УДК 629.7:061.5:[005.334:004 УДК 355.02:004:[629.7:061.5

NEW CYBERSECURITY CHALLENGES IN AVIATION INDUSTRY

Tomislav Tuntev[1]
Civil Aviation Agency of North Macedonia

Gjorgji Alceski[2]
TAV Macedonia Airport St. Paul the Apostle Ohrid

Abstract: The increased usage of Information and Communication Technology (ICT) tools into the mechanical devices in manner of normal everyday use within the aviation industry raised the concerns about cybersecurity. The extent of common flaws and vulnerabilities in the software tools that power these systems grows as their level of integration increases. Moreover, these concerns are becoming even more acute as the implementation of modern electronic smart devices on aircraft and airports in the aviation industry is increasing. The data on cyber-attacks and threats to air traffic security over the past twenty years can help identify, map and analyze trends and insights that are important to maintaining the security and resilience of aviation systems. The main objective is to identify the subjects of the common threat, their motivations, types of attacks and mapping the vulnerabilities of those elements of the aviation critical infrastructure, which are most often the subject of constant attack campaigns. Such analyzes should enable improved understanding both the current and potential future challenges to cybersecurity protection in the aviation sector. The main threats to the industry come from Advance Persistent Threat (APT) groups, which in cooperation with certain criminal structures and state intelligence institutions, steal intellectual property data in order to advance their own national aviation capabilities, as well as to monitor, to infiltrate and undermine the capabilities of other sovereign nations. The most commonly attacked segment of the aviation industry is the information technology (IT) infrastructure, while the most prominent type of attack is malicious hacking with the intention of gaining unauthorized access to confidential and sensitive information. Analysis of the range of attacked platforms and existing threat dynamics is used as a basis for predicting future cyber-attacks trends. Insights arising from the review should support future definition and implementation of proactive measures that protect aviation critical infrastructures from cyber-incidents that erode customer confidence in a key service-oriented industry.

Keywords: aviation industry; cybersecurity; cyber-threats; cyber-attacks; cyber-incidents; information and communication technology.

Introduction

Over recent years we have witnessed important attacks on large corporations, critical infrastructures of all kinds, governments and small and medium-sized enterprises with varying

[1] Contact address: tomislav.tuntev@tav.aero

[2] Contact address: Gjorgji.Alcheski@tav.aero

levels of sophistication and varied severity in their impact. As we might expect, the aviation industry is no exception to this. However, there is a big difference with other industries such as financial services, insurance or e-commerce to name just a few. In transportation and especially in aviation there is a key issue of life safety. The constant trend of increasing the levels of integration of information and communication technology tools in mechanical devices in everyday use within the aviation industry has raised concerns about the resilience of current cybersecurity protective frames. Thus, considering the needs of the sector in terms of cybersecurity compliance emerges as another challenge in the evolution of aviation industry, through the adoption of smart airports and e-enabled aircraft infrastructures. The aerospace industry has a strategic global position as a gateway between nations. The resilience of infrastructures to support its operational integrity is vitally important as a lower errors or oversights result in a range of significant damages and losses, e.g., deaths, loss or exposure of personally identifiable information to stakeholders, staff and customers; credential theft, intellectual property and intelligence. A cyber-attack, if successful, could end up with the loss of numerous lives - resulting in total disaster. In addition, aviation and aerospace systems must support real-time behavior and require ultra-high reliability. Many of these systems are critical to security and require strong certification and rigorous cybersecurity controls. As a consequence, software verification represents an important cost, and certification is not a quick process. There is clear evidence that major threat actors cooperate with state actors to acquire intellectual property and intelligence in order to advance their domestic airspace capabilities, as well as to monitor, infiltrate and suppress the capabilities of other nations. Therefore, there is an industry imperative to define and implement proportionate cyber-defenses strategies that protect against malicious threats that threaten the operational integrity of a key industry. The ultimate objective is to support the security and resilience of civil aviation against cyber-threats and risks.

1. Major challenges for the civil aviation industry

The aviation industry relies on a very complex infrastructure integrated into multiple systems that need to be individually and holistically protected. A thorough cyber assessment is needed that will involve aircraft and equipment manufacturers, air traffic control, airports, airlines and all other elements of the aviation infrastructure such as information systems. This should include penetration testing or red teaming where cyber experts try to gain access to systems, as well as vulnerability testing to look for security gaps. Another very important element to consider is the "insider" threat. Reports indicate that the "insider" threat is on the rise, requiring employees to educate themselves about their role in mitigating such threats and adhere to cybersecurity policies and best practices. Processes and books should be periodically reevaluated and rigorously tested to ensure continuous improvement. Additionally, access controls should be in place to allow only people who absolutely need clearance to specific areas of the airport or aircraft.

Over the last two decades, the introduction of e-enabled or digital aircraft and widespread connectivity have increased the operational efficiency of airlines. However, this also includes increased interaction with many information systems that are outside the traditionally defined security perimeter. Moreover, traditionally, one line of defense in aviation has been the rather specific knowledge required by an attacker or cybercriminal due to the

use of aviation-specific software and hardware that was unavailable to the general public. A lot of incidents were identified compromising various aviation organizations, with stolen data types ranging from budget information, business communications, equipment maintenance records and specifications. Other data includes organizational charts and company directories, personally identifiable information, product designs, product blueprints, manufacturing processes and commercial information about products or services, research reports, security procedures, system log files and test results and reports, potentially enabling a spectrum of harmful consequences.

The threat actors could be categorized according to their motivations: cyber-criminals, whose activities are responsible for more than 450 billion dollars in annual loss of the global economy; cyber-activists or "hacktivists", whose concern is philosophy, politics and non-monetary goals of the discipline; cyber-spies, motivated by financial, industrial, political and diplomatic espionage; and cyber-terrorists, driven by political, religious, ideological or social violence. Cyber-attackers supported by a nation state, in order to prosper the strategic objectives in the future, are classified as cyber-warriors. The threat actors are motivated by the ability to cause business disruption and theft of information about political as well as financial benefits. Recent reports reinforce the likelihood of a significant rise in cyber-threats such as global passenger volumes are increasing, and embedded systems are being deployed in response in order to maintain the quality of services. The integration of hardware and software, to increase the efficiency of operations through advanced levels of automation, represents a larger attack surface, further stimulating the motivation of threat actors. Therefore, it is timely to highlight the significant challenges facing the civil aviation industry in ensuring cybersecurity, as the number and classes of cyber-threats increase. The growing level of cyber-threats have to be urgently treated through research and innovation in proactive approaches within cybersecurity through design tools that mitigate the risks and deterrence of malicious activities.

2. Critical elements within the civil aviation industry

Important changes in recent years have created significant challenges today:

- Increasing the use of proprietary software and solutions that do not require specific aviation knowledge to attack;
- Smart aircraft with Flight By Wire (FBW) capabilities;
- Multiple interconnected systems: the security of the interoperability of all these systems should be tested from a red pooling perspective;
- The airplane of the future is heading towards software updated in flight, which also creates important additional challenges;
- Bring Your Own Device (BYOD) into the cockpit;
- Certification of aircraft is becoming more complex and it is likely that the strategy of issuing "special conditions" to harden systems that could be at risk may not be sufficient as they do not cover either the entire interoperability of the systems or its adaptability;
- The modernization of air traffic control and management systems:
  - Next-Generation Air Transportation System (NextGen), is a modernization of the US air transportation system led by the FAA, which requires information

systems to be networked with IP technology into a comprehensive system of interoperable subsystems;
- Single European Sky ATM Research (SESAR) project, is the technological backbone of the Single European Sky and aims to improve the performance of Air Traffic Management (ATM) by modernizing and harmonizing ATM systems.

These upgrades make sense from a management, communications and modernization point of view, but it also opens up air transport to unforeseen vulnerabilities. As the new functionality is added, also an attack vectors are added that need to be properly analyzed. But there are other factors that pose serious risks to the aviation industry:

- Lack of budget resources for example in small airports or developing countries;
- Existence of multiple regulations: this makes it difficult to adapt to the speed of new regulations in the rapidly evolving threat landscape;
- Multiple stakeholders: there are countless stakeholders in the mix and data constantly flows back and forth between numerous internal and external systems;
- Complex business relationships and important geopolitics at play.[3]

The introduction of "connected aircraft" and "smart airport" concept brings new vulnerabilities to the table. The key elements vulnerable to attack from a system-wide perspective are:

- Access, departure and passport control systems;
- Cargo and transportation management;
- Reservation systems;
- Fuel gauges;
- Management of the transport of hazardous materials;
- Inflight entertainment and connectivity systems;
- E-enabled ground and board systems;
- Electronic Flight Bags (EFB) - an electronic information management device that helps flight crews perform flight management tasks easily and efficiently;
- Cabin crew devices;
- Flight traffic management systems: primary and secondary radar, Automatic Dependent Tracking Broadcast (ADTB), Global Navigation Satellite System (GNSS), including GPS, GLONASS, GALILEO, BEIDOU and some other regional satellite systems IRNSS (India), Zenith (Japan) and Compass (China);
- Aircraft Information Management System (AIMS), including, but not limited to, Flight Management System, Thrust Management System, Data Link Management (Datalink) / Aircraft Communications Addressing and Reporting System (ACARS), Maintaining and Acquiring Flight Data Central System, etc.[4]
-

[3] Jose Monteagudo, Founder & Chief Analyst, Cyber Startup Observatory - Aviation Cyber Security – High Level Analysis, Major Challenges and Where the Industry is Heading - https://cyberstartupobservatory.com/aviation-cyber-security-major-challenges/

[4] Jose Monteagudo, Founder & Chief Analyst, Cyber Startup Observatory - Aviation Cyber Security – High Level Analysis, Major Challenges and Where the Industry is Heading - https://cyberstartupobservatory.com/aviation-cyber-security-major-challenges/

The stakeholders within the aviation industry are aware of the cyber security challenges and they are working very hard to solve them. In the current climate, with increasing concerns about cyber security in all different areas of our lives, including financial transactions, the internet, personal data and privacy, the aviation industry needs to show leadership and be at the forefront of cyber security.

3. Analysis and critical reviews of cyber-attacks in the civil aviation industry

Data processed in relation to all studied cyber-attacks in civil aviation globally shows that in 71% the attackers focused on stealing login details such as administrative passwords and malicious hacking to gain unauthorized access to IT infrastructure (Figure 1). Denial-of-service attacks, such as Distributed Denial-of-Service (DDoS), which compromise data availability, rank second at 25%. Attacks aimed at corrupting the integrity of files, either by intercepting them while in transit or at rest, are next, accounting for about 4% of the total number of cyber attacks. These data are an indicator that the dominant nature of cyber threats, e.g. the main motivation of cyber attackers, is the theft of intellectual property and intelligence.

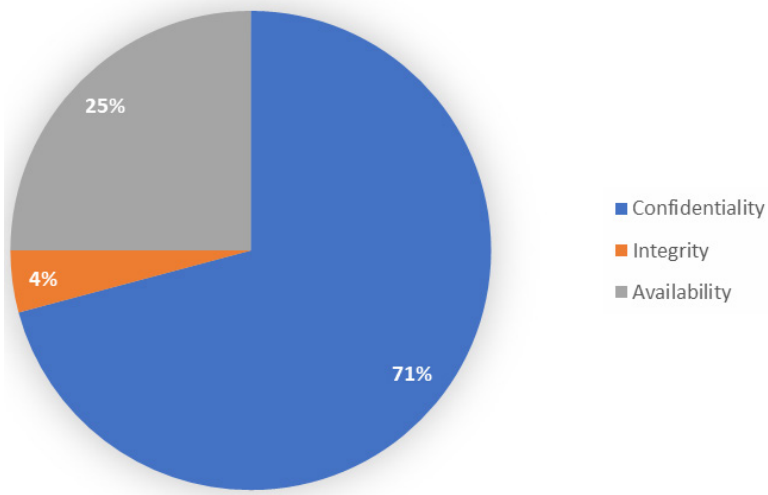

Figure 1. *Cyber-attacks class based on security triad*[5]

The assessment of cyber-attacks by type is presented in Figure 2, the results of which supporting the evidence presented in Figure 1, showing that malicious hacking activities are on the rise the list of types of cyber-attacks of 26%, the goal is to gain unauthorized access using known malicious password cracking techniques, for example, brute force or dictionary attacks. Data breach and ransomware attacks came in second at 14% each, while attacks related to phishing and malware follow at 11% each. Cyber incidents classified as human error, bot attacks, worms and DDoS are the least common, with 4% each.

[5] Elochukwu Ukwandu, Mohamed Amine Ben-Farah, Hanan Hindy, Miroslav Bures, Robert Atkinson, Christos Tachtatzis, Ivan Andonovic, Xavier Bellekens. Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. MDPI, Basel, Switzerland, 2022.- www.mdpi.com/2078-2489/13/3/146

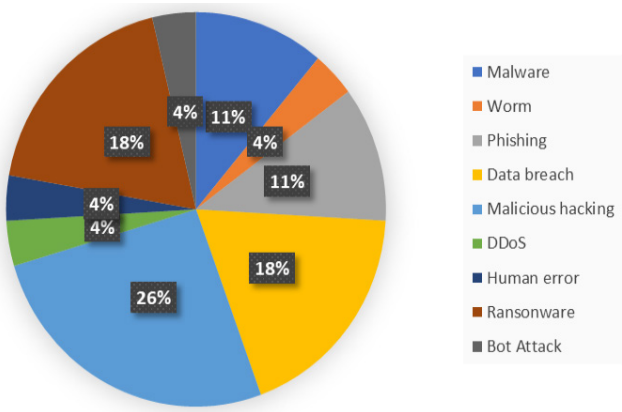

Figure 2. *Cyber-attacks by type*[6]

Figure 3 shows that most cyber-attacks in aviation industry occur in North America, with 11 of the 26 recorded incidents in USA and only 1 in Canada. The relatively high number of incidents in USA is likely related to the large number of airports, as in 2019 there were 5,080 public and 14,556 private airports in USA. Europe is second with an attack rate of 44% of incidents, with Great Britain topping the list of European countries. States in Asia are in third place with 8%, etc. To date, cyber incidents in 2018 remain the most numerous, representing the highest rate of cyber attacks in the history of the aviation industry, with 94,500,000 people affected and more than 5 consecutive days of grounded aircraft. However, the most concerning incident to date was crypto-mining malware, discovered by "Cyberbit" through its Endpoint Detection and Response (EDR) software in 2019. It was about the installation of malware that infected more than 50% of workstations at European airports.

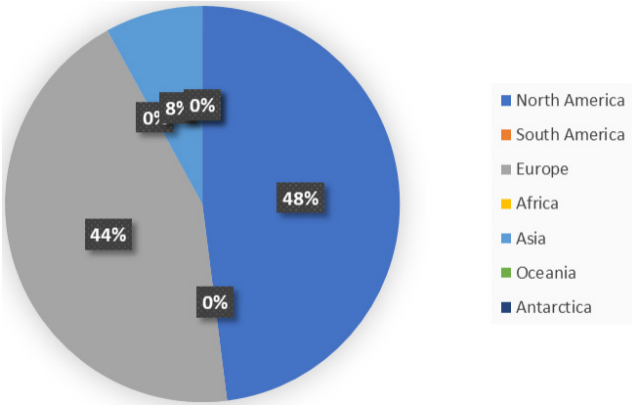

Figure 3. *Cyber-attacks by location*[7]

[6] Elochukwu Ukwandu, Mohamed Amine Ben-Farah, Hanan Hindy, Miroslav Bures, Robert Atkinson, Christos Tachtatzis, Ivan Andonovic, Xavier Bellekens. Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. MDPI, Basel, Switzerland, 2022.- www.mdpi.com/2078-2489/13/3/146

[7] Elochukwu Ukwandu, Mohamed Amine Ben-Farah, Hanan Hindy, Miroslav Bures, Robert Atkinson, Christos Tachtatzis, Ivan Andonovic, Xavier Bellekens. Cyber-Security Challenges in Aviation Indus-

The precise number of losses due to a cybersecurity breach is hampered by the lack of transparency in keeping records, documenting and publishing relevant incidents for public knowledge. The monetary value of the losses paid by the industry due to cyber-crime are never published nor documented, especially the level of compensation to victims of these attacks, as well as those paid as ransom during ransomware attacks. Other records not published are the number of shutdowns suffered by the attacked airports, as well as the number of flight hours lost as a result of cyber-incidents.

Cybersecurity culture in civil aviation industry

Regarding the increasingly frequent cyber-threats in the aviation industry and the growing number of affected operators and users of aviation services from cyber-attacks, the International Civil Aviation Organization (ICAO) in 2022 published guidance material for Cybersecurity Culture in Civil Aviation. This guidance material aims to support member states and stakeholders in designing and implementing a robust cybersecurity culture within their organizations. The ultimate objective is to support the security and resilience of civil aviation against cyber-threats and risks. According to the guidance, cybersecurity culture is commonly understood to be a set of assumptions, attitudes, beliefs, behaviors, norms, perceptions, and values that are inherent in the daily operation of an organization and are reflected by the actions and behaviors of all entities and personnel in their interaction with digital assets. A positive cybersecurity culture aims to make cybersecurity considerations part of the organization's habits, conducts, and processes, by embedding them in daily operations as reflected by the actions and behaviors of all personnel. The establishment of a strong and effective cybersecurity culture, as an integral part of an organizational culture, assists organizations in improving their overall performance through the early identification of potential cyber risks. Cybersecurity culture in civil aviation builds upon the sector's experience, efforts, and success in implementing robust aviation safety and security cultures, and shares with them many core elements. This cross-domain nature of cybersecurity culture not only leads to enhancing cybersecurity posture, but also results in positive spillovers across the three domains in supporting the promotion and reinforcement of positive safety, security and cybersecurity cultures.

In summary, cybersecurity culture allows every person in the organization, regardless of their role, to better perform in the digital environment. Examples of benefits of designing and implementing an effective and robust cybersecurity culture include:

- enhanced cybersecurity maturity of the organization;
- appropriate handling of information by all personnel;
- improved cybersecurity posture that supports the effectiveness and efficiency of the organization in mitigating cyber risks;
- enhanced awareness of all personnel to cyber risks and the role that they individually play in identifying and mitigating those risks; and

try: A Review of Current and Future Trends. MDPI, Basel, Switzerland, 2022.- www.mdpi.com/2078-2489/13/3/146

- willingness to report personal oversight in applying organizational cybersecurity processes and procedures as well as reporting of suspicious cyber-activities, leading to pro-activeness and better detection of cyber-risks.[8]

The core elements of an effective organizational aviation cybersecurity culture are illustrated in the guidance material. However, although these core elements are well defined, cybersecurity culture should be uniquely designed within each organization. It should take into account different aspects, including the organizational cybersecurity maturity level, existing cultures and values, and the overall cybersecurity threat landscape. The core elements of a robust and effective cybersecurity culture in civil aviation are:

- leadership;
- cross-domain links;
- communication;
- awareness, training and education;
- reporting systems;
- continuous review and improvement; and
- positive work environment.[9]

As for leadership, an effective cybersecurity culture depends on the commitment of every person in the organization, starting with senior management. Senior management should provide their full commitment to cybersecurity culture, at all times and across all activities, strategies, policies and organizational objectives. Senior management should comply with cybersecurity policies, led by example, and become role models for the organization's managers and personnel. They should also advocate for cybersecurity as an organizational and personal value while similarly working towards aligning their behaviors with such value.

As for constructing strong and efficient cross-domain links, a multidisciplinary task force reporting to senior management might be established as a means to support coordination of cybersecurity culture across the organization. The task force's objectives would include periodically assess the maturity of cybersecurity culture within the organization, identify risks and opportunities with regards to cybersecurity culture implementation, bridge the perspectives of different internal stakeholders with regards to cybersecurity culture and support the development and implementation of cross-domain activities related to fostering cybersecurity culture in the organization.

Senior management should ensure that internal policies and guidelines regarding cybersecurity, as well as the reason for their introduction, are duly communicated to all personnel. A robust internal communication program contributes to the acceptance and understanding of cybersecurity measures by all personnel, and helps promote cybersecurity culture in the organization. In order for communication to be effective, certain skills should be considered as part of a robust cybersecurity culture:

- Active listening – process through which verbal and non-verbal signals are observed, in order to recognize the other individual's values and needs, and contribute to the improvement of team communication;

[8] ICAO – International Civil Aviation Organization. Cybersecurity Culture in Civil Aviation. ICAO, Montreal, Canada, 2022. P. 1

[9] ICAO – International Civil Aviation Organization. Cybersecurity Culture in Civil Aviation. ICAO, Montreal, Canada, 2022. P. 2

- Adapting communication style to different audiences and situations – understanding how others communicate and customizing the message in order to better reach them; and
- Clarity of communication – identify what and how to communicate.

Awareness, training and education are key areas of the learning process that should be leveraged for a robust cybersecurity culture. Awareness provides people with knowledge, training teaches skills, and education provides knowledge and skills within a theoretical framework, hence integrating awareness and training. All civil aviation personnel who interact with the organization's digital assets, regardless of their roles or functions, should undertake a cybersecurity awareness, training, and education program in order to ensure that they are equipped with required knowledge and skills on aviation cybersecurity risks, measures and objectives. These programs should be adapted to the audience, as necessary and possible. Furthermore, the cybersecurity awareness programs should be delivered to all personnel upon their hiring, as well as a recurrent training. Cybersecurity awareness programs should be delivered by professionals that possess the required technical knowledge.

A cornerstone of cybersecurity culture is the development and implementation of an internal cybersecurity reporting system. Such system allows the organization to proactively manage its cyber-risks, measure the development of the organization's cybersecurity posture, identify and plan awareness and training needs of staff, and adapt its internal processes, controls, and measures in line with the development of cybersecurity trends and with the maturity of cybersecurity culture.

Cybersecurity reporting systems gather elements from both aviation safety and aviation security reporting systems. As such, they address two areas: the first area is reporting of self-actions/errors that are not in line with the organizational information security policies and processes, and the second area is reporting of suspicious/erroneous behavior of other employees. When developing their cybersecurity reporting mechanism, organizations are encouraged to benefit from the experience gained in developing and implementing aviation safety and aviation security reporting systems.

Organizations should encourage their personnel to report cybersecurity incidents through the adoption of a just culture. Just culture is a concept implemented in safety reporting which could be of great value in promoting a cybersecurity culture. In a cybersecurity reporting context, a just culture encourages all personnel to report cybersecurity incidents and errors. It is an environment where everyone understands that they will be treated fairly based on their actions rather than the outcome of their actions. In a just culture environment, all personnel clearly understand that it is not fair to punish all errors regardless of their circumstances, while at the same time they also understand that it is unacceptable to provide a blanket immunity from punishment as some actions could have malicious intent, or could be the result of pure negligence and/or nonchalance. As such, it is important to draw the line between acceptable and unacceptable actions when designing a just culture.

Organizations should implement quality control programs designed to monitor the effective implementation of cybersecurity measures. Quality control programs can be an effective tool in keeping personnel alert and committed to cybersecurity culture principles. The frequency and rigidity with which quality controls are carried out may have a positive influence on personnel by demonstrating management's commitment to cybersecurity objectives and

compliance. Regular quality controls of the reporting mechanisms in place should be carried out as part of the quality control programs.

Organizations should develop a performance indicator framework designed to assess the impact of measures in place on cybersecurity culture as well as to determine the gap existing between desired and actual culture outcomes. As some elements of cybersecurity culture may not be directly observed, a range of possible indicators can be used to measure the effectiveness of cybersecurity culture. Such measures may include: statistics on reported incidents to measure cybersecurity performance of personnel, their level of awareness, and the progress achieved in promoting cybersecurity reporting, then results of recurrent training sessions, results from simulations of malicious attacks to test response of personnel and questionnaires or interviews.

Finally, a general positive work environment may also greatly influence commitment of personnel to cybersecurity culture and enhance cybersecurity performance. A positive work environment should include: the involvement of personnel in decision-making processes; the allocation of sufficient time for personnel to complete training on proper cyber hygiene; a mechanism for recognizing good performance, the provision of feedback to personnel on suggestions and on cybersecurity reports, setting clear, achievable and measurable goals with regards to cybersecurity incidents, and periodic feedback to personnel on how the organization is advancing in that regard; the provision of the necessary procedures, awareness, training, and tools to enable personnel to perform their duties; and providing personnel with the appropriate levels of autonomy and responsibility.

Conclusions

The field of aviation security is very fast changing continuously and becoming more challenging with new frontiers of cyber-crime. While many states and stakeholders in the global civil aviation community are aware of the seriousness and catastrophic consequences that can become reality from cyber-threats, many of them are still hesitate and procrastinate with tackling these challenges. Some of them are not necessarily ready or equipped to deal with such threats confronting them, at both the individual level and national system-wide level. However, the use of more advanced and sophisticated IT, AI and computer-based systems in civil aviation operations will continue and expand even more in the future. This will exceed even the most basic functions such as data collection and processing, where heavy reliance on the security of IT systems are critical. The cyber frontier is massive and there are numerous ways that terrorists and malicious persons can use to conduct a cyber-attack on civil aviation services providers and critical infrastructure. Therefore, it is crucial that all states, ICAO and other international organizations and associations, and all civil aviation stakeholders, work together to raise the level of awareness and recognition of the cyber security threats and cyber-crime.

The main cyber-threat to the industry stem from APT groups, in collaboration with state actors, the goal being to acquire intellectual property and intelligence in order to advance domestic aerospace capabilities as well as monitor, infiltrate and subvert other nations' capabilities. As is the obligation of any industry, the aviation sector continues to strive to improve the quality of services provided and enhance customer experience. The higher levels of integration and connectivity spawn a spectrum of new cyber-attack surfaces and, given the ability of attackers to automate attack processes through AI, there is an immediate need to develop holistic cybersecurity strategies to protect the cyber-integrity of the emerging "smart

airport" and e-enabled aircraft systems. Otherwise, there exists a great likelihood that APT groups could advance beyond attacking airport facilities only to breach on-board and in-flight aircraft by using sophisticated remote attack tools with severe concomitant damages and loss of life.

The combination of digital transformation, connectivity, segmentation and complexity currently experienced in the industry due to the surge in global travel will continue to pose challenges in terms of cybersecurity. The increased levels of integration and automation to meet the needs of the business exposes the sector by presenting new opportunities for cyber-attacks. No doubt, evolution will improve the quality of the services provided and the improvement of the customer experience, but at the expense of exposing new attack surfaces to cyber threat actors, which will stimulate proliferation in the number of cyber-attacks. In this context, the difficulty of providing accurate information with a sufficient volume of the nature and magnitude of cyber-incidents in the industry remains an open challenge which hinders innovation. There are a lot of challenges in developing fit-for-purpose solutions which support the evolution of the aviation sector. The cybersecurity solutions should address the major threats to operational integrity of the aviation industry. Innovating a proactive protection measures of aviation infrastructures, based on cybersecurity culture ICAO recommendations, characterized by increased levels of automation and, in turn, creating additional attack surfaces, presents a rich storage of opportunities for the future.

References

- *ICAO – International Civil Aviation Organization*. Security and Facilitation Strategic Objective: Aviation Cybersecurity Strategy. ICAO, Montreal, Canada, 2019.
- *ICAO – International Civil Aviation Organization*. Cybersecurity Culture in Civil Aviation. ICAO, Montreal, Canada, 2022.
- *Jose Monteagudo.* Aviation Cybersecurity – High Level Analysis, Major Challenges and Where the Industry Is Heading. Cyber Startup Observatory, Global Internet Platform, 2020.
- *Elochukwu Ukwandu, Mohamed Amine Ben-Farah, Hanan Hindy, Miroslav Bures, Robert Atkinson, Christos Tachtatzis, Ivan Andonovic, Xavier Bellekens*. Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. MDPI, Basel, Switzerland, 2022.
- *IATA – International Air Transport Association*. Compilation of Cyber Security Regulations, Standards and Guidance Applicable to Civil Aviation. IATA, Montreal, Canada, 2020.
- *Cyber Risk International*. Cyber Threats to the Aviation Industry. Cyber Risk International, Dublin, Ireland, 2020.
- *Pierluigi Paganini.* Cryptocurrency Miners Infected More than 50% of the European Airport Workstations. Cyber Defense Magazine, Cyber Defense Media Group, Washington DC, USA, 2019.