Vol. 12 No. 2 ISSN: 0976-3570

Emerging Trends in Aviation Cyber-Security: Study of European Air Traffic Control (Euro-Control)

Dr. Jitender Loura[1]
Prof. (Dr.) Kanwal DP Singh[2]

Abstract

Civil Aviation is a critical infrastructure. The cyber-attacks on Civil Aviation infrastructure leads to significant impact not only on the safety and security of the airports, airlines and air traffic control units but also on the passengers and staff working at these airports, airlines and air traffic control units. Cyber Security threats in the aviation sector have tremendously increased owing to extensive use of information technology and paucity of appropriate cyber-defence mechanisms and framework. The increase in cyber-attacks in civil aviation are predominantly due to increased use of information technology, higher susceptibility of data, advanced methods and tools of attack, instant and high exposure coupled with increased motivation of attackers. In the following parts, an overview has been given on these very aspects, with a particular focus on recent trends that are present in the aviation industry with special reference to air traffic control. The measures undertaken by Euro Control have also been evaluated. European Union Aviation Safety Agency (EASA) regulates the cyberspace certifications and licensing to keep a check on the technicians and mechanics in aeronautical department. EASA undertakes standardized inspections for monitoring applicability of EU legislations in a uniform manner. EUROCONTROL has been nominated as the Network Manager for Europe and acts as the central unit for managing air traffic flow.

To gain an understanding on the possible threats, the various instances where malware or other attacks have rendered losses or caused problems for the aviation industry have also been discussed.

Keywords: Cyber Security, Civil Aviation, Air Traffic Control, Euro Control

[1] Dy. Director, Directorate General of Civil Aviation (DGCA), Ministry of Civil Aviation, Govt.of India and Research Scholar, USLLS, GGS IP University, Delhi-110078, India. Email: Jloura.dgca@gmail.com

[2] Professor & Former Dean, University School of Law and Legal Studies (USLLS),GGS IP University, Delhi-110078, India. Email: Kanwal.als@gmail.com

I. Introduction

Aviation industry in the modern times has become a very critical and lucrative target for the state sponsored cyber warfare initiatives and for the hackers. The disruption of operations of any airport BAS (Building Automation System) is a matter of few hours, resulting in loss of millions of dollars in airlines and even for the related vendors. In addition to this, the air transport covers highly complicated operations, which arrange and guide a range of critical systems, which includes air fleet management, Airline Operations Centre (AOC) networks, APRON and tarmac operations, surveillance, luggage and goods management and Air Traffic Management (ATM) networks among other things. The complexities of these systems, makes securing them a critical task.

Worldwide, cyber-security has been facing despair over the past decade as compared to past years because of the virtual financial infrastructure that has been created at a fast pace. Furthermore, with the emergence of cyber-physical networks that form the Digital revolution, like "smart" domestic goods, the importance of cyber protection continues to grow every day[3]. In the face of this digital transition, though, the public and private sectors remain unable to keep up with cyber-security challenges. In the news features, it is obvious the sadness of the dominant attitude to cyber-security. Various businesses around the globe surpassed each country in the last years and non-national program-makers are understood.

The research focuses on an overview of various cyber threats and resilience in aviation and particularly in air traffic control. The study specifically underpins the role of Euro Control and other safety agencies in Europe taking care of safety in Air traffic control (ATC) and their raising attention on cyber protection.

II. International Regulatory Measures

ICAO or the International Civil Aviation Organization is the UN professional body that codifies the strategies and values of aerospace around the world. To ensure that global air travel is secure and has orderly progress, ICAO encourages the planning and construction facets of this. It was set up on 04

[3] Sujeet Kumar Sharma, *Internet Banking Adoption in India*, 6 Journal of Indian Business Research (2014).

April 1947 and came into effect. It was accepted, and ratified on 07th day of December 1944 at Chicago, Illinois, the "Convention on international civil aviation[4]." The conference has taken on based on these factors a middle path whereby a new international organization named "ICAO" should be formed. In addition to the general supervision tasks, ICAO was assigned the main duties of professional norm description. The bilateral regulation (agreements), excluding the regulation of prices, tariffs and fares, has been subject to economic regulations. These elements were exempt from multilateral self-regulation according to conferences in the sector, but also subject to government approval. In addition to the tax growth of air travel, the ICAO's key strategic priorities included defence and assistance, environmental conservation, safety (main objective), air navigation capability and quality.

In different facets, this arrangement was manifested. The first was the "Convention of International Civil Aviation" which would have been the Conference's key instrument and formed the structure of the ICAO. The above was protected by the Multinational Air Transit Service deal, which requires transit privileges to be mutually shared. The third was secured by the Five Freedoms Agreement that guarantees that traffic privileges are collectively assumed but that remains a dead text. Finally, the fourth and last one was entered into via the Interim Civil Aviation Agreement, which required the creation of the PICAO, which remained pending entry into force in the key Convention[5].

ICAO has established 19 Annexes to the Convention centred on the Civil Aviation Organization Convention alone, particularly Article 54 thereof (1). This leads to the development and introduction of both the PANS (Air Navigation Services Procedures) and the SARP. In compliance with Article 54(m) and Chapter XX of the Convention, ICAO updates technical annexes if and when appropriate. In Annex 13, aircraft crash analysis is centred and

[4] Ruwantissa Abeyratne, *Aviation Cyber Security: A Constructive Look at the Work of ICAO*, 41 Air and Space Law (2016).
[5] Ruwantissa Abeyratne, *Regulation of Commercial Space Transport.* (2014).

included; in Annex 17, the defence is addressed and in Annex 19, security control systems are dealt with[6].

Currently ICAO, business and national agencies are driving various efforts to defend vital cyber-attack networks. The need for improved comprehension and recognition of the data protection threats in this sector and the need to synchronize aviation cyber readiness internationally and the interest to establish mutual understanding and implementation of risk management practices are both recognized among the local community experts and stakeholders[7]. This group seeks to encourage the creation of a stable and resilient aviation environment that encourages members to share their business expertise and best practices in all essential device segments of the aviation industry.

The more critical thing is the growth of an aviation cyber readiness community in the industry and further is cyber protection personnel. The world community has acknowledged these challenges. In the 2019 ICAO Cyber-security Aviation Plan, capability development and the culture of cyber-security were recognised and discussed, as core components of a successful cyber resilience programme[8]. The ICAO Strategy says that the civil aviation sector is taking tangible action to expand the amount of trained and experienced staff engaged in aviation and cyber protection.

The backbone of European Union aviation safety system is covered under the common safety rules. The new generation aviation safety rules at the first place were adopted in 2002 by the European Union and these rules were based on the Regulation (EC) No 1592/2002[9]. Along with this, European Union Aviation Safety Agency (EASA), the cornerstone of European aviation's safety system, was also established. The maintenance, airworthiness, environmental certification of aeronautical products and licensing and training of technicians and mechanics in aeronautical department was set up through the initial set of

[6] Ewa Dudek, *The Concept of a Method Ensuring Aeronautical Data Quality*, 37 Journal of KONBiN (2016).

[7] Jean Claude Geofrey Mahoro, *ICAO's Role in Environmental Protection and Its Shortcomings Under Rapid Growth of Aviation Industry*, 4 Diponegoro Law Review (2019).

[8] John Macilree, *Aero politics in a Post-Covid-19 World*, 88 Journal of Air Transport Management. (2020).

[9] Regulation (EC), 2002, No. 1592, European Parliament and the Council, 2002 (Europe).

these rules. As a result of Regulation (EC) No 216/2008[10], brought forth in 2008, EASA's common aviation safety rules, and its associated duties were extended by EU to the aircrew training and licensing, and to aircraft operations. The very next year saw the adoption of second extension of such common rules, which clearly covered the provision of air traffic management and air navigation services, and safety aspects of aerodrome operations, through Regulation (EC) No 1108/2009[11]. The European Commission adopts the aviation safety rules based on the technical opinions, which are issued by EASA. The commission is responsible for the proper execution of such rules and EASA provides its assistance in this context, as it undertakes inspections on regular basis for all the member states. Where the detected safety deficiencies are not corrected, enforcement actions can be undertaken. This can also lead to the certificates' mutual recognition being suspended or even imposition of penalties on the certificate holders.

III. Aviation Industry and Cyber-Security

There are numerous attack points for a hacker or cybercriminal and at separate phases i.e. manufacture of the aircraft and its equipment; the Air Navigation Service Provider and the Airport Service Provider. Cybercriminal has a capacity; it does not matter if Governments, entities and businesses do the same thing, to attack the electronic system of organisations. Any electronic device utilized in air traffic control systems, airlines and airports that designs or improves software and hardware may be an aim. Also, cyber terrorism could threaten those sectors which are engaged in the construction of aircraft or its part regardless of the construction for military or civil use. Currently, the aviation sector, which encompasses a gambit of sectors including airports, air traffic control, air fleet management, air transport operations (AOCs), air traffic control, baggage and materials tracking, aircraft manufacturers, Maintenance Repair and Overhaul Organizations (MROs), is a very important and lucrative

[10] Regulation (EC), 2008, No. 216, European Parliament and the Council, 2008. (Europe).
[11] Regulation (EC), 2009, No. 1108, European Parliament and the Council, 2009 (Europe).

target for state-sponsored cyber warfare and hackers[12]. These networks are dynamic and there is a real challenge to protect them.

IV. Rapid Changes in Civil Aviation

Over the past decades, Civil Aviation has changed rapidly, with technological advances and legislative changes that have brought in greater resilience and growth in the aviation industry and business models. Cyber challenges, which threatens both networks and IT infrastructure, threaten the high efficiency of activities, alongside the benefits of the technology, as the worldwide structures are interconnected. To remain ahead of today's world, the organization or company must ensure the identification, prevention, and the implementation of incident management plans and the remedy of any responsibility resulting from any danger vector at an early point[13].

The technological challenges and related cyber-threats, the usage of IoT in operations (such as luggage handling, passenger check-in, landside operational tracking, common-use passenger systems, and traveller network services), and intelligent technologies implemented by smart airports to achieve operational performance. While several airports have comprehensive frameworks in place for mitigating popular cyber challenges, it is important to mitigate cyber protection hazards in terms of a systemic approach to the cyber world, which encompasses both internal and external threats[14].

The CIA (Internal/Sensitive Knowledge and Authentication) trip (Confidentiality-Integrity-Availability) information management trio focused on its relevance for business operations encompasses a large variety of various asset categories (mainly covering contact networks, VoIP systems, server and access control systems). Some properties have critical criteria for secrecy (such as corporate secrets), some may have critical requirements for honesty

[12] Stefan Katzenbeisser, *Envisioning Smart Building Botnets* (2014).
[13] Ravi Kumar Jain, *A DEA Study of Airlines in India*, 20 Asia Pacific Management Review (2015).
[14] Himanshu Gupta, *Evaluating Service Quality of Airline Industry Using Hybrid Best Worst Method and VIKOR*, 68 Journal of Air Transport Management (2018).

dependent on financial activity values, and some have critical requirements for availability (like e-commerce web servers and communication systems)[15].

European Union Agency for Network and Information Security (ENISA) says smart airports use networked, data-driven sensitive capabilities that provide travellers with a more efficient flying experience, and on the other side, seek to maintain a higher degree of protection for passengers, operators and the wide public.

V. Cyber Threats, Impact Evaluation and Resilience Measures

Significant cyber-security risks to modern aviation industry may be segregated into (i) attacks on the network and communication; (ii) malware; (iii) smart devices on airports; (iv) Authorization Misuse; and (v) phishing attacks on the social security infrastructure[16]. The object of these vectors of danger is:-

i. Obstruction in the operations of the computer
ii. Stealing confidential data like personal, organizational and financial records.
iii. Obtain unapproved entry
iv. Spying
v. Indulged in Distributed denial-of-service attacks (DDOS)
vi. Locking and keeping down the data for ransom on the device

Some of the prominent threats that the aviation industry faces include the following:

A. DDoS and Botnet Attacks

There is a growing popularity of Distributed-denial-of-service attacks with the purpose of undertaking different malware injection activities. Through such measures, the hackers use botnets of the networks, which have been compromised, for flooding the ATC and other crucial systems related to traffic, resulting in the platforms crashing entirely. At such instances, the attackers, with

[15] Georgia Lykou et al., *Implementing Cyber-Security Measures in Airports to Improve Cyber-Resilience*, Global Internet of Things Summit (GIoTS) (2018).
[16] E Shahbazian, *Meeting Security Challenges Through Data Analytics and Decision Support* (2016).

the threat of disrupting flight control and management systems, often ask for ransom amount.

B. Jamming Attacks

When a ghost flight is injected in air traffic control system by an attacker, with the purpose of altering mapping and projection of airplanes, or that of deleting the position from the radar screen, it is deemed as jamming attacks. As these attacks compromise the very accuracy of the data, which is provided to the aircraft management, these attacks, have a big negative impact.

C. Phishing Attacks

These are the most successful ones, working against the aviation industry. The nature of these threats qualified under advanced persistent threats, meaning unauthorized individuals/ groups attaining access to network of the organization.

D. Remote Hijacking

The hackers are able to attack or control, the on-board systems and flights remotely because of the security flaws in ICT, contributing to such attacks. The Flight Management System was shown to be attacked by a hacker, which showed how the varied elements like surveillance systems, engine and fuel systems, aircraft displays, engine and fuel systems, and the others, could be easily manipulated.

E. Wi-Fi based Attacks

Weaknesses have been identified in the on-board systems of modern aircrafts, which enable attackers in using the inflight entertainment system or the Wi-Fi signal to hack the avionics equipment of planes, and for disrupting/ modifying satellite communications. One view is that after such attacks, with remote control, the planes could be landed in a successful manner. It just requires a framework of codes, by such actors, to get inside the system of planes and to override the security measures[17].

Unless system owners have decided to extract private details, spy on the compromised system, or seize over the system, ransom ware or malicious software infiltrates and retains control over a specified system or mobile

[17] *Id.*

device[18]. The malware is a software, application, client or computer network harm program built deliberately. There are several harmful programs such as viruses, worms, Trojan horses, malware, spyware, adware, rogue applications and scare ware[19]. Similar attacks may be carried out by an intruder downloading the malware on the website or intranet on the airport, where airport users' computers may be compromised, enabling malicious attackers to use these infected devices to enter airport's sensitive information system and network[20].

For future attacks to trigger network interruption, flight termination, customer disruptions, lack of trust, serious financial damage, and Smart airports networks are interconnected to improve their internal connectivity. The usage of data manipulation from critical functionalities and safety criteria, including air navigation and air traffic control systems, communications, air crash avoidance systems is also helpful in improving connectivity[21].

A counter-measure can be introduced that involves anti-malware and IDS/IPS programs. To keep smart airport systems up-to-date with reduced access to popular defects, both software fixes and hardware upgrades are critical[22]. Moreover, the surveillance and auditing of networks and log files is also important for smart airports, as any unwanted alteration by malicious insiders must be identified and remediated immediately. It states, "What you can't avoid, you should be capable of detecting and, if you detect anything, it means you couldn't prevent it" so that protective and detective controls for the resilient device can function together.

---

[18] Georgia Lykou et al., *Smart Airport Cyber-Security: Threat Mitigation and Cyber Resilience Controls*, 19 Sensors (2018).

[19] Ramjee Prasad, *Cyber Threats and Attack Overview*, Springer Series in Wireless Technology. (2019).

[20] Bryan Watkins, *The Impact of Cyber Attacks on the Private Sector*, Amo.Cz (Feb. 27 2021, 06:22am) http://www.amo.cz/wp-content/uploads/2015/11/amocz-BP-2014-3.pdf.

[21] Xiaoqian Sun, *Network Similarity Analysis of Air Navigation Route Systems*, 70 Transportation Research Part E: Logistics and Transportation Review (2014).

[22] Alan J Stolzer, *Implementing Safety Management Systems In Aviation* (2011).

VI. Cyber Security in Air Traffic Control

A. Air Traffic Control /Air Navigation System

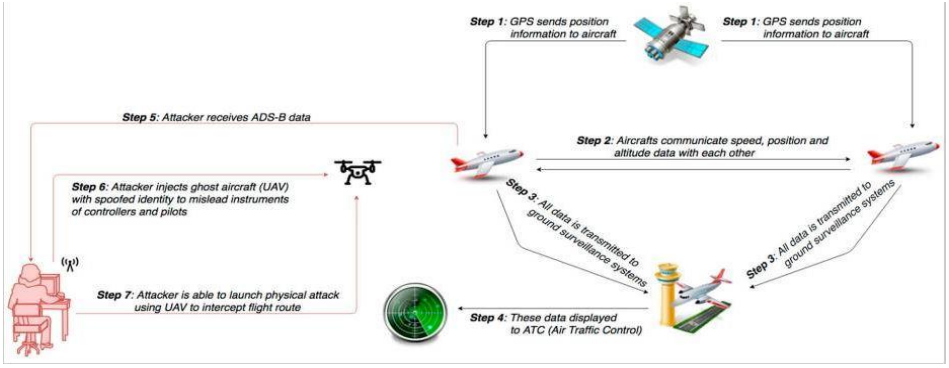
The air transportation sector has seen digital technologies gaining lot of traction, as they have a major impact over the passenger and flight safety. The air traffic management is increasingly becoming a data driven force, which makes it crucial for it to be properly safeguarded. The Network Manager function of Euro control has the responsibility for taking care of the ATM in forty three nations, and in order to fulfill its objectives of protecting the information systems from any and all kinds of cyber threats, has adopted outside help. One of this outside assistance is provided by Thales to modernize the air transport sector, and to help in developing five markets of space, defense, security, ground transportation and aerospace[23].

Cyberspace puts forth a cheap heaven for undertaking varied disruptive activities, which leads to the inference that hackers consider aviation sector as their key target. Apart from this, the low risks associated with this makes it easier for cyber terrorism to replace hijackers and bombers, thereby becoming the leading option for attaching aviation industry. One of the most complex and integrated mode of Information and Communication Technology, i.e. ICT is hosting. This, when coupled with the increased inter connectivity, results in growth of threats on aviation industry from multiple fronts hiding behind anonymity. The actors of such cyber threats focus over malicious intent, physical damage, political motivations, hactivist national, financial gains and theft of personal data. In short, by adopting an informed risk cyber security roadmap that is attained by analyzing the threats, thereby strengthening the resilience of aviation industry against cyber threats, takes the centre-stage[24]. A depiction of communication attacks on ATM system is presented below:

---

[23] Thales, *Euro-control Chooses Thales For Cyber security And Digitalization Of Air Traffic Services* (Feb.26, 2021, 08:07pm) https://www.thalesgroup.com/en/worldwide/security/press-release/eurocontrol-chooses-thales-cyber security-and-digitalization-air

[24] Dan Virgillito, *Cyber Threat Analysis for the Aviation Industry* (Feb,.26 2021, 10:40pm), https://resources.infosecinstitute.com/cyber-threat-analysis-aviation-industry/#gref



(Source: Georgia Lykou, Argiro Anagnostopoulou, and Dimitris Gritzalis, 2019[25])

Air traffic control applies, in its simple sense, to geographic and integrated networks that execute multiple functions such as land control, runway lighting control, separation and routing, as well as radar control. Within ATC, the essential infrastructure is cyber defence. This is how the environment is intricately and misleadingly interested in the cyber hazard scenery. Sometimes, the critics blame numerous organisations which have now contributed to assaults on vital infrastructure[26]. The facility that computers can be interlinked with all forms of networks raises the probability of certain attacks in the field of hyper-connected Internet of Things (IoT). The shifting IoT world presents a challenge over the ATC networks as airports are seeking to modernize their essential functions. A potential cyber assault on ATC networks may contribute to the abuse of physical processes such as airport road lights and radar controls[27].

B. Emerging Threats in Air Traffic Control

Air traffic control networks are prone to Internet threats and there has been a shortage of sufficient intrusion detection capability for the Federal Aviation Administration to identify future cyber penetration. Assessors will take

[25] Georgia Lykou et al., *Smart Airport Cyber security: Threat Mitigation and Cyber Resilience Controls,* 19 Sensors (2019).

[26] Andrew Cook, *Applying Complexity Science to Air Traffic Management*, 42 Journal of Air Transport Management (2015).

[27] Martin Strohmeier, *Realities and Challenges of Nextgen Air Traffic Management: The Case of ADS-B*, 52 IEEE Communications Magazine (2014).

advantage of technical weaknesses in commercial IP devices for the manipulation of ATC networks, which is especially alarming at a period when the nation is experiencing more and more danger from sophisticated nation-state-supported cyber-attacks[28].Innovations have been gaining a lot of momentum in the air travel business, as they have a significant effect on passenger and air welfare. The control of air traffic is becoming more and more a data engine, which makes it necessary to be adequately protected. As a result of the computer systems available both on-board and off board, the rampant usage of data networks, coupled with navigation systems, data breaches and cyber-attacks are deemed as the top most growing threats for this sector.

VII. Cyber-Security in European Air Traffic Control (Euro Control)

To achieve its goals of securing information networks from some kind of cyber danger, the network manager role of Euro Control must look after the ATM in forty-three countries, and has been given outward assistance[29]. Thales is one of several external supports for the modernization of aviation and the growth of five space, safety, security, land and aerospace markets.

Air transport is a crucial sector for the European economic sector with nearly sixteen thousand air traffic controllers in 65 control centers. This momentous magnitude led to EU taking proper steps towards safeguarding the ATC. This was done through the EUROCONTROL Mission. Through the European Organization for the Safety of Air Navigation/Traffic, efforts were made to integrate and harmonize the Air Navigation /Traffic Services in Europe, with the purpose of forming unified Air Traffic Management System for both the civil and the military users. This was done with the purpose of attaining safe, orderly and expeditious flow of air traffic throughout Europe. EUROCONTROL has been nominated as the Network Manager for Europe and acts as the central unit for managing air traffic flow. It also supports the placement of all technology-based improvements in the ATM network of Europe. Apart from this, it also implements the contingency plans and the security management system, along

[28] Donald McCallie, *Security Analysis of the ADS-B Implementation in the Next Generation Air Transportation System*, 4 International Journal of Critical Infrastructure Protection (2011).

[29] James P Farwell & Rafal Rohozinski, *Stuxnet and the Future of Cyber War*, 53 Survival (2011).

with presiding over the operations of EACCC, i.e. European Aviation Crisis Coordination Cell[30]

One of the key enabler identified in EASA's Cyber-Security in Aviation project and roadmap is the European Centre for Cyber Security in Aviation (ECCSA) which has to function as a catalyst to achieve the core identified objectives of:

i. Situational Awareness,
ii. Readiness & Resilience,
iii. Reactiveness, and
iv. Cyber-Security Promotion.

ECCSA, set up with ENISA's CERT-EU platform, as Aviation Computer Emergency Response Team (CERT), establishes an aviation-focused cross-sectorial risk landscape as well as coordinates the prevention of threat scenarios and response to future attacks. The purpose is to use as a clearing house for (confidential) incident information that builds on existing safety reporting in aviation.[31] Because of the increase demand in air traffic, the Single European Sky was brought forth in 1999. Through these, two packages were brought forth, for regulating Functional Airspace Blocks, new technologies, interoperability regulations and SESAR. SESAR is the program, which modernized the air traffic management system for Europe.[32]

VIII. Conclusion

The focus of this research was to discuss many views about how the global aviation industry is addressing cyber-security challenges. The research concluded that while there are several views on how to develop a common view of the aviation cyber-security challenge, there is potential for and a move forward. Adversaries have a large attack surface and potential, with growing numeration and accessibility. A further weakening of physical controls which shielded the aviation industry so long is the increasing complexities of systems, procedures, and supply chains, combined with an increase in wireless

[30] Antonio Nogueras, *Air Traffic Management moving into European Critical Infrastructure*, (Mar. 01, 2021), http://www.motia.eu/webfm_send/85.pdf.
[31] EASA, *EASA cooperate with CERT-EU on cyber-security*, (Feb. 14, 2021 09:31am), https://www.easa.europa.eu/newsroom-and-events/news/easa-cooperate-cert-eu-cybersecurity.
[32] *Id* at 19.

connectivity. In addition to highly competent threat entities, the aviation industry faces an essential challenge, spanning from terrorists to nations. Where necessary the industry wants to pursue rapid gains, but still understand that it is still an evolving challenge to protect the aviation industry from cyber adversaries. Europe has many regulations and legislative instruments safeguarding the aviation sector of this region. EASA regulate the cyberspace certifications and licensing to keep a check on the technicians and mechanics in aeronautical department. EASA undertakes standardized inspections for monitoring applicability of EU legislations in a uniform manner. On the other hand, EUROCONTROL has been nominated as the Network Manager for Europe and this act as the central unit for managing air traffic flow. The bodies like EACCC, ECSCG and ECCSA, along with the adopted ENISA's CERT-EU, SESAR and the like are just a few of bodies and frameworks working in this direction.

Consequently, particularly though the market is global and time-consuming, it has to be equipped to solve significant, structural problems. ICAO can be seen as a world pioneer and regulator in aviation with a concrete reform policy. It cannot drive reforms in the isolation mechanism and needs help and collaboration, if it is to be successful and sustainable, from states, industry organizations and the people involved in the aviation field. While progress has been made, there are still major challenges both in obtaining visibility into and in the global management of aviation cyber-security risk. Leadership and time would be required to properly prepare the aviation industry to resolve these cyber-security challenges. Steps should be taken to speed up this improvement phase, increase accountability and confidence, and enhance objectivity and cooperation. The aviation cyber protection infrastructure is without a single solution and will need positive cooperation among different stakeholders. Strengthening relationships around defence, security, cyber-security, and IT businesses are often complicated; however contribute to a dramatically enhanced perception of comprehensive risk, representing better the essence of the dynamic attack surface being guarded. It must be noted, along with this initiative, that air travel is a global business, with differing domestic and regional sophistication and capacity. It would be necessary to strengthen aviation cyber protection and getting all players together is vital if we want to reduce global, structural risks.