovation, and stakeholder cooperation is important. The aviation industry should adopt an objective approach and exercise caution in the secure and seamless integration of technologies. The challenge of aviation cybersecurity may not be solved solely through defense strategies relying on technological solutions. The aviation industry must make progress through leadership and teamwork. Achieving compliance, orientation, and advancement for a secure and evolving aviation industry in the future is of critical importance under strong international leadership.

According to the ICAO cyber security strategy; Cyber security risks in the aviation sector should be handled with a holistic approach and integrated with aviation security. Working with aviation industry stakeholders, IATA focuses on mitigating cybersecurity risks and developing a global cybersecurity framework. In this process, an integrated risk management approach combined with threat intelligence and real information should be adopted and standards covering the entire supply chain should be developed. IATA's efforts are vital to ensuring that the aviation industry continues to grow safely and reliably.

3.2. The Cybersecurity Structure of Turkish Civil Aviation under SHT-SIBER[4]

Turkish Civil Aviation Cyber Security Instruction is a regulatory document that includes rules and guidelines for organizations in the civil aviation sector in Turkey to provide cyber security. The instruction was published by the General Directorate of Civil Aviation and is a guide for civil aviation organizations. It establishes specific requirements for these organizations to develop and implement information security policies, identify and manage cybersecurity threats, protect critical infrastructure, ensure secure software development and network security, and safeguard their systems and networks against cyber attacks. Among these requirements are technical measures such as firewalls, data encryption, authorization, and authentication. The directive mandates that all personnel working in the civil aviation sector receive cybersecurity training and emphasizes the reporting and analysis of significant cybersecurity incidents. Additionally, it highlights the need for organizations to regularly review and update their cybersecurity policies and procedures. The Turkish Civil Aviation Cybersecurity Directive aims to promote awareness and preparedness for cybersecurity among organizations in the civil aviation sector. It provides a comprehensive framework to assist these organizations in effectively protecting themselves against cybersecurity threats.

The National Cyber Incident Response Center (USOM) is an institution responsible for establishing, updating, and coordinating defense mechanisms against cyber attacks in Turkey. USOM monitors cyber security threats, takes necessary measures to respond to these threats, and works to ensure Turkey's cyber security. USOM is an organization with capabilities to provide protection, detection, analysis, and response against cyber attacks. Within the National Cyber Incident Response Center (USOM), there are teams called Cyber Incident Response Teams (SOME). SOME is one of the most important components of USOM. There are two SOME teams under USOM: Enterprise SOME and Sectoral SOME. Enterprise SOME works in coordination with ministries, independent public institutions, and other public institutions. It can also provide coordination when necessary for critical infrastructure operators in a sectoral basis. Sectoral SOME helps critical infrastructure operators determine and implement sectoral cybersecurity measures. This team also organizes trainings and awareness campaigns to increase sectoral cybersecurity awareness.

The ISO/IEC 27001 standard provides a framework aimed at establishing and managing an information security management system (ISMS) within organizations and businesses. It gives

[4] Cybersecurity Directive for Civil Aviation Operators.

organizations the flexibility to choose their implementation methods while defining their security requirements. Basically, it sets the expectations necessary to protect information from misuse or malicious activity. The TS ISO/IEC 27001 booklet published by TSE explains that the standard aims to provide a model for the monitoring, improvement and sustainability of the operating process after the creation and implementation of an ISMS (Yılmaz, 2014). (Yılmaz, 2014).

Conclusion and Recommendations

While Turkish Civil Aviation is experiencing rapid growth as one of the important centers of the aviation industry, it also faces risks specific to international air transport. With its potential opportunities and threats, the sector will inevitably lead the future together with its international stakeholders. SHT-CYBER legislation has provided a common understanding and approach to cyber security in Turkish civil aviation by reflecting the international cyber security framework in terms of scope. It defines the necessary methods to identify, manage and mitigate cybersecurity vulnerabilities for all organizations in the industry. The implementation of this instruction provides better protection against cyber attacks in the aviation industry and ensures the security of sensitive data within the industry. In addition, compliance with international cybersecurity standards is critical to running safe and reliable businesses in the global aviation industry.

Within the framework of the instruction, various solution proposals can be implemented to reduce the cyber security risks in the aviation industry. These recommendations include providing cyber security training to employees, using Security Management Systems, implementing data protection methods, implementing risk management techniques, complying with supply chain security standards, creating backups for critical systems, installing intrusion detection and response systems, and performing cyber security tests. Adopting and implementing these recommendations together with the internal and external stakeholders of the aviation industry will contribute to the reduction of cyber security risks and the reliable growth of the industry.

Newly established space agencies and countries accelerating their defense industry efforts must inevitably integrate into their cyberspace defense and security strategies. Due to the rapid reflection of the aviation and space industry studies on the sector, it is necessary to transform the institutional structuring in economic and military terms and to develop the relevant public and private institutions according to the conjuncture of cyberspace dominance. This situation necessitates the transformation of the air transport sector along with the increase in the necessary R&D investments. To meet these challenges, the aviation industry must continually adapt its cybersecurity strategies and technologies. This includes steps such as implementing strong security measures, conducting regular risk assessments, training staff on cybersecurity best practices, and collaborating with cybersecurity experts and government agencies.

REFERENCES

Akleylek, N. Ç. S. HAVACILIK SİSTEMLERİNDE SİBER GÜVENLİK. *Siber Güvenlik ve Savunma Kitap Serisi 6: SİBER GÜVENLİK ONTOLOJİSİ, TEHDİTLER VE ÇÖZÜMLER*, *6*, 293, s.297-311.

AKTEL, M., & GÜRKAYNAK, M. KÜRESELLEŞEN TERÖRİZM: BİR ETKİLEŞİM ÇALIŞMASI. *38. ICANAS*, 77.

Bachmann, S. D. (2011). Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats-mapping the new frontier of global risk and security management. *Amicus Curiae*, *88*, 24, s.15.

Bicakci, S. (2014). NATO'nun gelişen tehdit algısı: 21. yüzyılda siber güvenlik. *Uluslararası İlişkiler Dergisi*, *10*(40), 100-130.

CHERTOFF, M., (2011). 9/11: Before and After, Homeland Security Affairs, Volume 7, 1-6.,

Goutam, R. K. (2015). Importance of cyber security. International Journal of Computer Applications, 111(7).

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security*, *4*(2), 49-60, s.55.

https://bilgiguvenligi.org.tr/BGD/Siber_Guvenlik_ve_Savunma_Kitap_Serisi_1_Farkindalik%20ve%20Caydiricilik.pdf,s.25). (Erişim 23.04.2023)

https://bilgiguvenligi.org.tr/BGD/Siber_Guvenlik_ve_Savunma_Kitap_Serisi_1_Farkindalik%20ve%20Caydiricilik.pdf, s.24.(Erişim 23.04.2023)

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=legissum:l33260.(Erişim 23.04.2023)

https://siberbulten.com/efsane-hackerlar/ilk-bilgisayar-solucaninin-mucidi-robert-morris/.(Erişim 23.04.2023)

https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/#.(Erişim 23.04.2023)

https://tr.wikipedia.org/wiki/Morris_solucan%C4%B1

https://tr.wikipedia.org/wiki/Ulusal_Siber_Olaylara_M%C3%BCdahale_Merkezi.(Erişim 23.04.2023)

https://web.archive.org/web/20160304195221/http://www.bloomberght.com/haberler/haber/1378717-ulusal-siber-olaylara-mudahale-ekipleri-geliyor.(Erişim 23.04.2023)

https://web.shgm.gov.tr/documents/sivilhavacilik/files/mevzuat/sektorel/taslaklar/2022/SHT-Siber.pdf.(Erişim 23.04.2023)

https://www.atlanticcouncil.org/wpcontent/uploads/2017/11/Aviation_Cybersecurity_web_1107.pdf,s.1.(Erişim 23.04.2023)

https://www.atlanticcouncil.org/wp-content/uploads/2019/12/AVIATION-CYBERSECURITY-12-19-.pdf, s.5.(Erişim 23.04.2023)

https://www.hsaj.org/resources/uploads/2022/05/7.2.13.pdf, s.4..(Erişim 23.04.2023)

https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/sin_roundtable_readout.pdf,s.3. .(Erişim 23.04.2023)

https://www.icao.int/Meetings/MIDCyberSec/PublishingImages/Pages/Presentations/10_5_%20Cyber%20Security.pdf, s.24-26.(Erişim 23.04.2023)

https://www.icao.int/Newsroom/NewsDoc2014/COM.46.14.EN.pdf.(Erişim 23.04.2023)

Ulaştırma, T. C., & Bakanlığı, A. (2020). Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023),s.23.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Yılmaz, H. (2014). TS ISO/IEC 27001 bilgi güvenliği yönetimi standardı kapsamında bilgi güvenliği yönetim sisteminin kurulması ve bilgi güvenliği risk analizi. *KİDDER Kamu İç Denetçileri Derneği*, *15*(1), 45-59, s.51.

[1] https://www.computerworld.com/article/2592849/sabre-airline-reservation-system-down-for-two-hours.html

[2] Riley, C. and Cerchio, D. R. Aircraft Systems Cyber Security. In Institute of Electrical and Electronics Engineers

[3] https://en.wikipedia.org/wiki/Stuxnet

[4] https://www.iha.com.tr/haber-thynin-web-sitesine-saldiri-240640/

[5] https://www.reuters.com/article/us-cybersecurity-iran-idUSKCN0JG18I20141202

[6] https://www.euractiv.com/section/justice-home-affairs/news/hackers-bombard-aviation-sector-with-more-than-1000-attacks-per-month/

[7] https://www.theguardian.com/world/2015/jan/26/malaysia-airlines-website-hacked-by-lizard-squad

[8] https://www.theguardian.com/business/2015/jun/21/hackers-1400-passengers-warsaw-lot

[9] https://www.reuters.com/article/us-cyber-attack-ukraine-airport-idUSKBN19I1OR

[10] https://en.wikipedia.org/wiki/British_Airways_data_breach

[11] https://www.timesofisrael.com/israeli-airports-fend-off-3-million-attempted-attacks-a-day-cyber-head-says/

[12] https://www.bridewell.com/insights/blogs/detail/lessons-from-the-travelex-cyber-attack

[13] https://en.wikipedia.org/wiki/EasyJet_data_breach

[14] https://www.ainonline.com/aviation-news/business-aviation/2020-07-24/garmin-cyberattack-affects-aviation-data-services

[15] https://www.phocuswire.com/sita-cyber-attack-accesses-passenger-data-for-multiple-airlines

[16] https://en.wikipedia.org/wiki/Air_India_data_breach

[17] https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-757.pdf

[18] https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-427.pdf

[19] https://securityaffairs.co/wordpress/137087/data-breach/dji-drone-tracking-data-exposed-in-us.html

[20]https://www.securityweek.com/air-france-klm-customers-warned-loyalty-program-account-hacking?j=75396619&sfmc_sub=1106273297&l=1926764_HTML&u=860332643&mid=152878&jb=1

[21] https://thecyberexpress.com/pro-russia-atp-killnet-hitlist-ukraine-war/

bildiri 21.05.2023

ORİJİNALLİK RAPORU

%12	%11	%6	%
BENZERLİK ENDEKSİ	İNTERNET KAYNAKLARI	YAYINLAR	ÖĞRENCİ ÖDEVLERİ

BİRİNCİL KAYNAKLAR

1	socradar.io İnternet Kaynağı	%3
2	websites.fraunhofer.de İnternet Kaynağı	%1
3	www.mdpi.com İnternet Kaynağı	%1
4	pure.port.ac.uk İnternet Kaynağı	%1
5	dergipark.org.tr İnternet Kaynağı	%1
6	www.defensedaily.com İnternet Kaynağı	%1
7	www.irjsmi.com İnternet Kaynağı	%1
8	Frank Schätter, Marcus Wiens, Frank Schultmann. "A new focus on risk reduction: an ad hoc decision support system for humanitarian relief logistics", Ecosystem Health and Sustainability, 2017 Yayın	<%1

9	dokumen.pub İnternet Kaynağı	<%1
10	Jorja B. Wright, Darrell Norman Burrell. "chapter 7 Cybersecurity Leadership Ethics in Healthcare", IGI Global, 2023 Yayın	<%1
11	Iosif I. Androulidakis. "VoIP and PBX Security and Forensics", Springer Science and Business Media LLC, 2016 Yayın	<%1
12	www.icao.int İnternet Kaynağı	<%1
13	www.iata.org İnternet Kaynağı	<%1
14	www.giplatform.org İnternet Kaynağı	<%1
15	hukuk.medeniyet.edu.tr İnternet Kaynağı	<%1
16	aviationweek.com İnternet Kaynağı	<%1
17	export.arxiv.org İnternet Kaynağı	<%1
18	www.saujs.sakarya.edu.tr İnternet Kaynağı	<%1

19	"Exploring English Preservice Teachers' Digital Competence Perceptions Regarding the C3 Matrix-cyber Ethics, Cyber Security and Cyber Safety: An Empirical Study Executed in China", International Journal of New Developments in Education, 2023 Yayın	<%1
20	Hakan Aydın, Zeynep Orman, Muhammed Ali Aydın. "A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment", Computers & Security, 2022 Yayın	<%1
21	earsiv.anadolu.edu.tr İnternet Kaynağı	<%1
22	en.wikipedia.org İnternet Kaynağı	<%1
23	hdl.handle.net İnternet Kaynağı	<%1
24	www.caa.co.za İnternet Kaynağı	<%1
25	www.jinfowar.com İnternet Kaynağı	<%1
26	Odd Sveinung Hareide, Øyvind Jøsok, Mass Soldal Lund, Runar Ostnes, Kirsi Helkala.	<%1

"Enhancing Navigator Competence by Demonstrating Maritime Cyber Security", Journal of Navigation, 2018
Yayın

---

27 Ruwantissa Abeyratne. "Rulemaking in Air Transport", Springer Science and Business Media LLC, 2016 <%1
Yayın

---

28 Wenting Yu, Fei Shen. "The relationship between online political participation and privacy protection: evidence from 10 Asian societies of different levels of cybersecurity", Behaviour & Information Technology, 2021 <%1
Yayın

---

29 press.armywarcollege.edu <%1
İnternet Kaynağı

Alıntıları çıkart üzerinde
Bibliyografyayı Çıkart üzerinde
Eşleşmeleri çıkar < 3 words