LLM Non-Thesis Student Maria C. Iannini
Supervise Research Project ID# 260663143

Civil Aviation and Cybersecurity: New Challenges

Research Supervisor
Prof. Pierre-Emannuel Moyse
McGill Faculty of Law

Word count:
14172

Due date August 15, 2016

1. CYBERSECURITY

1.1 Introduction

For many years the use of computer-based systems and information technology systems (IT systems)[1] has been developing in almost every aspect of civil aviation[2]. Aviation is expected to grow16 billion passengers and 400 million tonnes of cargo by 2050[3]. With the possibility of cybersecurity breaches or threats ranging from opportunistic exploitation from terrorists or innocent mistakes made by personnel operating the IT systems, cybersecurity is the next frontier of threats and challenges to civil aviation operations.

The following research project will focus on the threats to civil aviation by devices that use the Internet or cyberspace and will show different efforts made by different stakeholders –States, air carriers, manufacturers and international organizations– to address this issue and the future plan to assess the risk of such threats from a legal perspective. Furthermore, this research project will show how the stakeholders in civil aviation need to change the paradigm to address cybersecurity because the industry can no longer be reactive to an incident related to cybersecurity in civil aviation. It needs to be proactive to successfully address this issue.

The Internet has become widely available and has hastened the forces of economic globalization and is radically reshaping the economic and political landscape of almost every major country in the world[4]. By the late 1990's, the constant use of computers and the Internet developed the

[1] A complete definition of this concepts will be provided in the Cybersecurity in Civil Aviation chapter.
[2] Bernard Lim, "Emerging Threats from Cyber Security in Aviation - Challenges and Mitigations" (2014) Journal of Aviation Management at 85.
[3] IATA, Vision 2050 Report (12 February 2011) at 7 online: <https://www.iata.org/pressroom/facts_figures/Documents/vision-2050.pdf>
[4] Richard A. Spinello, "Regulating Cyberspace: The Policies and Technologies of Control" (Connecticut: Greenwood Publishing Group, 2002) at 1.

concept of the "information society"[5] because the individuals were able to interact with each other, exchange ideas, share information, provide social support, conduct business, play games, etc.[6] The use of the Internet, network and digital communication was compiled as cyberspace and defined as the notional environment in which communication over computer networks occurs[7]. Today, the Internet has become widely available, the cost of connecting has decreased, more devices are being created with Wi-Fi capabilities and technology prices are going down. All these facts have created the concept of the "Internet of Things" (IoT), which is the concept of connecting any smart object to the Internet to enable the exchange of data allowing users to access and/or transfer information. The IoT can be seen in common activities that people perform daily, such as e-mail access from anywhere in the world or online banking through a smart-phone[8]. Moreover, products are being designed so people can turn them on and off as long as there is Internet access, such as coffee makers, a laundry machines, headphones, cameras, factories, automobiles, oil rigs and aircrafts. Aircrafts, since they are sophisticated systems of engineering, are comprised of a complex network of components that include base systems, communication links, sensors, avionics, ground control systems, and air navigation service providers[9]; "just as any other computer, these components and communication links are prone to

[5] Joanne Armitage & John Roberts, "Living with Cyberspace: Technology and Society in the 21st Century" 1st ed (New York: The Athlone Press 2003) at 1.

[6] Lance Strate, "The varieties of cyberspace: Problems in definition and delimitation" (California: Western Journal of Communication 1999) at 403.

[7] The Oxford Dictionary, *sub verbo* "cyberspace", online: <http://www.oxforddictionaries.com/us/definition/american_english/cyberspace>

[8] Jacob Morgan, "A Simple Explanation of 'The Internet of Things'", Forbs Magazine (13 May 2014) <http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#6070fd616828>

[9] Deepika Jeyakodi, "Cyber Security in Civil Aviation", (LLM Thesis, Leiden University, International Institute of Air and Space Law 2015), [unpublished] at 3 online: <https://www.google.ca/search?q=Cyber+Security+in+Civil+Aviation,+Deepika+Jeyakodi.+Adv.LL.M&rls=com.microsoft:en-CA&ie=UTF-8&oe=UTF-8&startIndex=&startPage=1&gfe_rd=cr&ei=vp2OV72vA-Gh8weEjZ-4CQ&gws_rd=ssl?>

cyber-attacks that include but are not limited to hacking, jamming[10], and spoofing[11"12]. Specifically in the civil aviation arena, sophisticated air navigation systems like NexGen or SESAR[13], on-board aircraft control and communications systems, airport ground systems including flight information and security screening to simply inventory, and day-today office data management systems are being used twenty four hours a day, seven days a week.

Thus, in a globalized world where interconnection is instantaneous thanks to the Internet, the transfer of information, also known as the transfer of data, imposes a risk when it is not performed in a secure way. Cybersecurity has become a major concern in society since technology is a force that is shaping the domain of global interactions in aspects like telecommunications, commerce, transport, finance, banking and data storage. Arriving at a discrete definition of cybersecurity is crucial, so that there can be no mistake when it is infringed upon.

1.2 Definition and Relevance of Cybersecurity in Civil Aviation

Cybersecurity is a relatively new discipline. It is so new that there is no agreed-upon spelling for the term nor is there a broadly accepted definition[14]. Furthermore, the term "cybersecurity" has

---

[10] Jamming is the emission of radio signals aiming at disturbing the transceivers operations. Alvaro Herrero, "International joint conference SOCO'13-CISIS'13-ICEUTE'13 - *Advances in Intelligent Systems and Computing International Joint Conference*" (New York: Springer, 2014) at 14.

[11] Spoofing is the activity of faking the sending address of a transmission to gain illegal unauthorized entry into a secure system. Cyber Security Glossary, National Initiative for Cybersecurity Careers and Studies (NICCS), online: < http://niccs.us-cert.gov/>.

[12] *Jeyakodi, supra* note 9 at 3.

[13] NexGen from the United States and SESAR from the European Union, are the initiatives to modernized the national airspace system moving from ground-based to satellite-based navigation communication from 2012 up until 2025. This technology, which will be using global position satellite (GPS), creates great benefits for the aviation industry because it will shorten aircraft routes, safe time and fuel, reduce traffic delays, increase capacity and permit air traffic controllers to monitor and manage aircraft with greater safety margins. United States Department of Transportation, "Impacts of the Light Squared Network on Federal Science Activities", (8 September 2011) online: < http://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/090811_%20Appel.pdf>

[14] Gregory J. Touhill & C. J. Touhill, "Cybersecurity for Executives: A Practical Guide" (Hoboken: John Wiley & Sons, 2014) at 2.

been the subject of academic and popular literature[15] and there is no consensus on the key elements of this term. Thus, for a better understanding of this concept, it is proposed that the term cybersecurity should be interpreted as "the deliberate synergy of technologies, processes, and practices to protect information and the networks, computer systems and appliances, and programs used to collect, process, store, and transport that information from attack, damage, and unauthorized access"[16]. Additionally, cybersecurity includes the technologies employed to protect information. It includes the processes used to create, manage, share, and store information. It includes the practices such as workforce training and testing to ensure information is properly protected and managed from hackers and others who attempt to gain access to information for reasons that include curiosity, personal profit, or competitive advantage[17].

But what happens when the technology and the information contained within is accessed criminally, attacked or damaged? This is what is commonly known as a "cyber-attack" or "hacking". In contemporary society, a cyber-attack is important because it is the way users are targeted to gain access to their personal information, intellectual property or control over devices that operate under the IoT concept. Some experts have defined cyber-attack as "a hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions"[18]. Moreover, all types of online or IoT crimes continue to grow as hackers and organizations become more sophisticated in the way they illegally access information. Furthermore, it is important to mention that the Internet has made

[15] Dan Craigen, Nadia Diakun-Thibault & Randy Purse, "Defining Cybersecurity" online: Technology Innovation Management Review <http://timreview.ca/article/835>.
[16] *Supra* note 9 p.2
[17] *Ibid* at 1.
[18] Department of Defense United State of America, "Memorandum for Chiefs of the Military Services Commanders of the Combatant Commands Directors of the Joint Staff Directors - Subject: Joint Terminology for Cybersecurity Operations" online: <http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf >

our world smaller. Hacking can be performed in a location other than where the crime is taking place, making hacking a no-national boundaries activity.

In a "cyber age", the key element is to learn how to manage risk and maintain a competitive advantage. Civil aviation cybersecurity is about risk management, States and private companies –such as airlines or manufacturers- need to understand the risk environment, know the weaknesses, understand the risks, and make intelligent decisions to carefully avoid, mitigate, and accept cyber-threats. Awareness and legal enforcement are the key elements for cybersecurity to be successful and capable to fight against the illegal access obtained by a cyberattack. In order to tackle a misuse of the IoT and the Internet, cooperation between the private (air carriers, manufacturers, etc.) and public (States) sector is needed. Such cooperation between the public and private sector is relevant in order to address cybersecurity in civil aviation because since the Deregulation Acts in the United States in the late 1970's[19], "the role of the US government over commercial aviation was more reduced, and market forces came to dominate the destiny of the industry. The United States began to export its deregulation ideology abroad and by the early 1990s the European Union (EU) had created a free internal European market in air services"[20]. Thus, even though according to the Convention on International Civil Aviation signed in in 1944, also known as the Chicago Convention (CC), the safety and security of civil aircraft navigation shall be performed with due regard by the members States[21]. Since the Deregulation Acts, industries worldwide became stronger in the market playing a much important role in order

[19] Three major acts promulgated by the United States congress allowed the deregulation of the aviation industry: the Air Cargo Deregulation Act of 1977, the Airline Deregulation Act of 1978, and the International Air Transportation Competition Act of 1979.

[20] Brian F. Havel, "In Search of Open Skies" (Boston: Kluwer Law International, 1997) at 123-124.

[21] Convention on International Civil Aviation, 7 December 1944, 15 UNTS 295, ICAO Doc 7300/6 (entered into force 4 April 1947) [*Chicago Convention*]. The Chicago Convention states in the preamble and in Article 3 that member States shall create and preserve friendship and understanding among the nations and peoples of the world bearing in mind the principle of general security and the safety of navigation of civil aircraft.

to address important factors like cybersecurity, making the aviation industry responsible while dealing with a possible threat or cyberattack.

2. IMPORTANCE OF CYBERSECURITY IN CIVIL AVIATION

2.1 Safety in Civil Aviation

This chapter will explain safety and security and its relation to cybersecurity within the civil aviation stakeholders. "Safety and security are two sides of the same coin. The regulation of both is designed to avoid injuries to persons and property, and the deprivation of man's most valuable attribute – life. Yet the two are quite different as well"[22]. While safety regulation focuses on preventing accidental harm, security regulation focuses on preventing intentional harm. Moreover, safety also includes security, in the context of civil aviation "safety" is related to the operational safety of aircraft, including personnel licensing and airworthiness, whereas "security" means safeguarding civil aviation against acts or attempts to jeopardize the safety of civil aviation[23] such as hijacking, destruction of an aircraft in service or communication of false information that jeopardize the safety of an aircraft in flight or on the ground, of passengers, crew, ground personnel or the general public, at an airport or on the premises of a civil aviation facility.

Safety has been of paramount importance since the development of civil aviation. However, due the international nature of civil aviation, the only way to achieve safety is through uniformity and by securing global harmony in law. In 1944, the world community acknowledged the need to

[22] Paul Dempsey, "Public International Air Law" (Montreal: McGill University 2008) Chapter IV Safety at 3.
[23] Jiefang Huang, "Aviation Safety Through the Rule of Law, ICAO's Mechanisms and Practice", (The Netherlands: Kluwer Law International, 2009) at 7.

achieve safety in international aviation through uniformity in law[24] by establishing an organization to govern international aviation, conferring upon it quasi-legislative power to prescribe standards governing international aviation safety, and obliging member States to implement these standards through their domestic laws[25]. The given name of the institution is the International Civil Aviation Organization, also known as ICAO. As professor Michael Milde observes, "civil aviation could not have evolved without worldwide uniformity in regulations, standards and procedures in relation of air navigation"[26]. Such uniformity is achieved when the Member States of the CC are bound by a treaty but also when ICAO prescribes standards and recommends practices (SARPs); however, it is important to mention that the SARPS promulgated by ICAO are considered by some authors as "soft law"[27] and other scholars consider them as "de facto hard law"[28]. Although States have an obligation under the CC to keep their own regulations uniform[29] to the greatest possible extent with SARPs, the way the Convention was drafted gives a contracting State a means of avoiding the implementation of standards on the basis of impracticality. Thus, some States may find it impractical to comply[30] on

[24] Michael Milde, "Essential Air and Space Law; International Air Law and ICAO" (The Netherlands: Eleven International Publishing, 2008) at 203.
[25] Paul Stephen Dempsey, "The Role of the International Civil Aviation Organization on Deregulation, Discrimination & Dispute Resolution" (1987) 52 J Air L & Com 529 at 533.
[26] Supra note 15.
[27] *Huang*, *supra* note 23 at 172.
[28] Herbert V. Morais, "The Quest for International Standards: Global Governance vs. Sovereignty" (2002) 50 Kan L Rev 779 at 780-81 "For the most part, international standards have been developed and disseminated as norms or principles for voluntary acceptance by countries and other persons. In this sense, international standards would not be legally binding norms and would be generally viewed as 'soft law'. However, it is important to recognize at the same time that several standards have taken the form of binding legal rules established by international treaty or national legislation, and, in these cases, the standards constitute 'hard law'".
[29] Article 12 from the Chicago Convention states "[…] Each contracting State undertakes to keep its own regulations in these respects uniform, to the greatest possible extent, with those established from time to time under this Convention. […]"
[30] Article 38 from the Chicago Convention states "Any State which finds it impracticable to comply in all respects with any such international standard or procedure, or to bring its own regulations or practices into full accord with any international standard or procedure after amendment of the latter, or which deems it necessary to adopt regulations or practices differing in any particular respect from those established by an international standard, shall give immediate notification to the International Civil Aviation Organization of the differences between its own practice and that established by the international standard. In the case of amendments to international standards, any

the basis of insufficient human or financial resources, or its unique geographic or technological characteristics. Under such circumstances, the State has a duty to immediately notify ICAO "of the differences between its own practice and that established by the international standard"[31]. Subject to the notification of differences, the legal regime effectively assumes that States are in compliance with these safety mandates[32]. Although member States retain the right to restrict particular aircraft from their skies, they lose the right to ignore the safety mandates of ICAO. This assumption of universal compliance goes further with the CC requirement that an airman or operator certificate, or certificate or airworthiness, properly issued by one contracting State shall be recognized as valid by all others[33]. According to Article 33[34], member States are obliged to recognize the validity of the certificates of airworthiness and personnel licenses issued by the State in which the aircraft is registered, so long as the standards under which such certificates or licenses are rendered are at least as stringent as those established under the CC.[35] But this principle of mutual recognition works only if all States are implementing the SARPs with an equal or superior degree of diligence required under the Annexes[36]. Although ICAO has attempted to facilitate compliance by the publication of numerous manuals instructing member

---

State which does not make the appropriate amendments to its own regulations or practices shall give notice to the Council within sixty days of the adoption of the amendment to the international standard, or indicate the action which it proposes to take. In any such case, the Council shall make immediate notification to all other states of the difference which exists between one or more features of an international standard and the corresponding national practice of that State."

[31] Supra note 19. pp 18 Chapter III Chicago Convention.

[32] *Dempsey, supra* note 22 at 9.

[33] *Ibid* at 9.

[34] Article 33 of the Chicago Convention states "Certificates of airworthiness and certificates of competency and licenses issued or rendered valid by the contracting State in which the aircraft is registered, shall be recognized as valid by the other contracting States, provided that the requirements under which such certificates or licenses were issued or rendered valid are equal to or above the minimum standards which may be established from time to time pursuant to this Convention."

[35] United States courts have recognized the duty of the FAA to abide by its Article 33 Chicago Convention obligation to recognize as valid licenses issued by another signatory State, provided that the requirements underlying such licenses are equal or superior to those required under the Annexes. *Professional Pilots v FAA*, 118 F (3D) 758, 768 (DC CIR 1997); *British Caledonian Airways v Bond*, 665 F (2d) 1153 (DC Cir 1981) [*British Caledonian*]. See also, *In the Matter of Evergreen Helicopters*, (2000 FAA *Lexis* 247 (2000)).

[36] *Dempsey, supra* note 22 at 10.

States on how to comply,[37] many States either could not, or would not, implement their international legal aviation safety obligations[38]. States fail to comply with the minimum standards required by ICAO for different reasons:

i. Their aviation legislation and regulation may be either non-existent or inadequate;

ii. The Civil Aviation Authorities (CAA) or institutional structures that regulate and supervise aviation safety often do not have the authority and/or autonomy to effectively satisfy their regulatory duties;

iii. They lack the appropriate expertise in human resources due to inadequate funding and training by States; and

iv. They lack the financial resources allocate to civil aviation safety. Many developing countries do not consider aviation safety a high priority compare to other demands such as health care, education, poverty, etc.

When States fail to comply, other States are not obliged to recognize the validity of the certificates of airworthiness issued by the delinquent State, and may therefore ban its aircraft from their skies, even when they have conferred traffic rights to the State pursuant to Article 6[39] of the CC[40]. This is an important incentive for compliance with the international obligations established by ICAO.

---

[37] See ICAO, Manual of Procedures for Operations Inspection, Certification and Continued Surveillance, ICAO Doc 8335; Manual of Civil Aviation Medicine, ICAO Doc 8924; Preparation of an Operations Manual, ICAO Doc 9376; Manual of Procedures for Establishment and Management of a State's Personnel Licensing System, ICAO Doc 9379; Manual of Model Regulations for National Control of Flight Operations and Continuing Airworthiness of Aircraft, ICAO DOC 9388; Manual of Procedures for an Airworthiness Organization, ICAO DOC 9389; Continuing Airworthiness Manual, ICAO DOC 9642; Safety Oversight Audit Manual, Part A — The Establishment and Management of a State's Safety Oversight System, ICAO DOC 9734; and Safety Oversight Audit Manual, ICAO DOC 9735.

[38] *Dempsey, supra* note 22 at 20.

[39] Article 6 from the Chicago Convention states "No scheduled international air service may be operated over or into the territory of a contracting State, except with the special permission or other authorization of that State, and in accordance with the terms of such permission or authorization."

[40] *Dempsey, supra* note 22 at 16.

Furthermore, some of the aviation leading countries such as the United States (US) through the Federal Aviation Administration (FAA) and the European Union (EU) through the European Aviation Safety Agency (EASA), have developed additional mechanisms to implement safety and security procedures. Although the US and the EU have used different methods, both try to achieve safety and security in civil aviation[41]. For example, the US government deployed additional security procedures for foreign airport and foreign air carriers that server the US through the Foreign Air Security Act of 1985. Foreign airports are assessed by the Department of Transportation (DOT) to determine whether they satisfy the requirements established by ICAO under Annex 17, which deals with security. The DOT conducts a security audit of foreign airports, and if it finds that an airport has failed to take appropriate security measures, it notifies the appropriate authorities of its decision, recommends steps to achieve compliance and certifies or decertifies foreign airports on the basis that the security audit concluded that "a condition exist[ed] that threaten[ed] the safety or security of passengers, aircraft, or crew traveling to or from that airport; and the public interest requires an immediate suspension of transportation between the US and that airport"[42]. Various airports around the world have been certified and decertified by the DOT. For example the Murtala Mohammed International Airport in Lagos, Nigeria, El Dorado International Airport in Bogotá, Colombia and the Hellenikon International Airport in Athens, Greece[43]. This process is also known as blacklisting of airports. Additionally, since 1991 the US also implemented the International Aviation Safety Assessment Program (IASA) where members from the FAA were sent to the CAA and airlines from other countries to collect evidence to discern whether the foreign CAA and airlines were in compliance with

[41] *Dempsey, supra* note 22 at 21.
[42] *Ibid* at 21.
[43] See DOT Order 98-1-24 (1998) (Port-au-Prince International Airport, Haiti); DOT Order 92-10-17 (1992) (Murtala Mohammed International Airport, Lagos - Nigeria); DOT Order 95-9-15 (1995) (El Dorado International Airport, Bogotá - Colombia); DOT Order 96-3-50 (1996) (Hellenikon International Airport, Athens - Greece);

SARPs[44]. Blacklisting an airport works by "name a shame" where the FAA disclose publicly the results from the audits and classifies countries in two categories; category I -in compliance with the SARPs; category II - not in compliance with the SARPs. Blacklisting of airports have the following consecuences:

- Category II airports may be ban access to fly to/from the US;
- Category II airports may deny code-share arrangements between category I air carriers; and
- The carrier's aircraft from category II are subject to additional inspections at US airports[45].

All these procedures will cause economic harm to the State, peer pressuring the airlines and CAA to comply quickly with the SARPs. A criticism made to the IASA program often related with the politicization of audit criteria, where a sovereign State like the US can objectively analyze the CAA of another sovereign, particularly when the audited authority is a body of auditor's closest allies[46] or vibrant and expanding Middle East and Asian air carriers[47].

On the other hand, in 2005 the EU implemented a different method[48]. They banned foreign air carriers that did not comply with the safety regulations. Also known as blacklisting of airlines. This EU regulation provides that bans are to be imposed "according to the merits of each

---

[44] Federal Regulation, Vol. 60, No. 210, 57 38,342 (24 August 1992).

[45] *Dempsey, supra* note 22 at 30.

[46] Joe Del Balzo, "AAI's Return to IASA Category I is A Reminder of the Value of that Status Enhances Aviation Safety" JDA Journal (1 November 2012) online: <http://jdasolutions.aero/blog/caai%E2%80%99s-return-to-iasa-category-1-is-a-reminder-of-the-value-of-that-status-enhances-aviation-safety/>.

[47] Jad Mouawad, "U.S. Airlines Face Uphill Struggle Against Mideast Rivals" , The New York Times (14 December 2015) online: <http://www.nytimes.com/2015/12/15/business/us-airlines-face-uphill-struggle-against-mideast-rivals.html?_r=0>.

[48] European Parliament, *EC, 2005* Ordinary Sess, The establishment of a Community list of air carriers subject to an operating ban within the Community and on informing air transport passengers of the identity of the operating air carrier, and repealing Article 9 of Directive 2004/36/EC (Text with EEA relevance), *2111/2005*, (2005) OJ L 344/15.

individual case"[49] evaluating "whether the air carrier is meeting the relevant safety standards"[50]. The phrase "relevant safety standards" is defined as the international safety standards contained in the CC and its Annexes as well as, where applicable, those in relevant Community law[51]. Though this ban method has been criticized because it is broad, according to Professor Stephen Dempsey does not help safety standardization[52] and as air carriers may be banned from European skies even if it meets the requirements of the CC and its Annexes, if it nonetheless violates the safety standards "in relevant Community Law". As professor Dempsey argues "it is difficult to comprehend how the EU can lawfully impose requirements beyond those contained in the Annexes to the CC for its member States are parties to the CC and have an obligation to be bound by it. Though the EU itself is not a party to the CC, its members are and they are bound by Article 33 to recognize as valid the certificates of airworthiness issued by the registering State so long as they comply with the SARPs, irrespective of whether they comply with "relevant Community Law."[53] Additionally, this method is also criticized because it is easy to assumed that if one airline of a registering State is blacklisted by the EU, a presumption might be appropriate that the other airlines of that State also have deficiencies, perhaps attributed to the deficiencies of regulatory oversight by the registering State[54].

Regardless the method imposed to try to comply with aviation safety, some States responded with hostility and complained about the EU and US blacklisting of airports and airlines since no single nation should act like a policeman, however the consensus among nations was that the

[49] *Ibid* at 49.
[50] Ibid at 49.
[51] *Dempsey*, *supra* note 22 at 34.
[52] The civil aviation authorities of Member States of the European Union are only able to inspect aircraft of airlines that operate flights to and from EU airports; and in view of the random nature of such inspections, it is not possible to check all aircraft that land at each EU airport. European Union, List of Air Carriers Which are Banned from Operating Within the Union, with Exceptions, (16 June 2016), online: < http://ec.europa.eu/transport/modes/air/safety/air-ban/doc/list_en.pdf>.
[53] *Dempsey*, *supra* note 22 at 34.
[54] *Ibid* at 38.

SARPs should be honored since multilateral cooperation was preferable to unilateral insistence[55]. Thus, in response ICAO created the Universal Safety Oversight Audit Programme (USOAP) where this organization started to perform a series of safety audits to member States evaluating member State compliance with Annex 1 -related with personal licensing, Annex 6 -related with operation of aircraft, and Annex 8 -related with airworthiness of aircraft. By 2004, ICAO had audited 181 States for safety compliance and performed 120 audit follow-up missions. USOAP had significant impact on the issue of filing of differences[56]. The ICAO Council approved a bilateral Memorandum of Understanding (MoU) between the audited States, where all audited differences "shall be deemed to have been notified to ICAO". It incorporates these differences in the Supplements to its Annexes, therefore notifying all ICAO member States. Through the MoU, ICAO created a vast database with respect to conformity and compliance with Annex 1 (Personnel Licensing), Annex 6 (Operation of Aircraft), Annex 8 (Airworthiness of Aircraft), and also it is allowed to audit on the implementation of the safety-related provisions in Annex 11 related with Air Traffic Services[57], Annex 13 -related with Accident Investigation, and Annex 14 -related with Aerodromes. In 2004, the 35th meeting of the ICAO General Assembly passed a resolution requiring the Secretary General to make the results of the audit available to all member States, and to post them on the secure portions of the ICAO website.[58] By 2006, the ICAO Council approved a procedure for disclosing information about a State having significant SARPs deficiencies in its aviation safety obligations. A more significant action was taken in 2006, when aviation directors general from 153 of 190 member States agreed that by March 23,

[55] Anthony Broderick & James Loos, "Government Aviation Safety Oversight – Trust, But Verify" (2002) 67 J Air L & Com at 1049.
[56] *Dempsey, supra* note 22 at 43.
[57] Air Traffic Services, Air Traffic Control Services, Flight Information Services, Alerting Services, ICAO, Thirteen Edition, Annex 11 to the Convention on International Civil Aviation.
[58] *Assembly Resolution A35-6, Doc. 9848* – Assembly Resolution in Force (as of 8 October 2004), superseding A33-8.

2008, the names of those States that fail to agree to full transparency of their USOAP audits, will be posted on the ICAO website as "blame and shame policy". By 2006, more than 100 States agreed to transparency[59]. ICAO and the International Air Transport Association (IATA) also signed a MoU, "to share safety-related information from their respective audit programs to better identify potential safety risks and prevent aircraft accidents"[60], as well as share accident and incident monitoring, and "experts from each organization will be allowed to participate as observers in audit missions of the other, upon request."[61] In 2003, IATA established an Operational Safety Audit (IOSA) program for air carriers, its audit standards focus on:

i) Corporate Organization and Management Systems;

ii) Flight Operations;

iii) Aircraft Engineering and Maintenance; vi) Cabin Operations;

iv) Ground Handling;

v) Cargo Operations;

vi) Operational Security; and

vii) Operational Control – Flight Dispatch[62].

2.2 Security in Civil Aviation

Terrorism has become a global menace in the modern world and aviation has been victim of it in different ways. Hijacking aircrafts, bombings and airport attacks are some of the common forms of terrorism towards civil aviation. Although, hijacking has been the most common activity

[59] *Dempsey, supra* note 22 at 44.
[60] *Ibid* at 43.
[61] *Ibid* at 44.
[62] IATA, Operational Safety Audit: Designed for the Aviation Industry, (2007). online: <http://www.iata.org/whatwedo/safety/audit/iosa/Pages/index.aspx>.

towards aircrafts[63], according to ICAO and its Annex 17 related with security, unlawful interference are the different acts or attempts that jeopardize the safety of civil aviation which, included but not limited to:

- Unlawful seizure of aircraft;
- Destruction of an aircraft in service;
- Hostage-taking on board aircraft or on aerodromes;
- Forcible intrusion on board an aircraft, at an airport or on the premises of an aeronautical facility;
- Introduction on board an aircraft or at an airport of a weapon or hazardous device or material intended for criminal purposes;
- Use of an aircraft in service for the purpose of causing death, serious bodily injury, or serious damage to property or the environment; and/or
- Communication of false information such as to jeopardize the safety of an aircraft in flight or on the ground, of passengers, crew, ground personnel or the general public, at an airport or on the premises of a civil aviation facility[64].

Additionally, different treaties related with aviation security have been adopted under the auspices of ICAO, these are:

i) the Tokyo Convention of 1963— technically named the Convention on Offenses and Certain Other Acts Committed on Board Aircraft[65] has been ratified by 186 States and gives the aircraft commander and crew authority to suppress an unruly or dangerous

[63] US, Transportation Security Administration, *Criminal Acts Against Civil Aviation* (2001) at 45 online: <http://nsarchive.gwu.edu/NSAEBB/NSAEBB165/faa8.pdf> .

[64] Safety, Safeguarding International Civil Aviation Against Acts of Unlawful Interference, ICAO, Ninth Edition, Annex 17 to the Convention on International Civil Aviation (2014) at 15.

[65] *Convention on Offenses and Certain Other Acts Committed On Board Aircraft*, 14 September 1963, 20 UST 2941, TIAS No 6768, 704 UNTS 219, 58 Am J Int'l L 566 (1959) (entered into force 4 December 1969) [*Tokyo Convention*].

passenger, and requires that a hijacked aircraft be restored to the aircraft commander and passengers be permitted to continue their journey.;

ii) The Hague Convention of 1970—the Convention for the Suppression of Unlawful Seizure of Aircraft has been ratified by 185 States and declares hijacking to be an international "offense" and requires the State to which an aircraft is hijacked to extradite or exert jurisdiction over the hijacker and prosecute him, imposing "severe penalties" if he is found guilty;

iii) The Montreal Convention of 1971—the Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation[66] has been ratified by 188 States and expands the definition of "offense" to include communications of false information and unlawful acts against aircraft or air navigation facilities, and requires prosecution thereof;

iv) Annex 17 to the Chicago Convention—in 1974, ICAO adopted Annex 17 to the Chicago Convention on Civil Aviation of 1944[67]. Beyond incorporating several of the requirements of the Tokyo, Hague, and Montreal Conventions, the Annex requires each member State to establish a governmental institution for regulating security and establishing a national civil aviation security program. The security program is to prevent the presence of weapons, explosives, or other dangerous devices aboard aircraft; require the checking and screening of aircraft, passengers, baggage, cargo, and mail; and require that security personnel be subjected to background checks, qualification requirements,

---

[66] Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 23 September 1971, 1974 UNTS 177; [1973] ATS 24; 10 ILM 1151 (1971) (entered into force on 26 January 1973, with 150 ratifications) [*Montreal Convention*]. See Paul Stephen Dempsey, William Thomas & Robert Hardaway, *Aviation Law & Regulation* (United Kingdom: Butterworth Legal Publishers, 1993) at § 9.13

[67] Convention on International Civil Aviation, 7 December 1944, 15 UNTS 295, ICAO Doc 7300/6 (entered into force 4 April 1947) [*Chicago Convention*]. See Paul Stephen Dempsey, "The Role of the International Civil Aviation Organization on Deregulation, Discrimination, and Dispute Resolution" (1987) 52 J Air L & Com at 529.

and adequate training. Annex 17 has been amended several times in since it was created[68];

v) The Montreal Protocol of 1988—the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation,[69] Supplementary to the Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, has been ratified by 173 States and added airport security to the international regime;

vi) The Montreal Convention of 1991—the Convention on the Marking of Plastic Explosives for the Purpose of Detection[70] has been ratified by 152 States and prevents the manufacture, possession, and movement of unmarked explosives; vii) The Beijing Convention and Protocol of 2010 – the Beijing Diplomatic Conference on Aviation Security held from 30 August to 10 September 2010 produced the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation and the Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft, it has been ratified by 10 States. Among the additional offenses criminalized were: using civil aircraft as a weapon, using dangerous materials to attack aircraft or other targets on the ground, the unlawful transport of biological, chemical and nuclear weapons and their related material, and making a threat against civil aviation. At this writing, neither the Convention nor the Protocol has entered into force; viii) The Montreal Protocol of 2014 – this Protocol amends the Tokyo Convention to expand jurisdiction to cover the State of the aircraft operator as well as of the State of landing. Jurisdiction of the State of registry

[68] The amendments of Annex 17 will be further discuss in Chapter 3.

[69] *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation*, 24 February 1988, ICAO Doc 951, 1589 UNTS 474, [1990] ATS 37,27 ILM 628 (1988) (entered into force 6 August 1989) [*Montreal Protocol 1988*].

[70] *Montreal Convention*, *supra* note 66.

and jurisdiction according to national legislation remain. Two new offenses were added: physical assault or threat thereof against a crew member, and refusal to follow a lawful safety instruction of the crew. The pilot-in-command may ask, but not require, an In Flight Security Officer (IFSO) to assist in restraining a disruptive passenger. ISFOs may take preventive action against passengers when they reasonably believe that an offense is about to be committed. Deployment of IFSOs is regulated by bilateral agreements between the concerned States[71]. This protocol has not entered into force since not enough States have ratified it[72].

Outside the UN-ICAO auspices, there has been other air security agreements such as:

- The European Convention on the Suppression of Terrorism from 1976, which provides that hijacking is not deemed to be a political offense exception that avoids extradition; and
- The Bonn Declaration on Hijacking from 1978, where the G-7 leaders agreed that all flights would be ceased immediately to or from any nation that refused either to return the hijacked aircraft or to prosecute or extradite a hijacker[73].

These different aviation security treaties are valuable legal instruments for combating unlawful interference against civil aviation. However, with the passage of time and changes of circumstances, there are new and emerging developments that have become a threat to civil aviation. Such of threats are not adequately covered by these treaties since the existing conventions only criminalize the commission of certain acts. As an example, cyber threat is a

[71] Paul Stephen Dempsey, "Public International Air Law" (Montreal: McGill University 2008) Chapter VI Security at 45.
[72] Michael Jennison, "ICAO Adopts Flawed Protocol to Amend the Tokyo Convention of 1963" (2014) 39 McGill Annals of Air & Space Law at 9.
[73] The seven economic powers that participated in the drafting of the Bonn Declaration were Canada, France, West Germany, Italy, Japan, the United Kingdom and the United States.

safety and security concern that none of the above mentioned treaties have address. As professor Jiefang Huang clearly expressed it "most of the ICAO instrument were concluded decades ago, they did not and could not possibly include the provisions that reflect the more recent development in international law"[74] such as cybersecurity.

3. CYBERSECURITY IN AVIATION

3.1 Cyber threats

Currently, there is no common vision, or common strategy, goals, standards, implementation models, or international policy for cybersecurity for civil aviation[75]. Making sure that a secured aviation system in well implemented, and staying ahead of evolving cyber threats is a shared responsibility for the aviation shareholders (governments, airlines, airports, and manufacturers). The threat against to civil aviation operation it is not new; from more than 25 years different CAA around the globe have used what it is called computer-based systems or IT systems[76], which is a complementary network of computer-based hardware or software used to collect, filter, distribute and process data or other relevant information. These systems make it easier to user to generate, analyze and use necessary information from computer as individuals or within organization spheres[77]. In civil aviation, computer-based systems and IT systems are used to preformed operations such as sophisticated air navigation systems (NexGen or SESAR), on-board aircraft control, communications systems, airport ground systems including flight

[74] *Huang*, *supra* note 23 at 147.
[75] AIAA, The World's Forum for Aerospace Leadership, The Connectivity Challenge: Protecting Critical Assets in a Networked World, Decision Paper (August 2013) at 5 online: <https://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final.pdf>
[76] IT systems is part of computer-based systems and means the use of hardware, software, services and supporting infrastructure to manage and deliver information using voices, data and video. Mehdi Khosrow-Pour, "Encyclopedia of Information Science and Technology, Third Edition" (Hershey: Ideal Group References, 2006) at 336.
[77] Richard T. Watson, "Information Systems" (Georgia: University of Georgia, 2007) at 16 online: <http://www.uky.edu/~gmswan3/777/IS_Book.pdf>.

information and security screening, and they are also use to simply inventory and day-today office data management systems.

Such a systems are used in civil aviation to "achieve great efficiency, reduction in the use of manpower and greater use of IT to reduce cost and increase synergies between and amongst stakeholders"[78]. As the world is moving towards the IoT, many airports and airlines are introducing more efficient ways for passengers facilitation, for instance using mobile devices such as Personal Digital Assistance[79] for electronic ticketing, check-in and immigration clearance. The use of technology and its interaction between passenger-airport-airlines it is expanding rapidly and it is very much appreciated since the number of passengers traveling is increasing worldwide.

Some security experts are concerned because cyber security today is bringing more modern computer-based systems and IT systems into the aviation industry, where the information about how the system works might be exploited if published. It can increase the risk of a cyber-attack because the engineers are no longer a small highly-expert group of people, but more a large group of people with enough hacking knowledge. In contrast, other security experts believe that responsibly disclosing security issues creates positive pressure on stakeholders, like manufacturers and airlines, to address these issues more effectively[80].

---

[78] *Lim, supra* note 2 at 83.

[79] Personal Digital Assistant is a term for any small mobile hand-held device that provides computing and information storage and retrieval capabilities for personal or business use, often for keeping schedule calendars and address book information. See Margaret Rouse, "Personal Digital Assistant (PDA)" (June 2007) online: <http://searchmobilecomputing.techtarget.com/definition/personal-digital-assistant>; US Federal Aviation Administration, Personal Digital Assistants (PDAs) and Records (9 January 2012) online: <https://www.faa.gov/about/initiatives/records/faq/personal_digital_assistants/>.

[80] Tim Erlin, "Hacking Aviation Technology: Vulnerability Disclosure and the Aviation Industry", Tripwire (30 April 2015) online: <http://www.tripwire.com/state-of-security/security-data-protection/security-hardening/hacking-aviation-technology-vulnerability-disclosure-and-the-aviation-industry/>.

Aviation is not the only industry in this situation, the automobile and banking industry are some of the business also at risk of a cyber-attack since the operational technology is being integrated or replaced with more IT components. The banking or financial industry has a great deal of similarities with the aviation industry since both industries are highly regulated, their operations are costly and itself carry multiple risks, in case of an accident the losses can be catastrophic and it can compromise the consumer confidence, and in some cases, the industry can be held legally responsible[81]. Nevertheless, the banking industry, in its vast majority, has implemented a solution to address and mitigate a cyber-attack through "cyber risk management", which is the coordinated management of intelligence, technology, and business operations to effectively manage an organization's business information assets to prevent unwanted consequences. It is the process by which a business protects its critical assets and reputation from external and internal threats from individuals or organizations, but it is not limited to technical measures[82]. This process is divided in five steps:

i) Identify the internal al external cyber risks;

ii) Protect the organizational systems, assets, and data;

iii) Detect system intrusions, data breaches, and unauthorized access;

iv) Respond to a potential cybersecurity events; and

v) Recover from a cybersecurity event by restoring normal operations and services[83].

---

[81] Just as a financial crisis can affect a nation financial stability, so it can cause an aviation accident. For instance, the terrorist attack to the World Trade Center in New York, US on September 11, 2001 caused an economic impact of $123 billion USD. See *Dempsey*, *supra* note 71 at 93; Shan Carter & Amanda Cox "One 9/11 Tally: $3.3 Trillion" , The New York Times (8 September 2011), online: http://www.nytimes.com/interactive/2011/09/08/us/sept-11-reckoning/cost-graphic.html?_r=0.

[82] PricewaterhouseCooper United States, "Threat smart: Building a cyber resilient financial institution" (October 2014), online:<https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/pwc-cyber-resilient-financial-institution.pdf>

[83] Johan W. Ryan, "101 Cybersecurity. A Resource Guide for Bank Executives. Executive Leadership of Cybersecurity", (Guide paper issued at the Conference on State Bank Supervisors (CSBC) in Washington D.C., 17 December 2014), online:

Thus, the way the banking industry is addressing cybersecurity is primarily dealing with risk management by minimizing the risk through smart and homologize practices, ensuring the systems are properly configured, patched and audited, and also by ensuring the workforce is properly trained and regularly tested.

Since the banking and the aviation industry share similar risks, it would be reasonable if the aviation industry implements the cyber risk management process in order to effectively address cybersecurity to mitigate and to reassess all facets of their business establishing internal protocols to effectively manage the threats.

3.2 Incidents in civil aviation related with cybersecurity

As above-mentioned, today civil aviation depends heavily on computer-based systems and IT systems, and this dependency will only continue to grow as it facilitates and improves civil aviation activities[84]. However, with the implementation of these technologies there is also cyber security breaches or threats, such as computer viruses and more malicious deliberate attacks on computer systems by hackers. The fact that terrorists are becoming more sophisticated and equally *au fait* with the use of computer-based and IT systems, also makes cyber security the next frontier of threats and challenges to civil aviation operations[85]. The following incidents demonstrate that the civil aviation system is vulnerable to cyber threats:

- The Internet attack in 2006 that forced the US FAA to shut down some of its air traffic control (ATC) systems in Alaska[86]. The attack primarily disrupted the mission-support which

<https://www.csbs.org/CyberSecurity/Documents/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf >

[84]"NextGen", United States Federal Aviation Administration (24 July 2016), online: <"NextGen"https://www.faa.gov/nextgen/>

[85] *Lim, supra* note 2 at 84.

[86]Siobhan Gorman, "FAA's Air-Traffic Networks Breached by Hackers", The Wall Street Journal (7 May 2009), online: <http://www.wsj.com/articles/SB124165272826193727>

is the technical services that promotes efficiency and effectiveness of an aircraft in the US airspace according to National Airspace System (NAS)[87];

- The crash of Spanair flight 5022, a McDonnell Douglas MD82, just after take-off in Madrid-Barajas Airport on August 20 2008, killing 154 people, where the Civil Aviation Accident and Incident Investigation Commission of Spain, reported that the crash occurred because the central computer system used for monitoring technical problems on board the aircraft was infected with malware[88]. The infected computer failed to detect three technical problems with the aircraft, which if detected, may have prevented the plane from taking off[89]. Additionally, U.S. National Transportation Safety Board reported in a preliminary investigation that the plane had taken off with its flaps and slats retracted — and that no audible alarm had been heard to warn of this because the systems delivering power to the take-off warning system failed[90];
- The attack on an FAA computer in February 2009, where hackers allegedly obtained access to personal information on 48,000 past and present FAA employees[91];
- The alleged cyber-attack that led to the shutdown of the passport control systems at the departure terminals at Istanbul Atatürk and Sabiha Gökçen airports in July 2013, causing many flights to be delayed[92];

---

[87] NAS is the different flight rules that apply to each aircraft which might contain flight information, regulation, policies and procedures to flight safety. Since each aircraft has a classification provided by the FAA, depending on the class and flight conditions, the ATC will give instructions to the pilot in command in order to take off, during the flight and until the aircraft lands.

[88] *Lim*, *supra* note 2 at 84.

[89] Leslie Meredith, "Malware implicated in fatal spainair plane crash- computer monitoring system was infected with a Trojan horse, authorities say", NBC News (20 August 2010), online: <http://www.nbcnews.com/id/38790670/ns/technology_and_science-security/t/malware-implicated-fatal-spanair-plane-crash/#.V3b3IZMrL3A>

[90] National Transportation Safety Board Federal Aviation Administration, Safety Recommendation, 20594 (17 August 2009) online: <http://www.ntsb.gov/safety/safety-recs/recletters/A09_67_71.pdf>

[91] *Gorman*, *supra* note 86.

- The alleged cyber-attack that involved malicious hacking and phishing targeted at 75 airports in the US in 2013[93]; and
- The operations disruption on June 21, 2015 at Warsaw Chopin Airport by what LOT Polish Airlines described as a cyber-attack on flight-planning computers. Ten flights were canceled and others were grounded for several hours affecting 1,400 passengers[94].

As a different example of possible cyber threats, two different publications have shown the vulnerabilities that exist in civil aviation when it comes to computer-based systems or IT systems. The first publication was performed by the Financial and Information Technology Audit in 2009; according to the Homeland Security Presidential Directive (HSPD), which designates ATC systems as part of the US critical infrastructure due to the important role that aviation plays in fostering and sustaining the national economy and ensuring citizens' safety and mobility. The HSPD requires that the US DOT[95] ensure that the ATC system is protected from both physical and cybersecurity threats to prevent disruption in air travel and commerce[96]. The need to protect the ATC systems raised since the FAA has increasingly turned toward the use of commercial software and Internet Protocol[97]-based technologies to modernized the ATC system.

---

[92] Pierluigi Paganini, "Istanbul Ataturk International Airport Targeted by a Cyber Attack" *Security Affairs* (28 July 2013), online: <http://securityaffairs.co/wordpress/16721/hacking/istanbul-ataturk-international-airport-targeted-by-cyber-attack.html>

[93] *Lim, supra* note 2 at 84.

[94] "Hackers ground 1,400 passengers at Warsaw in attack on airline's computers", The Guardian (15 June 2015) online: <https://www.theguardian.com/business/2015/jun/21/hackers-1400-passengers-warsaw-lot>.

[95] The FAA was created in 1958 through the Federal Aviation Act. It is an independent federal aviation agency that promotes safety and efficiency use of the US airspace. In the other hand, the US DOT is the economic authority when it comes to aviation matters.

[96] Federal Aviation Administration, Review of the Web Applications Security and Intrusion Detection in Air Traffic Control Systems, Report Number: FI-2009-049 (4 May 2009) at 1, online: https://www.oig.dot.gov/sites/default/files/ATC_Web_Report.pdf.

[97] Internet Protocol is a communications standard describing how data are sent from one computer to another over the Internet.

While use of the commercial IP (IP) products, such as web applications[98], has simplify the FAA to efficiently and widely collect information to facilitate ATC services, it inevitably poses a higher security risk to ATC systems than when they were developed primarily with a proprietary software. The audit conclusion states that "the web application used in supporting ATC systems operation [were] not properly secure to prevent attacks or unauthorized access. The FAA has not established adequate intrusion-detection capability to monitor and detect potential cybersecurity incident at ATC facilities. […] The public could gain unauthorized access to information stored on web application computers and these vulnerabilities could allow attackers to compromise FAA user computers by injecting malicious code into computers"[99].

The second publication that shows an example of a possible upcoming cyber threat, is the report from the US Government Accountability Office (GAO) in 2015 title "FAA Needs a More Comprehensive Approach to Address Cybersecurity as Agency Transitions to NexGen"[100]. GAO pointed out that NexGen remains with significant security-control weaknesses that threaten the FAA's ability to ensure the safe and uninterrupted operation of the national airspace system. The major critic by this organization is that the FAA has not developed a cybersecurity threat model, GAO recommended that such a model is needed to identify potential threats to information systems, and as a basis for aligning cybersecurity efforts. While FAA has taken some steps toward developing such a model, it has no plans to produce one, and has not assessed the funding

[98] A web application is a software program running on a web server that can be accessed by using a web browser. A web server may host multiple web applications.

[99] *Federal Aviation Administration, supra* note 96 at 3.

[100] United States Government Accountability Office, Report to Congressional Requesters, GAO-15-370, "Air Traffic Control - FAA Needs a More Comprehensive Approach to Address Cybersecurity as Agency Transitions to NextGen" (April 2015) online: <http://www.gao.gov/assets/670/669627.pdf> at 1.

or time that would be needed to do so[101]. Similar conclusions have been reached for SESAR by a study performed by Helios in the EU[102].

4. EFFORTS TAKEN TO ADDRESS CYBER SECURITY THREATS

4.1 Efforts pursued by ICAO

As it was previously discussed, Annex 17 of the CC –entitle Safeguarding International Civil Aviation Against Acts of Unlawful Interference- was adopted by ICAO in 1974 and addresses aviation security. This Annex, requires that each member State "have as its primary objective the safety of passengers, crew, ground personnel and the general public in all matters related to safeguarding against acts of unlawful interference with civil aviation."[103] It also "binds [member States] to establish a national civil aviation security program[104] and to create a governmental institution, dedicated to aviation security that would develop and implement regulations to safeguard aviation[105]. Member States must also develop a security training program,[106] share aviation threat information,[107] and otherwise cooperate with other States on their national security programs[108]. The inclusion of several of these requirements in Annex 17, means their applicability extends to many nations that never ratified one or more of the multilateral conventions addressing aviation security since several of this requirements try to reaffirm the

---

[101] *Ibid* at 23.
[102] European Union SESAR, Study Release, "SESAR Strategy and Management Framework Study for Information Cyber-Security Application to System Wide Information Management Research and Development" (September 2015), online: <http://www.sesarju.eu/newsroom/all-news/study-details-rd-roadmap-atm-cyber-security>
[103] Safety, Safeguarding International Civil Aviation Against Acts of Unlawful Interference, ICAO, Ninth Edition, Annex 17 to the Convention on International Civil Aviation (2011), § 2.1.1 at 19.
[104] *Ibid* at 21 § 3.1. Airports and aircraft operators must also establish security programs and § 3.2.1 and §3.3.1 at 20.
[105] *Ibid* at1 9 § 2.1.2 and 3.1.2 – 3. States must also establish a national aviation security committee that coordinates security activities between various governmental institutions. See *supra* note 103 at 21 § 3.1.6
[106] Each contracting State must establish a security training program. See *ibid*, § 3.1.7. They are also obliged to cooperate with other States in the development and exchange of training program information. See *ibid*, § 2.3.3.
[107] *Ibid* at 19 § 2.3.4.
[108] *Ibid* at 19 § 2.3.2.

provisions of the Tokyo, the Hague, and the Montreal Conventions [109]. Some other specifications of Annex 17 recognize that it is not possible to achieve absolute security. Nevertheless, States must ensure that the safety of passengers, crew, ground personnel and the general public is a primary consideration in the safeguarding action which they initiate[110].

Furthermore, Annex 17 has been maintained under constant review to ensure that the specifications are current and effective. It has been amended and updated on several occasions to reflect the practical experience and the changing nature of the threats to civil aviation[111]. Amendment 12 was the first to include provisions to strengthen SARPs[112] in order to address new and emerging threats to civil aviation such as cyber threats. It states that "each contracting State should develop measures in order to protect information and communication technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation"[113]. Additionally, on February 2014 the ICAO Council adopted two Recommended Practices (RP) to Annex 17 which became effective on 17 November 2014. These two provisions stipulate that each Contracting State should, in accordance with the risk assessment carried out by its relevant national authorities, ensure that measures are developed in order to protect critical information and communications technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation[114]. The new provisions also exhort

[109] *Dempsey, supra* note 71 at 31.
[110] *Dempsey, supra* note 71 at 128.
[111] *Ibid* at 129.
[112] SARPs are intended to assist States in managing aviation safety risks, in coordination with their service providers. Given the increasing complexity of the global air transportation system and its interrelated aviation activities required to assure the safe operation of aircraft, the safety management provisions support the continued evolution of a proactive strategy to improve safety performance. ICAO, "SARPs - Standards and Recommended Practices" *ICAO Safety*, online: <http://www.icao.int/safety/safetymanagement/pages/sarps.aspx>.
[113] Safety, Safeguarding International Civil Aviation Against Acts of Unlawful Interference, ICAO, Ninth Edition, Annex 17 to the Convention on International Civil Aviation (2011) at 29 § 4.9.
[114] *Ibid* at 29 § 4.9.1.

States that they should encourage entities involved with or responsible for the implementation of various aspects of the national civil aviation security programme to identify their critical information and communications technology systems, including threats and vulnerabilities there to, and develop protective measures to include, inter alia, security by design, supply chain security, network separation, and remote access control, as appropriate[115]. Thus, amendment 12 to Annex 17 introduced cyber security provisions, while amendment 14 ensured a risk-based cyber security regime takes place. Scholars like Ruwantissa Abeyratne have criticized ICAO's job because it should provide strategic direction, which involves ICAO's assisting member States and industry towards employing new and innovative security measures, including and not limited to the use of advanced technology. Instead ICAO has come up with two RP on what States ought to be doing by themselves. This raises the question as to how States could encourage each other to adopt measures without any assistance by ICAO with regard to the introduction of new and innovative security measures"[116]. Also whether ICAO, as UN specialized agency for aviation institution, should play the role it has been assigned in cybersecurity in a perspective manner[117]. Although, ICAO has been a non-prescriptive because SARPs are non-binding, since States can file differences if they are unable to comply for on the basis of insufficient human or financial resources or its unique geographic of technological characteristics, but to some extent, at least a difference filed would provide some indication as to why a State does not agree to implement a Standard and therefore have some degree of persuasive authority. Moreover, ICAO should not just give recommendations on what States ought to be doing by themselves in terms of cybersecurity, since historically SARPS have taken

[115] *Ibid*, Recommendation 4.9.2; Ruwantissa Abeyratne, "Aviation Cyber Security: A Constructive Look at the Work of ICAO" (The Netherlands: Kluwer Law International 2016) 41 Air & Space Law at 33.
[116] *Ibid* at 34.
[117] *Jeyakodi, supra* note at 9.

the form of binding legal rules established by international treaty or national legislation, and, in these cases, the standards constitute "hard law"[118].

ICAO's main goal should be focusing on creating standards instead of recommendation and to start playing a pro-active role as an institution instead of reactive[119], since the key to achieve cybersecurity in civil aviation is through standardization and harmonization of the law. Neither international nor domestic law will effectively deter cyber security in civil aviation without worldwide cooperation to strengthen airport and aircraft security, prosecute terrorists, and impose meaningful sanctions on States that provide safe havens for, or support, hackers [or cyber threats] and other aerial terrorists[120].

In 2011 ICAO developed the guidance material on mitigating cyber threats for aviation security, airports and aircraft operators. Chapter 18 of Document 8973 (ICAO, 2011) elaborates on basic measures which organizations should take to mitigate cyber threats to critical aviation information and communication technology systems. Contracting States and air navigation service providers (ANSPs) should also take note of the need to comply with Standard 3.5 of Annex 17 (ICAO, 2013a), which states that "each Contracting State shall require ANSPs operating in that State to establish and implement appropriate security provisions to meet the requirements of the national civil aviation security programme of that State." The ICAO's Document 9985 (ICAO, 2013b) provides guidance on the development of adequate requirements and measures for the protection of air navigation services from both physical and cyber-attacks[121].

---

[118] *Morais, supra* note 28 at 780-81.
[119] *Dempsey, supra* note 71 at 9.
[120] Paul Stephen Dempsey, *Law & Foreign Policy in International Aviation* (Ardsley: Transnational Publishers Inc. 1987) at 349-82.
[121] Martin Siu, Daniel Goh & Cheri Lim, "Aviation Cyber Security: A New Security Landscape" Journal of Aviation Management (2014) at 78 online:

Another important step towards cybersecurity was the agreement signed in 2013 by ICAO, the Airports Council International (ACI), the Civil Air Navigation Services Organization (CANSO), the International Air Transport Association (IATA) and the International Coordinating Council of Aerospace Industries Associations (ICCAIA). It established an Industry High-level Group (IHLG) as a mechanism for high-level cooperation on issues of common interest and importance, which includes cybersecurity[122]. The IHLG established a "roadmap" and determined that cybersecurity in civil aviation was a high priority transversal issue requiring collective alignment. ICAO claims that this cooperation enables the participating parties to draw together all elements of the aviation industry to ensure a shared vision, strategy and set of commitments to tackle the cyber threats[123].

Thanks to the IHLG, a new working paper dealing solely with cyber security is being draft by the ICAO Council for the 39th Assembly in September 2016. Even though this paper is not official yet, the draft recognizes the job performed by the IHLG to promote a consistent and coherent approach in managing cyber threats and risks. Additionally, determines that ICAO and the members of the IHLG developed a draft resolution that aims at addressing cybersecurity in civil aviation through a horizontal, cross cutting and functional approach. The objectives are to reaffirm the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyber threats. Also obtain global commitment to action by ICAO, its member States and industry stakeholders, with a view to collaboratively and systemically addressing cybersecurity in civil aviation and mitigating the associated threats and risks[124]. The information

---

<http://www.saa.com.sg/saaWeb2011/export/sites/saa/en/Publication/downloads/AviationCyberSecurity_A_NewSecurityLandscape.pdf >.

[122] IATA, Fact Sheet Cybersecurity Three-Pillar Strategy (June 2016) Online: <https://www.iata.org/pressroom/facts_figures/fact_sheets/Documents/fact-sheet-cyber-security.pdf>

[123] *Abeyratne*, *supra* note 115 at 34.

[124] ICAO, Assembly - 39th Session, Working Paper Assembly, Agenda Item 16: Aviation Security – Policy Addressing Cybersecurity in Civil Aviation A39-WP/17 EX/5../5/16 (2016) [unpublished] at 1.

upon which this statement relies has not yet been made available publicly. However, it is an important step towards cybersecurity since it involves all the different stakeholders in civil aviation and urge them to work collaboratively towards the development of an effective and coordinated global framework for civil aviation to address the challenges of cybersecurity, along with short-term actions to increase the resilience of the global aviation system to cyber threats that may jeopardize the safety of civil aviation[125]. Plus, it instructs the Secretary General of ICAO to assist and facilitate States and industry in taking above-mention actions and ensure that cybersecurity matters are fully considered and coordinated across all relevant disciplines within ICAO.

4.2. Efforts Pursued by Other Organizations

4.2.1 International Air Transport Association (IATA)

IATA it is the biggest passenger and cargo airline conglomerate and relies on computer systems extensively in their ground and flight operations. Thus, this association is fully aware of the cybersecurity challenges faced by the aviation industry and understands the need for industry coordination and cooperation to address the constant cyber threats. It is why IATA has developed a three-pillar strategy to understand, define and assess the threats and risk of attacks, the basis for appropriate regulation and the mechanisms for increased cooperation throughout the industry with the support of governments. The three-pillar strategy is based first on risk management, second on advocacy and reporting and third on communication. Additionally, IATA also developed an aviation Cyber Security Toolkit to assist airline in raising awareness,

[125] *Ibid* at 4.

understanding and better defining the cyber risks to their organizations[126]. All of these programs can be purchase by the airlines.

4.2.2 International Federation of Airline Pilots Associations (IFALPA)

In 2013, IFALPA identified as a significant and emerging threat the possibility of a cyber-attack, reason why this association issued a paper that articulated the threat of cyber security attacks against aircraft, ground and other critical facilities and infrastructure supporting civil aviation operations[127]. This paper also includes measures that can be taken to enhance the security of an entity's computer software and hardware – including data protection, access control, physical separation of sensitive systems, training of flight crew, governance and control, protection of air traffic services and aircraft design and operation[128].

4.2.3 American Institute of Aeronautics and Astronautics (AIAA)

In 2013, AIAA issued a paper called "The Connectivity Challenge: Protecting Critical Assets in a Networked World. A Framework for Aviation Cybersecurity". It identifies that the aviation industry is expanding, changing, becoming increasingly connected and introducing new technologies that benefit the users and the stakeholders. However, it also recognizes that without robust cybersecurity measures in place the use of IT systems is a risk to the industry, since it can become a cyber threat. Thus, the AIAA developed a general framework for aviation cybersecurity with different requirements that the stakeholders need to implement in order to

---

[126] IATA, Aviation Cyber Security Toolkit, 2nd edition (July 2015), online: <http://www.iata.org/publications/Pages/cyber-security.aspx>.

[127] IFALPA, Cyber threats: who controls your aircraft? 14POS03, (2 June 2013) at 2 online: <http://www.ifalpa.org/downloads/Level1/IFALPA%20Statements/Security/14POS03%20-%20Cyber%20threats.pdf.>.

[128] *Lim, supra* note 2 at 87.

ensure that this mode of transportations keeps being one of the safeties. These requirements are:

a) Establish common cyber standards for aviation systems;

b) Establish a cybersecurity culture;

c) Understand the threat;

d) Understand the risk;

e) Communicate the threats and assure situational awareness;

f) Provide incident response;

g) Strengthen the defensive system;

h) Define design principles;

i) Define operational principles;

j) Conduct necessary research and development; and

k) Ensure that government and industry work together.

4.2.4 Civil Air Navigation Services Organization (CANSO)

In 2014, CANSO developed a cyber security and risk assessment guide. It provides "air navigation service providers with an introduction to cyber security in air traffic management, including the cyber threats and risks and motives of threat actors, as well as some considerations to managing cyber risks and implementing a cyber security programme"[129]. One of the main objectives of this guide is to help organize efforts for responding to cyber threats applying an approach that divides the ongoing security process into four complementary areas: plan, protect, detect, and respond. This quadrant includes the creation of design strategies and an enterprise-wide or overall system-of-systems architecture that enhances security, provides agility, and

[129] CANSO, Cyber Security and Risk Assessment Guide, (June 2014) at 4 online: < https://www.canso.org/canso-cyber-security-and-risk-assessment-guide >.

reduces overall costs. To effectively implement the guide, organizations must develop policy and fund security solutions throughout the enterprise with total management commitment.

Throughout the guide CANSO makes sure that the air navigation services providers address cyber security proactively in terms of security, through awareness of the possible cyber threat in civil aviation and risk assessment to determine the greatest risk making it sure that the infrastructure of ATC systems is itself resilient to attacks, but also that the system will provide information that can be used by other organizations to act and protect air transport and the aviation system as a whole.

4.2.5 International Coordinating Council of Aerospace Industries Associations (ICCAIA)

ICCAIA has not issued its own paper related with cyber security but, as a member of the IHLG, has discussed and worked on key topics for the aviation industry co-operation such as cyber security. ICCAIA participation on these topics has created a positive outcome with agreements on a number of specific actions for joint effort and advocacy. Furthermore, ICAO has granted observer status to ICCAIA in many of the ICAO's Committees and Panels including Air Navigation Commission[130].

4.2.6 Aircraft Manufacturers

Developing commercial airplane systems involves a structured and highly complex design and verification process, from the component level to the system and airplane level. With millions of parts on each airplane, it is critical that manufacturers ensure that the design process also address

[130] ICCAIA, International Coordinating Council of Aerospace Industries Associations, (August 2016), online: <http://www.iccaia.org/about-us>

the evolving nature of cyber threats[131], especially when interconnectedness can potentially provide unauthorized remote access to aircraft avionics systems, in particular to the newer planes such as the Boeing 787 Dreamliner, and long-haul Airbus models such as the A350 and A380.[132]Aircraft design must consider capabilities, threat surfaces, and cost of mitigation strategies for the lifespan of the aircraft. Secure by default must remain the industry standard. [133]. The four major aircraft manufactures (Boeing, Airbus, American Technologies and Lockheed Martine[134]) have taken some kind of appropriate measures in terms of cyber security to mitigate the potential risks to the IT technology and other operations. Thus, Boing has created Cyber-Range-in-a-Box (CRIAB) which is a compact system used to support the development, test, and experimentation of cyber tools and techniques, as well as to train cybersecurity personnel[135]. Airbus has developed Keelback Net, a service for detection and advanced investigation of sophisticated cyber-attacks. Lockeed Martine has created the Cyber Kill Chain which enhance visibility into an cyber-attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures[136]. However, the fact that the aircraft manufactures develop cybersecurity measures does not warranty a cyber-attack will not happen, it is necessary that the stakeholders start preforming a holistic approach to cyber security matters instead of each manufacturer, airline or State acting independently.

---

131 *Jeyakodi*, *supra* note 9 at 3.
132 United States Government Accountability Office, *supra* note 100 at 24.
133 *AIAA*, *supra* note 75 at 10.
134 *Revenue of the worldwide leading aircraft manufacturers and suppliers in 2014 (in million U.S. dollars)* (June 2016), *online:* The Statistic Portal <http://www.statista.com/statistics/264366/revenue-of-the-worldwide-leading-aircraft-manufacturers-and-suppliers/>
135*Cybersecurity & Information Management*, (June 2016), online: Boeing <http://www.boeing.com/defense/cybersecurity-information-management/>.
136*Cyber Kill Chain – Proactively detect persistent threats*, (Junes 2016) online: Lockheed Martine <http://cyber.lockheedmartin.com/solutions/cyber-kill-chain> .

4.2 Efforts Pursued by Leading State in Civil Aviation

4.2.1 United States

In 2013, the US president Barack Obama expressed in State of the Union speech that "America must also face the rapidly growing threat from cyber-attacks [. . .] our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy[137]". The US president concern related with cyber security and the safety of civil aviation have been addressed by the FAA with cyber security regulations for airplane manufacturers, amid warnings that the criss-crossing of onboard networks poses risks to flight safety[138], and taking into account the criticism from the US GAO report, related with NexGen and the FAA's ability to ensure the safe and uninterrupted operation of the national airspace system[139] as well as ICAO's cyber security guidance. The FAA has created an Aviation Rulemaking Advisory Committee (ARAC) to develop a comprehensive cybersecurity protection for aircraft, seeking to cover everything from the largest commercial jetliners to small private planes[140]. However, the fact that the FAA has taken cyber security measures related with civil aviation will not make this organization immune to a cyber-attack, the FAA needs to be proactive and seeking the best aviation risk management.

---

[137] United States, Press Release, "Seeking Comments on the Preliminary Cybersecurity Framework" (29 October 2013) online: <https://www.whitehouse.gov/blog/2013/10/29/seeking-comments-preliminary-cybersecurity-framework>.

[138]Aliya Sternstein, "FAA Working on New Guidelines for Hack-Proof Planes", Nexgov (4 March 2016) online: <http://www.nextgov.com/cybersecurity/2016/03/faa-has-started-shaping-cybersecurity-regulations/126449/>.

[139]United States Federal Aviation Administration, Document Information, 1370.47, "FAA Cybersecurity Roles and Responsibilities" (24 December 2015) online: <https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/1028713>.

[140] Andy Pasztor, "U.S. Panel Aims to Shield Planes From Cyberattack", The Wall Street Journal (29 June 2015) online: <http://www.wsj.com/articles/u-s-panel-aims-to-shield-planes-from-cyberattack-1435537440>.

Furthermore, the US has created the Aviation Information Sharing and Analysis Center (A-ISAC). A-ISAC is a focal point created in 1998 for relevant security information sharing for the aviation sector. It was created to enhances the ability of our sector to prepare for and respond to security threats, vulnerabilities, and incidents so that aviation sector firms can best manage their business risks[141]. Its members include airlines, airports, manufacturers equipment suppliers, service providers, technology providers, infrastructure providers and/or general aviation entities from where it gathers threat, vulnerability and risk information about security risks facing the aviation sector around the world.

In terms of enacted laws related to tackle a cyber-attacks, the US federal government created the US Patriot Act of 2001 and Homeland Security Act of 2002[142].

It is also worth mentioning that the US has been one of the leading countries brining forward the cyber security in civil aviation as a threat in ICAO's agenda.

4.2.2 European Union

EU is aware that cyber security is essential to keep the online economy running and to ensure prosperity. The EU has been working on a number of fronts to ensure cybersecurity in civil aviation in Europe by raising the capabilities of the Member States to implementing the international cooperation on cybersecurity and cybercrime[143]. Created by the Regulation (EC) No.216/2008 EASA is the agency in charge civil aviation cyber security always promoting the highest common standards of safety and security. In 2015, the Commission to the European Parliament and the Council, the European Economic and Social Committee, and the Committee

[141] Aviation Information Sharing and Analysis Center, A-ISAC, online:<http://www.a-isac.com/>

[142] US Homeland Security Act of 2002, Public Law 107–296, 107th Congress Cyber Security Enhancement Act of 2002. 6 USC 145 (2002) at 22 online: <https://www.gpo.gov/fdsys/pkg/PLAW-107publ296/html/PLAW-107publ296.htm>

[143] European Commission, Press Release, "Cybersecurity Strategy for the European Union" (7 June 2016) online: <https://ec.europa.eu/digital-single-market/en/cybersecurity>.

of the Regions suggested to modified the aviation strategy for Europe recognizing that "high aviation security standards are imperative for the functioning and competitiveness of the air transport system"[144] including cybersecurity risks. Thus, commanded EASA to cooperate in two important matters. First, to revise Basic Regulation for common rules in the field of civil aviation safety, replacing the current Regulation (EC) No 216/2008. Second, revised European Aviation Safety Programme document, describing the way in which safety is managed in Europe today. Additionally, EASA in May 2016 has acknowledged "the necessity for to mitigate the safety effects stemming from cybersecurity risks due to acts of unlawful interference with the aircraft on-board electronic networks and systems"[145]. It also has taken into account the FAA recommendation from ARAC regarding rulemaking, policy, and guidance on best practices for airplanes seeking cybersecurity protection. Thus, the EU through EASA will start reviewing its certification activities of the "Security Assurance Process to isolate or protect the Aircraft Systems and Networks from internal and external Security Threats" and will also start working on new certifications specifications[146]. Additionally, since the EU is also developing SESAR the satellite-based navigation communication, it needs to start "putting in place a structure to alert airlines of cyber-attacks", as EASA director Patric Ky expressed in a press release[147]. A study completed by Helios in 2015, reveled it is necessary to introduce a holistic approach to cyber-security and to develop a comprehensive response to cyber threats, which includes a roadmap

---

[144] EC, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions an Aviation Strategy for Europe, [2005] OJ, Document 52015DC0598, online: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52015DC0598>

[145] EC, European Aviation Safety Agency, Terms of Reference for a rulemaking task Aircraft cybersecurity 17 May 2016, [2016] OJ, ToR Issue 1 RMT.0648 at 2 online: <https://www.easa.europa.eu/system/files/dfu/ToR%20RMT.0648%20Issue%201.pdf>.

[146] *Ibid* at 3.

[147]Rene Millman, "Head of European aviation body EASA warns of cyber-attack risk against aircraft", Airportwatch (13 October 2015) online: <http://www.airportwatch.org.uk/2015/10/head-of-european-aviation-body-easa-warns-of-cyber-attack-risk-against-aircraft/>.

for increasing the maturity of cybersecurity and cyber-resilience processes in preparation for SESAR 2020[148].

In terms of enacted laws related to tackle a cyber-attacks related with civil aviation, the EU has developed two Directives. First the 2002 ePrivacy Directive, whereby providers of electronic communications services must ensure the security of their services and maintain the confidentiality of client information. Second the 2013 Directive, related with attacks against information systems, which aims to tackle large-scale cyber-attacks by requiring EU Member States to strengthen national cyber-crime laws and introduce tougher criminal sanctions[149].

It is also worth mentioning that the EU members' states have been one of the leading countries brining forward the cyber security issue in civil aviation as a threat in ICAO's agenda.

4.2.3 Other Countries

Another leading country in civil aviation is the United Arab Emirates (UAE). In 2015 it organized workshops related with the security and safety of civil aviation in the country. The workshop was "intended to showcase latest technologies and certified software in the capacity of maintaining the highest levels of safety and reliability, as well as the procedures to be taken to raise safety levels, and their expected impact and effectiveness in the near future. The discussions also focused on the most important challenges and opportunities related to the aviation industry and the points that should be the focus of scientific research in this field in the future, in order to improve safety standards and promoting them on a global level."[150] However,

---

[148] *European Union SESAR, supra* note 102.

[149] European Commission, Media Release, "Cybercrime: What's Cybercrime?" (18 April 2016) online: <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm>.

[150] UAE Telecommunications Regulatory Authority (TRA), Press Release, "The TRA's UAE Computer Emergency Response Team (aeCERT) organizes an aviation security workshop" (31 March 2015) online: <https://www.tra.gov.ae/aecert/en/media/news-archive/2015/3/31/the-tras-uae-computer-emergency-response-team-aecert-organizes-an-aviation-security-workshop.aspx>.

there is no laws in place yet that punish cyber-attacks. Additionally, in 2016 UAE signed an agreement between the Telecommunications Authority (TRA), Computer Emergency Readiness Team (aeCERT) and the Dubai Financial Services Authority (DFSA) [151] to jointly promote information security at the DFSA and provide companies with measures to avert all forms of attacks in cyberspace. TRA will provide guidance, education and awareness about online threats, apart from assisting DFSA in protecting their information systems against intrusion, as well as consultation and coordination with all relevant authorities.

Other countries have taken a different approach, although their CAA have not taken security measures directly related with civil aviation. For example, Brazil has enacted a law punishing the manipulation of data by unauthorized public servants[152]. In China the punishment for interfering with computer systems in punishable with imprisonment for 7 years. In India hacking is penalized and the punishment for it is 3 years imprisonment and/or a fine equivalent to 1000 Euros[153], and in Korea the country with the strongest cyber laws, wherein any damage to Critical Information Infrastructure, would attract a 10 year imprisonment and a fine of 100 million Korean currency[154].

5. CONCLUSIONS

The civil aviation forecast anticipates that air traffic will grow at 4.5 per cent annually, flying 16 billion passengers, requiring dedicated freighter aircraft at a value of US$ 5.2 trillion over the

[151] Aasha Bodhani, "RA, DFSA join forces to promote online security", ITP.net (7 June 2016) online: <https://www.itp.net/mobile/607846-tra,-dfsa-join-forces-to-promote-online-security>.
[152] Brazil, Law No. 9.983 of 7 July 2000, Insertion of fake data into systems of information, online: <http://www.cybercrimelaw.net/Brazil.html>.
[153] *Jeyakodi, supra* note 9 at 14.
[154] *Ibid* at 14.

next 20 years[155]. Furthermore, the global aviation industry relies on computer based and IT systems for their daily operations, fact that it is likely to increase since aviation is moving towards device digitalization, increasing the use of IoT. Civil aviation worldwide unquestionably needs to keep up with the use of more computer-based and IT systems since it has brought innovation and efficiency, including systems that enhance safety and security[156]. However, the use of computer-based systems and IT systems raises concerns related with security threats from a cyber-attack since "more modern airports are developed, new aircraft introduced into service and stakeholders seek to meet the growing demand of more IT-savvy passengers with new passenger facilitation processes using digital and IT-based systems"[157].

Currently, none of the ICAO safety regulations, which focus on preventing accidental harm, deal with cybersecurity provision. Neither the different standards of safety developed and implemented by the US nor EU banding the State or airline respectively, required that cybersecurity measures. Moreover, it is possible to say that cyber interference, cybercrime and cyber terrorism against air transport are all offenses against civil aviation that end up in unlawful interference with civil aviation, which has been adopted in three different treaties -the Tokyo Convention of 1963, The Hague Convention of 1970 and the Montreal Convention of 1971- under the auspices of ICAO. However, none of these conventions refer, directly or indirectly, to cyber security leaving a cybercrime against civil aviation in a normative limbo and the possibly of no consequence.

---

[155] Global Market Forecast 2016-2035 – Mapping Demand, online: Airbus <http://www.airbus.com/company/market/global-market-forecast-2016-2035/>.
[156] *Lim, supra* note 2 at 81.
[157] *Ibid* at 81.

Although, different efforts to deal with cybersecurity in civil aviation have been addressed by ICAO SARPs in diverse opportunities, such as the different amendment of Annex 17 in particular the measures related with cyber threats, Chapter 18 of Document 8973 related with basic measures to mitigate cyber threats to critical aviation information and communication technology systems, and Document 9985 as guidance material on the development of adequate requirements and measures for the protection of air navigation services from both physical and cyber-attacks. It is undeniable that many States tent to consider these provisions issued by ICAO as "soft law". However, as professor Michel Milde has stated "while it may be argued that SARPs represent only "soft law" they cannot be disregarded with impunity. A phrase has been coined that the force of the SARPs could be compared with that of the "law of gravity": compliance is simply unavoidable in practice and non-compliance would have serious consequences."[158] At the moment not many nations have implemented cybersecurity measures related with civil aviation in their national legislations.

The draft proposed by IHLG dealing solely with cybersecurity for the 39 Assembly of ICAO has not enter into force, but it would be a great achievement in terms of cybersecurity. It promotes a consistent and coherent approach in managing cyber threats, risks and would address cybersecurity in civil aviation through a horizontal, cross cutting and functional approach. The objectives reaffirm the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyber threats and obtain global commitment to action by ICAO, its member States and industry stakeholders, with a view to collaboratively and systemically addressing cybersecurity in civil aviation and mitigating the associated threats and risks. However, at this writing this draft has not been accepted by ICAO the Assembly, it would

[158] *Milde, supra* note 24 at 164.

be necessary to wait until September 27, 2016 to see what the Assembly decides. Meanwhile the provisions issued by ICAO do not have enough teeth to really address the cybersecurity threat and risks, and it is likely that if ICAO emphasize in cybersecurity as a safety and security measure, many countries will start implementing these provision nationally but other will not for lack of expertise and/or resources.

Furthermore, as many of the different stakeholders in civil aviation have instigated in their papers or guides, such as CANSO guidance material, which provides effective cyber security risk managements through the four complementary areas; plan, protect, detect, and respond. It suggest how air navigation services providers should address cyber security proactively in terms of security, through awareness of the possible cyber threat in civil aviation and risk assessment to determine the greatest risk. It makes sure that the infrastructure of ATC systems is itself resilient to attacks, but also that the system will provide information that can be used by other organizations to act and protect air transport and the aviation system as a whole. Additionally, AIAA also recognizes that without robust cybersecurity measures in place the use of IT is a risk to the industry, since it can become a cyber threat. Thus, the AIAA general framework for aviation cybersecurity with different requirements for stakeholders to implement in order to ensure that aviation sector keeps being one of the safeties. However, it is necessary that the aviation industry address cybersecurity with a paradigm shift since it cannot longer wait until a cyber-attack, or threat with catastrophic implication happens, for the stakeholders to react against it. A cybersecurity attack can lead to passengers deaths and damages, terrible infrastructure indemnities and billions of dollars in economic losses; cyber terrorism may replace the hijacker and bomber and become the weapon of choice on attacks against the aviation community[159].

[159] Ellie Zolfagharifard, "'Hackers Are a Serious Threat to Aircraft Safety': Aviation Chiefs Warn of the Devastating Consequences of a Cyber-Attack", Mail Online (11 December 2014) online:

Thus, the paradigm shift means that stakeholders need to start implementing proactive measures in order to safeguard civil aviation so it can remain the safest mode of transportation[160].

Cybersecurity in civil aviation will be achieve when the stakeholders and ICAO learn how to manage risk and maintain a competitive advantage, just as a private company dealing with human resources, finance, operations, infrastructure, etc. cybersecurity should be treated as any other core function within the company, so attention and focus on cyber security efforts and measures can work accordingly with the organization's operations[161] and goals.

Unfortunately, the key to a cybersecurity strategy is cooperation achieved through standardization and harmonization of the law, and this is yet to be achieved in aviation security[162].s Cooperation and participation within civil aviation stakeholders to draw together a share vision, strategy and set of commitment to tackle cyber threats should be address holistically and aim for cyber resilience, just as the banking and financial institutions have worked together to solve cyber threats. Civil aviation and cybersecurity still have a far way to go.

<http://www.dailymail.co.uk/sciencetech/article-2869827/Hackers-threat-aircraft-safety-Aviation-chiefs-warn-devastating-consequences-cyber-attack.html.>.

[160] ICAO, 2011 State of the Global Aviation Safety. A Coordinated, Risk-based Approach to Improving Global Aviation Safety, Special ed (Montreal: ICAO 2011) at 6 online: <http://www.icao.int/safety/documents/icao_state-of-global-safety_web_en.pdf>.

[161] *Lim, supra* note 2 at 89.

[162] *Abeyratne, supra* note 115 at 35.

6. BIBLIOGRAPHY

Legislation

- Airline Deregulation Act of 1978, Pub.L. 95-504 on October 24, (1978).
- International Air Transportation Competition Act of 1979, S.1300 — 96th Congress (1979-1980)
- US Homeland Security Act of 2002, Public Law 107–296, 107th Congress Cyber Security Enhancement Act of 2002. 6 USC 145 (2002)
- US Homeland Security Act of 2002, Public Law 107–296, 107th Congress Cyber Security Enhancement Act of 2002. 6 USC 145 (2002)
- Brazil, Law No. 9.983 of 7 July 2000, Insertion of fake data into systems of information, online: <http://www.cybercrimelaw.net/Brazil.html>.

Secondary Materials

- Abeyratne, Ruwantissa. "Aviation Cyber Security: A Constructive Look at the Work of ICAO" (The Netherlands: Kluwer Law International 2016) 41 Air & Space Law.
- Armitage, Joanne & Roberts, John. "Living with Cyberspace: Technology and Society in the 21st Century" 1st ed (New York: The Athlone Press 2003).
- Broderick, Anthony & Loos, James. "Government Aviation Safety Oversight – Trust, But Verify" (2002) 67 J Air L & Com at 1049.
- Dempsey, Paul Stephen. "Public International Air Law" (Montreal: McGill University 2008) Chapter IV Safety.
- Dempsey, Paul Stephen. "The Role of the International Civil Aviation Organi-zation on Deregulation, Discrimination, and Dispute Resolution" (1987) 52 J Air L & Com at 529.

- Dempsey, Paul Stephen. *Law & Foreign Policy in International Aviation* (Ardsley: Transnational Publishers Inc. 1987).
- Dempsey, Paul Stephen. Thomas, William & Hardaway, Robert. *Aviation Law & Regulation* (United Kingdom: Butterworth Legal Publishers, 1993)
- Havel, Brian F. "In Search of Open Skies" (The Netherlands: Kluwer Law International, 1997).
- Herbert V. Morais, 'The Quest for International Standards: Global Governance vs. Sovereignty" (2002) 50 Kan L Rev 779.
- Herrero, Alvaro. "International joint conference SOCO'13-CISIS'13-ICEUTE'13 - *Advances in Intelligent Systems and Computing International Joint Conference*" (New York: Springer, 2014).
- Huang, Jiefang. "Aviation Safety Through the Rule of Law, ICAO's Mechanisms and Practice" (The Netherlands: Kluwer Law International, 2009).
- Khosrow-Pour, Mehdi. "Encyclopedia of Information Science and Technology, Third Edition" (Hershey: Ideal Group References, 2006).
- Lim, Bernard. "Emerging Threats from Cyber Security in Aviation - Challenges and Mitigations" (2014) Journal of Aviation Management at 85.
- Michael Jennison, "ICAO Adopts Flawed Protocol to Amend the Tokyo Convention of 1963" (2014) 39 McGill Annals of Air & Space Law.
- Milde, Michael. 'Essential Air and Space Law; International Air Law and ICAO" (The Netherlands: Eleven International Publishing, 2008).
- Morais, Herbert V. 'The Quest for International Standards: Global Governance vs. Sovereignty" (2002) 50 Kan L Rev 779.

- Siu, Martin. Goh, Daniel & Lim, Cheri. “Aviation Cyber Security: A New Security Landscape” Journal of Aviation Management (2014) online: <http://www.saa.com.sg/saaWeb2011/export/sites/saa/en/Publication/downloads/AviationCyberSecurity_A_NewSecurityLandscape.pdf >.
- Spinello, Richard A. “Regulating Cyberspace: The Policies and Technologies of Control” (Connecticut: Greenwood Publishing Group, 2002).
- Strate, Lance, "The varieties of cyberspace: Problems in definition and delimitation" (California: Western Journal of Communication 1999
- Strate, Lance. "The varieties of cyberspace: Problems in definition and delimitation" (California: Western Journal of Communication 1999).
- Touhill, Gregory J. & Touhill, C. J. “Cybersecurity for Executives: A Practical Guide” (Hoboken: John Wiley & Sons, 2014)
- Watson, Richard T. “Information Systems” (Georgia: University of Georgia, 2007) at 16 online: <http://www.uky.edu/~gmswan3/777/IS_Book.pdf>.

Articles & Newspapers

- “Hackers ground 1,400 passengers at Warsaw in attack on airline's computers”, The Guardian (15 June 2015) online: <https://www.theguardian.com/business/2015/jun/21/hackers-1400-passengers-warsaw-lot>.
- Bodhani, Aasha. “RA, DFSA join forces to promote online security”, ITP.net (7 June 2016) online: <https://www.itp.net/mobile/607846-tra,-dfsa-join-forces-to-promote-online-security>.
- Carter, Shan & Cox, Amanda. “One 9/11 Tally: $3.3 Trillion”, The New York Times (8

September 2011), online: <http://www.nytimes.com/interactive/2011/09/08/us/sept-11-reckoning/cost-graphic.html?_r=0>.

- Craigen, Dan. Diakun-Thibault, Nadia & Purse, Randy. "Defining Cybersecurity" online: Technology Innovation Management Review <http://timreview.ca/article/835>.
- Del Balzo, Joe. "AAI's Return to IASA Category I is A Reminder of the Value of that Status Enhances Aviation Safety" JDA Journal (1 November 2012) online: <http://jdasolutions.aero/blog/caai%E2%80%99s-return-to-iasa-category-1-is-a-reminder-of-the-value-of-that-status-enhances-aviation-safety/>.
- Erlin, Tim. "Hacking Aviation Technology: Vulnerability Disclosure and the Aviation Industry", Tripwire (30 April 2015) online: <http://www.tripwire.com/state-of-security/security-data-protection/security-hardening/hacking-aviation-technology-vulnerability-disclosure-and-the-aviation-industry/>.
- Gorman, Siobhan. "FAA's Air-Traffic Networks Breached by Hackers", The Wall Street Journal (7 May 2009), online: <http://www.wsj.com/articles/SB124165272826193727>
- Johan W. Ryan, "101 Cybersecurity. A Resource Guide for Bank Executives. Executive Leadership of Cybersecurity", (Guide paper issued at the Conference on State Bank Supervisors (CSBC) in Washington D.C., 17 December 2014), online: <https://www.csbs.org/CyberSecurity/Documents/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf>.
- Meredith, Leslie. "Malware implicated in fatal spainair plane crash- computer monitoring system was infected with a Trojan horse, authorities say", NBC News (20 August 2010), online: <http://www.nbcnews.com/id/38790670/ns/technology_and_science-security/t/malware-implicated-fatal-spanair-plane-crash/#.V3b3IZMrL3A>

- Millman, Rene. "Head of European aviation body EASA warns of cyber-attack risk against aircraft", Airportwatch (13 October 2015) online: <http://www.airportwatch.org.uk/2015/10/head-of-european-aviation-body-easa-warns-of-cyber-attack-risk-against-aircraft/>.
- Morgan, Jacob. "A Simple Explanation of 'The Internet of Things'", Forbs Magazine (13 May 2014) <http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#6070fd616828>
- Mouawad, Jad. "U.S. Airlines Face Uphill Struggle Against Mideast Rivals", The New York Times (14 December 2015) online: <http://www.nytimes.com/2015/12/15/business/us-airlines-face-uphill-struggle-against-mideast-rivals.html?_r=0>.
- Paganini, Pierluigi. "Istanbul Ataturk International Airport Targeted by a Cyber Attack" *Security Affairs* (28 July 2013), online: <http://securityaffairs.co/wordpress/16721/hacking/istanbul-ataturk-international-airport-targeted-by-cyber-attack.html>
- Pasztor, Andy. "U.S. Panel Aims to Shield Planes from Cyberattack", The Wall Street Journal (29 June 2015) online: <http://www.wsj.com/articles/u-s-panel-aims-to-shield-planes-from-cyberattack-1435537440>.
- Rouse, Margaret. "Personal Digital Assistant (PDA)" (June 2007) online: <http://searchmobilecomputing.techtarget.com/definition/personal-digital-assistant>.
- Sternstein, Aliya. "FAA Working on New Guidelines for Hack-Proof Planes", Nexgov (4 March 2016) online: <http://www.nextgov.com/cybersecurity/2016/03/faa-has-started-shaping-cybersecurity-regulations/126449/>.

- Zolfagharifard, Ellie. "'Hackers Are a Serious Threat to Aircraft Safety': Aviation Chiefs Warn of the Devastating Consequences of a Cyber-Attack", Mail Online (11 December 2014) online: <http://www.dailymail.co.uk/sciencetech/article-2869827/Hackers-threat-aircraft-safety-Aviation-chiefs-warn-devastating-consequences-cyber-attack.html.>.

ICAO Documents

- Air Traffic Services, Air Traffic Control Services, Flight Information Services, Alerting Services, ICAO, Thirteen Edition, Annex 11 to the Convention on International Civil Aviation.
- *Assembly Resolution A35-6, Doc. 9848* – Assembly Resolution in Force (as of 8 October 2004), superseding A33-8.
- *Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation*, 23 September 1971, 1974 UNTS 177; [1973] ATS 24; 10 ILM 1151 (1971) (entered into force on 26 January 1973, with 150 ratifications) [*Montreal Convention*].
- *Convention on International Civil Aviation*, 7 December 1944, 15 UNTS 295, ICAO Doc 7300/6 (entered into force 4 April 1947) [*Chicago Convention*].
- *Convention on Offenses and Certain Other Acts Committed On Board Aircraft*, 14 September 1963, 20 UST 2941, TIAS No 6768, 704 UNTS 219, 58 Am J Int'l L 566 (1959) (entered into force 4 December 1969) [*Tokyo Convention*].
- ICAO, "SARPs - Standards and Recommended Practices" *ICAO Safety,* online: <http://www.icao.int/safety/safetymanagement/pages/sarps.aspx>.
- ICAO, 2011 State of the Global Aviation Safety. A Coordinated, Risk-based Approach to Improving Global Aviation Safety, Special ed (Montreal: ICAO 2011) at 6 online:

<http://www.icao.int/safety/documents/icao_state-of-global-safety_web_en.pdf>.

- ICAO, Assembly - 39th Session, Working Paper Assembly, Agenda Item 16: Aviation Security – Policy Addressing Cybersecurity in Civil Aviation A39-WP/17 EX/5../5/16 (2016) [unpublished].
- ICAO, Continuing Airworthiness Manual, ICAO Doc 9642.
- ICAO, Manual of Civil Aviation Medicine, ICAO Doc 8924.
- ICAO, Manual of Model Regulations for National Control of Flight Operations and Continuing Airworthiness of Aircraft, ICAO Doc 9388.
- ICAO, Manual of Procedures for an Airworthiness Organization, ICAO Doc 9389.
- ICAO, Manual of Procedures for Establishment and Management of a State's Personnel Licensing System, ICAO Doc 9379.
- ICAO, Manual of Procedures for Operations Inspection, Certification and Continued Surveillance, ICAO Doc 8335.
- ICAO, Preparation of an Operations Manual, ICAO Doc 9376.
- ICAO, Safety Oversight Audit Manual, ICAO Doc 9735.
- ICAO, Safety Oversight Audit Manual, Part A — The Establishment and Management of a State's Safety Oversight System, ICAO Doc 9734.
- *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation*, 24 February 1988, ICAO Doc 951, 1589 UNTS 474, [1990] ATS 37,27 ILM 628 (1988) (entered into force 6 August 1989) [*Montreal Protocol 1988*].
- Safety, Safeguarding International Civil Aviation Against Acts of Unlawful Interference,

ICAO, Ninth Edition, Annex 17 to the Convention on International Civil Aviation (2014).

- Safety, Safeguarding International Civil Aviation Against Acts of Unlawful Interference, ICAO, Ninth Edition, Annex 17 to the Convention on International Civil Aviation (2011).
- Safety, Safeguarding International Civil Aviation Against Acts of Unlawful Interference, ICAO, Ninth Edition, Annex 17 to the Convention on International Civil Aviation (2011).

European Union Documents

- EC, European Aviation Safety Agency, Terms of Reference for a rulemaking task Aircraft cybersecurity 17 May 2016, [2016] OJ, ToR Issue 1 RMT.0648 online:< https://www.easa.europa.eu/system/files/dfu/ToR%20RMT.0648%20Issue%201.pdf>.
- EC, European Union, List of Air Carriers Which are Banned from Operating Within the Union, with Exceptions, (16 June 2016), online: <http://ec.europa.eu/transport/modes/air/safety/air-ban/doc/list_en.pdf>.
- EC, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions an Aviation Strategy for Europe, [2005] OJ, Document 52015DC0598, online: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52015DC0598>
- European Commission, Media Release, "Cybercrime: What's Cybercrime?" (18 April 2016) online: <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm>.
- European Commission, Press Release, "Cybersecurity Strategy for the European Union" (7 June 2016) online: <https://ec.europa.eu/digital-single-market/en/cybersecurity>.

- European Parliament, *EC, 2005* Ordinary Sess, The establishment of a Community list of air carriers subject to an operating ban within the Community and on informing air transport passengers of the identity of the operating air carrier, and repealing Article 9 of Directive 2004/36/EC (Text with EEA relevance),*2111/2005*, (2005) OJ L 344/15.
- European Union SESAR, Study Release, "SESAR Strategy and Management Framework Study for Information Cyber-Security Application to System Wide Information Management Research and Development" (September 2015), online: <http://www.sesarju.eu/newsroom/all-news/study-details-rd-roadmap-atm-cyber-security>.

United States Documents

- DOT Order 92-10-17 (1992) (Murtala Mohammed International Airport, Lagos - Nigeria).
- DOT Order 95-9-15 (1995) (El Dorado International Airport, Bogotá - Colombia).
- DOT Order 96-3-50 (1996) (Hellenikon International Airport, Athens – Greece).
- DOT Order 98-1-24 (1998) (Port-au-Prince International Airport, Haiti).
- Federal Aviation Administration, Review of the Web Applications Security and Intrusion Detection in Air Traffic Control Systems, Report Number: FI-2009-049 (4 May 2009) online: https://www.oig.dot.gov/sites/default/files/ATC_Web_Report.pdf.
- National Transportation Safety Board Federal Aviation Administration, Safety Recommendation, 20594 (17 August 2009) online: <http://www.ntsb.gov/safety/safety-recs/recletters/A09_67_71.pdf>.
- "NextGen", United States Federal Aviation Administration (24 July 2016), online: <"NextGen"https://www.faa.gov/nextgen/>

- Department of Defense United State of America, "Memorandum for Chiefs of the Military Services Commanders of the Combatant Commands Directors of the Joint Staff Directors - Subject: Joint Terminology for Cybersecurity Operations" online: <http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf >
- *Professional Pilots v FAA*, 118 F (3d) 758, 768 (DC Cir 1997); *British Caledonian Airways v Bond*, 665 F (2d) 1153 (DC Cir 1981) [*British Caledonian*]. *Evergreen Helicopters*, (2000 FAA *Lexis* 247 (2000)).
- United Sates Federal Regulation, Vol. 60, No. 210, 57 38,342 (24 August 1992).
- United States Department of Transportation, "Impacts of the Light Squared Network on Federal Science Activities", (8 September 2011) online: <http://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/090811_%20Appel.pdf>
- United States Federal Aviation Administration, Document Information, 1370.47, "FAA Cybersecurity Roles and Responsibilities" (24 December 2015) online: <https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.information/documentID/1028713>.
- United States Government Accountability Office, Report to Congressional Requesters, GAO-15-370, "Air Traffic Control - FAA Needs a More Comprehensive Approach to Address Cybersecurity as Agency Transitions to NextGen" (April 2015) online: <http://www.gao.gov/assets/670/669627.pdf>.
- United States, Press Release, "Seeking Comments on the Preliminary Cybersecurity Framework" (29 October 2013) online:

<https://www.whitehouse.gov/blog/2013/10/29/seeking-comments-preliminary-cybersecurity-framework>.

- US Federal Aviation Administration, Personal Digital Assistants (PDAs) and Records (9 January 2012) online: <https://www.faa.gov/about/initiatives/records/faq/personal_digital_assistants/>.
- US, Transportation Security Administration, *Criminal Acts Against Civil Aviation* (2001) online: <http://nsarchive.gwu.edu/NSAEBB/NSAEBB165/faa8.pdf>.

Other materials

- AIAA, The World's Forum for Aerospace Leadership, The Connectivity Challenge: Protecting Critical Assets in a Networked World, Decision Paper (August 2013) online: <https://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final.pdf>.
- Aviation Information Sharing and Analysis Center, A-ISAC, online: <http://www.a-isac.com/>.
- CANSO, Cyber Security and Risk Assessment Guide, (June 2014) online: <https://www.canso.org/canso-cyber-security-and-risk-assessment-guide >.
- Cyber Kill Chain – Proactively detect persistent threats, (Junes 2016) online: Lockheed Martine <http://cyber.lockheedmartin.com/solutions/cyber-kill-chain>.
- Cyber Security Glossary, National Initiative for Cybersecurity Careers and Studies (NICCS), online: < http://niccs.us-cert.gov/>.
- Cybersecurity & Information Management, (June 2016), online: Boeing <http://www.boeing.com/defense/cybersecurity-information-management/>.
- Global Market Forecast 2016-2035 – Mapping Demand, online: Airbus

<http://www.airbus.com/company/market/global-market-forecast-2016-2035/>.

- IATA, Fact Sheet Cybersecurity Three-Pillar Strategy (June 2016) Online: <https://www.iata.org/pressroom/facts_figures/fact_sheets/Documents/fact-sheet-cyber-security.pdf>
- IATA, Operational Safety Audit: Designed for the Aviation Industry, (2007). online: <http://www.iata.org/whatwedo/safety/audit/iosa/Pages/index.aspx>.IATA, Aviation Cyber Security Toolkit, 2nd edition (July 2015), online: <http://www.iata.org/publications/Pages/cyber-security.aspx>.
- IATA, Vision 2050 Report (12 February 2011) online: <https://www.iata.org/pressroom/facts_figures/Documents/vision-2050.pdf>
- ICCAIA, International Coordinating Council of Aerospace Industries Associations, (August 2016), online: <http://www.iccaia.org/about-us>.
- IFALPA, Cyber threats: who controls your aircraft? 14POS03, (2 June 2013) online: <http://www.ifalpa.org/downloads/Level1/IFALPA%20Statements/Security/14POS03%20-%20Cyber%20threats.pdf.>.
- PricewaterhouseCooper United States, "Threat smart: Building a cyber resilient financial institution" (October 2014), online:<https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/pwc-cyber-resilient-financial-institution.pdf>.
- Revenue of the worldwide leading aircraft manufacturers and suppliers in 2014 (in million U.S. dollars) (June 2016), online: The Statistic Portal <http://www.statista.com/statistics/264366/revenue-of-the-worldwide-leading-aircraft-manufacturers-and-suppliers/>.
- The Oxford Dictionary, *sub verbo* "cyberspace", online:

<http://www.oxforddictionaries.com/us/definition/american_english/cyberspace>.

- UAE Telecommunications Regulatory Authority (TRA), Press Release, "The TRA's UAE Computer Emergency Response Team (aeCERT) organizes an aviation security workshop" (31 March 2015) online: <https://www.tra.gov.ae/aecert/en/media/news-archive/2015/3/31/the-tras-uae-computer-emergency-response-team-aecert-organizes-an-aviation-security-workshop.aspx>.