



**UNIVERSITY OF THE AEGEAN
SCHOOL OF BUSINESS STUDIES
DEPARTMENT OF SHIPPING, TRADE AND TRANSPORT**

CYBER SECURITY IN AIR TRANSPORTATION

BACHELOR THESIS

SUPERVISOR:

PROFESSOR THEODORE LILAS

STUDENT INFORMATION:

FULL NAME: MARIA KOSSENA

STUDENT IDENTIFICATION NUMBER: 2212015062

CHIOS

MAY 30th 2019

EXPRESSION OF GRATITUDE AND APPRECIATION

Before the presentation of this bachelor thesis, I wish to express my gratitude and appreciation to the people who were an important part of its actualization and completion.

First and foremost, I would like to express my warm thanks to the supervisor of my bachelor thesis, Professor Theodore Lilas, for his valuable guidance, trust, appreciation and support.

Moreover, I would like to thank Professor Nikitas Nikitakos for his beneficial advice and recommendations.

Lastly, I feel the urge to express my utmost respect, gratefulness and admiration to the most important people in my life, my family, my mother Aspasia Benardis, my grandmother Despoina Benardis, my late grandfather Steve (Efstathios) Benardis and my twin sister Despoina Kossena. Their patience, encouragement, support and belief in me throughout my studies were an integral part of the successful completion of this bachelor thesis as well as my studies. I dedicate this bachelor thesis to them as they have dedicated their lives to raising me and my sister with integrity, values, ethics, honesty, a lot of love and have always strived to offer me the best life possible.

TABLE OF CONTENTS

ABSTRACT.....	6
1. INTRODUCTION.....	8
2. CYBER SECURITY IN AIR TRANSPORTATION	9
2.1. TYPES OF THREAT AGENTS.....	11
2.2. CAUSES OF THE LACK OF COMMUNICATIONS SECURITY IN THE AIR TRAFFIC SYSTEM.....	13
3. CYBER SECURITY RISKS AND THREATS RELATED TO AIR TRANSPORTATION.....	15
4. CYBER THREATS FOR AIRPORTS.....	18
5. CYBER SECURITY POLICIES, MEASURES AND ACTION PLANS.....	25
5.1. THE CIVIL AVIATION CYBERSECURITY ACTION PLAN	25
5.2. DRAFT ASSEMBLY RESOLUTION ON ADDRESSING CYBER SECURITY IN CIVIL AVIATION.....	30
5.3. ICAO CIVIL AVIATION AUTHORITY TOOLS (ICAAT).....	33
5.4. ICARD	34
5.5. IMPLEMENT.....	34
5.6. SIMS.....	34
5.7. DECLARATION ON CYBERSECURITY IN CIVIL AVIATION	35
5.8. GLOBAL AVIATION SECURITY PLAN	36
5.9. FIRST TRANSPORT CYBERSECURITY CONFERENCE	36
5.10. AVIATION ISAC.....	38
5.11. EUROCONTROL	39
5.12. THE SESAR PROGRAM.....	40
5.12.1. SESAR’S VISION	42
6. MEASURES FOR THE MITIGATION OF CYBER RISKS AND TREATS....	45
7. TECHNOLOGIES DEVELOPED TO DEAL WITH CYBER THREATS	47
7.1. AIRBUS’S AND SITA’S CYBERSECURITY SERVICES FOR AIR TRANSPORT INDUSTRY	47
7.1.1. AIRBUS CYBERSECURITY.....	48
8. CYBER RISK MITIGATION AND ASSESSMENT.....	49
8.1. MEASURES FOR AIRPORTS	49
8.2. MEASURES FOR ORGANIZATIONS	53

8.3. POLICIES AND STANDARDS FOR AIRPORTS AND ORGANIZATIONS	56
9. CONCLUSIONS AND RECOMMENDATIONS.....	58
10. REFERENCES	62

ABSTRACT

Cyber security is a crucial matter affecting all transport modes. In the era of the 4th industrial revolution, technological advancements related to digitalization and automation of services provide opportunities to cyber threat agents to attack and cause damage to companies and transportation systems. This is especially true for the air transportation industry, since constant evolution of the technologies used for aircraft and airport systems and networks makes them more efficient, but at the same time more vulnerable to cyber threats. There are various types of cyber-attacks that could have a negative and even destructive impact on aircraft operations, airport systems and passenger services, as well as the safety of human life and social and economic stability of countries. The air transportation industry is global and interconnected. Thus, policies and regulations regarding cyber security are established by international organizations and implemented by the majority of the nations worldwide. This dissertation seeks to analyze the various cyber threats affecting aircraft and airport operations. Moreover, it researches the technologies, policies and regulations established to prevent and mitigate cyber risks in aviation. The dissertation concludes with recommendations on specific technological measures that could offer better protection against cyber threats and suggestions for further research on the subject. The methodology followed consists of first analysing related scientific articles from conferences and journals together with information from internet sources and then synthesizing a complete study addressing the critical issues regarding cyber security in air transportation.

Index terms: air transportation, cyber security, cyber threats, best practices, aircraft systems, airport networks, aviation cyber risks, aviation actors, threat agents

1. INTRODUCTION

Cyber security is a major issue for every company, organization, industry and even country. Cyber threats do not only affect companies and organizations, but also individuals, for this reason there is an urgent need for adequate protection against them in all aspects of everyday life.

«Cyber security consists of technologies, processes and controls designed to protect systems, networks and data from cyber-attacks. Effective cyber security reduces the risk of cyber-attacks and protects against the unauthorized exploitation of systems, networks and technologies. » (What is Cyber Security?)

«Robust cyber security involves implementing controls based on three pillars: people, processes and technology. This three-pronged approach helps organizations defend themselves from both organized attacks and common internal threats, such as accidental breaches and human error. » (What is Cyber Security?) Cyber security also includes the «preservation of Confidentiality, Integrity and Availability of information in the Cyberspace» (LOUKIL, 2017).

Cyber threats have become more persistent and technologically evolved over the years. (LOUKIL, 2017) The number of security breaches has increased significantly forcing even more organizations and companies to develop cyber security programs capable of dealing with this problem. (White, 2011)

One of the different types of cyber threats is a computer “glitch”, which causes problems to a service or infrastructure of an organization. Such an attack happened on June 17, 2011 and shut down all the systems of the United Airlines for several hours causing its flights to be cancelled. As a result, many of the passengers were displaced and dissatisfied although there was no damage to property or loss of life. (White, 2011) United Airlines is a subsidiary of the United Continental Holdings, Inc. (UNITED STATES SECURITIES AND EXCHANGE COMMISSION, 2019) and a member of the Star Alliance (Airline partners and global alliances). Its headquarters are located at Chicago, Illinois in the United States of America. (UNITED STATES SECURITIES AND EXCHANGE COMMISSION, 2019)

Regarding the three pillars of cyber security mentioned above, a more detailed description could be made: with regard to the people, there is a need for every employee of an organization or company to be informed about their role in preventing

and minimizing the number of cyber threats. It is crucial for the specialized technical cyber security staff in particular, to stay up to date with the latest skills and qualifications so as to reduce the amount of cyber-attacks and respond to them efficiently. As for the processes, it is important that they are constantly re-evaluated in order to adapt to the rapidly changing nature of cyber threats. Last but not least, technology can be used to prevent and minimize the impact of cyber threats based on the risk assessment of the company or organization. (What is Cyber Security?)

Cyber security is crucial for many reasons. Some of them are:

A) The high costs that a company or organization undertakes as a result of security breaches. These costs include fines related to personal data protection regulations as well as damages to the companies' reputation and loss of clients and assets. (What is Cyber Security?)

B) Cyber-attacks have evolved and have become more sophisticated. The intruders use social engineering («social engineering is used to deceive and manipulate victims to gain computer access. This is achieved by tricking users into clicking malicious links or by physically gaining access to a computer through deception» (What is Cyber Security?)), and new types of malware («malware is any file or program intended to harm a computer, and encompasses trojans, social engineering, worms, viruses and spyware» (What is Cyber Security?)) and ransomware (« ransomware is a type of malware that demands payment after encrypting the victim's files, making them inaccessible (What is Cyber Security?)) to attack a system. (What is Cyber Security?)

C) As mentioned above, companies and organizations are obligated to have a cyber-security program in order to deal effectively with malicious cyber-attacks and comply with new regulations and reporting requirements. (What is Cyber Security?)

2. CYBER SECURITY IN AIR TRANSPORTATION

Wireless communications technology and wireless data networks are becoming increasingly crucial as communication tools for aircraft and ground surveillance. The quickly advanced technology of the last two decades has allowed the development of commercial-off-the-shell hardware (COTS), which has the ability to affect wireless

aviation systems. Due to the fact that these systems do not provide enough protection against cyber threats, new threat models need to be developed. Additionally, information about aviation protocols has become accessible; it is possible for inexperienced actors with limited resources to gain access to the wireless communication systems that ensure air safety. (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016)

Wireless technological achievements that lead to recent advancements include: SDRs (software-defined radio technology), that were initially developed for military and closed commercial use in the 1990s. The availability of COTS SDRs enabled many people to program these systems using software available on the Internet. Moreover, there is a trend towards unauthenticated digital communication networks that increases the chances of a successfully undetected attack on the data link level of the aviation systems. Also, it is possible for anyone using a COTS SDR to track any flight they wish. Data collected by flight trackers have been used in investigations of flight incidents such as the two Malaysian Airlines aircrafts that were lost over the Ukraine and Indian Ocean in 2014 (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016) Malaysia Airlines Berhad is the national carrier of Malaysia, a subsidiary of the Malaysia Aviation Group Corporate. Its headquarters are in Sepang, Malaysia. (Malaysia Aviation Group). The SDRs make it possible for a user to manipulate virtually every aspect of a wireless channel used by aviation protocols. (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016)

2.1. TYPES OF THREAT AGENTS

Table 1. «Overview of threat agents» (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016)

Threat	Resources	Type	Goal/Motivation
Passive Observers	None - Very low	Passive	Information collection / Financial or personal interest
Script Kiddies / Hobbyists	Low	Active	Any noticeable impact / Thrill and recognition
Cyber Crime	Medium - High	Active	Maximising impact / Financial gains using e.g. blackmail or valuable information
Cyber Terrorism	Low - Medium	Active	Political or religious motivation / Massive disruption and casualties
Nation State	Unlimited	Active	Weapons / Targeting specific, potentially military objects

The threat agents that are presented in Table 1 above are related to wireless security in aviation.

- Passive observers are those people who take advantage of the open nature of air traffic communication protocols to gather information about private or secret air traffic movements. Instead of actively interfering with air traffic communication, they use websites and mobile applications, which demonstrate air traffic and communications in real time or even SDR receivers. The information collected by these threat agents can be used in many ways, including privacy concerns and detection of military operations. (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016)

- Script kiddies aim to utilize well-known security gaps with low sophisticated attacks. They do not have specific goals, but instead seek thrill and recognition through identifiable impacts. (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016)

- Hobbyists are mostly focused on plane spotting and happen to be more familiar with the protocols in air traffic communication. They, also, have knowledge about radio communication and the basic characteristics of the wireless channel as well as access to SDRs. Their attacks are difficult to detect. (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016)

- Cyber-crime attackers attack systems for monetary gains. They exploit software-defined radios and even small unmanned aerial vehicles (UAV) in order to insert new messages or modify existing ones so that they will not be easily detected by current detection systems. Their main interest is to cause maximum damage, blackmail and exploit inside knowledge and effective ways to attack Air Traffic Controllers (ATC) and aircraft systems. (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016) Cyber-crime also, generally includes any criminal act related to computers and networks, also known as “hacking”, as well as traditional crimes conducted through the Internet. Examples of cyber crimes are: illegal access to computers and systems, illegal interception, system and data interference, misuse of devices and fraud. (LOUKIL, 2017)

- Cyber terrorism consists of attacks on cyber-physical systems of infrastructure in aviation (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016). «Cyber-physical systems are complex, multi-disciplinary, physically- aware, next generation engineered systems that integrate imbedded computing technology (cyber part) into the physical phenomena by using transformative research approaches. This integration mainly includes observation, communication and control aspects of the physical systems from the multi-disciplinary perspective» (Gunes, Peter, Givargis, & Vahid, 2014). Terrorists and politically motivated actors could take advantage of the vulnerabilities in wireless aviation communications and attack planes from safe distances on the ground. (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016)

- Nation state actors use their knowledge of intrusion detection systems and unlimited resources in order to avoid plausibility checks and defences of a system. (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016)

Table 2 beneath illustrates the capabilities of each threat agent as well as the costs of the necessary equipment in order to for them to actualize their attacks.

Table 2. «Overview of attacker capabilities» (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016)

Threat Agent	Capabilities	Hardware / Cost
Passive Observers	Eavesdropping, use of website & mobile apps.	Internet access, \$10 SDR receiver stick
Script Kiddie / Hobbyist	Eavesdropping, replay attacks, denial of service.	COTS SDR transmitter, \$300-\$2,000.
Cyber Crime	Resources for large-scale operations with sophisticated transponders.	Directional antennas, small UAVs with SDR transmitters, \$5,000-\$10,000.
Cyber Terrorism	Resources for specific high-impact operations, though usually on a limited scale	As with cyber crime but potentially on a smaller, more targeted scale.
Nation State	Anything physically and computationally possible.	Military-grade radio equipment, capability for electronic warfare.

2.2. CAUSES OF THE LACK OF COMMUNICATIONS SECURITY IN THE AIR TRAFFIC SYSTEM

There are several reasons why there is a gap in the security of the air traffic communication systems. The most important are:

- «Long development and certification cycles» (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016): In aviation, the development and certification cycles for new technologies require more time, even more than two years. This happens due to the number of tests and certifications related to safety that are necessary before giving a technology the green light. The drawback of this approach is that, even though it is highly effective in minimizing technical failures, it does not take into account the constantly changing threat model and the possible negative impacts of the recent advances in wireless technologies. (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016)

- «Legacy and compatibility requirements» (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016): Civil aviation is a global and interconnected industry. Its technical protocols and procedures ought to be comprehended at a large scale. However, due to the differences in local authorities and available infrastructure, new protocols and technical advances are not launched in all airspace at the same time. As a consequence, older technologies are kept in service as a backup and so as to provide a vast compatibility for air traffic control all around the globe. (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016)

- Costs: The aviation industry is characterized by a high level of competition and substantial cost pressures. Thus, alterations to the existing aircraft equipment are usually avoided unless they offer significant cost or operational benefits. Critical equipment changes happen mainly through regulatory directives, which take a lot of time and substantial industry lobbying. As a result, legacy technologies are oftentimes maintained to reduce costs. (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016)

- «Frequency overuse» (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016): Due to the fact that a constantly increasing number of aircrafts share the same frequencies, in addition to the UAVs that are set to enter the controlled airspace in the near future, some Air Traffic Control (ATC) frequencies are seriously engorged. This results in significant message loss, impeding possible cryptography-based security solutions simultaneously. (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016)

- Open systems preference: The International Civil Aviation Organization plans future protocols to be openly accessible, regardless of the security and privacy problems that may arise. (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016)
«The International Civil Aviation Organization (ICAO) is a UN specialized agency, established by States in 1944 to manage the administration and governance of the Convention on International Civil Aviation (Chicago Convention). ICAO works with the Convention's 193 Member States and industry groups to reach consensus on international civil aviation Standards and Recommended Practices (SARPs) and policies in support of a safe, efficient, secure, economically sustainable and environmentally responsible civil aviation sector.» (About ICAO) The Organization's headquarters are located at Montreal, Canada. (Contact Us: ICAO)

Open systems will meet the typical aviation requirements for the effectiveness of air traffic control such as ease of communication, compatibility and effectively facing administrative differences across the global airspace, but it is crucial to mitigate the disadvantages of the rapidly shifting technology. Open systems and insecure wireless technologies could result in dominant actors losing their information peak and privacy due to the wide availability of aircraft information on the Internet. (Strohmeier, Schafer, Smith, Lenders, & Martinovic, 2016)

3. CYBER SECURITY RISKS AND THREATS RELATED TO AIR TRANSPORTATION

The air transportation industry is highly important to the global economy. In 2013, its global economic value was estimated at 2.2 trillion dollars, while the global air transportation network carried over 2.6 billion passengers and over 48 million tons of freight. It is easy presumed that a possible cyber-attack would have significant social and economic consequences. (Duchamp, Bayram, & Korhani, 2017)

It would also pose a threat to life itself, in case it would result in a plane crushing. (Transport cybersecurity: Raising the bar by working together, 2019)

Cyber security is considered a significant risk for 85 percent of airline CEOs, regarding the extremely sensitive nature of flight systems and passenger data, based on PwC's 2015 Global Airline CEO Survey. (LOUKIL, 2017)

An example of a cyber-attack is the one that happened on June 21, 2015 when LOT Polish Airlines' (LOUKIL, 2017) operations system was hacked resulting in cancellation or delay of 22 flights. It was a Distributed Denial of Service (DDoS) attack on a private network responsible for publishing flight plans. (LOUKIL, 2017) LOT Polish Airlines is a polish airline company that connects Poland and Central-Eastern Europe with more than 100 destinations worldwide. Its major transfer hub and headquarters are located at Warsaw, Poland. (LOT Polish Airlines)

Moreover, certain systems on an aircraft such as the on-board radios and the Aircraft Communications Addressing and Reporting System (ACARS), which uses messages or information about the airplane rather than voice transmissions, could be hacked by an attacker with good knowledge on the aircraft's systems and cause severe problems to its normal operation. An example of such manipulation of a system is the

one presented by a security researcher named Hugo Teso at a conference, who reported that he was able to manipulate the ACARS using his Android smartphone. (Duchamp, Bayram, & Korhani, 2017)

Cyber-attacks that affected systems and operations of airlines occurred in 2013. One of them involved the Istanbul airport where there was an immediate shut down of the passport control systems at the departure terminals of the airport and as a result many flights were delayed. The other one involved malicious hacking of 75 airports in the United States of America (USA). (Duchamp, Bayram, & Korhani, 2017)

Some of the reasons for the increasing risks regarding cyber security in air transportation are: the growing number of travelers, the modernization of airports, the manufacturing of complex aircrafts, the use of advanced IT systems, technology and software in order for the airline companies and airports to offer effective and digital solutions to the personnel and the passengers with the introduction of online ticketing and booking as well as the tend to minimize manpower so as to reduce the costs by using more sophisticated and automated technology. In addition, the interactions between people and devices have increased in number and diversity and that makes the possible cyber-attacks less predictable. Furthermore, the way the sector itself deals with cyber incidents is a factor. Based on observations made after some cyber-attack cases, when there is a breach or vulnerability in the system, the suppliers of the system do not always care to fix it. Additionally, stakeholders are reluctant to accept responsibility for a breach or vulnerability. Also, it has been noticed that essential systems and cabin systems as well as the principal internal communication protocol on aircrafts are not isolated properly from external threats. (Duchamp, Bayram, & Korhani, 2017)

Cyber security breaches on aviation systems could be categorized in two types:

- The «opportunistic» (Duchamp, Bayram, & Korhani, 2017): these breaches take advantage of errors made by internal users such as employees who use the IT systems and their main goal is to cause disruption to all the entities involved in the aviation ecosystem. (Duchamp, Bayram, & Korhani, 2017)

- The «calculated and premeditated» (Duchamp, Bayram, & Korhani, 2017): their goal is to disturb operations or impose a threat to human lives. It is a high risk category related to terrorism. (Duchamp, Bayram, & Korhani, 2017)

Cyber security protection faces some difficulties. The reason for that is the lack of resources, budget and skills of the Cyber Security teams. Air transportation stakeholders need to reinforce their Cyber Security teams and provide sufficient resources to commence solid projects. It is estimated that airlines spend an average of 7% of their total IT budget on cyber security compared to the airport investment that reaches a 10%. However, that percentage was expected to increase up to 12% in 2018, reflecting the importance of protecting personal data and systems from unauthorized access. The highest priorities seem to be regulatory compliance and data privacy. In addition, introducing a dedicated Chief Information Security Officer is critical to effective response to cyber threats, still only a small percentage of the organizations have one. Furthermore, recruiting specialized skilled staff is a major challenge for the companies' executives as is the capacity for personnel training. It would be wise for the industry to combine internal resources with external expertise. Lack of employee awareness in combination with the lack of a long-term cyber security strategy aligned with the company's business objectives and IT systems, could weaken the ability of the company to defend against cyber threats. Almost 77% of aviation organizations introduce their security policies to their employees and 69% of them have a formal training program active. Nevertheless, only 40% of the organizations maintain an inventory of critical business processes and IT systems. It is important for organizations to connect IT systems and business processes and manage cyber security based on the financial or operational impacts that those two have. (SITA, 2018) Some of the frequent cyber threats that air transportation industry faces are ransomware and phishing (SITA, 2018) (phishing is a cyber-crime in which the threat agents contact the targets by email, telephone or text message, pretending to be representatives of a legitimate institution so as to lure the targets into providing sensitive and personal data). The information gained is then used to access accounts resulting in identity theft or even financial loss. (What Is Phishing?)) and advanced persistent threats. External threats are consider to be of utmost importance in comparison to threats from internal actors, although based on analysts' reports, over a quarter of attacks involve insiders. (SITA, 2018)

4. CYBER THREATS FOR AIRPORTS

The successful daily operation of an airport's cyber security is based on its technology and IT teams (employees or contractors). Information technology systems support all aspects of the operations of a modern airport, so if there is a cyber security breach or related incident that disrupts any network operations, it will have a huge impact on the airports operations. It could jeopardize the airport's capability to move passengers, cargoes and aircrafts and even affect other airports and passengers throughout the system. It could also disrupt traditional administrative processes, building operations, baggage and cargo handling, electronic signage, parking operations, airbridge operations, energy management, sewage handling and heating, ventilation and air conditioning (HVAC). A possible cyber-attack could result in significant monetary costs. (National Safe Skies Alliance, Inc., 2018) For example, according to a study conducted by the Ponemon Institute, the aggregate organizational cost of a typical cyber breach in the United States of America was estimated at around 7 million US dollars per incident. Furthermore, a data breach in the private sector in the United States of America costs an average of 158 US dollars per compromised record. Additional risks that could possibly affect the cyber security of an airport are: physical security breaches, aircraft incidents, public unrest due to noise complaints and changes in airport operations. (National Safe Skies Alliance, Inc., 2018) «The Ponemon Institute was founded in 2002. The Institute conducts independent research on data protection and emerging information technologies. In addition, its research informs organizations on how to improve upon their data protection initiatives and enhance their brand and reputation as a trusted enterprise.» (Ponemon Institute) It is located in Traverse City, Michigan, in the United States of America. (Contact Us: Ponemon Institute)

There are four categories of cyber threats that could diminish an airports ability to operate effectively and provide its services to the community and passengers. (National Safe Skies Alliance, Inc., 2018)

I. «Political or Military» (National Safe Skies Alliance, Inc., 2018). The most severe attacks are usually conducted by foreign military or intelligence-related sources. The purpose of these attacks is to gain military, political or strategic insight

and to compromise the trust of the public or leaders to the systems by destroying their availability and integrity. The attackers mostly focus on military organizations, government agencies, or any related public and non-governmental organizations to disrupt their operations and withdraw information. A disruption of the systems, operations and services of important airports could sabotage public trust and confidence in the entire National Airspace System. (National Safe Skies Alliance, Inc., 2018)

II. «Commercial Espionage» (National Safe Skies Alliance, Inc., 2018). Organized cybercrime entities or foreign governments that aim at destroying or extracting confidential information from private and public companies use this type of cyber-attack. Their motives are monetary driven, social activist or corporate strategic. Their main document targets are airport planning, construction, budget, and public or government-relations documents. (National Safe Skies Alliance, Inc., 2018)

III. «Disruption» (National Safe Skies Alliance, Inc., 2018). The main goal of such attacks is the disruption of access to resources. The attackers are oftentimes vandals, activists or outsiders with a wide agenda. The attacks aim at systems or networks so as to deny user access, cause damages, or steal and alter data. An example of such an attack would be a Distributed Denial-of-Service (DDoS) attack (mentioned above), where the attacker fills the airport website with more traffic than it can handle, so as to prevent access from users. (National Safe Skies Alliance, Inc., 2018)

IV. «Cybercrime» (National Safe Skies Alliance, Inc., 2018). Attacks of this kind are increasing in number. Although they are less complicated than the above, cybercrime techniques and tools have improved and are easier to obtain and utilize. Their main goal is to steal data from networks and systems, such as customer identification, credit cards, or banking information, so as to resell them. Moreover, threat agents can encrypt or destroy data or threaten to expose sensitive communication and important information if their victims refuse to pay a fee, using ransomware or malware. Their main targets are airports that acquire credit card information, offer parking services of charge baggage fees. (National Safe Skies Alliance, Inc., 2018)

The four categories above are not exhaustive; there are many ways by which an actor could attack the systems and networks of an airport. (National Safe Skies Alliance, Inc., 2018)

Some of them are:

- i. Attacks on electronic signage so as to change the content of signs or disable them.
- ii. Ransomware attacks on airline, vendor or airport systems.
- iii. Disruptions and misconductions of the baggage systems.
- iv. Disruptions to electricity, HVAC or other building functions.
- v. Parking system problems.
- vi. Larceny of credit or debit cards.
- vii. Larceny of sensitive and personal emails or documents so as to blackmail airport management or other parties.
- viii. Impairment of airport websites.
- ix. Attacks on access control systems.
- x. Disturbance of jetway functions.
- xi. Prevention of access to airport systems and networks.
- xii. Publishing of airport executives' personal information and data.
- xiii. Creation of fake airport websites to spread misinformation or collect personal information.
- xiv. The use of phishing emails in order to disrupt airport systems via malware.
- xv. Attacks to physical security systems.
- xvi. Unauthorized access to confidential files. (National Safe Skies Alliance, Inc., 2018)

Commercial airports have designated areas with different levels of security. Those are the Secured Areas, the Security Identification Display Areas (SIDAs), the Air Operations Areas (AOA), and the Sterile Areas, where passengers wait to board the departing aircrafts after they have passed through screening. The SIDA and AOA normally consist of baggage loading areas, areas near terminal buildings, and areas close to parked aircrafts and airport facilities. Aside from the traditional IT systems and networks that include emails and the Internet, there are targets for potential cyber-attacks within the sphere of internal airport operations. (Cherdantseva, et al., 2015)

Those are:

- a) Systems related to access control and perimeter intrusion,
- b) e-Enabled aircraft systems,

- c) Systems regarding credentiality and document management, such as blueprints,
- d) Radar systems (i.e. ground radar),
- e) Baggage systems that are network-enabled,
- f) Wireless network systems,
- g) Heating, ventilation and air conditioning (HVAC) systems
- h) Facility and utilities management systems
- i) SCADA (Supervisory, Control and Data Acquisition) systems.

(Cherdantseva, et al., 2015)

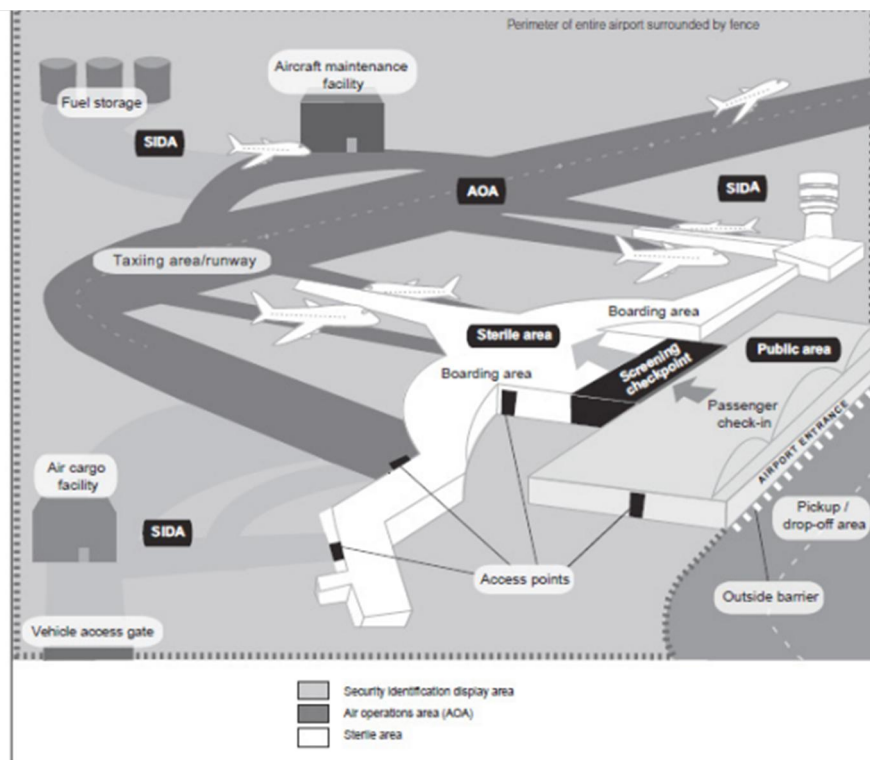


Figure 1. «Commercial airport areas with varying levels of physical security»
(Cherdantseva, et al., 2015)

Figure 1 above illustrates the areas mentioned above.

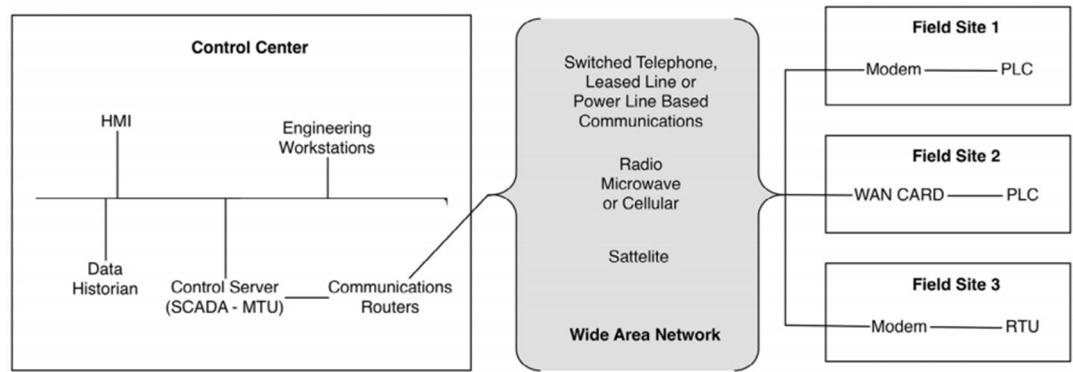


Figure 2. «Generic SCADA hardware architecture» (Cherdantseva, et al., 2015)

The Figure above (Figure 2) illustrates the generic SCADA hardware architecture. «An architecture is formed by one or more control centers and a number of field devices such as a Remote Terminal Unit (RTU), an Intelligent Electronic Device (IED) and a Programmable Logic Controller (PLC) connected by a communication infrastructure. An RTU receives data from field devices, converts it to digital data and sends it to the control center as well as receives digital commands from the center and handles alarms. A PLC is a digital computer that monitors sensors and takes decisions based upon a user created program to control valves, solenoids and other actuators. A control center includes a Master Terminal Unit (MTU), which issues commands to and gathers data from RTUs, it also stores and processes data in order to display information to human operators to support decision making. Human operators monitor and control the system from a control center via Human–Machine Interface (HMI) displays. » (Cherdantseva, et al., 2015)

Cyber threats to the internal airport operations are becoming a primary concern due to the increase of the use of mobile applications and hardware. Both small and large airports depend heavily on networked computer systems for day-to-day operations and are extremely vulnerable to cyber threats. There were several cyber incidents at Los Angeles World Airports (LAWA) in the United States of America including malware intrusions to private network baggage systems, intrusions by zombie armies, which consist of internet-connected computers with breached security defenses, set to spread spam without the owners’ knowledge and consent, or botnets getting in charge of public safety private networks, hacking attempts and internet abuse attempts. (Gopalakrishnan, Govindarasu, Jacobson, & Phares, 2013)

Figure 3 below illustrates the major cyber threats to an airports infrastructure mentioned above.

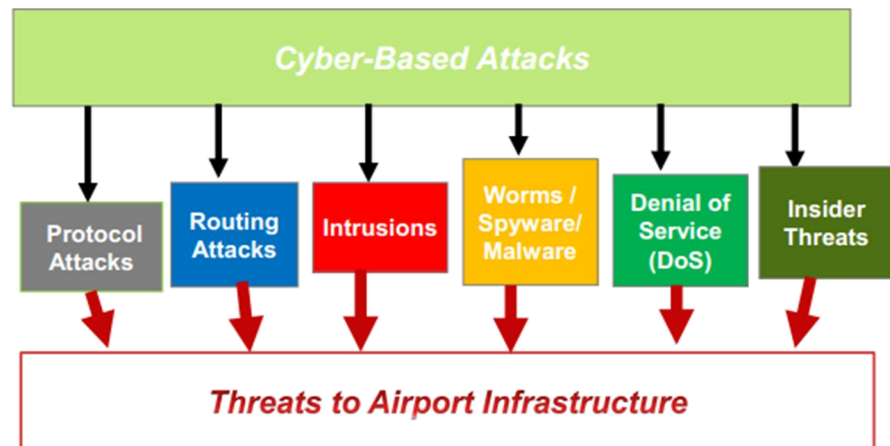


Figure 3. «Cyber-based threats to airports» (Gopalakrishnan, Govindarasu, Jacobson, & Phares, 2013)

There are many devices, networks and state-of-the-art technologies that could pose a threat to airports systems and infrastructure as well as human-related actions. (Gopalakrishnan, Govindarasu, Jacobson, & Phares, 2013)

Those are:

- USB drives,
- Netbooks and laptops,
- Digital access points, such as wireless access points,
- Multifunction and electronic devices, such as digital cameras,
- The possibility of employees borrowing other people's devices to access airport systems,
- Threat agents disguised as personnel or contractors, also known as the Trojan Human,
- Optical media, such as DVDs and CDs,
- Absence of employee vigilance,
- Smartphones,
- E-mails,
- Social networks,
- Cross-site scripting web attacks,
- DDoS attacks

- Cloud computing issues,
- Data removals and threats from the inside,
- Online fraud. (Gopalakrishnan, Govindarasu, Jacobson, & Phares, 2013)

Another threat is the Bring Your Own Device (BYOD) trend, where airport users and even airport personnel are willing to bring their own portable devices such as iPhones, iPads, Androids and Tablets, to their workplace. The issue here is that if those devices interact with enterprise systems, like e-mails and VPN systems, they could forward viruses to the airport's systems or be used by threat agents to collect confidential information. The fact that there is no need for permission from the administrator for the personnel to connect their unsanctioned devices to the airports networks, but only the need for enterprise login credentials means that airport networks are exposed to a wide number of security threats. To effectively deal with the risks related to unmanaged portable devices connecting to airport networks, new technologies were established. Those are: the Wireless Intrusion Prevention System (WIPS), the Network Access Control (NAC) and the Mobile Device Management (MDM). Apart from the BYOD trend, the expanding usage of mobile Wi-Fi hotspots could also be a serious threat. An estimated 20% of enterprises have Rogue Access Points (RAPs) in their networks, resulting in the later becoming more vulnerable to several targeted cyber-attacks. Employee personnel could in absentia insert viruses and allow threat agents to gain access to corporate systems by visiting popular websites, media sites or by connecting an infected USB drive to their computer or portable device. (Gopalakrishnan, Govindarasu, Jacobson, & Phares, 2013)

It is estimated that an airport encounters almost 1,000 cyber-attacks per month worldwide, targeted on its aviation systems according to the European Aviation Safety Agency (EASA) (INTERNATIONAL AIRPORT REVIEW, 2018) EASA's goals are: «to ensure the highest common level of safety protection for EU citizens, the highest common level of environmental protection, single regulatory and certification process among Member States, to facilitate the internal aviation single market and create a level playing field and to work with other international aviation organizations & regulators.» (The Agency: EASA) It has 32 member states which are

European countries (EASA by Country) and its headquarters are located in Germany. (Can we help you?: EASA)

Furthermore, another trend that could become a potential target of cyber threats is the ability of the airports to provide remote control and monitoring for air traffic control systems and on the airfield. Nevertheless, remote towers are extremely contingent on the data links that transfer information from one place to another, making a possible cyber or physical attack to them even more perilous. Such an attack could disturb the operations of the airport or allow the attackers to manage airport traffic. (INTERNATIONAL AIRPORT REVIEW, 2018)

5. CYBER SECURITY POLICIES, MEASURES AND ACTION PLANS

5.1. THE CIVIL AVIATION CYBERSECURITY ACTION PLAN

In the Civil Aviation Cyber security Action Plan signed in Montreal, Canada on December the 5th, 2014, the undersigned organizations, the “Participants”, (Li, 2016) were:

➤ The Airport Council International (ACI): «In 1991 airport operators around the world created Airports Council International – the first worldwide association to represent their common interests and foster cooperation with partners throughout the air transport industry». (Overview - The Community of Airports: ACI) Its headquarters are located in Montreal, Quebec, in Canada. (Contact Us: ACI)

➤ The Civil Air Navigation Services Organization (CANSO): «CANSO's purpose is to create value for its Members by being the global and regional voice of air traffic management (ATM) and by facilitating and supporting improvements in global and regional ATM performance.» (About CANSO) Its headquarters are located in Transpolis Schiphol Airport in the Netherlands. (Contact CANSO)

➤ The International Air Transport Association (IATA): «the International Air Transport Association (IATA) is the trade association for the world's airlines, representing 290 airlines or 82% of total air traffic. The Association supports many areas of aviation activity and helps formulate industry policy on critical aviation issues.» (About us: IATA) The Associations headquarters are located in Montreal, Quebec, in Canada. (IATA Office Addresses)

- The International Civil Aviation Organization (ICAO).
- The International Coordination Council of Aerospace Industries Associations (ICCAIA): «ICCAIA has traditionally focused its efforts on specific technical issues that are the subject of work in ICAO that affect the products manufactured by the aerospace industry. These include such subjects as international aircraft noise and engine emissions standards, aircraft safety, aviation security, air traffic management, and aviation financial and liability issues.» (About Us: ICCAIA) Its headquarters are located in Montreal, Quebec, in Canada. (Contact us: ICCAIA)
- The Aerospace and Defence Industries Association of Europe (ASD): «ASD represents European Aeronautics, Space, Defence and Security Industries, as well as over 3,000 companies and actively supports the competitive development of the sector in Europe and worldwide. It has direct members, active in 18 countries, including 16 major European industries and 23 National Associations.» (ASD at a Glance) Its headquarters are located in Brussels, Belgium. (ASD at a Glance)

The “Participants” declared that they will collaborate on the following commitments:

- Establish a collective understanding of cyber risks and threats,
- Have common and shared assessment of risks,
- Accept common terminology and language,
- Unfold joint recommendations and positions,
- Introduce a consistent and comprehensible approach to the public,
- Propel collaboration among State-level pertinent authorities and industry to inaugurate coordinated aviation cyber security policies, strategies and plans,
- Promote a vigorous cyber security culture in every organization related to civil aviation,
- Impel the usage of existing cyber protection and information security best practices, design principals, and standards and create new ones, where it is considered necessary,
- Set up the means and mechanisms to communicate and forward information, such as threats identification, incidents reports and evolution and progress in defenses,
- Share information related to threats and ensure situational awareness,

➤ Rectify operational principles, best practices and defensive systems, as suitable. (Li, 2016)

Also, they agreed to uphold the actions included in the roadmap (tables 3, 4 and 5) presented below. (Li, 2016)

Table 3. «Civil aviation cyber security action plan» (Li, 2016)

Roadmap

Commitment	Short Term (0-6 months)	Mid Term (6-12 months)	Long Term (12-18 months)
Develop a common understanding of cyber threats and risks	Task: Develop and provide input to common risk and threat matrices. Deliverable: First draft input to threat and risk analysis.	Deliverable: 2015 Aviation Security Panel Paper. Deliverable: Input to ICAO Working Group on Threat and Risk and ECAC Risk Assessments.	Task: Continue to review and communicate threats, update threat and risk analysis.
Share assessments of risks	Task: Compare risk assessment processes from different stakeholders.	Task: Identify mechanism or platform for ongoing sharing of information. Task: Share risk assessments (at the system type level). Deliverable: Input to ICAO Aviation Security Panel Working Group on Threat and Risk.	Task: Continue to review and communicate threats, update threat and risk analysis. Deliverable: Process/platform for sharing of high level risk assessments across industry.
Agree common language and terminology	Deliverable: Industry High Level Group (IHLG) commitment to promote use of existing standards and frameworks. Task: IHLG organizations and their members provide input to a Glossary of Terms.	Deliverable: Glossary of terms for ICAO guidance material.	

Develop joint positions and recommendations	<p>Deliverable: Agree, sign and announce Cybersecurity Action Plan.</p> <p>Task: Identify key areas where regulation is emerging.</p> <p>Task: Industry stakeholders to develop joint positions and recommendations for appropriate regulation.</p>	<p>Task: Prepare joint paper on key issues for regulation during 2015 AVSEC Panel.</p> <p>Task: Identify key areas where regulation is emerging.</p> <p>Task: Industry stakeholders to develop joint positions and recommendations for regulation.</p>	<p>Task: Provide input to development of regulation including standards, recommended practices and guidance material.</p> <p>Deliverable: New and updated guidance material.</p>
Present to the public a joint, consistent and coherent approach to the management of cyber threats and risks	<p>Deliverable: Agree the format and means of communication to the public of a joint position to be used by all signatories</p> <p>Publish the first such communication(s).</p>	Publish refined and updated communication(s)	Publish refined and updated communication(s)

Table 4. «Civil aviation cyber security action plan» (Li, 2016)

Commitment	Short Term (0-6 months)	Mid Term (6-12 months)	Long Term (12-18 months)
Promote cooperation among State-level appropriate authorities and industry to establish coordinated aviation cybersecurity strategies, policies, and plans	<p>Deliverable: Agree, sign and announce Cybersecurity Action Plan.</p> <p>Task: Determine/promote mechanisms for regional and State-level appropriate authority/industry coordination.</p>	<p>Deliverable: Joint workshops in each region</p> <p>Task: Determine/promote mechanisms for regional and State-level appropriate authority/industry coordination.</p>	<p>Deliverable: Commitment from States for coordinated action during the 39th Assembly, September/October 2016.</p>
Promote a robust cyber-security culture in all organizations in civil aviation	<p>Deliverable: IHLG commitment to promote use of existing standards and frameworks.</p>	<p>Task: Raise awareness of cyber security and the need for a cyber-security culture, and provide guidance on implementation.</p> <p>Deliverable: Awareness program and guidance.</p>	<p>Deliverable: 80 percent of industry organization members commence implementation of cyber security culture.</p>
Promote the use of existing information security, cyber protection standards and design principles, and establish new ones, where necessary	<p>Deliverable: IHLG commitment to promote use of existing standards and frameworks.</p>	<p>Task: Compile and share best practices and standards such as International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST).</p>	<p>Deliverable: 80 percent of industry organization members agree to implement standards and best practices.</p>

Promote the use of existing information security, cyber protection standards and design principles, and establish new ones, where necessary	Deliverable: IHLG commitment to promote use of existing standards and frameworks.	Task: Compile and share best practices and standards such as International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST).	Deliverable: 80 percent of industry organization members agree to implement standards and best practices.
Establish the mechanisms and means to share and communicate information including identification of threats, reporting of incidents and developments in defenses	Deliverable: Agree confidentiality of information shared amongst IHLG members and at the working group level.	Task: Assess requirements for data sharing and identify possible solutions.	Deliverable: Implement means to share threat and incident information in a secure environment.
Communicate threat-related information and assure situational awareness	Task: Exchange information, develop a common understanding of specific issues as they arise and coordinate responses to potential or emerging threats. Deliverable: Establish communication channels between industry partners.	Task: Exchange information, develop a common understanding of specific issues as they arise and coordinate responses to potential or emerging threats.	Deliverable: Establish mechanism to more systematically and efficiently coordinate analysis and responses to potential or emerging threats.

Table 5. «Civil aviation cyber security action plan» (Li, 2016)

Commitment	Short Term (0-6 months)	Mid Term (6-12 months)	Long Term (12-18 months)
Refine best practices, operational principles and defensive systems, as appropriate	Deliverable: IHLG commitment to promote use of existing standards and frameworks, 25 June 2014	Task: Continuous review and development of guidance material with ICAO and standard setting bodies. Task: Promote implementation of processes for quality assurance and continuous improvement of cyber security defenses and mitigations in all organizations. Deliverable: Share findings and best practices informally among industry stakeholders.	Deliverable: Implement mechanism to coordinate continuous improvement of operational and technical best practices across industry stakeholders.

5.2. DRAFT ASSEMBLY RESOLUTION ON ADDRESSING CYBER SECURITY IN CIVIL AVIATION

The Draft Assembly Resolution on Addressing Cyber Security in Civil Aviation was adopted on May the 30th, 2016 by the Assembly- 39th Session of the Executive Committee of the International Civil Aviation Organization (ICAO) and was developed by the ICAO and members of the Industry High Level Group (IHLG). (Li, wp_017_en, 2016)

The Industry High Level Group (IHLG) was established in 2013 by the Airport Council International (ACI), the Civil Air Navigation Services Organization (CANSO), the International Air Transport Association (IATA), and the International Coordination Council of Aerospace Industries Associations (ICCAIA) as a tool for high-level collaboration on issues of common interest and significance such as cyber security. (Li, wp_017_en, 2016)

The goal of the draft Resolution is to prompt the International Civil Aviation Organization (ICAO), its Member States and industry stakeholders to identify and recognize the importance of protecting civil aviation's infrastructure systems and data against cyber threats and undertake a global commitment to take cooperative and systematic measures to mitigate and address the risks. (Li, wp_017_en, 2016)

The Assembly,

«1. Calls upon States and industry stakeholders to take the following actions to counter cyber threats to civil aviation:

a) Identify the threats and risks from possible cyber incidents on civil aviation operations and critical systems, and the serious consequences that can arise from such incidents;

b) Define the responsibilities of national agencies and industry stakeholders with regard to cyber security in civil aviation;

c) Encourage the development of a common understanding among Member States of cyber threats and risks, and of common criteria to determine the criticality of the assets and systems that need to be protected;

d) Encourage government/industry coordination with regard to aviation cyber security strategies, policies, and plans, as well as sharing of information to help identify critical vulnerabilities that need to be addressed;

e) Develop and participate in government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts;

f) Based on a common understanding of cyber threats and risks, adopt a flexible, risk-based approach to protecting critical aviation systems through the implementation of cyber security management systems;

g) Encourage a robust all-round cyber security culture within national agencies and across the aviation sector;

h) Determine legal consequences for activities that compromise aviation safety by exploiting cyber vulnerabilities;

i) Promote the development and implementation of international standards, strategies and best practices on the protection of critical information and communications technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation;

j) Establish policies and allocate resources when needed to ensure that, for critical aviation systems: system architectures are secure by design; systems are resilient; methods for data transfer are secured, ensuring integrity and confidentiality of data; system monitoring, and incident detection and reporting, methods are implemented; and forensic analysis of cyber incidents is carried out; and

k) Collaborate in the development of ICAO's cyber security framework according to a horizontal, cross-cutting and functional approach involving air navigation, communication, surveillance, aircraft operations and airworthiness and other relevant disciplines.

2. Instructs the Secretary General to:

a) Assist and facilitate States and industry in taking these actions; and

b) Ensure that cyber security matters are fully considered and coordinated across all relevant disciplines within ICAO. (Li, wp_017_en, 2016)

Furthermore, ICAO established the Secretariat Study Group on Cyber security (SSGC) under the command of the Deputy Director, Aviation Security and Facilitation. The SSGC convened to define its Terms of Reference and its technical working groups that will focus on current and future air navigation systems, airworthiness (including remotely piloted aircraft systems (RPAS)), aerodromes and legal aspects. The SSGC is in collaboration with the Working Group on Threat and Risk (WGTR) to create cyber security risk matrices. (Cyber Safety and Security: ICAO)

The SSGC:

- functions as the pivotal point for all ICAO cyber security work,
- determines areas to be taken into consideration by the Working Groups of the SSGC and confirms that there are no overlapping of duties and responsibilities,
 - reviews ICAO Annexes in order to integrate existing Standards and Recommended Practices (SARPs) focused on cyber security,
 - examines the proposals of the Working Groups for amendments to ICAO provisions,
 - supports the development of partnerships between governments and the industry on a national and international level, in order to exchange information on «cyber threats, incidents, trends and mitigation efforts» (CIVIL AVIATION CYBERSECURITY INFORMATION REPOSITORY: ICAO),
 - enhances cyber security awareness amongst the aviation community. (CIVIL AVIATION CYBERSECURITY INFORMATION REPOSITORY: ICAO)

After the 39th Session of the ICAO Assembly, ICAO took the following measures regarding the response rate to State Letters (Table 6) (Implementation: ICAO):

Table 6. Measures regarding response rate to State Letters (Implementation: ICAO)

•	A registry was implemented in the ICAO Secretariat for continuous tracking of the status of replies.
•	Staff in Headquarters and the Regional Offices were provided training and issued instructions on the use of the system with a view to providing assistance to States in order to increase responses.
•	The format of State letters was reviewed, and based on an analysis of letters issued in the past, the Secretariat began working on a proposal to reduce by 30 per cent the number of State letters issued, by developing other means of communication with States.

The State Letters refer to proposals for amendments to Annexes and Procedures for Air Navigation Services (PANS) and the response rate to such letters is measured via Corporate Key Performance Indicator (CKPI) that belong to the “Stakeholder Management” subject area. (Implementation: ICAO)

5.3. ICAO CIVIL AVIATION AUTHORITY TOOLS (ICAAT)

The ICAO Civil Aviation Authority Tools (ICAAT) aim to provide key services to aviation operators via a common network facilitating data exchange, in order to alleviate the daily operations of basic stakeholders in the aviation community, such as Member States and airline operators. (Implementation: ICAO)

The ICAAT includes:

- The Data Network for Aviation (DNA). Its major function is to provide a single interface for users so that they have the ability to manage essential data utilized for various subsequent services. This will allow stakeholders to preserve the integrity and security of their information, conduct daily operations successfully and interact at their own will. (Implementation: ICAO)

- The Aircraft Registration Network (ARN). It consists of a global digital platform that contributes information related to manned and unmanned registered aircrafts. It is the refined descendant of the existing Aircraft Registration System (ARS), which facilitates the identification and registration of all Remotely Piloted Aircrafts (RPA), including small-sized drones. The ARN will also provide an interface for States' registration systems and offer inter-State operability features enhancing the welfare of the global aviation community. (Implementation: ICAO)

5.4. ICARD

«ICARD (International Codes and Route Designators) is a database of 230000 five-letter name-codes (5LNCs) and 16000 route designators (RDs) required for global air navigation, Air Traffic Services, Aeronautical Information Services, and the Procedures for Air Navigation Services - Aircraft Operations (PANS-OPS). A significant update was made to ICARD to keep the software up to date with current demands which included the roll-out of a new, enhanced ICARD platform to provide system stability, increased processing speeds and a more user-friendly design which will greatly improve efficiency for ICAO and State users.» (Implementation: ICAO)

5.5. IMPLEMENT

«IMPLEMENT is a data-driven decision-making process aimed at assessing the current status of aviation in States, identifying major problems and solutions available in order to maintain or improve the aviation capability of a State, and evaluating the needs of the aviation system.» (Implementation: ICAO)

5.6. SIMS

«The Safety Information Monitoring System (SIMS) is a web-based safety data and information system comprised of different applications, which generate indicators in support of SSP and safety management systems (SMS), allowing for the exchange

and sharing of safety data among SIMS participating States.» (Implementation: ICAO)

In 2017, the Safety Information Monitoring System (SIMS) was launched to States in the South American (SAM), North American, Central American and Caribbean (NACC), and Western and Central African (WACAF) Regions. ICAO aspires to create an implemented global information exchange platform through SIMS. (Implementation: ICAO)

5.7. DECLARATION ON CYBERSECURITY IN CIVIL AVIATION

The Declaration on cyber security in Civil Aviation was convened by the International Civil Aviation Organization (ICAO), from 4 to 6 April, 2017, in Dubai, United Arab Emirates, to discuss and address the perils of cyber threats that affect aviation. (Lambropoulos, 2018)

The declaration's conclusions regarding the protection of civil aviation's data and infrastructure systems against cyber threats and attacks were the following:

- Every State has the responsibility to take action so as to minimize the risks related to cyber threats, to establish the ability and capacity to address cyber threats in civil aviation and assure a legislative framework capable of taking measures against cyber-attack actors.
- Measures and capabilities regarding cyber security should serve peaceful purposes and be used solely for enhancing security, safety and efficiency.
- Cooperation between States and other stakeholders is a condition for the establishment of an efficacious and organized global framework, which will address the challenges of civil aviation's cyber security.
- All disciplines related to cyber security within State aviation authorities are obliged to regulate cyber security matters in a holistic way.
- Cyber-attacks targeted at civil aviation should be considered an offense against the principles, regulations and alignment for the safe and punctilious development of the international civil aviation. (Lambropoulos, 2018)

5.8. GLOBAL AVIATION SECURITY PLAN

The Global Aviation Security Plan (GASeP) is a plan that pledges ICAO, states and the aviation industry to ameliorate aviation security by 2030, in compliance with the direction provided by the 39th Session of the ICAO Assembly. The GASeP was sanctioned at the seventh meeting of the 212th Session of the ICAO Council (212/7) on November the 10th, 2017. (Security: ICAO)

Moreover, in 2017, ICAO collaborated with international agencies, States, the United Nations Office on Drugs and Crime (UNODC), the United Kingdom's Department for Transport, and the United States' Department of State to forward and support aviation security and assist in developing ideas and programs. In addition, ICAO partnered with Montréal's Concordia University to offer the Aviation Security Professional Management Course (PMC) with three sessions in three regions in 2017 and, also, collaborated with Airports Council International (ACI) to establish a Management of Airport Security Course in 2017. (Implementation: ICAO)

5.9. FIRST TRANSPORT CYBERSECURITY CONFERENCE

The first Conference on Transport Cyber Security was organized by the European Union Agency for Network and Information Security in Lisbon, on January 23rd, 2019. (Transport cybersecurity: Raising the bar by working together, 2019)

«The European Union Agency for Network and Information Security (ENISA) is a center of expertise for cyber security in Europe. ENISA is actively contributing to a high level of network and information security (NIS) within the Union, since it was set up in 2004, to the development of a culture of NIS in society and in order to raise awareness of NIS, thus contributing to proper functioning of the internal market. The Agency is located in Greece with its seat in Athens and a branch office in Heraklion, Crete.» (About ENISA)

It was supported by:

- the European Commission,
- European Aviation Safety Agency (EASA),

- the European Maritime Safety Agency: «EMSA is one of the EU's decentralized agencies. The Agency provides technical assistance and support to the European Commission and Member States in the development and implementation of EU legislation on maritime safety, pollution by ships and maritime security. It has also been given operational tasks in the field of oil pollution response, vessel monitoring and in long range identification and tracking of vessels.» (ABOUT US: EMSA) Its headquarters are located in Lisbon, Portugal, (ABOUT US: EMSA) and

- the EU Agency for Railways: «ERA is established to provide the EU Member States and the Commission with technical assistance in the development and implementation of the Single European Railway Area.» (THE AGENCY: EUROPEAN UNION AGENCY FOR RAILWAYS) Its mission is to «make the railway system work better for society and contribute to the effective functioning of a Single European Railway Area without frontiers.» (Mission, vision and values: ERA) Its headquarters are located in Valenciennes Cedex, France. (ERA Headquarters) (Transport cybersecurity: Raising the bar by working together, 2019)

Participants in the event were a hundred and seventy private and public partners from all over Europe, representing all modes of transport. The main theme of the conference was the EU legal framework for cyber security, its implementation to the transport sector and potential alternatives for further collaboration. (Transport cybersecurity: Raising the bar by working together, 2019)

During the conference the following conclusions were reached:

- The European transport system should have the ability to prevent cyber-attacks and address them with resilience. Safety through cyber security should be ensured.

- Cyber security should be approached aggregately taking into consideration not only the internet-connected systems, but also the «human element» (Transport cybersecurity: Raising the bar by working together, 2019). To achieve that, there is a need for collaboration between the technical and operational levels.

- Non-regulatory actions, such as exchange of information, development of cyber skills, and enhancing of awareness and capabilities, should be taken to

establish the foundations of a «cyber security culture» (Transport cybersecurity: Raising the bar by working together, 2019) for all transport sectors.

➤ Organization of cyber security workshops and meetings for experts from different transport modes, in order to exchange and share information and ideas regarding cyber security.

➤ Maintain discussions on cyber security with third countries and collaborate with international organizations, such as the International Civil Aviation Organization (ICAO). (Transport cybersecurity: Raising the bar by working together, 2019)

5.10. AVIATION ISAC

«The Aviation Isac (Information Sharing and Analysis Center) is a unique focal point for security information sharing across the aviation sector. It enhances the ability of the sector to prepare for threats, vulnerabilities, and incidents so that businesses operating in the aviation industry can best manage their risks.» (THE AVIATION ISAC)

« The center facilitates the sharing of timely and actionable information related to threats, vulnerabilities, incidents, potential protective measures, and best practices. It provides cooperation and communication among members using a secure trusted network. The center conducts research and analyzes information to validate accuracy and severity and recommend mitigation strategies. It, also, enables the development of professional and trusted relationships across the public and private sector.» (THE AVIATION ISAC) Moreover, the center distributes information regarding threat and mitigation strategies that make use of secure and effective methods, issues best practices and promotes educational awareness. (About us: Aviation Isac)

5.11. EUROCONTROL

«Eurocontrol is an intergovernmental organization with 41 Members and 2 Comprehensive Agreement States. The organization is committed to building, together with our partners, a Single European Sky that will deliver the air traffic management (ATM) performance required for the twenty-first century and beyond. Over 1,900 highly qualified professionals spread over four European countries work at EUROCONTROL, deploying their expertise to address ATM challenges.» (Who we are: Eurocontrol)

The organization:

- Works on operational and technical elements,
- Provides advice and guidance civil as well as military aspects of ATM,
- Unites States with different necessities in the pursuit of a common goal. (Who we are: Eurocontrol)

The organization establishes a European network-centric information system and assures the dispersion of aeronautical information globally while ensuring interoperability. It collaborates with the European Commission, Member States and the aviation community to create a refined European route network, so that flights can become direct, saving time, fuel and money. (Our areas of expertise: Eurocontrol)

Furthermore, it counterpoises airspace capacity with demand, maximizing the efficiency and safety of European air traffic. It provides quality training, services and products in air traffic management (ATM) to a wide spectrum of actors in the aviation community. These include general introductory courses on ATM concepts and advanced operational training. It offers customized training activities, network management and deployment activities and supports the implementation of the Single European Sky and the SESAR program. Moreover, the organization assists civil-military coordination in European air traffic management. (Our areas of expertise: Eurocontrol)

Its initiatives focus on the air traffic management infrastructure of the future, so as to assure a free-flowing exchange of information between airspace users and a fully

integrated framework for the European air navigation system. (Our areas of expertise: Eurocontrol)

The organization consists of teams of economics experts, business cases and cost benefit analysis specialists that provide various economic analysis tools for many actors of the community such as airspace users, air navigation service providers, airports, military users and major ATM decision-makers. (Our areas of expertise: Eurocontrol)

Its main aim is to assure that organizational objectives and staff needs are in harmony so as to ensure an effective, efficient, and safe ATM system. It also runs a full set of simulation platforms for every phase of a flight: from en-route ATC to airports, the Network Management function and the cockpit. (Our areas of expertise: Eurocontrol)

Finally, the organization publishes statistics, forecasts, reports and studies on European air traffic trends and delays. In addition, it measures the progress made by the air transport industry regarding the sectors mentioned above. (Our areas of expertise: Eurocontrol)

5.12. THE SESAR PROGRAM

«SESAR is the mechanism which coordinates and concentrates all EU research and development (R&D) activities in Air Traffic Management (ATM), pooling together a wealth experts to develop the new generation of ATM. Today, SESAR unites around 3,000 experts in Europe and beyond.» (ABOUT: DICOVER SESAR)

The SESAR Joint Undertaking was established in 2007 in order to manage an international public-private partnership. (ABOUT: DICOVER SESAR)



Figure 4. Contribution of the European aviation industry to the EU's GDP (ABOUT: DICOVER SESAR)

The figure (Figure 4) above describes the contribution of the European aviation industry to the EU's GDP and employment of its citizens.

According to SESAR, ATM has various specific and important roles:

- «Acts as a guardian of safety,
- Connects European cities and Europe with the rest of the world,
- Addresses climate change by enabling green and efficient routes,
- Maximizes current infrastructure while delivering advanced information services,
- Acts as a catalyst for Europe's competitiveness and innovative capacity.»

Moreover, based on the SESAR's view, the European ATM system is based on ageing technology and procedures, which means that, considering the expected traffic growth until 2035, the system will have to undergo certain updates. SESAR belongs to the most innovative infrastructure projects of the European Union. Its main aim is to maximize European ATM performance and create an intelligent European air transport system. (ABOUT: DICOVER SESAR)

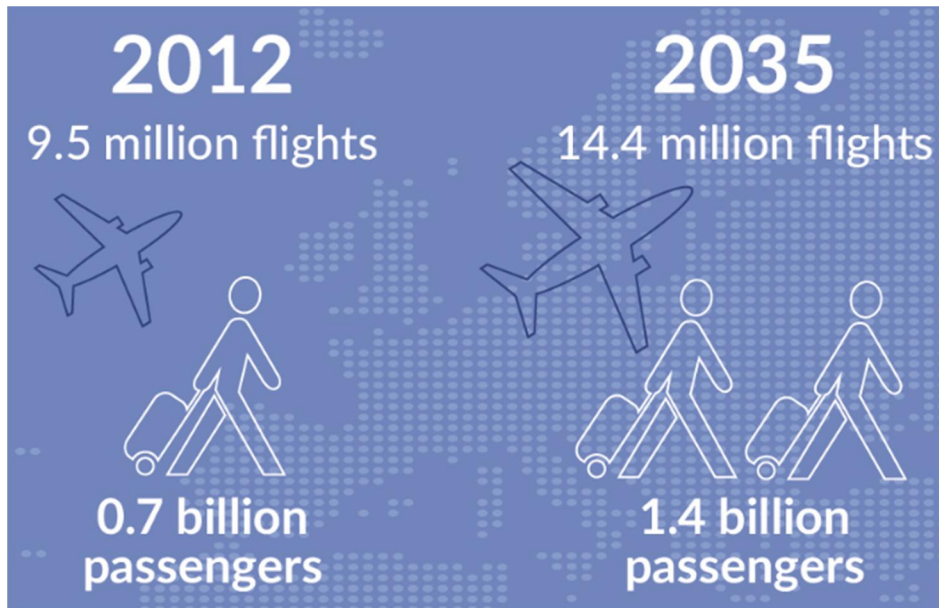


Figure 5. Growth of the number of flights and passengers until 2035 (ABOUT: DICOVER SESAR)

The figure (Figure 5) above summarizes the expected traffic growth in 2035, comparison to the traffic in 2012. It is evident that the number of flights will increase by almost 51%, while the number of passengers will rise by almost 100%. These percentages signify an important augmentation of the European aviation traffic. (ABOUT: DICOVER SESAR)

5.12.1. SESAR'S VISION

SESAR's goal is to update European ATM by developing and delivering new and improved technologies and procedures. It relies on the notion of trajectory-based operations and the provision of air navigation services (ANS) allowing aircrafts to fly their favored trajectories without being restrained by airspace configurations. (ABOUT SESAR'S VISION)

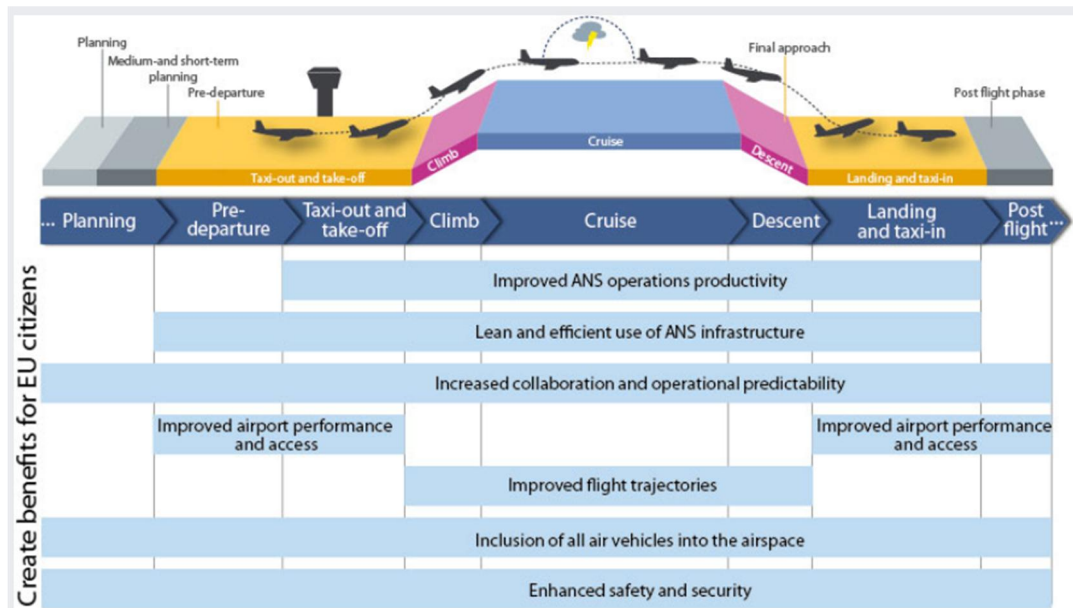


Figure 6. Operation and benefits of the SESAR program (ABOUT SESAR'S VISION)

Figure 6 above summarizes the aim of the SESAR program and the benefits it aspires to offer to all the actors of the European aviation community.

In order to accomplish its vision the program utilizes progressed automation support, virtualized technologies as well as the standardized and interoperable systems. The system infrastructure will evolve by using digitalization technology, and will enable air navigation service providers (ANSPs) to plug in their operations where needed, with the support of a variety of information services, regardless of national borders. The European ATM network level will include all European airports and will offer optimized airspace user operations. (ABOUT SESAR'S VISION)

Until 2050, there will be performance-based operations across all Europe, with multiple options such as free-flowing coordination between ANSPs and full end-to-end ANS provided at network level. Additionally, in order to maximize performance, the flight will be dealt with aggregately, within a flow and network context, instead of focusing on segmented portions of its trajectory, which is the current state. (ABOUT SESAR'S VISION)

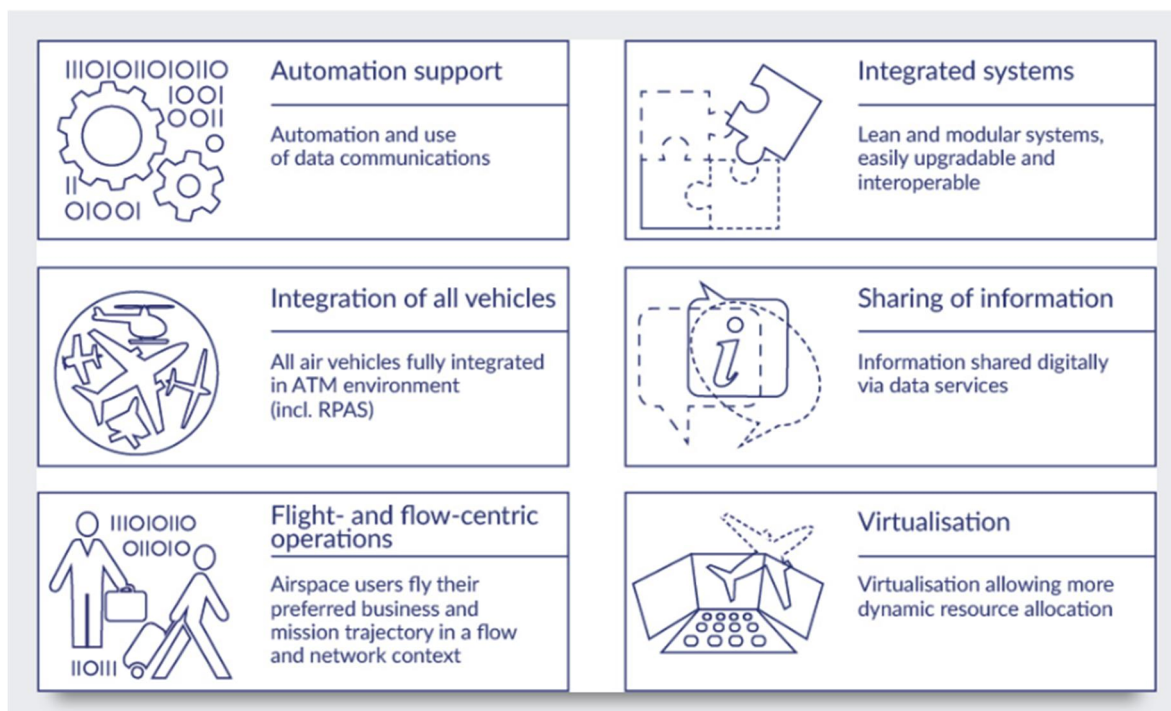


Figure 7. Basic goals of the SESAR program (ABOUT SESAR'S VISION)

Figure 7 above illustrates the basic aims of the SESAR program for the future of the European aviation system, which are:

- the support of aviation systems via automation and use of data communications,
- the full integration of all air vehicles in the ATM system,
- the realization of operations in a way that allow flowing and non-segmented flights for the airspace users,
- the development of integrated systems that are easily upgradable and interoperable,
- the facilitation of digital information sharing through data services and
- the virtualization of operations that will enable a dynamic resource allocation.

(ABOUT SESAR'S VISION)

6. MEASURES FOR THE MITIGATION OF CYBER RISKS AND TREATS

Table 7. Measures for the prevention, detection and mitigation of cyber threats in aviation (PricewaterhouseCoopers, 2016)






 <i>Develop quantified and measurable baselines</i>	 <i>Create current education and training</i>	 <i>Scope and prioritize assets</i>	 <i>Collaborate internally</i>	 <i>Acquire broad expertise</i>
By establishing baselines for data transmissions, volumes, and times, an airline can determine when an event has occurred that is outside the norm.	Employees need to be taught to recognize suspicious behaviors and how to deal with them.	It's important to prioritize assets to focus more detection capability on the "crown jewels," such as personal passenger data (including credit card data) and operational systems.	Airlines have to build collaborative systems within their own organizations. This requires breaking down walls with cross-functional operating procedures and creating incident response processes that are embedded into business processes. So when a breach is detected, relevant groups throughout the airline are alerted and can react in a more timely and unified way. There should also be formal processes for actively sharing new threat intelligence, to allow for more effective monitoring mechanisms going forward.	Leave "profiling" to the experts, those who can interpret activity reports and understand anomalies to recognize false positives and signs of a real attack. These experts have intimate knowledge of enterprise networks, endpoints, domains, and operations that is paired with industry-wide experience and knowledge of evolving threat actors, techniques, and tools.

Table 7 above analyses the measures that can be taken by the actors in the aviation sector so as to prevent, detect and mitigate cyber threats and attacks effectively and instantly. The actors are recommended to:

- «develop quantified and measurable baselines» (PricewaterhouseCoopers, 2016),
- establish up-to-date educational and training programs,
- «scope and prioritize assets» (PricewaterhouseCoopers, 2016),
- create cooperative systems within their organizations and
- obtain knowledge and expertise via outsourcing. (PricewaterhouseCoopers, 2016)

Table 8. Analysis of the prevention, detention and reaction measures to cyber threats
(PricewaterhouseCoopers, 2016)




Part 2: Prevention	Part 3: Detection	Part 4: Reaction
 <p>The first line of defense is to prevent attacks that can corrupt or destroy data and interrupt operations. We'll discuss key elements of attack prevention that include:</p> <ul style="list-style-type: none"> • The critical role of boards of directors • A proactive approach that includes knowledge of global threats—current and prospective, people and places • Expanding and formalizing industry standards • Dealing with risks from supply chain, parts, and third-party vendors 	 <p>Even with the best prevention systems, determined hackers will get through. It's essential to detect and isolate these attempts before they spread and do more damage. The key elements of a detection system include:</p> <ul style="list-style-type: none"> • Monitoring network and IT systems • Protecting customer and operational data • Understanding and dealing with insider threats 	 <p>Since no system is foolproof, airlines have to develop a methodology for responding quickly to an attack in order to limit reputational damage. And they need to use all details of the attack to enhance prevention. A good reaction plan includes:</p> <ul style="list-style-type: none"> • Notifying customers and other stakeholders as soon as possible and managing press stories • Collecting forensic data to identify security weaknesses • Minimizing damage caused by security breaches • Closing the loop by using new information to improve prevention methods

Table 8 above presents an analysis of the actions required to successfully prevent, detect and react to cyber-attacks and threats that are constantly evolving and becoming more persistent. (PricewaterhouseCoopers, 2016)

7. TECHNOLOGIES DEVELOPED TO DEAL WITH CYBER THREATS

7.1. AIRBUS'S AND SITA'S CYBERSECURITY SERVICES FOR AIR TRANSPORT INDUSTRY

«Airbus and SITA have launched new Security Operations Center Services customized for the specific needs of the air transport industry. These new incident detection services will provide airlines, airports and other air transport industry stakeholders with information about unusual cyber activity that may impact their businesses.» (Airbus and SITA Join Forces to provide Advanced Cybersecurity Services for Air Transport Industry)

SITA's Airline IT Trends Survey conducted in 2016 illustrates that 91% of airlines are looking to invest in cyber security programs until 2020. (Airbus and SITA Join Forces to provide Advanced Cybersecurity Services for Air Transport Industry)

«Almost every airline and airport in the world is a customer of SITA and it delivers solutions for the world's most extensive communications network. Airbus works with companies, critical national infrastructures, governments and defence organizations to detect, analyze and counter increasingly sophisticated cyber attacks. Together they will use their expertise to detect cyber activity relevant to airlines and airports. In case, the joint Security Operations Center Services will provide appropriate containment and remedial action ensuring that a company's digital assets are safe from attack.» (Airbus and SITA Join Forces to provide Advanced Cybersecurity Services for Air Transport Industry)

The Security Operations Center Service «combines real-time monitoring services for applications and communications dedicated to air transport and incident response services.» (Airbus and SITA Join Forces to provide Advanced Cybersecurity Services for Air Transport Industry)

SITA develops a portfolio of cyber security products and services. These products and services will assist airlines and airports in detecting and responding to cyber threats, as well as securing their company assets against cyber-attacks. (Airbus and SITA Join Forces to provide Advanced Cybersecurity Services for Air Transport Industry)

Airbus provides services related to aeronautics and space. Airbus offers a wide range of passenger airliners from 100 to more than 600 seats. In addition, the company supplies tanker, combat, transport and mission aircrafts to the European aviation industry and is Europe's major space enterprise as well as the world's second largest space business. Finally, Airbus manufactures civil and military helicopters and rotorcraft solutions for the global aviation industry. (Airbus and SITA Join Forces to provide Advanced Cybersecurity Services for Air Transport Industry)

7.1.1. AIRBUS CYBERSECURITY

«Airbus Cyber Security, a unit of Airbus Defence and Space, provides companies, critical national infrastructures and government and defence organizations with reliable, high-performance products and services to detect, analyze and respond to increasingly sophisticated cyber-attacks.» (Airbus and SITA Join Forces to provide Advanced Cybersecurity Services for Air Transport Industry)

SITA is «the world's leading air transport IT and communications specialist» (About SITA: Who we are). The organization provides information and communication technology (ICT) solutions to airlines, airports, aircrafts, ground handlers, governments, air cargo, aerospace, air navigation service providers and international organizations. It consists of 400 air transport owner-members from around the world. (About SITA: Who we are)

SITA's portfolio for the aviation industry includes:

- «Managed global communications, infrastructure and outsourcing services
- Services for airline commercial management, passenger operations, flight operations, aircraft operations, air-to-ground communications, airport management and operations, baggage operations, transportation security and border management and cargo operations» (About SITA: Who we are).

The organization offers its services and solutions to customers from over 200 countries and territories around the world and has offices all around the world. (About SITA: Who we are)

By 2021, the aviation industry is expected to implement technologies focused on protecting the core network of the aviation systems, developing Internet of Things (IoT) Security and preventing data leakage and Cloud access (Cloud Access Broker, CASB) of confidential and sensitive information related to aviation systems and networks. Additionally, network access control and multi-factor authentication technologies are expected to be implemented by the majority of aviation companies worldwide by the end of the same year. (SITA, 2018)

Furthermore, the majority of actors in the aviation industry are planning to develop a Security Operations Center (SOC), in order to achieve an immediate detection of cyber intrusions, by 2021. It has been observed that security outsourcing is steadily increasing considering that 80% of the Security Operations Centers that are already in place, are run by external providers. The cause of this is, mainly, the lack of sufficient internal skills and resources regarding the implementation of cyber security strategies. (SITA, 2018)

8. CYBER RISK MITIGATION AND ASSESSMENT

8.1. MEASURES FOR AIRPORTS

Good practices related to security mitigation and assessment for airports fall into three basic categories: Technical, Organizational and Policies and Standards. (Lykou, Anagnostopoulou, & Gritzalis, 2018) The figure below (figure 8) presents the constituent parts of these three categories.



Fig. 2. Cyber Security Good Practices Classification

Figure 8. Best technical, organizational practices and policies and standards (Lykou, Anagnostopoulou, & Gritzalis, 2018)

➤ «Antimalware» (Lykou, Anagnostopoulou, & Gritzalis, 2018): Antimalware software detects and quarantines malicious software. Smart airports (those that utilize smart applications to support fundamental airport activities, such as Internet of Things applications, Building Management Systems-BMS and HVAC equipment controls) use an antimalware to protect IT equipment at a rate of 60%, agile airports (those that gradually adapt to the constantly changing technological environment and utilize an airport platform network that provides shared services) at a rate of 50%, and basic airports (those that provide standard passenger services and utilize basic technology that is required in order to achieve effective management of all aircraft operations such as landings and departures) at a low rate of 33%. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

➤ «Software and hardware updates» (Lykou, Anagnostopoulou, & Gritzalis, 2018): It is highly recommended to airports to perform these updates regularly, so as to mitigate cyber-attacks and vulnerabilities of their systems. Smart

and agile airports apply these at a rate of 80% rate, while basic airports at 33% rate. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

➤ «Firewalls and network segmentation» (Lykou, Anagnostopoulou, & Gritzalis, 2018): Those are utilized so as to protect the airport network infrastructure and block unauthorized connections between networks. Smart and agile airports implement these practices at 100% rate, while basic airports reach a 67% implementation rate. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

➤ «Intrusion Detection Systems (IDS)» (Lykou, Anagnostopoulou, & Gritzalis, 2018): Those systems monitor both software and hardware devices throughout the network. These systems consist of two categories: «(i) network-based IDS, focused on the analysis of network traffic and (ii) host-based IDS, able to analyze activities on the host and raise alerts, in case of events like unauthorized access to applications, escalation of privileges and modification of file systems.» (Lykou, Anagnostopoulou, & Gritzalis, 2018) Both smart and agile airports utilize IDS at 60% rate, which indicates a security gap for these airports while basic airports do not apply these systems at all, indicating a significant security risk that should be mitigated. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

➤ «Strong user authentication» (Lykou, Anagnostopoulou, & Gritzalis, 2018): It is crucial for IT systems and devices to be protected via user authentication. That is critical for highly sensitive and remote services. Access to such services should be granted solely through biometric identifiers and/or multifactor authentication. Smart airports reported the use of user authentication at 80%, agile airports at 60% rate, while basic airports do not implement user authentication at all. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

➤ «Change default credentials of devices» (Lykou, Anagnostopoulou, & Gritzalis, 2018): This applies to devices that are connected to the airport network. Default passwords should be regularly changed and remote access to the network should be disabled at times when it is not needed, in order to deter remote-connection cyber-attacks. This remains a critical vulnerability for all airports since the implementation of such measures is poor. Smart airports comply at 40% rate, agile airports at 50% and basic airports at 33%. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

➤ «Data encryption» (Lykou, Anagnostopoulou, & Gritzalis, 2018): Its main purpose is to shield sensitive information shared in the network from

eavesdroppers and secure data storage and collection. Smart airports have the highest implementation rate of encryption methods at 80% rate, agile airports have a lower rate at 50% and basic airports do not utilize any encryption method. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

➤ «Bring your own device (BYOD) controls» (Lykou, Anagnostopoulou, & Gritzalis, 2018): As mentioned above, BYOD is a new trend that is significantly growing, affecting airport systems and weakening security and resilience to cyber threats and attacks. Even though airport employees should be prevented from connecting their personal devices to the airport's network, this is not the case. Therefore, in order to protect the airport's infrastructure and minimize the risk of compromised devices connecting to the network, technical controls should be performed frequently. All airports have low implementation rates (smart 40%, agile 33%, and basic 0%) and that underscores the necessity of the development of control methods suitable for airport networks. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

➤ «Disaster recovery plans for IT assets» (Lykou, Anagnostopoulou, & Gritzalis, 2018): Technical procedures should be in place to restore operation of critical IT assets to an adequate level of service, in case of an emergency. Both technical and organizational aspects must be included in disaster recovery plans. People involved must have a clear view of their roles, the sequence of actions to be performed and the actors involved. All smart airports responded positively to this practice with 100% rate, agile airports' implementation reached 60%, while for basic airports only one third stated to apply such procedures for IT assets. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

➤ «Application security and secure design» (Lykou, Anagnostopoulou, & Gritzalis, 2018): Secure design should be part of System/Services/Technology Acquisition. It should be combined with airport assets under provisioning risk assessment, privacy by design principle and security criteria requirements. Smart airports responded to apply secure design procedures at 80% rate, while agile and basic airports had implemented this practice at only 30% rate, which indicates a major security gap. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

Table 9. «Technical good practices» (Lykou, Anagnostopoulou, & Gritzalis, 2018)

Technical Good Practices	BASIC	AGILE	SMART	ALL
Antimalware	33%	50%	60%	50%
Software and hardware updates	33%	80%	80%	72%
Firewalls & network segmentation	67%	100%	100%	94%
Intrusion Detection Systems	0%	60%	60%	50%
Strong user authentication	0%	80%	60%	61%
Change default credentials	33%	50%	40%	44%
Data encryption	0%	50%	80%	50%
BYOD Controls	0%	30%	40%	28%
Disaster recovery plans	33%	60%	100%	67%
Appl. security & secure design	33%	30%	80%	44%
Average implementation rate	23%	59%	70%	56%

The table above (Table 9) shows the implementation rates of the technical good practices analyzed above for every type of airport as well as the average implementation rate for all of them aggregately. It is evident that smart airports use most of them at satisfactory levels, ensuring sufficient cyber security systems while basic airports are the most vulnerable to cyber threats due to the lack of adequate application of all of them. Overall, the most applied practices for all airports are: firewalls and network segmentation (94%), software and hardware updates (72%), disaster recovery plans (67%) and user authentication (61%). However, in order to efficiently secure airport infrastructure and minimize the possibility and the consequences of cyber-attacks, all airports should maximize the implementation of all practices. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

8.2. MEASURES FOR ORGANIZATIONS

Some of the cyber risk mitigation and assessment measures an organization could apply are:

- «User access control and management» (Lykou, Anagnostopoulou, & Gritzalis, 2018): This consists of logical and physical access control to airport IT systems as well as identity access to management systems. All airport types (smart, agile, basic) apply such procedures thoroughly (90-100%). This indicates that safety culture is already developed, regulated and implemented in airport infrastructure. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

▪ «Screen individuals prior to authorizing access to the airport's information system» (Lykou, Anagnostopoulou, & Gritzalis, 2018): Identity fraud risk could be mitigated with the use of biometric identification for employees prior to acquiring access to the airport's network. Smart airports implement this procedure at 60% rate, agile airports at 50%, while basic airports at 0%, according to their responds. However, there are some restrictions related to biometric identification. These are privacy and personal data protection regulations. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

▪ «Ensure individuals requiring access to airport IT systems sign appropriate access agreements» (Lykou, Anagnostopoulou, & Gritzalis, 2018): Those agreements include non-disclosure & acceptable use agreements, rules of behavior and conflict of interest agreements. This would ensure the identification of the individuals and them not being a possible threat agent. All airport types implement this practice at a 20-40% rate. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

▪ «Establish personnel security requirements for third-party providers» (Lykou, Anagnostopoulou, & Gritzalis, 2018): These requirements include security roles and responsibilities as well as monitoring of third party compliance. This procedure would ensure that third party providers do not impose a cyber threat and in the case of an incident they will have to suffer the consequences. Smart airports implement these requirements at 60% rate, agile and basic airports at 30% rate. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

▪ «Provide basic security awareness training to all information system users» (Lykou, Anagnostopoulou, & Gritzalis, 2018): The training program should align with the specific requirements of the airport and its IT systems. Smart airports provide such training at a 60% rate, agile airports are at 50% rate and basic airports are at a low 33% rate, indicating that it is crucial for them to improve cyber resilience through the development of such programs. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

▪ «Provide specialized information security training» (Lykou, Anagnostopoulou, & Gritzalis, 2018): It will be role-based and security-related. Specialized security training is a necessity for all airports in order to effectively respond to the increasing complexity of cyber security threats, since the implementation rate for all categories falls between 33%-40%. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

▪ «Train airport personnel in their incident response roles with respect to the information system» (Lykou, Anagnostopoulou, & Gritzalis, 2018): Incident response

training consists of «user training in the identification and reporting of suspicious activities, both from external and internal sources to handle the situation in a way that limits damage and reduces recovery time and costs» (Lykou, Anagnostopoulou, & Gritzalis, 2018). All airport categories have a low implementation rate, which falls between 33%-40%, and this indicates the need for more training programs so as to allow the personnel to deal with cyber incidents effectively and reduce any negative impacts. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

▪ «Test and regularly exercise the airport's incident response capability system» (Lykou, Anagnostopoulou, & Gritzalis, 2018): These tests aim at measuring incident response effectiveness and systems' capability to respond at a high level. Smart airports implement this procedure at 60% rate, agile at 50% rate and basic airports only at 33%. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

Table 10. «Organizational good practices» (Lykou, Anagnostopoulou, & Gritzalis, 2018)

Good practices about people, organization and processes	BASIC	AGILE	SMART	ALL
User access management	90%	90%	100%	95%
Screen individuals prior to authorize access to airport's IT system	0%	50%	60%	44%
Ensure access agreement to individuals prior to grant access	33%	20%	40%	28%
Personnel security requirements for third-party providers	33%	30%	60%	39%
Basic security awareness training to all information system users	33%	50%	80%	56%
Specialised info security training	33%	30%	40%	33%
Train airport personnel in incident response for IT system	33%	30%	40%	33%
Test and exercise incident response capability for IT system	33%	50%	60%	50%
Average implementation	36%	44%	60%	47%

Table 10 above presents the implementation rates of the good practices regarding people, organizations and processes for all airport categories as well as the average implementation rate for all of them aggregately. Except user access management, which is implemented at a very high rate from all airports (95%), all the other practices are applied at a significantly low rate. This situation does not allow organizations to respond effectively to cyber-attacks and form a strong protective

shield against them. Overall, the average implementation rate for all practices is very low (47%), which urges for drastic measures focused on a more persistent implementation of the procedures mentioned above. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

8.3. POLICIES AND STANDARDS FOR AIRPORTS AND ORGANIZATIONS

Some of the policies and standards airports and organizations could implement are:

- «Appoint an information security officer with the mission and resources to develop, implement and maintain an airport wide information security program.» (Lykou, Anagnostopoulou, & Gritzalis, 2018) This is an obligatory policy that aims at protecting intelligent applications, such as SCADA and IoT (Internet of Things) and fulfilling security requirements. Smart airports have implemented this policy at a 100% rate while agile and basic airports have a lower implementation rate at 50% and 33%. This indicates a crucial security inability. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

- Establish and implement strict rules that will regulate the installation of software, in compliance with contract agreements and copyright laws. The types of software that are permitted should be determined by explicit rules. Smart airports have an efficient implementation rate of 60%, while agile airports have a low rate at 30% and basic airports do not apply such rules at all, resulting in the augmentation of cyber risks and vulnerabilities. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

- Information security should be monitored frequently across the airport. Smart airports implement this practice at 80% rate, while agile and basic airports apply this at 50% and 33% rate respectively. It is critical for all airport security practices to incorporate monitoring strategies and constant reporting systems focused on the security state of the information system of the airport. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

- Organizations that comply with Information Security Management System (ISMS) implement international standards. In order to comply fully, they should establish an information security framework and use external audits, so as to effectively measure progress, spot gaps and demonstrate compliance. Smart airports

implement such practices at 60% rate, agile airports at 40% and basic at 33% rate. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

- In addition to the Information Security compliance of the airports, providers of external information services should also meet security standards and create a chain of trust with the airports. The majority of the providers of smart airports implement this practice at 80% rate, while agile and basic airports' providers apply it at 50% and 33% rate respectively. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

Table 11. «Policies and standards» (Lykou, Anagnostopoulou, & Gritzalis, 2018)

Good Practices for Policies and standards	BASIC	AGILE	SMART	ALL
Appoint IT security officer	33%	50%	100%	56%
Enforce rules governing installation of software	0%	30%	60%	33%
Continuous monitoring of information security	33%	50%	80%	56%
ISMS, International standards and compliance audits	33%	40%	60%	44%
Information security compliance from external providers	33%	50%	80%	56%
Average implementation	26%	44%	76%	50%

Table 11 above shows the implementation rates of «Good Practices for Policies and Standards» (Lykou, Anagnostopoulou, & Gritzalis, 2018) of all airport categories. It is evident that smart airports have the highest implementation rate of all practices (76%). The most implemented practices are: the appointment of an IT (Information Technology) security officer (56%), the consistent monitoring of information security (56%) and the information security compliance from external providers (56%). It is crucial for all airport categories to focus on a higher implementation rate of all these policies and standards to ensure security against cyber threats and risks. (Lykou, Anagnostopoulou, & Gritzalis, 2018)

9. CONCLUSIONS AND RECOMMENDATIONS

Increased automation of anti-hacking tools has resulted in a more effective protection against cyber-attacks and is a measure that could be used by organizations so as to protect their systems. (De Cerchio & Riley, 2011)

In addition to the measures and policies described above, some recommendations regarding the protection of aviation systems against cyber threats are:

➤ Cloud computing: The use of cloud computing could offer aviation companies and airports the ability to save and store sensitive data in remote storage units with impenetrable cyber security systems. This practice would offer a back-up storage unit for all passenger, system, aircraft and airport information that are targets of cyber-attacks. Moreover, the fact that this service is provided by third parties specialized in storing and protecting data from cyber threats ensures their trustworthiness and the safety of the information.

➤ Virtualization: Regarding the BYOD trend, a measure that could mitigate cyber risks is the use of virtualization. Virtualization is a cloud computing service that provides the ability to use one computer with multiple functions and great processing power, which provides different user interfaces to all the individual computers or portable devices that are connected to it. Every device utilizes processing power from the central CPU (Central Processing Unit) of the main computer in order to run its programs and applications. Each user has the ability to use a unique interface environment, completely different from the other devices and highly personalized. Another benefit from the use of virtualization is that in case of a cyber-attack to one of the devices, the rest of them, as well as the main computer, remain intact. The whole system remains risk-free. The only way a threat agent could cause damage to all the devices would be by attacking the main unit and specifically, the hypervisor that provides and controls all the interface environments. In order to prevent cyber-attacks to the hypervisor, strong firewalls and encryption methods could be implemented in addition to the measures that are already in place. Furthermore, in case that a threat agent attempts to create a fake main unit

(hypervisor) to deceive the users and have them connecting their devices to it, the existing system will respond immediately, by recognizing and blocking the threat.

➤ Virtual networks: The utilization of virtual networks could ensure cyber security for airport and aviation networks. Virtual networks provide different IP addresses and domain names to their users, allowing them to connect via covered and private addresses that are stealthy to threat agents. In this way, airport infrastructure and aviation networks are protected by cyber-attacks on IP addresses. Virtual networks prevent threat agents from locating the real IP addresses and domain names of the users of the actual networks, allowing an intrusion-free operation of its functions and a safe transfer of sensitive data and classified information.

➤ Data recovery plan: Sensitive data and crucial information of aircraft and airport systems require protection from destruction and loss due to infrastructure damage or error. The negative impacts of such events could severely vitiate airport and aircraft operations, cause delays and cancellation of flights and result in passengers feeling dissatisfied and frustrated. Aviation actors should develop plans focused on the recovery and preservation of data and critical aviation information such as passenger and system data. Some measures against those negative impacts could be: a) the maintenance of secure backup information at a remote storage facility, b) the maintenance of backup systems in hot or cold reserve, c) the implementation of security measures aimed at the control of excessive voltage, d) the utilization of appropriate batteries for the energy supply of the physical systems and e) the installation and usage of power generators at remote and secured areas.

In conclusion, cyber security is a major issue in the aviation industry as well as all transport industries, since more and more systems rely on interdependent computer networks. The rapidly evolving and spreading technological advancements can have a significant impact on aviation systems and network. Cyber threats and risks are constantly evolving, becoming more efficacious and challenging than before. On top of that, the majority of services and facilities provided at airports in addition to aircraft operational systems and networks are becoming even more automated, digitalized and interconnected, making them more vulnerable to cyber threats and intrusions. The use of portable devices from employees and passengers multiplies the potential targets of threat agents. This also increases the vulnerability of aircraft systems and operations, since these devices are also carried by passengers and

personnel during flights. Moreover, internet connections and the use of remotely controlled equipment on aircrafts provide openings to threat agents from around the world to attack systems and disrupt aviation operations. There is also a risk of personal data leakage and the use of such data in malicious ways by cyber threat agents with various goals and motivations. Furthermore, the fact that even personal devices are affected by cyber-attacks indicates that even passengers and employees could impose a threat to aviation cyber security even without being aware of it. Additionally, the global nature of the aviation industry signifies the large impact a possible cyber-attack could have on air transportation around the world. National airports and aviation companies are connected and cooperate in many levels to achieve maximum efficiency and offer quality services to all their passengers. Therefore, it is of paramount importance that all stakeholders collaborate effectively in order to create and establish strong cyber security and risk mitigating measures and policies as well as enhance the existing ones.

Aviation organizations and associations such as the International Civil Aviation Organization (ICAO), the European Aviation Safety Agency (EASA), the European Union Agency for Network and Information Security (ENISA), the Airport Council International (ACI), the Civil Air Navigation Services Organization (CANSO), the International Air Transport Association (IATA), the International Coordination Council of Aerospace Industries Associations (ICCAIA) and the Aerospace and Defence Industries Association of Europe (ASD) have developed policies and measures for the prevention and mitigation of cyber risks. Most airports and aviation actors comply with the policies and implement most of the measures established to minimize the negative impacts of cyber-attacks. However, it is important that all airports around the world apply the policies and best practices in order to shield their infrastructure systems and networks for the safety of aircrafts, passengers and employees. In addition, airport and aircraft personnel should be trained on best practices in order to mitigate cyber risks and contribute to the successful implementation of security policies. By the same token, it is necessary for passengers and other aviation actors such as third party companies that provide services to aviation companies and airports to apply cyber security practices and conform to policies and regulations. Cyber security is of paramount importance, not only for airports and aircrafts, but also for nations worldwide. A successful cyber-attack could

have a tremendous impact on country's economy, social conditions and its cooperation with other countries and organizations around the world. Therefore, the existence of a common line of action for all aviation actors worldwide is highly recommended. Finally, cooperation with the other transport modes (rail, road, and sea-transportation) to develop common policies and regulations in addition to the existing ones would result in an integrated approach of cyber security issues.

Further research needs to be carried out regarding the impact of the Internet of Things (IoT) and the use of Artificial Intelligence (A.I.) as cyber security measures. In addition, the rapidly evolving nature of cyber threats, as well as the variety of the negative impacts and the aviation actors affected by them, demand a more thorough examination of the diverse ways cyber-attacks could disrupt the operation of aircrafts and airports. Finally, a major factor related to cyber security is human intervention. The alternative ways employers, employees and passengers can contribute to the prevention and mitigation or the expansion of cyber threats and risks have to be assessed and analyzed. Such scrutiny could offer better knowledge of the sources of cyber-attacks and how those sources can be restricted if not completely eliminated.

10. REFERENCES

- About CANSO.* (n.d.). Last access date May 15, 2019, CANSO: CIVIL AIR NAVIGATION SERVICES ORGANIZATION: <https://www.canso.org/about-canso>
- ABOUT: DISCOVER SESAR.* (n.d.). Last access date May 15, 2019, SESAR: JOINT UNDERTAKING: <https://www.sesarju.eu/discover-sesar>
- About ENISA.* (n.d.). Last access date May 15, 2019, ENISA: European Union Agency for Network and Information Security: <https://www.enisa.europa.eu/about-enisa>
- About ICAO.* (n.d.). Last access date May 15, 2019, ICAO UNITING AVIATION: A UNITED NATIONS SPECIALIZED AGENCY: <https://www.icao.int/about-icao/Pages/default.aspx>
- ABOUT SESAR'S VISION.* (n.d.). Last access date May 15, 2019, SESAR: JOINT UNDERTAKING: <https://www.sesarju.eu/vision>
- About SITA: Who we are.* (n.d.). Last access date May 15, 2019, SITA: <https://www.sita.aero/about-us/who-we-are>
- About us: Aviation Isac.* (n.d.). Last access date May 15, 2019, AVIATION ISAC: Aviation Information Sharing & Analysis Center: <https://www.a-isac.com/aboutus>
- ABOUT US: EMSA.* (n.d.). Last access date May 15, 2019, EMSA: <http://www.emsa.europa.eu/about.html>
- About us: IATA.* (n.d.). Last access date May 15, 2019, IATA: <https://www.iata.org/about/pages/index.aspx>
- About Us: ICCAIA.* (n.d.). Last access date May 15, 2019, International Coordinating Council of Aerospace Industries Associations: <http://www.iccaia.org/about-us/>
- Airbus and SITA Join Forces to provide Advanced Cybersecurity Services for Air Transport Industry.* (n.d.). Last access date May 15, 2019, AIRBUS CYBERSECURITY: <https://airbus-cyber-security.com/news/airbus-and-sita-join-forces-to-provide-advanced-cybersecurity-services-for-air-transport-industry/>
- Airline partners and global alliances.* (n.d.). Last access date May 15, 2019, UNITED AIRLINES : <https://www.united.com/CMS/en-US/Marketing/CustComm/Promotions/Pages/AirlinePartners.aspx>

- AIRPORTS COUNCIL INTERNATIONAL. (2018). *ACI PRODUCTS: ACI World Corporate*. Last access date May 15, 2019, ACI: AIRPORTS COUNCIL INTERNATIONAL: <https://store.aci.aero/product-category/aci-world-corporate/>
- AIRPORTS COUNCIL INTERNATIONAL. (n.d.). *Smart Security: ACI*. Last access date May 15, 2019, ACI: AIRPORTS COUNCIL INTERNATIONAL: <https://aci.aero/about-aci/priorities/security/smart-security/>
- AIRPORTS COUNCIL INTERNATIONAL. (2016, June). *Smart Security Guidance Documents: ACI*. Last access date May 15, 2019, ACI: AIRPORTS COUNCIL INTERNATIONAL: <https://aci.aero/about-aci/priorities/security/smart-security/smart-security-guidance-documents/>
- AIRWAYS. (2018, April 3). *CYBERSECURITY RISKS WITHIN THE AIRLINE INDUSTRY: Airways Magazine*. Last access date May 15, 2019, Airways Magazine: <https://airwaysmag.com/tech/cybersecurity-risks-within-the-airline-industry/>
- ASD at a Glance*. (n.d.). Last access date May 15, 2019, ASD: <https://www.asd-europe.org/about-us/asd-at-a-glance>
- Boyson, S. (2014, July). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*(34), σσ. 342-353.
- Broderick, S. (2016, March 25). *Inside MRO*. Last access date May 15, 2019, MRO Network.com: <https://www.mro-network.com/maintenance-repair-overhaul/aviation-taking-systems-approach-cybersecurity-threats>
- Can we help you?: EASA*. (n.d.). Last access date May 15, 2019, EASA: European Union Aviation Safety Agency: <https://www.easa.europa.eu/can-we-help-you>
- Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., και συν. (2015, October 13). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*(56), σσ. 1-27.
- CIVIL AVIATION CYBERSECURITY INFORMATION REPOSITORY: ICAO* . (n.d.). Last access date May 15, 2019, ICAO UNITING AVIATION: A UNITED NATIONS SPECIALIZED AGENCY: <https://www.icao.int/cybersecurity/Pages/default.aspx>
- Community Manager, A. (2018, February 5). *Cyber Security in the Aviation Industry*. Last access date May 15, 2019, APVERA: <https://www.apvera.com/2018/02/05/cyber-security-in-the-aviation-industry/>
- Contact CANSO*. (n.d.). Last access date May 15, 2019, CANSO: CIVIL AIR NAVIGATION SERVICES ORGANIZATION: <https://www.canso.org/contact>

- Contact Us: ACI.* (n.d.). Last access date May 15, 2019, ACI: AIRPORTS COUNCIL INTERNATIONAL: <https://aci.aero/about-aci/contact-information/>
- Contact Us: ICAO.* (n.d.). Last access date May 15, 2019, ICAO UNITING AVIATION: A UNITED NATIONS SPECIALIZED AGENCY: https://www.icao.int/Pages/Contact_us.aspx
- Contact us: ICCAIA.* (n.d.). Last access date May 15, 2019, International Coordinating Council of Aerospace Industries Associations: <http://www.iccaia.org/contact-us/>
- Contact Us: Ponemon Institute.* (n.d.). Last access date May 15, 2019, PONEMON INSTITUTE: <https://www.ponemon.org/contact-information>
- Cyber Safety and Security: ICAO.* (n.d.). Last access date May 15, 2019, ICAO UNITING AVIATION: A UNITED NATIONS SPECIALIZED AGENCY: <https://www.icao.int/annual-report-2017/Pages/new-emerging-activities-cyber-safety-and-security.aspx>
- Davies, H. (2016, July 5). *VIEPOINT: MRO Network*. Last access date May 15, 2019, MRO Network.com: <https://www.mro-network.com/emerging-technology/airlines-look-invest-cyber-security>
- De Cerchio, R., & Riley, C. (2011, December 8). *Aircraft systems cyber security*. Last access date May 15, 2019, IEEE Xplore Digital Library: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6095969>
- Duchamp, H., Bayram, I., & Korhani, R. (2017, January 24). Cyber-Security, a new challenge for the aviation and automotive industries. *Journal of Strategic Threat Intelligence*.
- EASA by Country.* (n.d.). Last access date May 15, 2019, EASA: European Union Aviation Safety Agency : https://www.easa.europa.eu/easa-and-you/international-cooperation/easa-by-country?easa_relationship%5B%5D=field_easa_country_mbmo_target_id
- EASA: European Union Aviation Safety Agency. (2017, June 1). *Annual Safety Review 2017: EASA*. Last access date May 15, 2019, EASA: European Union Aviation Safety Agency: <https://www.easa.europa.eu/document-library/general-publications/annual-safety-review-2017>
- ERA Headquarters.* (n.d.). Last access date May 15, 2019, EUROPEAN UNION AGENCY FOR RAILWAYS: https://www.era.europa.eu/can-we-help-you/offices_en
- F-Secure Corporation. (n.d.). *Aviation: F-Secure Corporation*. Last access date May 15, 2019, F-Secure Corporation: https://www.f-secure.com/en/web/business_global/aviation

- Gohil, S. (2018, May 15). *Cyber Risks Rise at Airports*. Last access date May 15, 2019, Computer Business Review CBR: <https://www.cbronline.com/news/airport-cybersecurity-risks>
- Gopalakrishnan, K., Govindarasu, M., Jacobson, D., & Phares, B. M. (2013, August 19). CYBER SECURITY FOR AIRPORTS. *International Journal for Traffic and Transport Engineering*(3), σσ. 365-376.
- Gunes, V., Peter, S., Givargis, T., & Vahid, F. (2014, December 31). A Survey on Concepts, Applications, and Challenges in Cyber-Physical Systems. *KSII Transactions on Internet and Information Systems*(12), σσ. 4242-4268.
- Hollinger, P. (2018, October 17). *Cyber Security: Financial Times*. Last access date May 15, 2019, FINANCIAL TIMES: <https://www.ft.com/content/2e416eca-4e3d-11e8-ac41-759eee1efb74>
- IATA Office Addresses*. (n.d.). Last access date May 15, 2019, IATA: <https://www.iata.org/about/Pages/offices.aspx>
- Implementation: ICAO*. (n.d.). Last access date May 15, 2019, ICAO UNITING AVIATION: A UNITED NATIONS SPECIALIZED AGENCY: <https://www.icao.int/annual-report-2017/Pages/global-priorities-all-strategic-objectives-nclb-initiatives-implementation.aspx>
- INTERNATIONAL AIRPORT REVIEW. (2018, May 16). *Airports are ill-equipped to deal with a major cyber attack, says consultancy firm*. Last access date May 15, 2019, INTERNATIONAL AIRPORT REVIEW: <https://www.internationalairportreview.com/news/69301/airports-ill-equipped-cyber-attack/>
- International Air Transport Association (IATA). (2018, June). *IATA Publications: Annual Review*. Last access date May 15, 2019, IATA.org: <https://www.iata.org/publications/Pages/annual-review.aspx>
- Lambropoulos, P. (2018, November 27). *Documents: ICAO*. Last access date May 15, 2019, ICAO UNITING AVIATION: A UNITED NATIONS SPECIALIZED AGENCY: <https://www.icao.int/cybersecurity/Documents/Forms/AllItems.aspx>
- Li, L. (2016, June 14). *Documents WP: ICAO*. Last access date May 15, 2019, ICAO UNITING AVIATION: A UNITED NATIONS SPECIALIZED AGENCY: <https://www.icao.int/Meetings/a39/Documents/Forms/AllItems.aspx?RootFolder=%2fMeetings%2fa39%2fDocuments%2fWP&FolderCTID=0x01200042E756C43B81FD4BB950BFE50E166FC9>
- Li, L. (2016, November 21). *Site Assets ICAO*. Last access date May 15, 2019, ICAO UNITING AVIATION: A UNITED NATIONS SPECIALIZED AGENCY:

<https://www.icao.int/cybersecurity/SiteAssets/Forms/AllItems.aspx?RootFolder=%2fcybersecurity%2fSiteAssets%2fICAO&FolderCTID=0x012000072A3EC94A77484D9231948AC644496A>

LOT Polish Airlines. (n.d.). Last access date May 15, 2019, STAR ALLIANCE:
<https://www.staralliance.com/en/member-airline-details?airlineCode=LO>

LOUKIL, A. (2017, November 7-8). *Joint ACAC/ICAO MID Workshop on GNSS*. Last access date May 15, 2019, ICAO UNITING AVIATION: A UNITED NATIONS SPECIALIAZED AGENCY:
<https://www.icao.int/MID/Pages/2017/GNSS-Wksp.aspx>

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018, Nonvember 15). *Implementing Cyber-Security Measures in Airports to Improve Cyber-Resilience*. Last access date May 15, 2019, IEEE Xplore Digital Library:
<https://ieeexplore.ieee.org/abstract/document/8534523>

Malaysia Aviation Group. (n.d.). Last access date May 15, 2019, Malaysia Airlines:
<https://www.malaysiaairlines.com/hq/en/about-us/malaysia-aviation-group.html>

Mission, vision and values: ERA. (n.d.). Last access date May 15, 2019, EUROPEAN UNION AGENCY FOR RAILWAYS:
https://www.era.europa.eu/agency/mission-vision-and-values_en

National Safe Skies Alliance, Inc. (2018, January). *PARAS: REPORTS*. Last access date May 15, 2019, SAFE SKIES: <https://www.sskies.org/paras/reports/>

Our areas of expertise: Eurocontrol. (n.d.). Last access date May 15, 2019, EUROCONTROL: Supporting European Aviation:
<https://www.eurocontrol.int/articles/our-areas-expertise>

Overview - The Community of Airports: ACI. (n.d.). Last access date May 15, 2019, ACI: AIRPORTS COUNCIL INTERNATIONAL: <https://aci.aero/about-aci/overview/>

Peacock, C. (2018, August 30). *Documents: ICAO SAFETY*. Last access date May 15, 2019, ICAO SAFETY:
https://www.icao.int/safety/Documents/Forms/AllItems.aspx#InplviewHash4ca412bf-35af-4a41-8224-a623a1784b66=Paged%3DTRUE-p_SortBehavior%3D0-p_FileLeafRef%3DICA0%25fSafety%2520Brochure%255fENG%255fp2%252epdf-p_ID%3D1-PageFirstRow%3D31

Ponemon Institute. (n.d.). Last access date May 15, 2019, PONEMON INSTITUTE:
<https://www.ponemon.org/>

- PRESS RELEASE: Transport cybersecurity: Raising the bar by working together.* (2019, January 23). Last access date May 15, 2019, ENISA: European Union Agency for Network and Information Security: <https://www.enisa.europa.eu/news/enisa-news/transport-cybersecurity-raising-the-bar-by-working-together>
- PricewaterhouseCoopers. (2016). *Publications PWC*. Last access date May 15, 2019, PWC Global: <https://www.pwc.com/gx/en/industries/transportation-logistics/publications.html>
- PricewaterhouseCoopers. (2016). *Publications: PWC*. Last access date May 15, 2019, PWC Global: <https://www.pwc.com/gx/en/industries/transportation-logistics/publications.html>
- PricewaterhouseCoopers. (2016). *Publications: PWC*. Last access date May 15, 2019, PWC Global: <https://www.pwc.com/us/en/industries/industrial-products/library.html>
- PricewaterhouseCoopers. (2016). *Publications: PWC*. Last access date May 15, 2019, PEC Global: <https://www.pwc.com/gx/en/industries/transportation-logistics/publications.html>
- Security: ICAO.* (n.d.). Last access date May 15, 2019, ICAO UNITING AVIATION: A UNITED NATIONS SPECIALIZED AGENCY: <https://www.icao.int/annual-report-2017/Pages/progress-on-icaos-strategic-objectives-security-and-facilitation-security.aspx>
- SITA. (2018, December 13). *2018 CSEC*. Last access date May 15, 2019, ICAO UNITING AVIATION: A UNITED NATIONS SPECIALIZED AGENCY: <https://www.icao.int/NACC/Documents/Forms/AllItems.aspx?RootFolder=%2fNACC%2fDocuments%2fMeetings%2f2018%2fCSEC&FolderCTID=0x012000B49EFC07D0A49E4F85BA4F7EC2FC2B62>
- Strohmeier, M., Schafer, M., Smith, M., Lenders, V., & Martinovic, I. (2016, August 4). *Assessing the impact of aviation security on cyber power*. Last access date May 15, 2019, IEEE Xplore Digital Library: <https://ieeexplore.ieee.org/document/7529437>
- The Agency: EASA.* (n.d.). Last access date May 15, 2019, EASA: European Union Aviation Safety Agency: <https://www.easa.europa.eu/the-agency/the-agency>
- THE AGENCY: EUROPEAN UNION AGENCY FOR RAILWAYS.* (n.d.). Last access date May 15, 2019, EUROPEAN UNION AGENCY FOR RAILWAYS: <https://www.era.europa.eu/>
- THE AVIATION ISAC .* (n.d.). Last access date May 15, 2019, AVIATION ISAC: Aviation Information Sharing & Analysis Center: <https://www.a-isac.com/>

UNITED STATES SECURITIES AND EXCHANGE COMMISSION. (2019, February 28). *Investor Relations*. Last access date May 15, 2019, UNITED AIRLINES: <http://ir.united.com/>

What is Cyber Security? (n.d.). Last access date May 15, 2019, it governance: <https://www.itgovernance.co.uk/what-is-cybersecurity>

What Is Phishing? (n.d.). Last access date May 15, 2019, PHISHING.org: <http://www.phishing.org/what-is-phishing>

White, B. G. (2011, December 19). *The community cyber security maturity model*. Last access date May 15, 2019, IEEE Xplore Digital Library: <https://ieeexplore.ieee.org/document/6107866/?part=1>

Who we are: Eurocontrol. (n.d.). Last access date May 15, 2019, EUROCONTROL: Supporting European Aviation: <https://www.eurocontrol.int/articles/who-we-are>

