# CYBER TERRORISM AND CIVIL AVIATION: THREATS, STANDARDS AND REGULATIONS

DALIT KEN-DROR FELDMAN*
AND EMANUEL GROSS**



* Dr. Dalit Ken-Dror Feldman, Legal Supervisor, Legal Clinic for Law, Technology and Cyber, Faculty of Law, University of Haifa and Postdoctoral at the Interdisciplinary Center Herzliya .
** Prof. Emanuel Gross, Prof. Emeritus, Faculty of Law, University of Haifa.

## I. INTRODUCTION[***]

In recent years we have witnessed many conventional terror attacks. Some were unleashed at airports, for example, at Brussels' Zaventem Airport or Istanbul's Atatürk Airport. Conventional terrorism is, of course, here to stay and must not be ignored. However, the cyber era presents the aviation industry with new challenges, which might prove even more devastating than conventional attacks.

But this expanding feature has sparked hardly any legal discourse on the subject. No discussions have been held on what civil aviation regulators, local and international, or the private sector, should do. For example, should a minimal cyber security standard be set for the short or long run? Or should we neglect such action at the behest of "state-of-the-art" cyber security[1] so as not to hurt innovation?

*** The authors would like to thank the Lecturers of the school of law, Zefat Academic College for their comments of an earlier draft of the article and to the editorial board for their wonderful work and enlightening comments that helped to improve the article.

1. See for instance, Act on the Federal Office for Information Security (BSI Act—BSIG), Deutscher Bundestag [BT] 14/8/2009 I 2821 § 8a (Ger.). In this section the regulator

Moreover, a discussion in this field should have started years ago, considering that the number of flights and passengers began growing long ago and continues to do so. To handle the flow of passengers efficiently, airport processes will increasingly become automated. The more such processes become embedded, the higher the potential for cyber attacks to occur. Cyber security becomes crucial.

For the first time, to our knowledge, this article compares the United States with the European Union on the regulatory situation internationally, in respect of both legal and professional standards. In light of the flights' international nature, we chose to compare international with regional (and federal) regulations.

In part II of this article, before discussing the recommendation regarding legal ways to handle cyber terrorism in civil aviation, we try to understand what the risks are inside the airport and on the flight itself. We shall also show the complexity of the situation inside the airport and during the flight, such as multiple suppliers and multiple countries. We shall review most of the reported cyber attacks that have already occurred both inside airports and on aircraft. In part III we discuss the current legal response to cyber attacks in the civil aviation sector. In many ways air transportation can be recognized as an essential or critical infrastructure. We examine several levels of cyber security regulations in the civil aviation sector—international and regional or federal (USA and EU). We show that the current response does not cover all the situations that necessarily should be covered. Moreover, the multiple international standards create overlapping or partially overlapping standards, which might cause

---

determined that the "state of the art" should be adhered to. The law does not mention what will be considered the "state of the art," and it is left open to the operator and their industry associations to suggest—as mentioned in § 8a(2). Upon request, the Federal Office can determine, after consulting relevant state bodies, whether the "state of the art" suggestions are suitable for ensuring the requirements of § 8a(1).

Act on Reorganisation of Aviation Security Tasks (Luftsicherheitsgesetz, LuftSiG) (2005), https://germanlawarchive.iuscomp.org/?p=735 (Ger.), relates to the old-fashioned security threats such as physical hijacking, acts of sabotage and terrorist attacks (§ 1). The act authorizes the aviation security authority to avert attacks against aviation security. The act refers to searches with and without a machine and does not refer to cyber threats, although its scope can include these too, as long as it is connected to protecting the security of air traffic against attacks (§§ 5 and 1). However, the text shows that this act was not intended to include cyber threats as it refers to background checks (§ 7), security measures to be taken by airport operators such as construct and design of the airport (§ 8(1)), and store mail, hold baggage, cargo and supplies (§ 8(2)) and so on. Therefore, another act that may be related to the cyber security aviation field is the act concerning the Federal Office for Information Security, that is, the BSIG mentioned above. The latter act establishes the German Federal Office for Information Security. The Federal Office should promote the security of information technology in various instances (§ 3). The BSIG was also amended by the IT Security Act (ITSiG) in July 2015 and again in 2017.

problems if the standards requirement varies across countries. In part IV we argue that air transportation should not be viewed as merely a critical infrastructure but is unique among other critical infrastructures. By contrast with another critical infrastructure, a cyber attack in the aviation sector might affect many countries simultaneously. The circumstances are, therefore, very complicated considering that different legal systems may apply in different situations. In part V, we offer our conclusions and recommendations, namely to enact a convention or treaty covering all aspects of tackling cyber attacks in the civil aviation sector at airports and in aircraft alike. We recommend establishing a central and international authority that will handle cyber attacks in the civil aviation sector. Furthermore, we suggest establishing local authorities as well, which will be bound by the international authority but will be able to deliver a quick response to a cyber attack while reporting the incident to the international body, which will handle the situation globally if need be.

## II. The New Challenges of Cyber Attacks

Cyber terrorism can take several forms and may be defined in many ways. Usually, it is a terror attack or threat that targets computers and computer systems.[2] Computer systems control the ground handling of passengers, luggage, communication with the airplane, flight plans, and control of the flights themselves. Therefore, all these systems are vulnerable to cyber attacks.

For instance, in 2016, the Director of the European Aviation Safety Agency (EASA) revealed that aviation systems were subject to an average of 1,000 attacks each month.[3] Cyber attacks can be conducted by hacking into the system through vulnerabilities, by spoofing, by denial of service attack, by uploading malware to the system by a system update, by an employee inserting a flash disk during a maintenance process, or by other means. We shall now discuss the risks inside the airport and during the flight itself.

---

2. Scott Schober, *Cyber Terrorism - The Weapon of Choice a Decade after 9/11*, HOMELAND SEC. NEWS WIRE (Nov. 2. 2011) http://www.homelandsecuritynewswire.com/dr20111102-cyberterrorism-the-weapon-of-choice-a-decade-after-9-11.

3. Emilio Iasiello, *Cybersecurity Aviation — Are We there yet?*, CYBERDB, https://www.cyberdb.co/cybersecurity-aviation-are-we-there-yet/.

### *A. Threats inside the airport*

The airport itself has almost no interaction with the passengers, who are served by the airlines and the handling agents. Therefore the airport usually does not possess information about passengers, so when we talk about cyber security at airports we generally do not mean leakage of information but refer to the protection of the airport system against disruption.[4] Traditionally airport systems are divided into two types: operation-related (baggage, check-in, etc.) and business-related (human resources, emails, licenses, etc.).[5]

The problem with the check-in system is that usually, it is not run centrally by the airport itself but by several Departure Control Systems operated by the airlines or their subcontractors. A cyber attack on those systems might disrupt of the passenger flow at the airport. Moreover, some multinational systems exist that handle the process from check-in to take-off, for example, Amadeus or SITA.[6] If these systems come under attack, several airports may be affected simultaneously. We must bear in mind that quite soon the terror attack might be multinational rather than local and could cause chaos worldwide.

Cyber attacks are not a new element in the aviation field. In 2006 an internet attack forced the U.S. Federal Aviation Administration (FAA) to shut down a number of its air traffic control systems in Alaska. [7]

In 2009 a report published in the U.S. by the Inspector General (IG) of the Department of Transportation revealed that the increasing use of web applications linked to FAA systems exposed the air traffic system to potential cyber attacks through access-control vulnerabilities. The report also found weaknesses in the FAA's intrusion detection capabilities.[8]

---

4. Wayne Smith, *Cyber Security in Airports,* 9(3) J. AIRPORT MGMT. 232, 232–33 (2015).

5. *Id.* at 233.

6. Explanations about the systems can be seen at https://amadeus.com/en/industries/airports and at https://www.sita.aero/about-us.

7. Hélène Duchamp, Ibrahim Bayram & Ranim Korhani, *Strategic Report - Cyber-Security, A New Challenge for the Aviation and Automotive Industries—Seminar in Information Systems: Applied Cybersecurity Strategy for Managers*, J. OF STRATEGIC THREAT INTELLIGENCE 1, 5 (2016), http://blogs.harvard.edu/cybersecurity/files/2017/01/Cybersecurity-aviation-strategic-report.pdf.

8. Fed. Aviation Admin., *Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems*, OFF. OF INSPECTOR GEN., May 4, 2009, at 2–3.

In 2013 an attack at Istanbul airport caused severe problems in the passport control system, which resulted in delays of many flights. That year 75 airports in the US were targeted, possibly by malicious hacking and phishing.[9]

In 2014 the IG of the U.S. Department of Transportation discovered weaknesses in the FAA's traffic flow management system.[10]

In June 2017, Boryspil International Airport, Ukraine's largest terminal, came under cyber attack as part of a comprehensive cyber action against government infrastructures. The attack disabled the airport's computers and departure boards,[11] and in April 2018, almost half the European flights were delayed due to the Eurocontrol[12] system's failure. The failure was put right, but it affected up to half of all flights in Europe. It also seems that the system's failure caused data destruction due to the request made to airlines to resend all flight plans drawn up before 10:26 UTC. Eurocontrol claimed that a systems failure was rare and that it had occurred just once before, in 2001.[13] We must anticipate more systems failures soon if cyber risks are not appropriately handled.

Wayne Smith argues that to reduce these threats (and not wait for a provider of a certain system to appear and solve the problem), the airport may need to control a central system. Some airports are run as a club site, that is, all the airlines run the check-in system together. Also, a committee of all the airlines' executives assumes responsibility for the check-in system as they usually rely on the manufacturer to secure the system and respond immediately if something goes wrong.[14]

Similar problems might arise in the baggage systems. Numerous bodies constitute the luggage system, many of them

9. Duchamp, Bayram & Korhani, *supra* note 7, at 5.

10. Fed. Aviation Admin, *Weakness Exist in FAA's Security Controls for the Traffic Flow Management System*, OFF. OF INSPECTOR GEN., June 5, 2014.

11. Lizzie Dearden, *Ukraine cyber attack: Chaos as national bank, state power provider and airport hit by hackers,* INDEPENDENT (June 27, 2017, 2:04 PM), https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html.

12. Eurocontrol, https://www.eurocontrol.int/about-us (Eurocontrol is an intergovernmental organization. It has 41 members and 2 Comprehensive Agreement States. Its aim is to build a Single European Sky considering ATM, including cybersecurity). Eurocontrol has a resilience, monitoring and response role in cybersecurity. Eurocontrol is raising awareness about cybersecurity issues among member states and has a training center. *See* Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act"), 2017/0225(COD) (proposed Sept. 13, 2017).

13. *Half of European Flights Delayed due to System Failure*, BBC NEWS (Apr. 3, 2018), https://www.bbc.com/news/world-europe-43633094.

14. Smith, *supra* note 4, at 233–35.

handling the bags. Again—it is not necessarily a centralized system. From the moment the bag is tagged with a barcode according to the passenger's flight destination, to the moment the bag arrives at the right airport on the right conveyor belt, it is handled by many computer systems. These systems include tagging the bags, sorting them according to the tags, automated security scanning of the bags by a computer—(and if necessary the computer calling an operator to check the image) and so on.[15]

The worst damage a cyber attack can cause to the baggage systems is chaos and delays in flights. For instance, bags can be sent to the wrong destination.[16] But we can imagine a situation even worse than not getting our bags or being delayed until the problem is solved. A worst-case scenario, for example, is that the cyber attack disrupts the scanning system in a manner making explosive and similar materials undetectable. Worse still may be a combined attack, creating chaos or disabling an automatic security alert system in a restricted area and enabling a massive physical attack on more people.

The airport has another aspect, namely operating as a regular business site with regular databases and systems like other businesses. This aspect too must not be dismissed, but it is not our main focus in this article.

### *B. Threats up High in the Sky*

On August 20, 2008, Spanair Flight 5022 (JK5022) from Barcelona's El Prat airport (via Madrid's Barajas airport) to Gran Canaria airport in Spain, crashed minutes after taking off from Madrid airport. One hundred and fifty-three people died, and 18 survived.[17] Two years later, in a hardly circulated notice, Spanair reported that the company's main computer, which recorded aircraft malfunctions, had been contaminated with malicious computer programs and, therefore, might not have recognized the airplane's problems before takeoff.[18] It was thus possible that a ground system cyber attack had contaminated the aircraft itself.

---

15. *Id.* at 235.

16. *Id.*

17. *Spanish Plane that Crashed had Overheated Valve,* SINA.COM (Aug. 21, 2008, 12:56 PM), http://english.sina.com/world/p/2008/0821/180610.html.

18. José Antonio Hernández, *El Ordenador De Spanair Que Anotaba Los Fallos En Los Aviones Tenía Virus,* ELPAIS (Aug. 20, 2010), https://elpais.com/diario/2010/08/20/espana/1282255211_850215.html.

In 2014 Ruben Santamarta published an article about backdoors and remote control of SATCOM (Satellite Communication) aviation radios that he discovered. One of his disturbing conclusions was that until at least 2014, it was "almost impossible to guarantee the integrity of thousands of SATCOM devices."[19]

After 9/11, it was believed that hijacking an aircraft had become a rare event due to the new security measures worldwide; nevertheless, such a disaster may still happen. In February 2014, Ethiopian Airlines FL702 aircraft was hijacked—but in this case, the hijacker was the co-pilot, who locked the cockpit door when the captain went to use the restroom. Pilots do not personify the threat we try to avoid. Nowadays, most effort is invested in means to prevent potential old-fashioned hijackers. An Advanced Imaging Technology unit screens passengers for metallic and non-metallic threats. In addition, radiation scanners, chemical sensors, and closed-circuit television cameras serve to stymie such threats.[20]

The Allianz Risk Barometer of 2014 states that the threat of cyber risk reached the top ten (eighth position); it is expected to rise up the list as the years go by. According to the reports, the new generations of aircraft are using constantly more "data networks, data uplinks and downlinks, computer systems, aircraft-control navigation systems, environmental systems, propulsion systems and control surface systems."[21] Hence, these aircraft are more vulnerable to cyber attacks.[22] We have also heard about the motorist who installed a GPS jammer in his car so that his employers would not know where he was roaming. But his route was too close to Newark airport, and the jammer accidentally blocked the reception of GPS signals used by the air traffic control system.[23] Additionally, in July 2013, we were informed that Todd Humphreys of UT's Cockrell School of Engineering led his students in successfully performing the invited GPS spoofing attacks on a

19. Ruben Santamarta, *A Wake-Up Call for SATCOM Security*, Technical White Paper 1, 24 (2014), https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf. For further reading about aircraft communication and cyber threats *see* F. Shaikh et al., *A Review of Recent Advances and Security Challenges in Emerging E-Enabled Aircraft Systems*, 7 IEEE ACCESS 63164 (2019).

20. Allianz Global Corporate & Specialty, *Global Aviation Safety Study: A Review of 60 Years of Improvement in Aviation Safety*, ALLIANZ 1, 58 (2014), https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Global-Aviation-Safety-2014-report.pdf [hereinafter Allianz Global Corp.].

21. *Id.*

22. *Id.*

23. Chris Matyszczyk, *Truck Driver Has GPS Jammer, Accidentally Jams Newark Airport*, CNET NEWS (Aug. 11, 2013, 8:08 AM), https://www.cnet.com/news/truck-driver-has-gps-jammer-accidentally-jams-newark-airport/.

213-foot private yacht. The students stood on the yacht's upper deck and transmitted faint false GPS signals from a device they had made. These false signals gradually overpowered the true GPS signals, and the yacht moved off its course.[24] Spoofing GPS signals is a threat to airplanes as well.

Cyber attacks on these systems can help in hijacking an aircraft without necessarily being delivered physically from on board, that is, changing the flight's route and so on. For instance, the GPSs used for navigation, position, and timing can be easily targeted by cyber attackers because they rely on external networks.[25] Even the fact that many airlines offer Wi-Fi services onboard makes life more difficult for the security personnel.[26]

In June 2015, the Polish airline LOT reported a cyber-attack that affected its ground operation systems, which prevented the LOT personnel from developing flight plans.[27]

In October 2015, the director of the European Aviation Safety Agency (EASA) warned of the intensified possibility of a serious cyber-attack through a hacker hacking from the ground into an aircraft's critical systems. The vulnerability of the Aircraft Communications Addressing and Reporting System (ACARS), which regularly transmitted messages between aircraft and ground stations, was tested. After only five minutes, the system was hacked; within a few days, the hacker had gained access to the aircraft's control systems.[28]

In 2015, we also heard about the American researcher Chris Roberts who announced that he had successfully hacked about 15 different airplanes and caused one of the airplane's engines to rise, resulting in the plane's lateral or sideways movement during one of these flights. Roberts claimed that he had accessed the plane's controls via the in-flight entertainment system, his laptop, and an Ethernet cable using vulnerabilities he discovered in the in-flight entertainment systems of Boeing 737-800, 737-900 and 757-200 aircraft, as well as in Airbus A-320s.[29] Hugo Teso, a

---

24. Eric Zumalt, *Spoofing a Superyacht at Sea*, UT NEWS (July 30, 2013), https://news.utexas.edu/2013/07/30/spoofing-a-superyacht-at-sea.

25. Andrew V. Schmidt, Note, *Cyberterrorism: Combating the Aviation Industry's Vulnerability to Cyberattack*, 39 SUFFOLK TRANSNAT'L L. REV. 169, 193 (2016).

26. Allianz Global Corp., *supra* note 20, at 58.

27. Sarah Jane Fox, *Flying Challenges for the Future: Aviation Preparedness – in the Face of Cyber-Terrorism*, 9 J. TRANSP. SECUR. 191, 199 (2016).

28. *Id.* at 198.

29. *FBI Docs: Banned Hacker Says He Commandeered a Plane*, CBS NEWS (May 17, 2015, 8:56 AM), http://www.cbsnews.com/news/chris-roberts-fbi-court-documents-commandeered-plane/.

German security researcher, similarly developed an Android application that could redirect a virtual plane using a map application on a Samsung Galaxy Smartphone.[30]

In 2019 Bloomberg revealed that in 2014 U.S. government officials exposed that cellphones and other types of radio signals could pose a crash threat to some models of Boeing 737 and 777 airplanes. The cockpit screens were found as vulnerable to interference from Wi-Fi, cellphones, and more. The FAA settled a period of almost five years, until November 2019, to replace these systems. In the US, according to the FAA, there were about 1300 airplanes equipped with these cockpit screens. In 2019 there were still about 70 airplanes left that should be fixed.[31] This system vulnerability might have been used during a terror attack.

With these examples, we believe we have demonstrated how an airplane might be directly attacked. However, we should remember that the attack can be conducted by way of system maintenance, remote devices that connect to the airplane's systems, and the like. Through them, terrorists and criminals might gain control of the aircraft's systems by means of malicious software. Furthermore, the 9/11 event showed us that a terror attack on board does not just target the airplane but also uses the airplane itself as a weapon by crashing it into buildings.

## III. CURRENT REGULATORY RESPONSE

Air transportation, in many ways, can be recognized as an essential or critical infrastructure, as will be shown below. In the civil aviation sector, several levels of cyber security regulation exist—international and regional or federal. We shall examine some of them now.

### *A. International Standards and Guidelines*

On the international level, we find international organizations such as the International Civil Aviation Organization (ICAO) (part of the UN),[32] and general standardization organizations such as the European Organization for Civil Aviation Electronics

30. Andrew V. Schmidt, *supra* note 25, at 195–96; *see also* George Suciu et al., *Cybersecurity Threats Analysis for Airports*, *in* NEW KNOWLEDGE IN INFORMATION SYSTEMS AND TECHNOLOGIES 252 (Álvaro Rocha et al. eds., 2019).

31. Anita Sharpe, *Cellphones a Flight Risk? Could Be on Some Boeing Jets*, BLOOMBERG (July 18, 2019, 4:00 AM), https://www.bloomberg.com/news/articles/2019-07-18/are-cellphones-a-flight-danger-they-are-on-these-boeing-jets.

32. INTERNATIONAL CIVIL AVIATION ORGANIZATION, https://www.icao.int/about-icao/Pages/default.aspx (last visited Sept. 1, 2019).

(EUROCEA),[33] the Radio Technical Commission for Aeronautics (RTCA),[34] and the National Institute of Standards and Technology (NIST).[35] Many standards are concerned with data protection and security of information. The variety of standards can become a problem if there are too many to follow, and there is no central organization to supervise and arrange them as a coherent and complete codex. Below we review some of the foremost standards, among them standards of airworthiness and cyber security frameworks.

1. Airworthiness Standards

In 2006, RTCA formed the SC216 Committee on Aeronautical Security, in cooperation with the EUROCAE Working Group on Aeronautical Security (WG72). In 2014, RTCA and EUROCEA announced aviation-related guidelines dealing with airworthiness standards. These three standards are equivalent and parallel:[36] RTCA DO-326A[37]/ED 202A[38] — Airworthiness Security Process Specification (2014); RTCA DO-355[39]/ED 204[40] Security DO-355 — Information Security Guidance for Continuing Airworthiness; and RTCA DO-356[41]/ED 203[42] — Airworthiness Security Methods and Considerations.[43]

---

33. EUROPEAN ORGANIZATION FOR CIVIL AVIATION EQUIPMENT, https://www.eurocae.net/ (last visited Sept. 1, 2019).

34. RADIO TECHNICAL COMMISSION FOR AERONAUTICS, https://www.rtca.org/content/about-us-overview (last visited Sept. 1, 2019).

35. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, https://www.nist.gov/about-nist (last visited Sept. 1, 2019).

36. *See* EUROCAE, EUROCAE ED 201: Aeronautical Information System Security (AISS) Framework Guidance (Dec. 1, 2015), https://standards.globalspec.com/standards/detail?docid=9997842&familyid=EELNOFAAAAAAAAAA.

37. *See* RADIO TECHNICAL COMMISSION FOR AERONAUTICS, *RTCA DO-326: Airworthiness Security Process Specification* (Aug. 6, 2014), https://standards.globalspec.com/std/9869201/rtca-do-326 [hereinafter RTCA DO-326].

38. *See* EUROCAE, *EUROCAE ED 202 - Airworthiness Security Process Specification* (June 1, 2014), https://standards.globalspec.com/std/9862360/eurocae-ed-202.

39. *See* RADIO TECHNICAL COMMISSION FOR AERONAUTICS, *RTCA DO-355: Security DO-355 Information Security Guidance for Continuing Airworthiness* (June 17, 2014), https://standards.globalspec.com/std/9861922/rtca-do-355 [hereinafter RTCA DO-355].

40. *See* EUROCAE, *EUROCAE ED 204 – Information Security Guidance for Continuing Airworthiness* (June 1, 2014), https://standards.globalspec.com/std/1693893/eurocae-ed-204.

41. *See* RADIO TECHNICAL COMMISSION FOR AERONAUTICS, *RTCA DO-356: Airworthiness Security Methods and Considerations* (Sept. 23, 2014), https://standards.globalspec.com/std/9870299/rtca-do-356 [hereinafter RTCA DO-356].

42. *See* EUROCAE, *EUROCAE-ED-204: Information Security Guidance for Continuing Airworthiness* (Sept. 1, 2015), https://standards.globalspec.com/std/10027811/eurocae-ed-203 [hereinafter EUROCAE – ED-204].

43. RTCA DO-356, *supra* note 40.

The three standards refer to the civil aviation authorities and the aviation industry during several phases: manufacturing an aircraft and the maintenance stage of aircraft and related systems.

RTCA DO 326A/ED 202A sets guidelines for aircraft certification: how to handle the threat of intentional unauthorized electronic interaction to aircraft safety, including steps that should be taken to handle malware, distorted data, or penetration of aircraft systems. It deals with activities that should be conducted in operation and maintenance of the aircraft in relation to information security threats. However, it does not apply to

"a. Physical security or physical attacks on the aircraft (or ground element),

b. Airport, Airline or Air Traffic Service Provider security (e.g., access to airplanes, ground control facilities, data centers),

c. Communication, navigation, and surveillance services managed by national agencies or their international equivalents (e.g., GPS, SBAS, GBAS, ATC communications, ADS-B)."[44]

As we see, the above guidelines do not cover several main cyber vulnerability threats. These include communication, navigation, surveillance services for aircraft, and systems related to airport, airline, or air traffic services.

RTCA DO-356/ED 203 is connected to RTCA DO 326/ED 202A and therefore, does not apply to the same leading cyber vulnerability threats either. This guideline refers to the "development life cycle from project initiation until the Aircraft Type Certificate is issued for the aircraft type design."[45] It provides methods for handling the threat of intentional unauthorized electronic interaction to aircraft safety.[46] Similarly, RTCA DO-355/ED 204 refers to situations where aircraft safety might be affected by the operation and maintenance of aircraft security threats.[47]

These guidelines do not deal with all aspects of cyber security threats, as we have seen. They are not legally binding; however, the FAA Aircraft Systems Information Security Protection (ASISP) Working Group of the Aviation Rulemaking Advisory Committee (ARAC) recommended these guidelines as standards or as highly desirable guidance[48].

---

44. RTCA DO-326*, supra* note 36.
45. RTCA DO-356, *supra* note 40.
46. *Id.*
47. RTCA DO-355*, supra* note 38.
48. A REPORT FROM THE AVIATION RULEMAKING ADVISORY COMMITTEE (ARAC) AIRCRAFT SYSTEM INFORMATION SECURITY / PROTECTION (ASISP) WORKING GROUP TO THE FEDERAL AVIATION ADMINISTRATION, 80 Fed. Reg. 5880, 5880–81, (Proposed, Feb. 3, 2015).

ARNIC[49] Industry Activities also established standard ARINC 811[50]—Commercial Aircraft Information Security Concepts of Operation and Process Framework. This deals with the terms, definitions, and concepts gap between airline organizations and the terrestrial network security industry, in order to develop more ARINC standards in the field of aircraft equipment.[51]

In addition, a document of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) exists: it deals with critical infrastructure in general[52] and as such relates indirectly to aviation without necessary adjustments to the character of the aviation field.

2. Cyber Security

The Joint technical committee of ISO and IEC has set 27000 family standards that help organizations to keep information assets secure.[53] The best-known standard in this family is ISO/IEC 27001. It lays down the requirements for an information security management system (ISMS).[54] This standard is general, not specifically intended for aviation. It treats any size of business in any sector.[55] Since the 27000 family standards are not specially tailored for the aviation sector, they can help in managing some threats but cannot offer a comprehensive solution for security management in aviation.

A Specific Standard BS EN 16495 Air Traffic Management – Information Security for Organisations Supporting Civil Aviation Operations,[56] relating to ISO/IEC 27000 family standards,

---

49. *See* ARINC INDUSTRY ACTIVITIES, https://www.aviation-ia.com ("AEEC, AMC, and FSEMC are aviation industry activities organized by ARINC Industry Activities, an industry program of SAE Industry Technologies Consortia (SAE ITC), to establish consensus technical standards, known globally as ARINC Standards, and develop shared technical solutions that no one organization could accomplish independently.").

50. ARINC, *ARINC 811: Commercial Aircraft Information Security Concepts of Operation and Framework* (Dec. 20, 2005), https://standards.globalspec.com/std/320101/arinc-811 [hereinafter ARINC 811].

51. *Id.*

52. *See generally Framework for Improving Critical Infrastructure Cybersecurity - Version 1.1*, NAT'L INST. OF STANDARDS & TECH. (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

53. *ISO/IEC 27001 Information Security Management*, INT'L ORG. FOR STANDARDIZATION, https://www.iso.org/isoiec-27001-information-security.html.

54. *Id.*

55. *Id.*

56. *BS EN 16495 Air Traffic Management – Information Security for Organisations Supporting Civil Aviation Operations*, BSI STANDARDS PUBLICATION (July 31, 2014), https://shop.bsigroup.com/ProductDetail/?pid=000000000030269415.

"defines guidelines and general principles for the implementation of an information security management system in organizations supporting civil aviation operations."[57]

As we can see, the international standards are only partial, and they cover merely the tip of an iceberg of threats. Some are not even adjusted to civil aviation. We shall move on now to examine whether international conventions or initiatives are adequate.

### *B. International Conventions and Initiations*

In December 2014, five major key stakeholders (ICAO, the Airports Council International (ACI), the Civil Air Navigation Services Organisation (CANSO), the International Air Transport Association (IATA) and the International Coordinating Council of Aerospace Industry Associations (ICCAIA)) stated that the "global aviation system [is] *potentially* vulnerable to attacks from hackers and other cyber criminals."[58] They also agreed on a common roadmap to align their respective actions on cyber threats. [59]

#### 1. The Chicago Convention and Decisions of the ICAO

As freedom of movement remains a basic right, the ICAO adopted an amendment to Annex 17 (Security) of the Convention on International Civil Aviation, also known as the Chicago Convention.[60] The amendment came into force on March 26, 2011. It declares:

> 4.9 Measures relating to cyber threats
>
> 4.9.1 Recommendation. – 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.
>
> 4.9.2 Recommendation. — Each Contracting State should encourage entities involved with or

57. *Id.*
58. Fox, *supra* note 26, at 207–08
59. *Id.*
60. Schmidt, *supra* note 25, at 196.

> 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 thereto, and develop protective measures to include, inter alia, security by design, supply chain security, network separation, and remote access control, as appropriate.[61]

The member states were required to develop measures to protect communication technology systems from threats that might jeopardize the safety of the flights.[62]

In addition, the ICAO's 12th Air Navigation Conference in 2012 recognized cyber security as a serious concern in implementing the Global Air Navigation Plan. This is mainly because civil aviation organizations annually increase their reliance on electronic systems for essential components.[63] The ICAO estimated that in the following two decades, about $120 billion USD would be invested in air transportation systems. [64]

In 2016, the 39th ICAO Assembly adopted Cybersecurity Resolution A39-19, based on a joint EU-US submission. The Resolution highlighted the need for a holistic approach to cybersecurity, involving as many parties as possible, and emphasized the need to share information and best practices at the international level. The resolution won unanimous support.[65] Several Aviation Information Sharing Platforms exist: Aviation ISAC (US based), EuroControl (EU), OneSky (Australia), and ENISA-CRISTs by country (mainly EU).[66]

---

61. ICAO, INTERNATIONAL STANDARDS AND RECOMMENDED PRACTICES, SECURITY – SAFEGUARDING INTERNATIONAL CIVIL AVIATION AGAINST ACTS OF UNLAWFUL INTERFERENCE, ANNEX 17 TO THE CONVENTION ON INTERNATIONAL CIVIL AVIATION, at 4–5 (9th ed. 2011).

62. ICAO, INTERNATIONAL STANDARDS AND RECOMMENDED PRACTICES, SECURITY – SAFEGUARDING INTERNATIONAL CIVIL AVIATION AGAINST ACTS OF UNLAWFUL INTERFERENCE, ANNEX 17 TO THE CONVENTION ON INTERNATIONAL CIVIL AVIATION, at 2-1 (10th ed. 2017).

63. Schmidt, *supra* note 25, at 191.

64. *Id.* at 192.

65. ICAO RESOLUTIONS ADOPTED BY THE ASSEMBLY, 39TH SESSION: PROVISIONAL EDITION, (Oct. 2016), https://www.icao.int/Meetings/a39/Documents/Resolutions/a39_res_prov_en.pdf.

66. *See* ICAO UNITING AVIATION, https://www.icao.int/cybersecurity/Pages/default.aspx (last visited Feb. 3, 2020).

2. The Beijing Convention

The Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, also known as the Beijing Convention, categorizes cybercrime as an offense against international civil aviation. Therefore, terror attacks can also be treated under this Convention.[67] The Beijing convention was written on September 10, 2010, but it came into force only in July 2018, after Turkey became the 22nd country to deposit instruments of ratification, acceptance, approval, or accession.[68]

3. The Montreal Convention of 1971

The Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation is known as the Montreal Convention of 1971; the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation expanded the legal framework to also include unlawful violent acts that occur at airports. According to this Convention, a cyber attack can be deemed a violent act and the unlawful operation of an aircraft that would render it incapable of flying. [69]

4. Lack of Uniform Regulations

The main problem with international regulations is their lack of uniformity. Too many parallel regulations exist, so that different countries may need different standards. Airplanes usually cross borders and even continents, so how may an airplane manufacturer know which standards to follow? Does an airport allow only certain airplanes to land—namely those that meet certain regulations? All these matters can be resolved by the adoption of decisions on a clear and coherent international standard.

---

67. *Id.*

68. The list of countries that adopted the convention is available at: *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation Done at Beijing on 10 September 2010*, https://www.icao.int/secretariat/legal/List%20of%20Parties/Beijing_Conv_EN.pdf. (last visited Feb. 3, 2020). *See also Beijing Convention to Enter into Force on 1 July 2018*, ICAO, https://www.icao.int/Newsroom/Pages/Beijing-Convention-to-enter-into-force-on-1-July-2018.aspx. (last visited Feb. 3, 2020); Cyril-Igor Grigorieff, Charlotte Thijssen & Annick Sleeckx, *Attacks Against Aviation: Beijing Convention and Protocol Now in Force*, 44 AIR & SPACE L. (2) 125 (2019).

69. Schmidt, *supra* note 25, at 198.

The situation proves even more complex in respect of national and regional regulations. Usually, every country or region reacts differently to cyber attacks. We examine some of them next.

### *C. National and Regional Regulations*

1. The United States

a. Background

In the United States, the discussion also started in the early 2010s. President Obama stated in February 2013 that enemies of the US were bent on sabotaging air traffic control systems by hacking into them.[70] Note that, although the military-civil aviation was not the issue, the US army tried to shield its forces from cyber threats as well. The potential cyber threat to the US Air Force also started to be discussed publicly in the 2010s. For instance, in 2015, the Air Force in Ohio sought to shield from hackers its military-manned and remotely piloted aircraft; its on-board intelligence, surveillance, and reconnaissance (ISR) systems; its munitions; and any equipment, component, or subsystem that could compromise Air Force weapons. It reportedly invested $49.7 million USD in this project.[71]

b. The Government Accountability Office 2015 Report

In the US Government Accountability Office (GAO) Report to Congressional Requesters in 2015, the Federal Aviation Administration (FAA) was mentioned as being responsible for the national airspace system (NAS). The report described risks to air transportation. It carried 17 recommendations relating to the information security program and stressed the need to establish an integrated management approach to security risk. In a separate report, with limited public access, 168 specific actions were mentioned.[72]

---

70. *Id.* at 169.

71. John Keller, *Air Force Seeks to Shield Military Avionics from Computer Hackers,* MIL. & AEROSPACE ELECTRONICS, May 2015, at 4.

72. Fox, *supra* note 27, at 200.

c. Cyber AIR Act

In addition to several general acts that place airports among the critical infrastructures, there are signs of attempts to form a specific cyber aviation act to handle some of the required aspects. The bill, titled Cybersecurity Standards for Aircraft to Improve Resilience Act of 2017, also known as the Cyber AIR Act, was presented to the US Senate on March 21, 2017.[73] It suggests that the Department of Transportation (DOT) be able to ask "air carriers and manufacturers of aircraft or electronic control, communications, maintenance, or ground support systems for aircraft, to disclose to the Federal Aviation Administration (FAA) any attempted or successful cyber attack against any system onboard an aircraft or against any maintenance or ground support system for aircraft."[74] Based on that information the FAA will be able to improve regulations and add additional cybersecurity requirements for obtaining an air carrier operating certificate or a production certificate. It will be able to notify all the relevant players, including other federal agencies, of cybersecurity vulnerabilities in systems related to aviation—ground-support systems, maintenance systems, and on-board systems.[75] The bill also suggests that the Commercial Aviation Communications Safety and Security Leadership Group (an interagency working group established by the FAA and the Federal Communications Commission (FCC) in Jan. 2016[76]) will

"(1) be responsible for evaluating the cybersecurity vulnerabilities of certain broadband wireless communications equipment designed for consumer use on board aircraft; and

(2) require the implementation by air carriers, manufacturers, and communications service providers of technical and operational security measures it deems necessary to prevent cyberattacks that exploit such equipment."[77]

d. Code of Federal Regulations – Title 14

The current law has some aspects that already relate to cyber security: The Code of Federal Regulations – Title 14 deals with

73. *See* Cyber AIR Act, S. 679, 115th Cong. (2017).

74. *Id.*

75. *Id.*

76. MEMORANDUM OF UNDERSTANDING: FRAMEWORK FOR DOT-FCC COORDINATION OF COMMERCIAL AVIATION COMMUNICATIONS SAFETY AND SECURITY ISSUES (Jan. 29, 2016), https://www.fcc.gov/sites/default/files/signed-framework-agreement-jan-29-2016.pdf.

77. Cyber AIR Act, *supra* note 70.

Aeronautics and Space. Part 108 of Title 14 concerns Aircraft Operator Security. However, there are no special considerations as regards cyber attacks and threats. Although several clauses refer to information security, this is for reasons of privacy and prevention of impersonation rather than preventing a cyber threat.[78] As for subpart D, referring to "Threat" and "Threat Response," the threats described are conventional (bombs, air piracy, etc.) and not cyber.

Part 191 deals with Protection of Sensitive Security Information, which means protecting restricted information from being revealed by an unauthorized entity. This part does not refer especially to cyber threats as hacking the systems.

e. The Federal Information Security Modernization Act (FISMA) of 2014

The FISMA Act deals among other things with cyber threats. The act's goals are to protect federal agencies from security threats. It requires federal agencies to develop a comprehensive policy and to implement measures to protect information and information systems.[79] Cyber threats are mentioned in this act in several contexts. One concerns the Federal Information Security Incident Center, which should provide intelligence and other information about cyber threats, vulnerabilities, and incidents to agencies, thereby assisting them in assessing risks.[80] This law applies to the Department of Transportation and to the FAA as federal agencies, and therefore also applies to civil aviation. According to this act, the Department of Transportation, which also oversees the aviation sector, must produce a wide-ranging information security policy. In 2016 the IG's report declared that "DOT has been slow to take the corrective actions to address its cybersecurity weaknesses."[81]

78. *See* 14 C.F.R. §§ 108.223(g), 108.229(d)(8) (2002).
79. 44 U.S.C. § 3551 (2014).
80. 44 U.S.C. § 3556 (2014).
81. DEPARTMENT OF TRANSPORTATION, *Top Management Challenges for Fiscal Year 2016*, OFF. OF INSPECTOR GEN. 1, 11 (NOV. 16, 2015), https://www.faa.gov/about/plans_reports/media/FY_2016_IG_Top_Management_Challenges.pdf.

f. Cooperation between the US and the EU and the Role of the FAA

During the 2000s, the US made progress toward its transition to the Next Generation Air Transportation System (NextGen);[82] in 2011, it signed a Memorandum of Cooperation with the European Union and its Single European Sky ATM Research (SESAR) program. Thus, the US and the EU started cooperating to ensure harmony and secure global interoperability in the modernization initiatives of the two programs. This collaboration supports the International Civil Aviation Organisation (ICAO), Global Air Navigation Plan (GANP), and its Aviation System Block Upgrade (ASBU) program. [83]

Among other things, this collaboration deals with information management; trajectory management; communication, navigation and surveillance (CNS); and airborne interoperability. However, there is no special or separate part regarding cyber threats.[84] We assume that those threats are discussed along with other risks. In this respect, it is worth mentioning that in 2012 the IG of the Department of Transportation revealed that the FAA had not applied security requirements sufficient for the NextGen.[85]

In 2016, the FAA declared that the increasingly interconnected National Aviation Services (NAS) system presented new cybersecurity challenges. Therefore, the FAA announced: "[t]he FAA will take an active role in characterizing system deficiencies, and prioritizing investments to remedy the gaps; evaluate new technologies that provide cyber resilience; and provide testing and prototyping support for modifications."[86]

Among other things, the FAA would pursue promising research to find solutions for cyber attacks.[87] However, the DOT IG's report Top Management Challenges for Fiscal Year 2017 noted

82. *See* Federal Aviation Administration, *Modernization of U.S. Airspace*, FEDERAL AVIATION ADMINISTRATION, https://www.faa.gov/nextgen/.

83. SESAR JOINT UNDERTAKING, NextGen - SESAR State of Harmonisation 5–7 (2nd ed., 2016).

84. *Id.*

85. U.S. Department of Transportation, *FAA Has Not Adequately Implemented Security Requirements for Its En Route Automation Modernization System*, OFF. OF INSPECTOR GEN., Dec. 19, 2012.

86. *See generally* DEPARTMENT OF TRANSPORTATION, *The Future of the NAS* (2016), https://www.faa.gov/nextgen/media/futureofthenas.pdf.

87. *Id.* at 33.

that the FAA Security Operations Center (SOC) might not be complied with the federal law requirements. [88] In addition,

> FAA Air Traffic Organization (ATO) established the National Airspace System (NAS) Cyber Operations (NCO) to integrate with NAS services, programs, and infrastructure. The NCO is the focal point for all coordination of NAS cyber security activities. When NCO validates that a US-CERT reportable cybersecurity incident has occurred, NCO will notify the FAA SOC within a timeframe that ensures compliance with US-CERT Federal Incident Notification Guidelines.[89]

In our opinion, collaboration with the US-CERT is a necessary step toward the goal of effective containment of cyber threats in the aviation field, as we shall explain later. But this is not enough.

The FAA also publishes Special Conditions for a certain manufacturer, such as those issued for Boeing Model 787-8 Airplane on December 28, 2007. In this special-conditions clause, the FAA declared that this particular model had novel or unusual design features; above all, it allowed access to external systems and networks such as Wi-Fi, satellite communications, electronic mail, the Internet, etc. Therefore, the regulations of 2007 did not cover all the relevant security aspects. Hence the FAA published the special conditions that Boeing had to follow for its 787-8 airplane.[90]

g. Interim Summary

As we see, until recently, the US reacted to the current challenges sporadically and in a disorganized way. In the past few years, we have witnessed a change. There was an attempt to enact a cyber air law, but as we saw, this bill does not deal with all the relevant aspects. Even if it does, it is a local law that can solve some of the problems, but not all of them due to the special, complex, and international character of the aviation sector. In

88. DEPARTMENT OF TRANSPORTATION, *Top Management Challenges for Fiscal Year 2017*, OFF. OF INSPECTOR GEN. 1, 11 (Nov. 15, 2016), https://www.faa.gov/about/plans_reports/media/FY_2017_IG_Top_Management_Challenges.pdf.

89. *Id.*

90. FEDERAL AVIATION ADMINISTRATION (FAA), Special Conditions: Boeing Model 787-8 Airplane; Systems and Data Networks Security-Protection of Airplane Systems and Data Networks from Unauthorized External Access, 72 Fed. Reg. 73582 (2007) [hereinafter Fed. Reg. 73582].

addition, there is a tendency to move from sporadic handling of cyber attacks to a more comprehensive and systematic solution. A problem that should be answered as quickly as possible is the existence of multiple institutions in the cyber security field and the lack of a clear division of responsibility regarding the cyber threats in civil aviation. We now examine the current law concerning civil aviation in the EU.

2. The European Union

a. Background

In the EU, we can find several relevant directives and regulations; none was specific designed for cyber security and aviation. However, some of them may serve as a good starting point for responding to cyber threats as well.

b. Regulation (EC) No 2320/2002 and the Directive (EU) 2016/1148 – Civil Aviation Security and Network and Information Systems Security

In 2008 the regulation on Common Rules in the Field of Civil Aviation Security, which repealed Regulation (EC) No. 2320/2002, was enacted. This regulation is meant to cover all security risks that the aviation sector faces, although it does not explicitly mention cyber security threats. It also provides the basis for a common interpretation of Annex 17 to the Chicago Convention on International Civil Aviation mentioned earlier. The regulation's main goal is to create common rules to protect civil aviation from acts of unlawful interference that jeopardize its security. This goal will be achieved by setting common rules and standards for aviation security and by creating a mechanism for monitoring compliance with those rules.[91] The regulation applies to all suppliers in the aviation sector, and as such, it includes airports, operators, air carriers, and other entities that are related to airports:

> (a) all airports or parts of airports located in the territory of a Member State that are not exclusively used for military purposes;

91. Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on Common Rules in the Field of Civil Aviation Security and Repealing Regulation (EC), NO 2320/2002 (Mar. 11, 2008), at § 1.

> (b) all operators, including air carriers, providing services at airports referred to in point (a);
> (c) all entities applying aviation security standards that operate from premises located inside or outside airport premises and provide goods and/or services to or through airports referred to in point (a).[92]

However, the Annex of the regulation, in which the common basic standards are laid down, does not treat cyber security threats at all.[93]

The regulation was mentioned later in Directive (EU) 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union.[94] This directive categorized air transportation services, including private airport managing bodies and air carriers, as "operator[s] of essential services."[95] The directive came slowly and partially into force between 2017 and 2018.[96]

However, not all the services that an airport suggests will be recognized as essential, according to the Preamble paragraph 22:

> It is possible that entities operating in the sectors and subsectors referred to in this Directive provide both essential and non-essential services. For example, in the air transport sector, airports provide services which might be considered by a Member State to be essential, such as the management of the runways, but also a number of services which might be considered as non-essential, such as the provision of shopping areas. Operators of essential services should be subject to the specific security requirements only with respect to those services which are deemed to be essential. For the purpose

92. *Id.* at § 2(1).
93. *Id.* at § 4(1), Annex.
94. *See generally* Directive (EU) 2016/1148 of the European Parliament and of the Council Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, L 194/1 (JULY 6, 2016) [hereinafter Directive 2016/1148].
95. *Id.* art. 4(4), Annex II.
96. *See, e.g.*, *id.* art. 5, 10, 11, 12, 16, 21, 24, 25. § 23 (deals with reports that will start in 2019 and 2021).

> of identifying operators, Member States should therefore establish a list of the services which are considered as essential.[97]

According to this Directive, Member States will operate a national strategy for the security of network and information systems; each member state will designate one or more national competent authority/ies for the security of network and information systems and will designate a single national point of contact for the security of network and information systems. Each member state will also designate one or more computer security incident response team/s. All of these bodies should cooperate on the national level, on the EU level, and in some situations on the international level.[98]

According to article 14 of the directive:

> Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.
>
> Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.
>
> Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-

97. *Id.* at Preamble ¶22.
98. *Id.* art. 7–13.

> border impact of the incident. Notification shall not make the notifying party subject to increased liability.[99]

And according to article 16 of the directive:

> Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:
>
> (a) the security of systems and facilities;
> (b) incident handling;
> (c) business continuity management;
> (d) monitoring, auditing and testing;
> (e) compliance with international standards.

The EU, as noted, applies measures to ensure that air transportation services, as essential services, will not be able to ignore cyber threats.[100]

c. Directive 2013/40/EU on Attacks against Information Systems

More directives are considered related to cyber security in the aviation sector. One of them is Directive 2013/40/EU on Attacks against Information Systems.[101] The directive was enacted as a solution to a lacuna in the criminal law on cyber attacks against information systems. The directive proposed relevant definitions of criminal offenses and relevant sanctions (mainly in cases that are not considered minor). The directive also sought to improve the cooperation among competent authorities. These including the police and Eurojust, Europol and its European Cyber Crime

99. *Id.* art. 14.

100. Directive 2016/1148, *supra* note 94, art. 14.

101. *See generally* Directive 2013/40/EU of the European Parliament and of the Council on Attacks Against Information Systems and Replacing Council Framework Decision, 2005/222/JHA (Aug. 12, 2013).

Centre, and the European Network and Information Security Agency (ENISA), in order to obtain a complete picture of security regarding cybercrime at the Union level. Cooperation among the different authorities should contribute to the design of a more effective response. In addition, the directive declares that the Member States should take appropriate measures for efficient protection against cyber attacks. The directive does not relate to the aviation field in particular, but it is relevant to aviation as well.

d. Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection

This Directive recognized the air transport sector as a European Critical Infrastructure (ECI).[102] Its purpose was to prevent terror attacks against critical infrastructure. However, the Directive does not explicitly mention cyber threats, and they are not kept separate from physical threats. The Directive declares that every ECI should have an operator security plan (OSP) that will identify the ECIs' assets and will map the existing solutions and what protection has been implemented.[103] The Directive's main goal is to develop and facilitate improved protection of ECIs, among other ways, by their sharing information.[104] Therefore, this Directive is relevant to aviation as an ECI.

e. Directive 2002/58/EC on Privacy and Electronic Communications and the General Data Protection Regulation (GDPR)

Some directives refer to privacy protection, such as Directive 2002/58/EC on Privacy and Electronic Communications and the General Data Protection Regulation (GDPR). They are also relevant in some respects to aviation. For example, the protection of data collected on passengers may be subject to one or more directive/s.

---

102. Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve their Protection, L 345/75 (Dec. 8, 2008), art. 3(3), Annex I.

103. *Id.* art. 5, Annex II.

104. *Id.*

f. The European Union Agency for Network and Information Security (ENISA) and the European Aviation Safety Agency (EASA)

Moreover, the European Union Agency for Network and Information Security (ENISA) was established in 2004,[105] primarily to ensure the security of network and information within the EU. In 2013, Regulation (EU) No. 526/2013 renewed the Agency's mandate until 2020.[106] ENISA supports the European institutions, the member states, and the business community by responding to, and preventing, network and information security threats. ENISA provides information and expertise in security issues which helps to create policies, implement them in Member States, assist in developing training programs, raise awareness of cyber security, and fosters the network and information-security community.[107]

In 2017, the Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency," and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") was published.

This working document emphasized that the scope of the cybersecurity threats was rapidly widening, while the European Union relied increasingly on digital infrastructures and services. Moreover, the working document clearly stated that a central EU Agency should handle cyber threats and coordinate EU responses to them:

> Europe needs a focal point to address these new threats which are horizontal in nature impacting on multiple industrial sectors. The findings of this

105. Regulation (EC) n 460/2004 of the European Parliament and of the Council establishing the European Network and Information Security Agency, I.77/1 (Mar. 10, 2004), at Preamble ¶¶ 1, 2, 8, 11.

106. Regulation (EU) No 526/2013 of the European Parliament and of the Council Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC), No 460/2004 (May 21, 2013), at Preamble ¶ 52 [hereinafter Regulation 526/2013].

107. Regulation (EU) No 526/2013 of the European Parliament and of the Council Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004, art. 2 (May 21, 2013). *See generally* Commission Staff Working Document on the evaluation of the European Union Agency for Network and Information Security (ENISA) Accompanying the document Proposal for a regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), SWD(2017) 502 (Sept. 13, 2017) [hereinafter Comm'n Staff Working Doc.].

> evaluation suggest that there could be a need for an EU Agency organised on a cross sectoral/horizontal basis with a strong mandate. The evaluation also found that there is also a need for cooperation and coordination across different stakeholders. The need for a coordinating entity at EU level to facilitate information flows, minimise gaps and avoid overlapping of roles and responsibilities becomes ever more acute. A decentralised EU agency and a neutral broker, could ensure a coordinated approach to cyber threats in the EU.[108]

Annex 8 of the working document includes JRC's analysis and recommendations for a European certification and labeling framework for cyber security in Europe. Their recommendations must clearly indicate the need for a harmonized response and a central EU Agency to coordinate all the member states:

> 1. A European security certification scheme should be set-up to overcome the national differences.
> 2. The basis for the new European security certification scheme shall be based on the Common Criteria.
> 3. A process to define harmonized protection profiles for specific domains should be put in place with the collaboration of existing organizations like SOG-IS or agreements like CCRA.
> 4. The definition of harmonized protection profiles is the basis for the definition of a labelling scheme to support the comparability and visibility of the security certification for end-users.
> 5. Security and privacy requirements should be validated in the same certification process and with the same harmonized protection profiles.
> 6. A process to create accredited security testing centres should be defined. The experience from the Horizon 2020 Future Internet Research & Experimentation (FIRE) could be useful at least for the IoT related products.

108. *Id.*

> 7. A post certification framework to support the lifecycle of products and to mitigate gaps in the security certification process and execution should be investigated and deployed.
>
> 8. The application of testing models and automated testing suites should be investigated in security certification to improve the efficiency of the security certification process and to address the issue of re-certification after product changes.[109]

Thus, Annex 9 – Mapping of cybersecurity sectorial initiatives—relates specifically to the transportation sector, including aviation. As mentioned, the transportation sector is one of the sectors especially vulnerable to cyber-attacks as this sector relies increasingly on digital equipment and on complex IT architectures. A cyber threat to the transportation sector might cause massive loss of life as well. In Air Transport there is consensus among the aviation community that cyber threats should be addressed in a holistic response at the EU level based on existing policies in coordination with other parties.[110]

The commission also proposed that the role and mandate of the European Aviation Safety Agency (EASA)[111] (an agency of the EU with regulatory and executive tasks in the field of civilian aviation safety) be clarified in the Aviation Safety Regulation[112] related to cyber security and that essential cyber security requirements be outlined.[113]

EASA set up the European Centre for Cyber Security in Aviation (ECCSA). This body involves both the public and the private sector, including EU member states, airlines, manufacturers of aircraft, avionics and ground systems, airports, etc. EASA signed a memorandum of understanding with EU-CERT that ECCSA would provide a secured IT infrastructure in tandem with cybersecurity tools and management services. Thus, ECCSA can provide an assessment of cyber incidents

---

109. *Id.* at annex 8.

110. *Id.* at annex 9.

111. Commission Regulation 216/2008 of the European Parliament and of the Council on Common Rules in the Field of Civil Aviation and Establishing a European Aviation Safety Agency, and Repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC, L 79 (Feb. 20, 2008), at Preamble ¶ 4.

112. Directorate General of Communications for the European Union Comm'n, *New cooperation in support of Cyber Security in Aviation*, EUROPEAN AVIATION SAFETY AGENCY (Feb. 16, 2017), https://ec.europa.eu/digital-single-market/en/news/new-cooperation-support-cyber-security-aviation.

113. Comm'n Staff Working Doc., *supra* note 107, at annex 9.

and assistance in coordinating the response.[114] ECCSA is an information center for cybersecurity in aviation. It provides different services, including providing its members with secure means to exchange domain-relevant cybersecurity information, such as vulnerabilities. ECCSA's operational team of analysts aims to facilitate a comprehensive perspective on aviation cybersecurity threats.[115]

g. Single European Sky Air Traffic Management Research (SESAR)

Cybersecurity in aviation is also an integral part of the EU air traffic management (ATM) Master Plan, hence likewise of the Single European Sky Air Traffic Management Research (SESAR) Joint Undertaking 2020 Work Programme.[116] In addition, the European Civil Aviation Conference (ECAC) published in Doc 30 part II a policy statement on aviation security measures, including cyber security, which was adopted by all 44 ECAC member states.[117]

h. Procedures for Conducting Commission Inspections and Regulation that Focus on Traditional Threats

The Commission Regulation (EU) No 72/2010[118] covers procedures for commission inspections (according to Regulation 300/2008) in the field of aviation security. These consider the cooperation needed among member states in order to conduct annual inspections, as well as the exercise of commission powers.

---

114. *Id.*

115. *See European Centre for Cybersecurity in Aviation*, EUROPEAN UNION AVIATION SAFETY AGENCY [EASA], https://www.easa.europa.eu/eccsa (last visited Feb. 2, 2020).

116.Paul Ravenhill & Matt Shreeve, *SESAR Strategy and Management Framework Study for Information Cyber-Security*, HELIOS, (Sept. 2015), https://www.sesarju.eu/sites/default/files/documents/news/SESAR_Strategy_and_Management_ Framework_Study_for_Information_cybesecurity_FINAL.pdf; *see generally* Dimitris Gritzalis, George Iakovakis, & Georgia Lykou, *Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management*, *in* CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE 245, 245–60 (2019).

117. *See Security*, EUROPEAN CIVIL AVIATION CONF. [ECAC], https://www.ecac-ceac.org/security (last visited Feb. 2, 2020, 3:52 PM).

118. Commission Regulation 72/2010 Laying Down Procedures for Conducting Commission Inspections in the Field of Aviation Security, 2010R0072 (Jan. 26, 2010), at Preamble ¶ 1.

The Commission Implementing Regulation (EU) No. 2015/1998[119] also relates to regulation 300/2008 and lays down detailed measures for the implementation of the common basic standards in aviation security, but mainly focuses on traditional threats.

Similar regulations that mainly focus on traditional threats are Regulation (EC) No. 1592/2002 of the European Parliament and of the Council of 15 July 2002 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency. The Commission Implementing Regulation (EC) No. 1035/2011 concerns the provision of air navigation services,[120] including provisions for security management systems and ATM equipment; and Commission Implementing Regulation (EC) No. 923/2012[121] concerns common rules on air-traffic flow management (ATFM).

Similarly, Commission Regulation (EU) No. 677/2011[122] concerns detailed rules for the implementation of air traffic management (ATM) network functions. It mainly focuses on the establishment of a network manager and her tasks, strategy and operational plans for the network, and relations inside and outside it. These relations mainly involve the Single Sky Committee, cooperative decision-making, the consultation process, building detailed work arrangements and processes for operations, devising rules for monitoring, reporting and overseeing the network, and establishing the European Aviation Crisis Coordination Cell (EACCC). There are more regulations in this field,[123] but they are less relevant.

---

119. *See generally* Commission Implementing Regulation 2015/1998 Laying Down Detailed Measures for the Implementation of the Common Basic Standards on Aviation Security, L 299/1 (Nov. 5, 2015).

120. Commission Implementing Regulation 1035/2011 Laying Down Common Requirements for the Provision of Air Navigation Services and Amending Regulations 482/2008 and EU 691/2010, L 271/23 (Oct. 17, 2011), at Preamble ¶1, Annex 1.

121. Commission Implementing Regulation 923/2012 Laying Down the Common Rules of the Air and Operational Provisions Regarding Services and Procedures in Air navigation and Amending Implementing Regulation (EU) No 1035/2011 and Regulations (EC) No 1265/2007, (EC) No 1794/2006, (EC) No 730/2006, (EC) No 1033/2006 and (EU) No 255/2010, L 281/1 (Sept. 26, 2012), art. 1, 2.

122. *See generally* Commission Regulation 677/2011 Laying Down Detailed Rules for the Implementation of Air Traffic Management (ATM) Network Functions and Amending Regulation (EU) No 691/2010, L 185/1 (July 7, 2011).

123. Regulation 551/2004 of the European Parliament and of the Council of 10 March 2004 on the Organization and Use of the Airspace in the Single European Sky (The Airspace Regulation), 2004R0551 (Mar. 10, 2004), at Preamble ¶8; *see* Regulation 376/2014 of the European Parliament and of the Council on the Reporting, Analysis, and Follow-up of Occurrences in Civil Aviation, Amending Regulation (EU) No 996/2010 of the European Parliament and of the Council and Repealing Directive 2003/42/EC of the European Parliament and of the Council and Commission Regulations (EC) No 1321/2007 and (EC) No 1330/2007, 24.4.2014 (Apr. 3, 2014); *see also* Commission Regulation 73/2010 Laying Down Requirements on the Quality of Aeronautical Data and Aeronautical Information for the Single European Sky, 27.1.2010 (Jan. 26, 2010).

i. Interim Summary

As can be seen, the EU tries to respond to cyber threats. The problem is that too many regulations and formal institutions exist, but no central and distinct body is recognized as able to give a formal and final response to some of the threats. There is also the problem of a lack of a clear division of accountability among the different institutions across Europe. Perhaps ENISA is the answer. Still, there has to be a special and separate department able to take into account the special character of the civil aviation sector. This notion is analyzed in the following part.

## IV. CIVIL AVIATION IS UNIQUE COMPARED WITH OTHER CRITICAL INFRASTRUCTURES

The civil aviation sector is complex and unique. In contrast to other critical infrastructures such as hospitals, electricity companies, and even ground transportation, wherein a cyber attack will usually harm just one country, a cyber attack in the aviation sector might influence many countries simultaneously. One airplane may leave an airport in one country and land at a different one. During its flight, the airplane usually crosses other countries as well. Not only does the airplane usually leave from one state and fly to another, onboard one usually finds people of various nationalities. Hence the situation is highly complex, considering that different legal systems may apply in different situations.

Moreover, the international circumstances of many regulators, as noted, necessitates the determination of a proper standard and appropriate response. Sometimes one standard might be different from another on account of the different regulators. Airplane manufacturers must decide whether to apply to the RCTA standard to ISO, to FAA, or to others. If airports in the US do not allow airplanes from Africa to land because their airplanes do not meet one of the US standards, this might cause problems. On the other hand, these standards were written in order to prevent cyber security threats that might endanger many lives. But what should airplane manufacturers do if views differ as to the proper standard? If they follow the strictest one in order to be able to land everywhere, that should be considered the highest standard. In our opinion, this domain should be internationally regulated in order to equalize demands, so airplanes might land everywhere.

Also, in the civil aviation sector, there are many regulators in different areas—airplane manufacturers, baggage and passenger management systems, security device manufacturers, software-system maintenance companies, and so on. In addition, as we explained earlier, in one airport there are many suppliers, including, but not limited to, the airport itself, operators, and air carriers. The assumption that the parts and systems we buy today are cyber-security protected is mistaken due to the various cyber-security issues still to be covered—in our opinion, internationally.

We cannot stop technology progressing, as we explained above. The increasing dependence on computers and the internet, GPS, etc., will simply intensify. As we saw earlier, the aircraft is connected to ground websites, to government and non-government services that use radio frequencies, to GPSs, to aircraft communications addressing and reporting system (ACARS),[124] and to an electronic flight bag (EFB).[125] There will be more and more provision of Wi-Fi and Cellular connections as a service to the passengers. As we indicated earlier, due to all the foregoing, the aircraft is more exposed to cyber vulnerabilities. Every connection to the Internet might be subject to an attack. The vulnerabilities might lie in a device or in the external connection itself.

Then there might be legal forum shopping in the selection of the particular aircraft or particular country in which the attack will take place. The diversity of legal responses to cyber attack on an airplane in different countries, and the different regulations and standards of the cyber security level in the aircraft and the airport, might cause the attack to happen in some airplanes of some countries and above certain states so that the perpetrator might evade or reduce the charges and penalties if caught.

In our opinion, the uniqueness of the civil aviation infrastructure leads to the conclusion that a joint and global effort should be made to reduce cyber risks. There should be only one legal response to those risks to avoid the attempt at airborne forum shopping. Also, there should be just one global and international cyber security standard for the entire chain of suppliers, or at least similar and equivalent unified standards, in

---

124. ACARS is a digital data link radio transmission system of short messages between an aircraft and ground stations.

125. *See* Fed. Aviation Admin., AC No. 120-76B, *Guidelines for the Certification, Airworthiness, and Operational Use of Electronic Flight Bags,* Federal Aviation Admin., 1, 1 (2012), https://www.faa.gov/documentlibrary/media/advisory_circular/ac%20120-76b.pdf (last visited Feb. 2, 2020, 5:00 PM).

order to avoid different requests by different countries from the aircraft manufacturer, maintenance companies, airport and airport suppliers, and so on.

The understanding that government entities cannot handle cyber security separately from the industry is not new.[126] In the US, calls have also been made to set up a central agency of cross-stakeholder collaboration in cyber security that will focus on what has happened and not on whom to blame; such an agency could be akin to the National Transportation Safety Board.[127] Similar views are evident in the EU at least in respect of the new central and general (not just aviation) cyber agency. According to EU 526/2013 Explanatory Memorandum section 30, to achieve its objective the new cyber agency should maintain a continuous link with various bodies such as "CERT-EU, European Cybercrime Centre (EC3) at Europol, European Defence Agency (EDA), European Agency for the operational management of large-scale IT systems (EU-LISA), European Aviation Safety Agency (EASA) and any other EU Agency that is involved in cybersecurity."[128]

The recognition that a centralized reaction should be exerted in response to a cyber attack, as we have already seen, is even more important for civil aviation when different nationalities and different legal systems might be involved. We believe that such an agency that will handle cyber security in civil aviation should be international and global. As we have shown, steps have been taken in that direction in recent years, at least within continents. Collaboration is also in the offing between the EU and the US with the signing of a Memorandum of Cooperation between the US Next Generation Air Transportation System (NextGen) and the European Union Single European Sky ATM Research (SESAR). As we saw earlier, this collaboration supports international entities such as the International Civil Aviation Organisation (ICAO), the Global Air Navigation Plan (GANP), and its Aviation System Block Upgrade (ASBU) program.[129]

In our opinion, there should be an international and central policy, strategy, agreement, or standards, which define cyber security and define the necessary measures to be implemented in the civil aviation sector. The American Institute of Aeronautics and Astronautics (AIAA) shares this view. In its August 2013

126. Staff Writer, *UAS Symposium: FAA Can't Take on Cybersecurity Alone*, AVIONICS INT'L. (Mar. 31, 2017), https://www.aviationtoday.com/2017/03/31/uas-symposium-faa-cant-take-cybersecurity-alone/.

127. Duchamp, Bayram & Korhani, *supra* note 7, at 8.

128. REGULATION 526/2013, *supra* note 103, at 19.

129. Fed. Reg. 73582, *supra* note 87, at 5–7.

Decision Paper – The Connectivity Challenge: Protecting Critical Assets in a Networked World – A Framework for Aviation Cybersecurity, the AIAA stated:

> It is critical that all of these members adopt a collaborative, risk-informed decision-making model to set goals and define a cybersecurity framework and roadmap to strengthen the aviation system's resilience against attacks. This roadmap must be driven by a common vision and strategy, differentiate economic from safety-related concerns, and address all security layers including know, prevention, detect, respond, and recover.[130]

The AIAA also recommended, among other things, establishing common cyber standards for aviation systems, to globally understand the risk and the threat, to keep all the relevant members informed of threats and sharing information on how to tackle them, to conduct necessary research and development in the field and to ensure continuous communication and cooperation between governmental institutions and commercial industry.[131] Similarly, in 2016 the International Civil Aviation Organization (ICAO) recommended forging better and stronger collaboration among all the stakeholders of the civil aviation sector in order to identify threats and risks.[132]

According to Emilio Iasiello, the aviation ecosystem is expensive and too large to be secured holistically. However, even Iasiello believes that policies of managing cyber security can be standardized among international stakeholders.[133]

## V. CONCLUSIONS

In August 2017, the FDA announced the first-ever recall of a medical device due to cyber vulnerability. The configurable embedded computer systems inside the medical device might be vulnerable to cyber security intrusions and exploits.[134] Such a

130. *The Connectivity Challenge: Protecting Critical Assets in a Networked World – A Framework for Aviation Cybersecurity*, AM. INST. OF AERONAUTICS, (Aug. 2013), https://www.aiaa.org/uploadedfiles/issues_and_advocacy/aiaa-cyber-framework-final.pdf.

131. *Id.*

132. Duchamp, Bayram & Korhani, *supra* note 7, at 7.

133. Iasiello, *supra* note 3.

134. *Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude. Medical's) Implantable Cardiac Pacemakers*, U.S. FOOD & DRUG

recall is not efficient when new and old systems are implemented together. It will be almost impossible to recall an old device when necessary.

Cyber security vulnerabilities in civil aviation are increasing each year due to rising dependence on digital and similar systems and to air carriers' motivation to install Wi-Fi, Cellular reception, etc. as a service for the customers. As explained above, cyber attacks might occur inside the airport, in the air, in a joint attack with a traditional attack, or on several fronts. The consequences may well be devastating and international.

In addition to conventional terrorism such as an armed attack against an airport, planting explosives in a plane, or armed aircraft hijacking, new cyber threats must be dealt with. Most regulations on conventional terrorism do not apply to cyber security threats, at least not yet. The new cyber terrorism challenges are similar in some aspects to conventional terrorism, but in other ways they differ:

- The cyber attack may be covert and will not be noticed immediately, as a conventional attack would: for example, cyber terrorists will deflect the plane from its planned course without the pilot immediately observing it, in contrast to an armed attack on an airplane.
- The cyber attack may be delayed without being noticed – the plane or the airport perhaps already compromised by the malicious code without its being discovered for a long period. This contrasts with a delayed physical bomb that would probably be discovered fairly soon by conventional security procedures.
- The cyber attack can be launched from anywhere in the world, as opposed to conventional terrorism when at least one terrorist has to be physically in the attacked place.
- The cyber attack can easily be started without special means. All that is needed is a smart cellphone or any other computer. Thus, the cyber terrorist need not smuggle illegal materials onto the plane, unlike a conventional terrorist.

Current laws and regulations are insufficient. Technological solutions exist that can be applied. Considering that the airport itself depends on many suppliers, and many different legal systems may be relevant, a central body like the CRN should be in place to deal with these new threats locally and internationally. However, a legal answer to the threats should also be on hand.

---

ADMIN. (Aug. 29, 2017), https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm.

Creating such an entity is not easy, but it is essential in order to tackle cyber terrorism in general and cyber terrorism at airports and on airplanes in particular.

In our opinion, unified and international understanding is needed, regulated as an international treaty covering all current cyber threats to airports and aircraft. It is recommended that the treaty establish an international authority to coordinate all the necessary regulations concerning cyber security on the ground and in the air. In addition, every country must establish a local authority committed to the central and international authority but will be capable of delivering a rapid response to the local threats while reporting the attack to the international authority. This authority should also be the coordinator among professional institutions such as ICAO, EUROCEA, RTCA, and NIST.

In the international treaty, a policy should be set defining the minimal prevention measures that must be implemented. Public awareness must be raised regarding the potential risks and threats; this should become a consumer demand to maintain a certain level of cyber security. In this way, air carriers will take cyber security under consideration, resulting in a domino effect on aircraft manufacturers and other suppliers such as the maintenance companies and so on. A plethora of technical and professional institutions exist—private and governmental, and still more regulations and laws that can be applied to the civil aviation sector, but no international policy is to be found. Some steps have been taken toward global cooperation—such as the agreement between the EU and the US, but more must be done in this area.

The uniqueness of the civil aviation sector, caused by the multiple stakeholders and players active in it, makes it a unique critical infrastructure, as explained above. Hence this sector should be handled and dealt with differently from other critical infrastructures.

Finally, as mentioned earlier, when writing these lines, we discovered that hardly any legal academic discussion is ongoing on this important issue. Accordingly, an academic discourse should be initiated in this field, and more research conducted in the coming years.