DRAFT

Study on the Applicability of International Air Law Instruments to Cyber Threats against Civil Aviation

An overview and gap analysis of existing provisions

For readability and coherence, this study uses the terms and definitions presented in the attachment to this document. The terms are taken from known civil aviation and information security sources and referenced accordingly.

1. BACKGROUND INFORMATION

1.1 INTRODUCTION

1.1.1 Civil aviation transports passengers and goods around the world. It is a highly interconnected and valuable sector that has been challenged time and time again by various types of threats. The entire aviation sector consists of interconnected networks and systems creating a complex ecosystem that requires a holistic approach when assessing, preventing threats and prosecuting cyber-attacks.

1.1.2 The threats and risks to the aviation ecosystem have led to the creation of a strong and universal international air law framework. There is an urgent need at this point in time, as technology and cyber threats are rapidly evolving, to ensure that civil aviation is adequately protected by a strong legal framework that addresses and incriminates cyber intrusions threatening aviation safety and/or security.

1.1.3 The cyber threats to the civil aviation sector may be posed by malicious actors who could target information assets (including systems, data and information) of airports, air carriers, aircraft, air traffic control and air navigation facilities and could cause disruption or damage aircraft in service, potentially leading to injury or loss of life. Such attacks could also target manufacturers of aircraft and aircraft parts, their suppliers or maintenance, repair and overhaul facilities. It should be noted that, up until late 2021, while there were no known significant cyber-attacks on civil aviation leading to an accident[1], the consequences of a cyber-attack could be significant and should be taken into consideration when conducting the analysis of the applicable legal framework cyber-attack.

1.2 BACKGROUND OF THE STUDY IN ICAO's CYBERSECURITY WORK

1.2.1 The Secretariat Study Group on Cybersecurity ("SSGC") was established following the 39th Session of the ICAO Assembly. During the fourth meeting of the SSGC, the Research Subgroup on Legal Aspects ("RSGLEG") was established, with the aim of reviewing and analyzing (in relation to the identified threats, risks and actors) the adequacy of the current international air law framework in addressing cyber threats in civil aviation. The group comprises 22 experts from 15 States and 7 organizations. The group conducted its activity in virtual plenary meetings and Small Working Groups (on intent, effect, jurisdiction and scenarios).

1.2.2 The issue of addressing cyber threats to civil aviation has been introduced in the work programme of the ICAO Legal Committee during its 37th Session in 2018. ICAO Council approved during its 215th session the addition of the item *–consideration of the adequacy of existing international air law instruments in addressing cyber threats against civil aviation* to the programme of the Legal Committee. The ICAO Assembly, during its 40th Session in 2019 further agreed to maintain this item on the work programme of the Legal Committee.

1.2.3 Furthermore, ICAO 40th Assembly adopted the ICAO Aviation Cybersecurity Strategy which provides that the relevant international legal instruments should be analysed to identify existing or missing key legal provisions in air law for the prevention, prosecution, and timely reaction to cyber incidents in order to form the basis for consistent and coherent implementation of cybersecurity legislation and regulations throughout the global aviation sector.

1.2.4 Following the adoption of the ICAO Aviation Cybersecurity Strategy by the Assembly, ICAO Council adopted the ICAO Cybersecurity Action Plan (C-DEC 219/1 refers), focusing, among other actions, on the need to analyse the existing international air law framework to determine its adequacy in addressing cyber-attacks, as well as analyse and update or adopt, as necessary to allow for the deterrence,

[1] Incidents causing operational disruption have been reported.

investigation, and prosecution of cyber-attacks that impact the safety, security, efficiency, and/or continuity of civil aviation.

1.3 BROADER CONTEXT OF THE STUDY

1.3.1. Before analyzing the international air law instruments themselves, it is beneficial to assess the applicability of international public law to Information and Communications Technology (ICT)[2].

1.3.2 The applicability of international law to Information and Communications Technology (ICT) was determined by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security setup under the umbrella of the United Nations General Assembly (UN GA). The 2013 Report of the Group of Governmental Experts[3], as endorsed by the UN GA in 2014[4] determined that *"International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment".*[5]

1.3.3 The 2013 Report highlighted that *"The application of norms derived from existing international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability.*" Thereafter, the corresponding United Nations General Assembly (UN GA) Resolution[6] considered that *"further examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems"* could serve as strategies to address cyber threats.

1.3.4 More recently, in July 2021, the "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" established under the UN GA issued its conclusions and recommendations[7] for future work. One of these recommendations is the following:

"*95. The Group also identified potential areas for future work, which include but are not limited to: [...] c) Further sharing and exchanging of views on norms, rules and principles for responsible State behaviour and national and regional practices in norm and CBM implementation; and on how international law applies to the use of ICTs by States, including by identifying specific topics of international law for further in-depth discussion."*

1.3.5 The analysis of the existing international air law instruments with respect to their applicability to cyber threats or cyber-attacks against civil aviation is timely.

[2] **Information and communication technology**, abbreviated as **ICT**, covers all technical means used to handle information and aid communication. This includes both computer and network hardware, as well as their software. (Eurostat Glossary: https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:Information_and_communication_technology_(ICT)).

[3] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98*, 24 June 2013, Etpu (unidir.org), last retreived on 2 January 2022.

[4] A/RES/69/28

[5] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98*, 24 June 2013, Etpu (unidir.org), last retreived on 2 January 2022.

[6] A/RES/69/28

[7] Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, 14 July 2021, A_76_135-2104030E-1.pdf (un-arm.org), last retrieved on 2 January 2022.

1.4 OBJECTIVES, SCOPE AND FOCUS OF THE STUDY

1.4.1 The objective of the study[8] is to examine the adequacy of international air law instruments with regards to the deterrence from and prosecution of cyber-attacks against civil aviation and provide information and analysis on:

a) the interpretation of the existing international air law framework as it pertains to cyber threats against civil aviation;

b) the identification of potential gaps and possible options/solutions to address them;

c) the need for specific further study in order to propose solutions for the identified gaps, should the case may be; and

d) the best way to further promote the results of the study.

1.4.2 As methods of conducting cyber-attacks evolve over time and can be carried out with various technical means, this study takes a "technology neutral" approach. As such, it focuses on the effect or consequences of cyber-attacks on civil aviation, rather than the technology used in conducting the cyber-attack.

1.4.3 The following international air law instruments are analyzed:

- Convention on International Civil Aviation (Chicago, 1944 – "Chicago Convention");Annex *incl. Annex 17 – Security — Safeguarding International Civil Aviation Against Acts of Unlawful Interference.*
    - Protocol Relating to an Amendment to the Convention on International Civil Aviation [Article 3 *bis*] (Montreal, 1984 – "Protocol on Article 3 bis");

- Convention on Offences and Certain Other Acts Committed on Board Aircraft (Tokyo Convention 1963) (Tokyo, 1963 – "Tokyo Convention 1963");
    - Protocol to Amend the Convention on Offences and Certain Other Acts Committed on Board Aircraft (Montréal, 2014 – "Montréal Protocol 2014");

- Convention for the Suppression of Unlawful Seizure of Aircraft (Hague, 1970 – "Hague Convention 1970");
    - Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing, 2010 – "Beijing Protocol 2010");

- Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Montreal, 1971 – "Montreal Convention 1971");
    - 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 done at Montreal on 23 September 1971 (Montreal, 1988 – "VIA Protocol 1988");
        - Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing, 2010 – "Beijing Convention 2010").

1.4.4 Conclusions of this study relating to the international air law instruments will be reported to the 38th Session of the ICAO Legal Committee.

[8] When considering the adequacy of the existing international air law framework to address cyber threats, the UNGGE work could serve as reference.

2. PERSPECTIVE OF THE ANALYSIS

2.1 Object and purpose of the International Air Law framework

2.1.1 This study is carried out within the context, object and purpose of the legal regime created by the Chicago Convention. The principles enshrined in the Preamble of the said Convention, which have proven to remain relevant in today's context, serve as cornerstones for the analysis, the following provisions being particularly applicable:

> *"WHEREAS the future development of international civil aviation can greatly help to create and preserve friendship and understanding among the nations and peoples of the world, yet its abuse can become a threat to the general security; and*
>
> *WHEREAS it is desirable to avoid friction and to promote that cooperation between nations and peoples upon which the peace of the world depends;"*

2.1.2 The fact that a threat to civil aviation could prove to be a threat to general security was already recognized in 1944. Although the notion of cyber threats[9] could not have been explicitly included at the time." It could be considered that any such threats and attacks could fall within the context addressed by the Preamble to the Chicago Convention.

2.1.3 In parallel to the long-term vision enshrined by the Preamble of the Chicago Convention, the recurring theme throughout the whole international legal framework for civil aviation is the protection of the lives of passengers, crew, persons on the ground, and aviation assets by the introduction of measures regarding the safety and security of civil aviation. The Preamble and objectives of the Chicago Convention highlight the safety and security of international civil aviation as two of ICAO's five Strategic Objectives.

2.1.4 However, as there are not many explicit references to cyber threats in the framework as it stands today, this study will examine whether the existing international air law instruments could cover cyber threats either explicitly or implicitly, albeit using different terminology.

[9] See also UN General Assembly Resolution - A/RES/69/28 – expressing concern regarding the fact that ICT *"can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security*

3. STRUCTURE OF ASSESSMENT

3.0.1 The diversity of cyber threats and their possible effects, whether impacting the safety and/or security of civil aviation or not, necessitated a "structured reading" of the existing air law instruments. The methodology used to review the air law instruments, guide discussions and analyze the sample scenarios used in this study is based on the parameters outlined in this chapter.

3.0.2 It is important to note that the approach of each scenario/situation is different and implies that there is no one uniform answer/approach to the topic of "cyber threats". This stems from the fact that the cyber threat/cyber-attack represents just one method and means to affect civil aviation but not an end in itself.

3.1 Variety of actors

3.1.1 Various types of actors may be at the origin of a cyber-attack such as: individuals, State actors, groups, and legal entities. The diversity of actors implies that various motives may be found behind cyber-attacks such as sheer curiosity of tech-savvy teenagers, attempts to cause reputational damage, financial gains, and access to data or even more sinister motives driving international terrorist organizations.

3.2 The notion of intent (*mens rea*)

3.2.1 The various motives such as those mentioned above imply different levels of intent to harm civil aviation, directly or indirectly. Whether the intent behind a certain cyber-attack is to harm (such as affect safety or security or cause disruption and/or damage) civil aviation depends on each specific situation.

3.2.2 Proving the intent of a perpetrator, or lack thereof, is the prerogative, and one of the core legal arguments, of both the prosecution and defense in criminal law courts. Such an analysis will always depend on each specific case and it will ultimately be up to the courts to determine whether the prosecution or the defense will prevail.

3.2.3 Providing an in-depth discussion of this challenging topic is beyond the scope of this study. However, some of the key points touched upon in discussions can be summarized here.

3.2.4 While it can be argued that intent is inherent in a cyber-attack scenario, the question remains as to whether the attacker intended "only" the element of the attack with an impact on information security parameters (Confidentiality-Integrity-Availability) (; e.g., the effect on the information system and/or information/data) or whether the attacker intended the ultimate outcome of the cyber-attack (e.g., the grounding of aircraft due to non-reliable software, loss of life and aircraft, etc.).

3.2.5 Due to the interconnectivity of systems, an intended cyber-attack could even have consequences unintended by the attacker, and it may create cascading effects. For example, while the original intent of an attack might have been to access passenger information, this could lead to severe aviation disruption (e.g., through the sudden non-availability of passenger databases). Another situation may see civil aviation affected a cyber-attack that, does not target at civil aviation, but may nevertheless have significant effects on civil aviation, ranging from disruption to potential consequences on safety (e.g., cyber-attack on the operating system of tablets used as electronic flight bags).

3.2.6 The sub-group of the RSGLEG conducting the detailed analysis discussed that there is always a spectrum of intent ranging from intending the act itself to intending the full consequences of the act.

3.2.7 A look at the international air law instruments highlighted that a middle ground between intent to conduct the attack and intent vis-à-vis the full consequences of an attack has been chosen by ICAO in the international air law instruments for all types of acts, as illustrated by wording such as e.g. "[...] which is likely to endanger its safety in flight [..]." in Art. 1.1. b) of the Beijing Convention 2010.

3.3 Cyber-attack methods/means *(Actus reus element)*

3.3.1 The cyber-attack methods used by cyber criminals vary depending on their motives, the effect they wish to cause, as well as their capability to circumvent existing mitigation measures. Furthermore, methods will vary over time as new capabilities and technologies are developed, rendering their analysis less relevant for this study.

3.4 Variety of locations and attack paths *Actus reus element)*

3.4.1 The various cyber-attack methods used also imply different locations of the attacker and/or different paths. Some may be carried out from within the aircraft itself, others will be initiated from remote locations outside of the aircraft or even from a different country then the one where the attack took place.

3.4.2 Locating where the attack was initiated can be challenging in itself, as the international nature of the internet allows for the masking of attack paths. Sophisticated threat actors often masquerade behind a specific location, while hiding the true location where the attack was initiated. In addition, there may be further difficulties in identifying which act is considered the attack and how this may affect the location of the attack.

3.4.3 Furthermore, a cyber-attack could have origins and effects in multiple locations throughout its duration. Therefore, not only would this potentially raise issues in the application of certain international air law instruments (e.g., requiring the physical presence of the perpetrator on board), but it would also lead to multiple bases for jurisdiction. Jurisdictional considerations are further explored in a subsequent section of this study.

3.5 Various effects of successful cyber-attacks *(Actus reus element)*

3.5.1. Cyber-attacks vary not only by the methods used or by type of originator, but also by magnitude and scale. While some "attackers" may only wish to gain access to passenger information, others may be interested in placing a political message on a screen in an airport or even intend to adversely impact an aircraft in flight. As the motives, methods and mitigation measures vary, so does the magnitude of the potential effect.

3.5.2. The effects of cyber-attacks can be broadly classified into two categories:

a) **"impact(s) on information security[10][11]" -** technical impact on information security parameters (confidentiality, integrity and/or availability "C-I-A"[12]), cyber-attacks that do not have an impact on aviation safety and/or security, such as gaining access to passengers personal and/or financial details.

b) **"consequence(s) on civil aviation" -** the attack is successful and impacts information security (C-I-A) and if further mitigations regarding the effect on civil aviation are not in place or not effective leading to consequences on civil aviation itself, spanning from operational consequences with no impact on safety, to those having a direct impact on aviation safety and/or security (such as attacking a critical aviation system).

[10] Refer to definitions as per the Attachment to this study

[11] Please see for an illustration – MITRE analysis of the loss, denial and/or manipulation of functions or process. As an illustration and further background reading, possible technical impacts on industrial control systems (that differ from standard office IT systems in the fact that they have physical implications), can be found on Mitre ATT&CK for Industrial Control Systems: https://collaborate.mitre.org/attackics/index.php/Main_Page, accessed on 15.09.2020

[12] Refer to definitions as per the Attachment to this study

3.5.3 The applicability of international air law instruments may be related to which category the cyber-attack belongs to, depending on whether the instrument applies specifically to attacks that have a (potential) impact on the safety of civil aviation or can broadly apply to any attack on civil aviation.

3.5.4 However, these two categories are not mutually exclusive as they might intersect depending on the attack as well as its following (and sometimes unintended) consequences.

3.5.a) Impact(s) on information security

3.5.5 The different motives, whether conducted with intent to affect civil aviation or not, and the various methods used will lead to various information security impacts if a cyber-attack is carried out successfully.

3.5.6 In the IT field, the well-established way of classifying the main information security impacts on systems, information and/or data is to distinguish between threats that may affect the parameters of confidentiality, integrity and/or availability.

3.5.7 For the purposes of this report, potential information security impacts[13] can be briefly illustrated as follows:

- **Breach of confidentiality:** A cyber-attack could enable access to sensitive aviation information. This access could also enable the distribution of such sensitive information to persons who do not have the authorization to access the classified information with intent to plan another attack on civil aviation.

- **Loss of integrity of information:** A cyber-attack could compromise the integrity of information available to personnel working in aviation, e.g. to pilots or air traffic controllers.

- **Loss of integrity of system function:** A cyber-attack that seizes control of a system implies a loss of integrity of the system function itself, e.g. loss of control of a safety-relevant system on an airport or in an aircraft.

- **Loss of availability of information:** e.g. unavailability of information such as access to Notice-to-airmen (NOTAM) or weather information could also be the result of a successful cyber-attack scenario.

- **Loss of availability of system function:** e.g. loss of system availability could concern either an information system (flight information display system used at airports or an aircraft system such as a communication system or even an avionics safety system).

3.5.b) Consequence(s) on civil aviation

3.5.8 These various information security impacts of successful attacks each carry their own challenge for civil aviation, therefore the effects on civil aviation and most specifically on the safety of civil aviation may be direct or indirect and depend on:

- the type of threat;
- existing vulnerabilities;
- the cybersecurity mitigation measures in place;
- whether the attack is detected or not; and
- the aviation mitigation measures in place in aviation operations that will determine the reaction to the threat.

3.5.9 In any case, the impact of a cyber-attack on Confidentiality-Integrity-Availability of certain civil aviation critical systems may lead to situations that could be hazardous or even catastrophic for civil aviation safety.

3.5.10 Reference is made to the potential information security impacts under 3.5.7 above wherein a system displaying information that is incorrect or itself behaving incorrectly could lead directly to unsafe flight conditions. Decisions taken based on incorrect information could also lead to potentially unsafe situations.

3.5.11 Annex C of ICAO Annex 13 - *Aircraft Accident and Incident Investigation*, already highlights the following examples likely to be considered as serious aviation incidents:

- multiple malfunctions of one or more aircraft systems seriously affecting the operation of the aircraft;
- system failures, weather phenomena, operations outside the approved flight envelope or other occurrences which caused or could have caused difficulties controlling the aircraft; and
- failure of more than one system in a redundancy system mandatory for flight guidance and navigation.

3.5.12 The combination of a serious incidents just mentioned with the inappropriate response to the serious incident, could potentially lead to an accident in a worst case scenario.

3.5.13 To summarize, impacts on confidentiality, integrity and availability may lead to direct effects on safety and security of civil aviation, leading to major disruptions and damage, as well as indirect effects on aviation safety and security procedures.

3.5.14 On a broader note, even when safety is not necessarily impacted, a cyber-attack can have very negative reputational effects potentially leading to loss of confidence by passengers.

4. ANALYSIS OF TREATY PROVISIONS IN INTERNATIONAL AIR LAW INSTRUMENTS

4.1 ANALYSIS BY STRUCTURED REVIEW OF INSTRUMENTS

4.1.1 The potential cyber-attack scenarios against civil aviation are broad. Various types of actors with various intent, different potential attack methods and attack path and as presented herein, various impacts on information security. This broad variety of possible scenarios also leads to a large variety of possible effects on civil aviation.

4.1.2 The specificities of civil aviation and its historic attractiveness to "traditional" attacks have led to a far-reaching and historically strong international legal framework for civil aviation. Other sectors at risk from cyber-attacks, e.g. the financial or health sector, do not have such far-reaching international legal instruments.

4.1.3 The following analysis will summarize the extent to which this existing international legal framework originally created for physical attack scenarios, can also be applied to those attack scenarios involving a cyber means affecting civil aviation.

4.1.4 This study conducted a structured review of the existing air law instruments according to the following parameters:

- applicability by type of actor;
- applicability through the notion of intent (*mens rea*);
- applicability by method(s)/means of cyber threat/ attack (*actus reus element*);
- applicability by location(s)/attack vector (*actus reus element*);

- applicability by impact(s) on information security (Confidentiality - Integrity - Availability) regarding the information system/information/data itself (*actus reus element*);
- applicability by the consequence(s) on civil aviation (e.g. effect on safety) (*Actus reus element);*
- basis/bases for jurisdiction.

4.2 ANALYSIS OF THREE SAMPLES SCENARIOS

4.2.1 In addition to the structured review of the air law instruments according to the abovementioned parameters, three hypothetical scenarios were developed to aid the structured review by providing detailed examples of situations where the air law instruments may be applicable (see Attachment 3 for the detailed Scenarios and their analyses).

4.2.2 For the purpose of the scenario analysis, it was concluded that the hypothetical cyber-attack scenarios could be categorized in four categories[14], as follows:

Category 1: Acts/Threats relating to Air Traffic Management (ATM) Systems – Acts/attacks aimed at communications, navigation and surveillance systems.

Category 2: Acts/Threats relating to Aircraft Systems – Acts/attacks aimed at aircraft control systems, cabin operational systems, and cabin passenger systems.

Category 3: Acts/Threats relating to Airport or Airline Operations – Acts/attacks which, although not directly aimed at aircraft, could nevertheless facilitate a conventional hostile act/attack by degrading aviation security measures (e.g., screening, access control); and attacks intended to disrupt airport or airline operations, principally around passenger facilitation (e.g., departure control, baggage handling).

Category 4: Acts/Threats relating to other aviation systems or information/data – Acts/attacks which, although not directly aimed at aircraft, airports or airline daily operations, could nevertheless degrade aviation safety or security (e.g., maintenance information, leak of confidential AVSEC information) including attacks which facilitate a further conventional/physical attack; attacks intended to disrupt airport/airline operations; and attacks intended to facilitate criminal activity (e.g., stealing of data).

4.2.3 While categorizing cyber-attacks / scenarios in the aforementioned categories is not an easy task, as cyber-attacks could present elements of multiple categories or systems, therefore being a combination of elements, factors, systems and not fitting precisely in one of the identified categories. However, the categories were considered useful for the analysis of the scenarios.

4.2.4 In discussions, it was also pointed out that there is a need to understand and integrate the physical security component in the analysis. When looking at cyber-attacks, whilst on the one hand there are cyberattacks that envisage only the cyber component, on the other hand, there are cyberattacks that are a combination of a physical component with a cyber component (example – cyber threat - breach of access control).

4.2.5 The scenarios provided were analysed using a two prong approach. The first prong consisted of the prosecution aspect, referring to the analysis needed to ensure that the perpetrator of the cyber-attack against aviation could be prosecuted under the current air law instruments. In this regard, the facts of the scenario were analysed against the legal aspects, including the act itself, the effects of the attack, the intention and the jurisdictional basis for prosecution.

[14] Source Reference for categories 1-3: Aviation Security Global Risk Context Statement (ICAO Doc No. 10108, 2nd Edition (2019)), Appendix E

4.2.6 Once all applicable instruments and provisions were identified, the second prong was then to analyse any potential gaps in the identified instruments and provisions. One such example is the Tokyo and Hague Conventions that require the person to be on board the aircraft, which in a scenario where the perpetrator would not be on board, would render these two Conventions inapplicable. Similarly, the terms 'weapon' and 'device', which required an interpretation thereof in order to examine whether the relative provisions would apply, could suffer different interpretations in different jurisdictions.

4.3 RESULTS OF THE REVIEW OF INSTRUMENTS AND ANALYSIS OF SCENARIOS

4.3.1 The analysis of the current international air law instruments demonstrates that while cyber threats might not be explicitly mentioned in every instrument, the object and purpose of the international air law instruments is to safeguard civil aviation and could therefore cover cyber threat scenarios.

4.3.2 Each of the instruments provides some useful basis to address cyber threat scenarios - or more pertinently, to address the potential effects of successful cyber-attacks on civil aviation. However, certain instruments provide clearer applicability or broader coverage, making them easier to address cyber threats. As such, each situation must be analyzed on a case-by-case basis, and all instruments must be analyzed to identify all of which that could be applied.

4.3.3 Cyber-attacks may therefore potentially amount to various offences, depending on the nature of the attack, as well as where the attack is regarded as taking place and its consequences.

4.3.4 A common perspective found throughout all of the instruments is the element of effect or consequence on civil aviation. This is not surprising, as the main objective of the international air law system is to safeguard civil aviation. This section will provide the characteristics of all instruments following the methodology described above.

- **Convention on International Civil Aviation (Chicago, 1944 – "Chicago Convention");** ***incl. Annex 17 – Security — Safeguarding International Civil Aviation Against Acts of Unlawful Interference.***
    - **Protocol Relating to an Amendment to the Convention on International Civil Aviation [Article 3 *bis*] (Montreal, 1984 – "Protocol on Article 3 bis");**

4.3.5 In addition to the offence-creating air law instruments analyzed herein for their relevance in the prosecution of individuals and legal entities perpetrating cyber threats against civil aviation, the Chicago Convention and its Annexes provide a framework applicable to States that focuses on prevention and deterrence. As it complements the offence-creating air law instruments with certain obligations for States, mainly derived from Article 3 *bis* of the Chicago Convention, their analysis is of interest for the scope of this study.

4.3.6 Historically, Article **3 *bis*** of the **Chicago Convention** was introduced in the Chicago Convention by the *Protocol Relating to an Amendment to the Convention on International Civil Aviation* [Article 3 bis], signed at Montreal on 10 May 1984 (Doc 9436), following the outcomes of the KAL007 event. However, while the drafting and adoption of this provision was heavily influenced by this accident, its scope has been recognized as broader than simply providing obligations relating to the

interception of civil flights. Specifically, the first paragraph of Article 3 *bis* includes the obligation that *"every State must refrain from resorting to the use of weapons against civil aircraft in flight".*

4.3.7 While not all ICAO Member States are party to the Protocol introducing Article 3 *bis*, the obligations provisioned therein may nevertheless enjoy a broad applicability. As a matter of fact, eminent air law experts, such as Judge Guillaume and Professor Milde, have opined that Article 3 *bis* was declaratory of existing customary international law and recognized the principle of non-utilization of weapons against civil aircraft.[15] Moreover, the declaratory nature of the provision was further recognized by the ICAO Council in its Resolution adopted on 27 June 1996 in which it condemns "the use of weapons against civil aircraft in flight as being incompatible with elementary considerations of humanity, the rules of customary international law as codified in Article 3 *bis* of the *Convention on International Civil Aviation,* and the Standards and Recommended Practices set out in the Annexes to the Convention". Similarly, Resolution 1067 of the United Nations Security Council (26 July 1996) has condemned "the use of weapons against civil aircraft in flight as being incompatible with elementary considerations of humanity, the rules of customary international law as codified in article 3 bis of the Chicago Convention, and the standards and recommended practices set out in the annexes of the Convention".

4.3.8 However, to fall within the scope of Article 3 *bis*, the cyber threats and cyberattacks must be considered as "weapons". As the term "weapon" is not defined within the Chicago Convention, an interpretation of the extent of what is covered under the term must be made. As principles of international law apply, the Vienna Convention on the Law of Treaties (done at Vienna on 23 May 1969), notably its Articles 31 and 32, is relevant. As such, the term "weapon" must be given its ordinary meaning considering the context in which it is used.

4.3.9 The circumstances under which an attack conducted by cyber means meets the threshold of being the use of a "weapon" in terms of scale and effect (i.e. serious injury to persons and/or extensive damage to objects) is currently a subject of international debate between cybersecurity legal experts.

4.3.10 Within the context of cyber threats, the term "weapon" is being discussed in current literature as the following reference provides an illustration: *"Whether malicious cyber activities constitute a weapon depends on the actual outcome, and they cannot be classified without looking at the specific circumstances of each case".*[16]

4.3.11 In addition to this specific discussion regarding the applicability of Article 3 *bis* of the Chicago Convention, a recent Report of the "Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security", a Group set up under the United Nations General Assembly, indicated the following regarding general State behavior in its Norm 13 (f) "*A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public".*[17]

- **Actor(s):** State actors only;
- **Intent:** Not specified;
- **Method(s)/means:** It applies to an attack method using a "weapon";
- **Location(s)/attack vector(s):** Not specified;
- **Impact(s) on information security (C-I-A):** Not specified;
- **Consequence(s) on civil aviation:**

[15] G. Guillaume, "The Destruction on 1 September 1983 of the Korean Airlines Boeing (Flight KE 007)" ITA Magazine No. 0-18, September 1984, 27, at 34; and M. Milde, "Interception of Civil Aircraft vs. Misuse of Civil Aviation (Background of Amendment 27 to Annex 2)" (1986) XI Annals of Air and Space Law 105, at 113.

16 Cybersecurity, Key Legal Considerations for the Aviation and Space Sectors Federico Bergamasco, Roberto Cassar, Rada Popova & Benjamyn I. Scott, Wolters Kluwer 2020 (p. 52)

17 A_76_135-2104030E-1.pdf (un-arm.org), retreived on 28 December 2021

Applies depending on the consequence of an attack on the safety of civil aviation.
To be analyzed in conjunction with the definition of cyber threats as a "weapon"

4.3.12 **Annex 17** to the Chicago Convention includes Standards and Recommended Practices (SARPs) on preventive aviation security measures and more specifically includes a definition of acts of unlawful interference.[18] This definition focuses on the effects and consequences of such acts or attempts thereof to jeopardize the safety of civil aviation, rather than the means and methods of such unlawful interference. Contracting States are required to develop and implement regulations to safeguard civil aviation against acts of unlawful interference. Cyber-attacks may be considered an act of unlawful interference, where they have **the effect of jeopardizing the safety of civil aviation**, and consequently be treated as such. Furthermore, a preventive Standard has been included in Annex 17 (4.9.1 Measures relating to cyber threats) which requires States to develop and implement measures to protect their critical information, communications technology systems and data used for civil aviation purposes from unlawful interference.

ICAO Annex 17:

- **Actor(s):** Not specified; applicable to all types of actors (including non-State and individuals);
- **Intent:** Not specified;
- **Method(s)/means:** Provides an non-exhaustive list of possible methods/means;
- **Location(s)/attack vector(s):** Not specified;
- **Impact(s) on information security (C-I-A):** Not specified;
- **Consequence(s) on civil aviation:** Applies to cyber threats when the consequence of an attack (including attempted acts) is such that it jeopardizes the safety of civil aviation;
- **Basis/bases for jurisdiction:** N/A

- **Convention on Offences and Certain Other Acts Committed on Board Aircraft (Tokyo Convention 1963) (Tokyo, 1963 – "Tokyo Convention 1963");**
  - **Protocol to Amend the Convention on Offences and Certain Other Acts Committed on Board Aircraft (Montréal, 2014 – "Montréal Protocol 2014");**

4.3.13 The **Tokyo Convention 1963** is applicable to offences against penal law and any acts that **may or do jeopardize the safety of the aircraft**, of the persons or property on board, or any acts that jeopardize good order and discipline on board.[19] The Convention was mainly adopted to provide jurisdiction to States of Registration for offences perpetrated on board aircraft while the flight is over international territory.[20] If a cyber-attack is considered to be an act that is an offence (in national law directly or by virtue of applicability of other international law, such as e.g. the Budapest Convention) or a cyber-attack that, whether or not it is an offence, may or does jeopardize the safety of the aircraft, or of the persons or property on board, the Tokyo Convention is applicable. Its scope of application would appear to be more general than that of the other instruments presented herein. Unlike the instruments developed after it, the Tokyo Convention does not specify offences, but creates a cross-reference to existing offences in each Contracting State. Regarding jurisdiction, the Tokyo Convention clearly defines the jurisdiction of the State of registration for offences and acts committed on board.

- **Actor(s):** Not specified; applicable to all types of actors (including non-State and individuals);
- **Intent:** Not specified;
- **Method(s)/means:** Applies to offences against penal law. But it does not provide a list of methods/offences;

18 Annex 17 to the Chicago Convention, "Security", Tenth Edition, 2017, Chapter 1 - Definitions.
19 Convention on Offences and Certain Other Acts Committed on Board Aircraft, signed at Tokyo on 14 September 1963 [Tokyo Convention], Article 1(1).
20 Tokyo Convention, Article 3.

- **Location(s)/attack vector(s):** Applies to offences perpetrated on board aircraft while the aircraft is in flight or on the surface of the high seas or of any other area outside the territory of any State;
- **Impact(s) on information security (C-I-A)** Not specified;
- **Consequence(s) on civil aviation:** Applies to acts that may or do jeopardize the safety of the aircraft or good order and discipline on board the aircraft;
- **Basis/bases for jurisdiction:** State of registration, Article 4 provides other bases, inter alia, the offence has effect on the territory of such state; the offence has been committed by or against a national or permanent resident of such state; the offence is against the security of such state.

4.3.14 **The Montréal Protocol 2014** expands the grounds of jurisdiction of the Tokyo Convention by recognizing, under certain conditions, the competence of the State of landing and the State of the operator to exercise jurisdiction over offences and acts on board aircraft.[21] Therefore, the Protocol provides a wider scope for States to deal with offences and unruly and disruptive acts on board aircraft, which may help in the prosecution of a cyberattack.

- **Actor(s):** Not specified; applicable to all types of actors (including non-State and individuals);
- **Intent:** Not specified;
- **Method(s)/means:** Not specified**.**
- **Location(s)/attack vector(s):** Offences or acts perpetrated on board;
- **Impact(s) on information security (C-I-A):** Not specified;
- **Consequence(s) on civil aviation:** applies to acts that may or do jeopardize the safety of the aircraft or good order and discipline in the aircraft;
- **Basis/bases for jurisdiction:** State of registration, State of the operator and State of landing (with the alleged offender still on board).

- **Convention for the Suppression of Unlawful Seizure of Aircraft (Hague, 1970 – "Hague Convention 1970");**
    - **Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing, 2010 – "Beijing Protocol 2010");**

4.3.15 The **Hague Convention 1970** was adopted to combat aircraft hijacking and provides for the criminalization of offences committed on board an aircraft in flight whereby a person seizes or exercises control of the aircraft.[22] In addition to establishing the legal principle of "extradite or prosecute",[23] which obliges the State in which the alleged offender is found to either subject such person to prosecution or extradite such person to another State for prosecution, the Hague Convention sets out the jurisdiction of the State of the operator and of the State of landing in addition to the traditional jurisdiction of the State of registration.[24] The Hague Convention may be applicable to cybersecurity cases for which a person on board takes control of the aircraft through a cyber-attack.

- **Actor(s):** Not specified; applicable to all types of actors (including non-State and individuals). Also applies to accomplices;
- **Intent:** Not specified;
- **Method(s)/means:** Unlawful acts of seizure or exercise of control of aircraft in flight;
- **Location(s)/attack vector(s):** On board an aircraft in flight;
- **Impact(s) on information security(C-I-A):** Not specified;

[21] Montréal Protocol 2014, Article IV.
[22] Hague Convention, Article 1.
[23] Hague Convention, Article 7.
[24] Hague Convention, Article 4.

- **Consequence(s) on civil aviation:** It applies to the unlawful seizure or exercising of control aircraft in flight. Also applies to attempts;
- **Basis/bases for jurisdiction:** State of registration, State of the operator and State of landing. Extradition or prosecution of offenders as principle.

4.3.16 The **Beijing Protocol 2010** modernizes many aspects of the Hague Convention by adding concepts that reflect the evolution and state of technology that may be used against aviation. It directly refers to the exercise of control of an aircraft "by any technological means", and therefore broadens the type of attack methods that fall within its scope, and removes the requirement that the offender must be on board the aircraft during the perpetration of the offence.[25] In addition, it redefines the notion of aircraft "in-service" as being "from the beginning of the pre-flight preparation of the aircraft until twenty-four hours after any landing". This broader timeframe is relevant to scenarios where cyberattacks are conducted during the important pre-flight preparations, such as safety-relevant flight calculations and documentation, or cyberattack scenarios that happen during the defined post-flight phase, such as certain (limited) maintenance activities. As such, the Beijing Protocol expands the scope of acts contemplated under the Hague Convention with broader application which could more directly cover cyber-attacks, however the cyber-attack would need to amount to "seizing" or "exercising" control of an aircraft. In addition, two additional grounds of mandatory jurisdiction are included in the Beijing Protocol: when the offence is committed in the territory of that State or when committed by a national of that State.[26] Two optional bases are also included, when the offence is committed against a national or by a stateless person habitually resident in that State.[27] Both instruments require States to impose severe penalties for the offences.[28]

- **Actor(s):** Not specified; applicable to all types of actors (including non-State and individuals). Also applies to accomplices, "directors" etc. Includes legal entities within the potential actors to be held accountable;
- **Intent:** Intent is clearly stated as a criterion;
- **Method(s)/means:** Addition of "any technological means" to commit unlawful seizure or exercise of control of aircraft in flight. The Protocol also covers threats to commit the offence, the attempt to commit the offence, the organization or direction of the offence, participation as an accomplice in the offence or assisting in the evasion of investigation, prosecution or punishment. Also covers agreement to commit such an offence or contributing to the commission of such an offence;
- **Location(s)/attack vector(s):** Removes the requirement that the offender needs to be on board the aircraft. Changes the notion of "in-flight" to "in- service"[29];
- **Impact(s) on information security (C-I-A) :** Not specified;
- **Consequence(s) on civil aviation:** Seizure or control of an aircraft in service;
- **Basis/bases for jurisdiction:** Territorial jurisdiction, State of registry [when the offence is committed against or on board the aircraft]; State of Landing (with the alleged offender still on board); Leasing; nationality principle based on the perpetrator; and may establish jurisdiction based on the nationality of the victim; or committed by a stateless person whose habitual residence is in the territory of that State; or the alleged offender is present and does not extradite.

[25] Beijing Protocol, Article II.
[26] Beijing Protocol, Article VII.
[27] Beijing Protocol, Article VII.
[28] Hague Convention Article 2 and Beijing Protocol, Article III
[29] Hague Convention 1970, Art. 3, definition of **"in-flight"** - *an aircraft is considered to be in flight at any time from the moment when all its external doors are closed following embarkation until the moment when any such door is opened for disembarkation*. The Beijing Protocol 2010, Art. V, definition of **"in- service" -** *an aircraft is considered to be in service from the beginning of the pre-flight preparation of the aircraft by ground personnel or by the crew for a specific flight until twenty-four hours after any landing.*

- **Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Montreal, 1971 – "Montreal Convention 1971");**
    - **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 done at Montreal on 23 September 1971 (Montreal, 1988 – "VIA Protocol 1988");**
        - **Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing, 2010 – "Beijing Convention 2010").**

4.3.17 The **Montreal Convention 1971** takes an effect-based approach to determine the offences, which shall have the following in common: the acts are unlawful, intentional and likely to endanger the safety of aircraft in flight.[30] Compared to the provisions under the Hague Convention 1970, the Montreal Convention 1971 does not require an offender to be on board an aircraft while committing the unlawful act. Furthermore, jurisdictional bases also includes jurisdiction for offences committed "against or on board an aircraft registered in that State". This effectively broadens the scope of application of this Convention to remote cyber-attacks that may affect not only an aircraft but also air navigation facilities and providers of critical flight information sent to the aircraft.

- **Actor(s):** Not specified; applicable to all types of actors (including non-State and individuals). Also applies to attempted acts and accomplices;
- **Intent:** Intent is clearly stated as a criterion;
- **Method(s)/means:** The Convention lists specific offences. However, to be considered under the convention they must be "likely to endanger the safety of aircraft in flight.";
- **Location(s)/attack vector(s):** Refers to scenarios for aircraft both "in flight" and in service";
- **Impact(s) on information security (C-I-A):** possible Information security impact is mentioned "[...] causes damage to such an aircraft which renders it incapable of flight [...]"; "[...] interferes with the operation [...]" of air navigation facilities, "[...] communicates information which he knows to be false [...]";
- **Consequence(s) on civil aviation**: For each offence the link is made to the potential consequence "likely to endanger the safety of aircraft in flight";
- **Basis/bases for jurisdiction:** Territorial jurisdiction, State of registration including for offenses committed against the aircraft (not only on board), State of landing with alleged offender still on board.

4.3.18 The Montreal Convention 1971 was amended by the **VIA Protocol 1988** to broaden the offences by including acts of violence or of disruption of services at international airports.[31] The coverage of cybersecurity situations is similar to that of the Montreal Convention 1971, but the scope is expanded to attacks that would target airports. This could include situations such as the tampering of flight scheduling systems or of passengers checking and boarding systems with a disruptive effect to airport operations while endangering safety.

- **Actor(s):** The type of actor is not specified; applicable to all types of actors (including non-State and individuals). Also applies to attempted acts and accomplices;
- **Intent:** Intent is clearly stated as a criteria;
- **Method(s)/means:** The Protocol adds specific offences as they pertain to airports, however to be considered under the Protocol they must be "likely to cause serious injury or death or endanger/likely to endanger the safety at that airport";

[30] Montreal Convention 1971, Article 1.
[31] VIA Protocol, Article II.

- **Location(s)/attack vector:** Refers to scenarios for aircraft both "in flight" and "in service";
- **Impact(s) on information security C-I-A:** possible IT technical impact is mentioned "... disruption of services at the airport…";
- **Consequence(s) on civil aviation**: For each offence the link is made to the potential consequence "likely to cause serious injury or death or endanger/likely to endanger the safety at that airport";
- **Basis/bases for jurisdiction:** Each contracting state shall likewise take such measures as may be necessary to establish its jurisdiction over the offense mentioned in article 1 […] in so far as that paragraph relates to those offense, in the case where the alleged offender is present in its territory and does not extradite him.

4.3.19 The **Beijing Convention 2010** is designed to consolidate the provisions of the Montreal Convention 1971 and the provisions of the Airport Protocol 1988. In addition to repeating the offences found in the Montreal Convention and its Airport Protocol, the Beijing Convention further expands the scope of protection against attacks to air navigation services.[32] By introducing a specific definition for "Air navigation facilities" as including signals, data, information or systems necessary for the navigation of the aircraft[33], the definition provides further clarity to the scope of acts that could cover attacks to such facilities and aircraft by cyber means.

4.3.20 Additionally, the Beijing Convention 2010 establishes new forms of criminal participation. Unlike the Hague Convention 1970, the Montreal Convention 1971 and its VIA Protocol 1988, the Beijing Convention 2010 now makes it an offence to threaten to commit most of the offences listed.[34] Furthermore, the Beijing Convention also broadens the scope of criminal liability to cover attempts, organizing, participating as accomplice, and conspiracy to commit.[35] Furthermore, the Beijing Convention 2010 incorporates broader jurisdictional bases. These now include offences committed in the territory of that State or by a national of that State. The instrument also requires States to impose severe penalties for the offences.[36]

- **Actor(s):** Not specified; applicable to all types of actors (including non-State and individuals). Also applies to accomplices, "directors", etc. Includes legal entities within the potential actors to be held accountable;
- **Intent:** Intent is clearly stated as a criterion;
- **Method(s)/means:** The Convention lists specific offence. However, to be considered under the convention the deciding factor is that they must be likely to render an aircraft "incapable of flight" or likely to endanger "safety in flight.";
  Location(s)/Attack vector: various locations are applicable to each offence; for example (a) refers to performing an act of violence against a person "on board an aircraft in flight''; (b) refers to destroying an aircraft "in service''; (c) refers to placing "on an aircraft in service, by any means whatsoever, a device''; (f) refers to using an aircraft "in service'' for the purpose of causing death, serious bodily injury; sub-section 2 of Article 1, with regard to airports, refers to "an airport serving international civil aviation'';
- **Impact(s) on information security C-I-A:** IT technical impact is not specified. However, air navigation facilities and "their operation" are listed as "assets" which leads to an offence if destroyed, damaged or interfered with;
- **Consequence(s) on civil aviation:** For each offence the link is made to the potential consequence e.g. be likely to render an aircraft "incapable of flight" or likely to endanger "safety in flight.".
- **Basis/bases of jurisdiction:** *New jurisdictional bases:* offences committed against a national of that State; when the offence is committed by a stateless person whose habitual

[32] Beijing Convention, Article 1(1).
[33] Beijing Convention, Article 2(c).
[34] Beijing Convention, Article 1(3).
[35] Beijing Convention, Article 1(4).
[36] Beijing Convention, Article 3.

residence is in the territory of that State; in the case where the alleged offender is present in its territory and it does not extradite that person.

4.3.21 The Montréal Convention 1971, supplemented by the VIA Protocol of 1988, and the Beijing Convention of 2010 each provide broad bases under which a large variety of cyber-attacks could potentially be covered. However, certain situations may be particularly challenging in the application of certain instruments; for example, under the Beijing Convention of 2010:

- Article 1(1)(b): Destroying or causing damage to an aircraft in service – Did the cyber-attack in question "destroy", or "cause damage" to the aircraft?

- For Article 1(1)(c): Placing a device/substance on an aircraft likely to destroy it, cause damage, or endanger safety – Did the cyber-attack amount to a placement of a "device or substance" on an aircraft?

- For Article 1(1)(d): Destroying or damaging, or interfering with the operation of, air navigation facilities which is likely to endanger safety – Did the cyber-attack destroy or damage air navigation facilities, or interfere with their operation, in a way which is likely to endanger aircraft safety?

- For Article 1(1)(e): Communicating false information which endangers the safety of aircraft in flight – Did the cyber-attack amount to communication of false information, which thereby endangers safety of an aircraft in flight?

- For Article 1(2)(b): Destroying or seriously damaging airport facilities or aircraft not in service, or disrupting airport services – Did the cyber-attack result in such destruction, damage, or disruption, which then endangers or is likely to endanger safety?

4.3.22 For non-parties to the Beijing Convention (such that only the 1971 Montreal Convention and/or 1998 Montreal Airport Protocol applies), the same analysis as Articles 1(1) and 1(2) of the Beijing Convention applies. However, the definition of "air navigation facilities" in those earlier treaties is not as expansive as the definition in Beijing Convention, which expressly includes "signals, data, information or systems necessary for the navigation of the aircraft". Because of this, an argument could be made that cyber-attacks on an air navigation facility therefore does not fall within the scope of the Montreal Convention. However, possible counter-argument is that the Montreal Convention must be read purposively in the light of the current state of technology, and that the expanded definition in the Beijing Convention merely recognizes this fact.

4.4 Customary law, its codification and separate treaty provisions to be considered

4.4.1 As discussed above, the magnitude of the potential effect of a successful cyber-attack can vary significantly.

4.4.2 This study mainly considered the existing treaty provisions in international air law instruments. For some scenarios with large-scale effect of high magnitude, customary law will continue to be applicable even where specific instruments do not (yet) have universal coverage.

4.5 Potential overlap with "cyber-specific" instruments

4.5.1 Compared to "cyber-specific" instruments, e.g. notably the Convention on Cybercrime, Budapest - 2001[37], the international air law instruments focus on the effect on civil aviation and not on the specific technical impact of a cyber-attack on information system level.

4.5.2 A cyber-attack scenario against civil aviation could therefore also be covered by "cyber-specific" instruments - that would cover the technical impact on system/information level. In parallel, civil aviation instruments may also be applicable where the scenario is such that an effect on civil aviation is present.

4.5.3 However, for the purpose of this study, analysis has only been made on the air law instruments and not on the applicability or otherwise of the cyber specific instruments to cyber-attacks in aviation. Such applicability of cyber-specific instruments could however arise from either international or national cyber-specific instruments.

4.6 Prosecution as deterrence

4.6.1 The criminalization of attacks against civil aviation can be considered from two interconnected perspectives, namely the perspective of deterrence and the perspective of prosecution. Both are valid within the context of cyber-attack scenarios.

4.6.2 The concept of deterrence is used, e.g. in aviation security, as a supplementary strategy to other more technical preventive measures in order to minimize the actual intent to attack civil aviation. The knowledge about the "cost" of potential prosecution can have the effect of disincentivizing actors to conduct an attack.

4.6.3 Due to the challenges of attribution for cyber-attacks, as detailed below, the prosecution based on cyber-attack scenarios can be difficult. However, this attribution challenge is not aviation specific. Therefore, this report does not focus on attribution challenges per se. Rather, the focus is to analyze to what extent the existing air law provisions already foresee prosecution and can therefore be considered to contribute to the deterrence against cyber-attacks to civil aviation for situations where attribution can be realized.

[37] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

5. ATTRIBUTION AND JURISDICTION

5.0.1 As we have just summarized, it is possible that some cyber-attacks scenarios may be covered by the existing instruments**.** The analysis of each specific circumstance will be necessary to determine which instrument may be applicable and on a case by case basis.

5.0.2 After the applicability of an instrument (or instruments) is determined, some additional challenges regarding prosecution may remain.

5.1 ATTRIBUTION

5.1.1 Many specific and detailed papers have been written about the general challenges of attributing cyber-attacks to the correct actors. While the issues pertaining to attribution are of a technical nature, and therefore not within the purview of the current legal analysis, they remain relevant considerations for framing certain factors, such as jurisdiction. For certain attack methods, proximity to the target is not necessary. They can be carried out remotely from anywhere in the world. Furthermore, the origin and "route" of the attack is often masked. Finding the correct actor of a threat is a technical and legal challenge. And even if the actors(s) can be identified, challenges regarding jurisdiction for prosecution remain. But these challenges exist for all cyber threats and are not aviation specific.

5.1.2 Attribution refers to the process of assigning an action to an actor. Attribution is a national prerogative. Also regarding cyberspace, attribution is a very relevant topic and especially in this domain, attribution is a complex and time consuming matter. In order to assign a malicious cyber activity to an actor, the technical characteristics of an attack, the wider geopolitical context, the full range of information gathering and the legal criteria as set out in the ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts (see Yearbook of the International Law Commission, 2001, vol. II, Part Two) need to be considered. Attribution lays the basis for political decision-makers to develop and formulate a response (e.g. political, diplomatic, economic, legal, etc.)

5.2 JURISDICTION

5.2.1 Once the challenge of attribution in a specific scenario has been overcome, the necessary enforcement jurisdiction is required to ensure that the alleged perpetrator may be tried and prosecuted.

5.2.2 As questions regarding attribution for cyber threats and cyber-attacks are more general than the civil aviation sector, the question regarding cyber threats or cyber-attacks with effects on civil aviation is to consider whether the existing jurisdictional bases in the international air law treaties are adequate for cyber scenarios, or whether further jurisdictional bases are required.

5.2.3 As outlined earlier, a key characteristic of a cyber-attack is the lack of physicality (by the perpetrator at the time and location of the effect)**.**

5.2.4 With respect to jurisdiction, it was indicated that the particularities of a cyber-attack, such as physicality, raise a series of issues, as the existing air law instruments typically determine jurisdiction by several factors such as location of the act/offence, identity of the parties involved and other relevant ties to the act. Due to the lack of physicality of the cyber-attack, the cyber-attacker may be located in one jurisdiction, while the act/attack or the intended effect takes place in another jurisdiction. This makes cyber-attacks different from many traditional acts/crimes.

5.2.5 Several jurisdictional questions and issues need to be addressed, such as the potential existence of a gap in the air law treaties insofar as the existing treaties might not currently provide for jurisdiction on the basis of the location where the cyber-attack originated. One way this could be

addressed in some scenarios is through accessory/accomplice/conspiracy liability as provided for in certain instruments (e.g., Articles 1(4) and 1(5) of the 2010 Beijing Convention).

5.2.6 That being said, the general principle of "prosecute or extradite" remains present in the instruments, same as the criminal jurisdiction exercised in accordance with national laws.

5.2.7 Moreover, it is important to note that with regard to the State of Landing, for example, it is required that the perpetrator would be on board that aircraft. Moreover, a distinction is made in the international air law instruments with regard to the State or registration, wherein in the Montreal Convention of 1971, a distinction is made between "committed against or on board an aircraft'' registered. Therefore due to the cyber specificities mentioned herein, such a detailed analysis has been made with regard to jurisdiction.

5.2.8 It is therefore important to keep in mind that jurisdiction is a key component of prosecution, and it is essential that bases for jurisdiction are ensured in order to prevent the alleged perpetrator going unpunished due to a technical detail in the law. Therefore, in view of the analysis, it is imperative to continue to analyse the potential cyber threats against aviation and ensure that either the current international air law framework has sufficient bases for prosecution in each instrument.

6. POTENTIAL GAPS IN THE APPLICATION OF INTERNATIONAL AIR LAW INSTRUMENTS TO CYBERSECURITY

6.1 As detailed throughout this study, the applicability of international air law instruments to cyber threats is complex and may therefore introduce gaps which could prevent the prosecution of the perpetrator of a cyber-attack. While the instruments identified in this study may be said to apply depending on the scenario and interpretation to some extent to cybersecurity,.

6.2 A first potential gap could thus be inferred from the fragmentation of the international air law framework itself. While certain States may be parties to recent security instruments, others may only be party to some of the older instruments. As mentioned herein, the actors, attack and effects of a cyber-attack may include multiple jurisdictions, with different legal regimes, potentially creating situations in which prosecution may be difficult or impossible. It should however be noted that the principle of "prosecute or extradite" may apply in some situations, diminishing the possible exploit of this gap.

6.3 A second potential gap lies with the interpretative issues of certain terms used in some of the instruments. As further explored in other sections of this study, a number of instruments include broad terms (such as "weapon", "device", "air navigation facilities", and "use of force") that could be interpreted to cover cyber threats. However, the interpretation of such terms could suffer from being applied differently in different situations and jurisdictions, which may lead to disparities in the application of instruments between States.

6.4 A third potential gap in the application of the international air law framework to cybersecurity is the applicability criteria of older instruments that are less applicable to cyber threats than the criteria of newer security instruments. As a matter of fact, earlier instruments may require, for example, that the perpetrator be on-board of the aircraft, that the aircraft is in flight or that the attack results in the control of the aircraft. As cyber-attacks could be performed remotely, and initiated at any time prior to a flight, their prosecution on those bases may be difficult. Similarly, the consideration on whether a cyber-attack resulted in the control of the aircraft may be arduous depending on the means of the attack.

6.5 A fourth potential gap could be based on the fact that the international air law instruments generally cover safety and security of civil aviation. However, cyber threats may include numerous types of attacks that would not necessarily be considered as endangering the safety and security of a flight. For example, a cyber-attack could target passenger information databases which may not amount to safety or security risks as commonly understood. It should be noted that while such cyber threats would not presently be covered by the air law instruments, they may nevertheless be covered in cyber-specific instruments.

6.6 As presented herein, the international air law regime suffers from potential gaps in its applicability to cybersecurity. Although some interpretative issues may arise during prosecution, the Beijing instruments of 2010 are a good basis for dealing with cyber-attacks against civil aviation. As such, it could be said that the current international air law framework is partially adequate to cover cyber threats.

7. CONCLUSIONS

7.1. Cyber-attacks are different from traditional attacks: lack of physicality of the attack method/means (as physical presence of the attacker is often not associated with a cyber-attack) and lack of awareness (airport operator or systems operators may not be aware that a cyber-attack is happening);

7.2. It has been concluded that the analysis of the adequacy of international air law instruments in addressing cyber threats should focus on the intent, effects or consequences of the cyber threats on civil aviation as these are generally necessary in providing awareness of the cyber threats (due to the fact that there are various types of cyber threats, carried out by actors with various intent and methods, leading to various technical impacts on confidentiality, integrity and/or availability of civil aviation systems, information or data). Those technical impacts could in turn lead to effects ranging from simple nuisance to large scale disruption and / or potential consequences on civil aviation safety and security;

7.3. Four broad categories of cyber-attacks have been identified:

i. Cat 1 – cyber threats/attacks against ATM systems;
ii. Cat 2 – cyber threats/attacks against aircraft systems;
iii. Cat 3 – cyber threats/attacks against airports/airline systems;
iv. Cat 4 – cyber - threats/attacks relating to other aviation systems or information/data.

7.4. The analysis of the offence-creating international air law instruments as they exist today, demonstrates that while scenarios involving cyber-attacks might not be explicitly covered by each air law instrument, the object and purpose of the international air law instruments is to safeguard civil aviation. In this sense, depending on the nature of the attack, each of the instruments may be said to provide for certain offences that may be useful to address some cyber threat scenarios, notably those that have serious effects on civil aviation, such as e.g. effects on the safety of aircraft in flight. However, such an analysis would need to be done on a case-by-case basis.

7.5. Cyber-attacks may **potentially amount to various offences** under the existing international air law instruments, however, special consideration needs to be given to the **nature of the attack** and where the attacks including its effects have potentially taken place or are regarded to have taken place (e.g., on board the aircraft);

7.6. Questions of interpretation may arise when analysing the application of older air law instruments to cybersecurity situations. For example, under the Hague Convention of 1970, a cyber-attack would need to be considered as a “use of force or threat thereof, or by any other form of intimidation” to enable its application. Similarly, the extent of what is covered by “air navigation

facilities" and **"device"** in the Montreal Convention of 1971 or the Airport Protocol of 1988 could lead to different answers regarding the applicability of these instruments.

7.7. Through the detailed study of each instrument and their applicability criteria, it became apparent that the application of newer instruments such as the Beijing Convention of 2010 and the Beijing Protocol of 2010 contain provisions that can be more specifically applied to cyber threats and cyber-attacks. Some of the reasons being that the newer instruments introduced the broader **"aircraft in service"** requirement, removed the requirement of the perpetrator being on board the aircraft and specifically defines relevant terms such as "**air navigation facilities**". [and also makes reference to attacks by 'any technological means']

7.8. The existing international air law instruments are considered partially adequate for identified cyber threat/attack scenarios, analyzed on a case by case basis. Although there may still be a need for further interpretation of certain terms under the Beijing instruments of 2010 (e.g., "device", etc.), it would seem their scope provides a **good basis** for States to successfully prosecute individuals and entities conducting cyber-attacks against civil aviation. In accordance with ICAO Assembly Resolution A40-10, a wider ratification of these treaties is strongly encouraged.

7.9. When considering the application/implications of **Art. 3*bis* of the Chicago Convention**, it was concluded that, due the nature of customary law of the provision, as well as the various potential definitions of the term "weapon" in the context of cyber-attack (still under debate by cybersecurity legal experts), if a "weapon" may be interpreted to also refer to a cyber-attack or the effects of the cyber-attack might be considered crossing the threshold of the term "weapon", Art 3 bis would be deemed applicable , on the understanding however that its scope is **limited to States**.

7.10. In terms of jurisdiction, the **location where the cyber-attack originated** and the **location where the effect of the attack is felt** may be different and therefore, it must be ensured that the international aviation legal framework provides for jurisdiction upon which a State may prosecute in order to avoid any gaps in this regard. As such, international cooperation is crucial in overcoming jurisdiction matters when it comes to cyber-attacks.

7.11. It was further identified that as for all offences, gaps could exist in the application of air law instruments **depending on which States are party** to which instruments.

Appendix 1

Terms and definitions used in this study

Terms and definitions used have been chosen solely for the purposes of this study. Non-ICAO definitions used in this study do not represent official ICAO language.

Accident

An occurrence associated with the operation of an aircraft which, in the case of a manned aircraft, takes place between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked, or in the case of an unmanned aircraft, takes place between the time the aircraft is ready to move with the purpose of flight until such time it comes to rest at the end of the flight and the primary propulsion system is shut down, in which:

a) a person is fatally or seriously injured as a result of:

- *being in the aircraft, or,*
- *direct contact with any part of the aircraft, including parts which have become detached from the aircraft, or,*
- *direct exposure to jet blast,*

except when the injuries are from natural causes, self-inflicted or inflicted by other persons, or when the injuries are to stowaways hiding outside the areas normally available to the passengers and crew; or

b) the aircraft sustains damage or structural failure which:

- *adversely affects the structural strength, performance or flight characteristics of the aircraft, and*
- *would normally require major repair or replacement of the affected component,*

except for engine failure or damage, when the damage is limited to a single engine (including its cowlings or accessories), to propellers, wing tips, antennas, probes, vanes, tires, brakes, wheels, fairings, panels, landing gear doors, windscreens, the aircraft skin (such as small dents or puncture holes) or minor damages to main rotor blades, tail rotor blades, landing gear, and those resulting from hail or bird strike (including holes in the radome); or

c) the aircraft is missing or is completely inaccessible.

[Source: ICAO Annex 13]

Acts of unlawful interference

These are acts or attempted acts such as to jeopardize the safety of civil aviation, including 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 at premises of an aeronautical facility,*
- *introduction on board an aircraft or at an airport of a weapon or a 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,*
- *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. [Source ICAO Annex 17]*

Availability

Property of being accessible and usable on demand by an authorized entity. [Source: ISO/IEC 27001:2018]

Causes

Actions, omissions, events, conditions, or a combination thereof, which led to the accident or incident. The identification of causes does not imply the assignment of fault or the determination of administrative, civil or criminal liability. [Source: ICAO Annex 13]

Confidentiality

Property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [Source: ISO/IEC 27001:2018]

Consequences (on civil aviation)

The nature and scale of the consequences of the specific attack, in human, economic, political, and reputational terms under a reasonable worst-case scenario.
[Source: ICAO Aviation Security Global Risk Context Statement Doc. 10108 - Restricted, Second Edition 2019]

Cyber-attack.[38]

Refers to an attack against civil aviation perpetrated on or through cyberspace, i.e. the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace may be seen as a target for attack or as a vector or facilitator for other forms of attack. [Source: ICAO Aviation Security Global Risk Context Statement Doc. 10108 - Restricted, Second Edition 2019]

Denial

Temporary disruption of ability to view or control the process.
[MITRE ATT&CK® for Industrial Control Systems]

Hazard

A condition or an object with the potential to cause or contribute to an aircraft incident or accident. [Source: ICAO Annex 19]

(Aviation) Incident

An occurrence, other than an accident, associated with the operation of an aircraft which affects or could affect the safety of operation.
Note. the types of incidents which are of main interest to the International Civil Aviation Organization for accident prevention studies are listed in Attachment C. [Source: ICAO Annex 13]

Impact (on Industrial Control Systems ICS)

Disruption of essential functions of the industrial control system itself, such as, safety and protection, availability, automation, control, or quality assurance. [MITRE ATT&CK® for Industrial Control Systems]

Information (or cyber) security event

[38] Various legal debates exist about when a cyber threat qualifies as a "cyber-attack" and what this terminology implies. For the sake of simplicity of this report, the term "cyber-attack" will be used as in the existing ICAO Aviation Security Risk Context Statement. It is used as a generic term to cover different possible cyber threat scenarios that may be carried out (thereby distinguishing an "attack" scenario from a mere potential "threat"). More detailed analysis regarding terminology will be carried out by the RSGLEG in the work concerning the glossary.

Identified occurrence of a system, service or network state indicating a possible breach of information security policy, failure of controls or a previously unknown situation that can be security relevant. [Source ISO27002: 2018]

Information (or cyber) security incident

Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. [Source ISO27002: 2018]

Integrity

Property of accuracy and completeness. [Source: ISO/IEC 27001:2018]

Safety

The state in which risks associated with aviation activities, related to, or in direct support of the operation of aircraft, are reduced and controlled to an acceptable level. [ICAO Annex 19]

Safety risk

The predicted probability and severity of the consequences or outcomes of a hazard. [ICAO Annex 19]

Security

Safeguarding civil aviation against acts of unlawful interference. The objective is achieved by a combination of measures and human and material resources. [ICAO Annex 17]

Serious (aviation) incident

Serious incident means an incident involving circumstances indicating that there was a high probability of an accident and is associated with the operation of an aircraft, which in the case of a manned aircraft, takes place between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked, or in the case of an unmanned aircraft, takes place between the time the aircraft is ready to move with the purpose of flight until such time it comes to rest at the end of the flight and the primary propulsion system is shut down.

Note 1.- The difference between an accident and a serious incident lies only in the result.
Note 2.- Examples of serious incidents can be found in attachment C.
[Source: ICAO Annex 13]

Appendix 2

Additional background information regarding cybersecurity perspectives

1. Specificities of civil aviation

a) Similarities of air transport IT with general IT matters

1.1 Civil aviation is not different from other sectors when it comes to its dependency on the correct functioning of its ICT and OT systems. Similar to any other sectors, IT is becoming increasingly of paramount importance due to the accelerated digitalization of air transport in support of interconnectivity and inter-operability that enable enhancements to safety, efficiency, and capacity of civil aviation.

b) Specificities of transport modes

1.2 Compared to some other sectors, transport modes have the following specificities:

- transport of persons and goods (accidents are risks to life, limb and property); and
- transport modes are not static, implying that protective measures need to be international to cover the mobility of the vehicle;
- transport modes often require 24/7 availability of global systems.

c) Additional specificity of aviation

1.3 There is an additional specificity of aviation that needs to be fully understood when analyzing risks and developing measures and when building joint aviation cybersecurity know-how: An aircraft cannot stop mid-air.

1.4 This specificity of aviation is very important. Contrary to other transport modes such as trains or ships, which, while also transporting persons internationally, can stop en-route, a flight cannot suddenly be interrupted en-route as a mitigation measure in case of a cyber-attack without catastrophic results.

1.5 This is one of the reasons for which an extensive aviation safety and security framework is already in place.

2. Specificities of cyber threats

2.1 Before delving into the analysis of the international air law instruments, the following general considerations regarding the challenges of addressing cyber threats must be noted.

a) Terminology challenge

2.2 Addressing cyber threats, especially in civil aviation, introduces a significant challenge on the terminology to be used.

i) Technical terminology

2.3 As the topic is cross-cutting, it spans both aviation security and aviation safety. Furthermore, the world of information or cybersecurity has its own set of terminology, well-known in the information technology IT[39] field. This IT technical terminology sometimes uses identical words as civil aviation, but with a slightly different meaning. Therefore, discussions to bring the relevant elements of aviation security, aviation safety and cybersecurity closer together require a clear overview of key terms as used in their specific context.

ii) Translation of technical terminology

[39] Information technology (IT) - the technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data. (Merriam Webster Dictionary).

2.4 In doing so, technical terminology in the various ICAO languages is also a challenge, as the cybersecurity terminology from the IT field uses different translations than aviation for important terms such as "security". For example, in French "cyber security" is "cyber sécurité", which could be misunderstood by aviation experts to translate back to "cyber "safety".

iii) Legal terminology

2.5 To make matters even more challenging, the legal implications of some key terms used in cybersecurity are used in a continuum which has a fine line between civil and military terminology.

Appendix 3[40]

Summary of analysis according to three scenarios

1. Introduction

1.1. With regard to each Scenario, the hypothetical facts will be presented, followed by the analysis by the RSGLEG, and the conclusions thereof, focusing on the applicability or otherwise of the international air law instruments with regard to various legal issues, *inter alia,* prosecution and jurisdiction of cyber-attacks against civil aviation.

1.2. For the purpose of this study, a legal analysis has also been made as to the issues that might serve as an obstacle for the relevant provisions to apply. It must be further noted that the analysis provided must be seen as being carried out on a case by case basis, applicable therefor to the particular hypothetical facts in the identified scenario created for this exercise.

1.3. For the purpose of the offences relative to the scenarios, the air law instruments have been analysed taking into account the following: type of act(s) (actus reus), intent required (means rea), type of actor, location of actor, location of effect and the impact/effect of the act/attack (e.g. act likely to endanger safety of that aircraft).

1.4. With regard to jurisdiction, various bases for jurisdiction have been put forward as a possibility for each scenario; however, it would ultimately depend on the air law instrument which would be deemed applicable, and / or national law.

6. Scenario A

2.1. Scenario Description

2.1.1. State A's airport XYZ systems and controllers were hacked. The hack was launched on 3 stages, first all automatic doors were opened which allowed access between restricted and non-restricted security areas of the airport, second it disabled all CCTV cameras (i.e., security cameras), and third shut down the power in the whole airport.

2.1.2. An announcement was made on the dark web by hacker group H took responsibility of the act, claiming political reasons behind it.

2.1.3. As a result the airport was closed down to aircraft and passengers. All systems were disconnected and shut down. Power was restored through emergency power generators. The airport was evacuated and fully searched using security forces and K9. Additional personnel were brought in to manage access to/from airport facilities and areas. Overall, the airport was able to resume partial operations within 12 hours of the attack but CCTV remained non-operational for 36 hours as all systems needed to be formatted, reprogrammed, and reconfigured.

2.1.4. 26 hours after the attack, an aircraft operating from airport XYZ to airport DEF in State B with a transit stop in airport ABC in State C. During the flight from airport ABC to airport DEF, the aircraft lost all power and crashed into a city in State B, killing all occupants as well as many people on the ground in addition to destroying a large number of properties.

[40] The scenarios have been developed solely to further the analysis of the existing international air law instruments as applied to attacks against civil aviation utilizing cyber means. The scenarios are not intented to communicate any potential vulnerabilities.

2.1.5. Investigation of the accident led to believe that an EMP device was activated on-board the flight which disabled all electronic equipment on the airplane including disabling flight controls and led to the crash.

2.1.6. The investigation led to the belief that the device was smuggled on-board in airport XYZ benefiting from the absence of CCTV by an insider and considered four options for the activation of the device: by a person on-board, from outside the aircraft using a ground-based antenna (activation by an
2.1.7. RPAS was excluded after review of radar data in the area of the crash), through an internal timer, or through an altimeter trigger.

2.1.8. Hacker group H issued a second announcement claiming responsibility of the attack, and clarifying the initial political message related to State A was a hoax, whereas the actual reason behind the act was to target State B.

2.1.9. The investigation of the act against airport XYZ identified the hack as originating from State D where it is believed that hacker group H has a large operation. Assume all States are parties to all instruments.

2.2. Scenario Analysis

1.	**Scenario Category**	It was deemed that such scenario falls under Category 1, 2 and 3.
2.	**Type of act/attack**	Regarding the type of attack, it was concluded that it was a cyber-attack against country A's airport XYZ IT/OT systems and controllers, as well as a cyber-attack during the flight from airport ABC to airport DEF; however also entailing part thereof through a physical attack, wherein the device was smuggled on board, which was enabled through the cyber-attack of disabling the CCTV cameras and disabling the automatic doors.
3.	**Assumptions**	Assumptions have been made about XYZ being an international airport.
4.	**Type of actor**	The type of actor has been deemed to be the hacker group H who took responsibility of the attack, with the possibility of being a terrorist in view of the intent in point 5.
5.	**Intent**	The intent behind the act/attack has been deemed to be for political reasons.
6.	**Method used**	The method used is a cyber-attack against airport XYZ, an EMP against the aircraft, as well as a cyber-attack to assist the placing of the device on board the aircraft.
7	**Location of actor**	With regard to the location of the actor, it has been identified to be State D, where it is believed that hacker group H has a large operation. With regard to the location of the vector, four options were considered for the activation of the device: by a person on-board, from outside the aircraft using a ground-based antenna (activation by an RPAS was

		excluded after review of radar data in the area of the crash), through an internal timer, or through an altimeter trigger.
8.	**Location of potential device/weapon**	With regard to the location of the potential device/weapon, it was noted that the EMP device was activated on-board the flight; however, the cyber-attack having originated from State D and also attacking State A's airport systems.
9.	**Location of the effect**	Regarding the location of effect, it may be classified as having 3 effects: State A's airport, the aircraft losing power, and State B due to the crash.
10.	**Potential impact(s) on information security (IT/OT technical impact) Potential impact(s) on information and information systems used in civil aviation (on confidentiality/integrity/availability):**	With regard to the potential impact(s) on information and information systems used in civil aviation (on information security parameters: confidentiality/integrity/availability), the following was concluded: a) all automatic doors were opened (integrity of functioning as well as availability compromised) b) disabled all CCTV cameras (availability of CCTV compromised) c) shut down the power in the whole airport (availability of power compromised). d) it was noted that the aircraft lost all power, disabled all electronic equipment on the airplane including disabling flight controls (availability and integrity of functioning compromised.
11	**Consequences on civil aviation (safety and security)**	Regarding the consequence on civil aviation and therefore, the potential impact(s) on aviation safety and security it was concluded that a) automatic doors were opened which allowed access between restricted and non-restricted security areas of the airport; b) impact on security as no boundary between landside and SRA; c) impact on security and safety as no power; d) from a safety point of view, it resulted in an accident as it crashed into a city in country B killing all occupants as well as many people on the ground.
12.	**Consequences on civil aviation (other than above)**	Regarding potential impact(s) on civil aviation other than the above, it was noted that as a result, the airport was closed down to aircraft and passengers. Overall, the airport was able to resume partial operations within 12 hours of the attack but CCTV remained non-operational for 36 hours as all systems needed to be formatted, reprogrammed, and reconfigured.

13.	**Jurisdiction**	With regard to the jurisdictional aspect, the bases for jurisdiction put forward as a possibility are: a) State D was identified since it the attack is originating from there and where it is believed that hacker group H has a large operation and therefore based on their presence b) On the nationality principle, by or against a national of that State c) Against the security of that State d) State of operator e) State of registration of aircraft f) Effect in the territory of that State (State A and B).
14.	**The potential applicable air law instruments have been identified as the following:**	**a) The Beijing Convention 2010** Article 1 paragraph 1 (b), (c) and (f) relating to the attack against aircraft: *''Any person commits an offence if that person unlawfully and intentionally:* *b) destroys an aircraft in service or causes damage to such an aircraft which renders it incapable of flight or which is likely to endanger its safety in flight; or* *c) places or causes to be placed on an aircraft in service, by any means whatsoever, a device or substance which is likely to destroy that aircraft, or to cause damage to it which renders it incapable of flight, or to cause damage to it which is likely to endanger its safety in flight; or* *f) uses an aircraft in service for the purpose of causing death, serious bodily injury, or serious damage to property or the environment''* It was noted that whereas this article relates to the attack on the aircraft, the intent was discussed, since it is debatable on whether the intent in the scenario was to cause damage on the ground or not. **b) The Beijing Convention 2010 (and the Airport Protocol 1988)** Article 1 paragraph 1 (d), and 2(b) relating to the attack on the airport 1. *''Any person commits an offence if that person unlawfully and intentionally (d) destroys or damages air navigation facilities or interferes with their*

operation, if any such act is likely to endanger the safety of aircraft in flight;

2. *Any person commits an offence if that person unlawfully and intentionally, using any device, substance or weapon: (b) destroys or seriously damages the facilities of an airport serving international civil aviation or aircraft not in service located thereon or disrupts the services of the airport, if such an act endangers or is likely to endanger safety at that airport.''*

However, it has been brought forward whether under this scenario, the relative cyber-attack would fall under the terms ''device, substance or weapon.'' Therefore, in view thereof, one would need to either interpret broadly such terms, such as device and weapon, and or provide a definition or guidance material on the interpretation thereof. However, it must be noted that in a court of law, especially in a court of criminal judicature, the adjudicating judge would need to have the specificity of the offence, rather than leaving it open to a subjective interpretation.

Moreover, the challenge regarding this article is that the scenario did not relate per se to the safety at the airport itself, since the article requires ''if such act endangers or is likely to endanger safety at that airport''. In view thereof, as well as the interpretation of ''device / weapon'', it might render these articles of Beijing Convention and the Airport Protocol inapplicable for this part of the scenario.

Moreover, it can also be added that in this scenario, Article 1(4) (c) would apply, wherein it would be an offence for whosoever ''participates as an accomplice in an offence set forth in paragraph 1, 2, 3 or 4(a) of this Article.'' In this manner, through this ancillary offence, the law may be viewed as offering a wider 'net' of offences to ensure prosecution.

c) The Beijing Protocol 2010

Article 1(1)

Any person commits an offence if that person unlawfully and intentionally seizes or exercises control of an aircraft in service by force or threat thereof, or by coercion, or by any other form of intimidation, or by any technological means

However, it was noted that it is not clear whether an EMP attack that downs an aircraft would be treated as a seizure, since the attacker never exercised control or even attempted to.

Moreover, the latter is to be discussed in view of the interpretation that rendering an aircraft uncontrollable brings about, whether such may be interpreted to refer to an exercise of control. Therefore, in view of the interpretative obstacle, this might mean that this specific article would not apply in this scenario.

d) The Tokyo Convention 1963

Article 1

1. *''This Convention shall apply in respect of:*

a) offences against penal law;

b) acts which, whether or not they are offences, may or do jeopardize the safety of the aircraft or of persons or property therein or which jeopardize good order and discipline on board.''

With regard to the 'offences against penal law', this would depend on the applicable offenses, as well as that the national law of a State would have to have its legislative framework that would provide for offences of cyber-attacks, whether specifically in aviation or in a general legal framework.

Moreover, applicability would hinge on Article 2 whether it was ''offence(s) committed or act(s) done by a person on board any aircraft registered in a Contracting state; and whether the aircraft was in flight outside of the territory of any State or on the surface of the high seas.''

In view thereof, the Tokyo Convention is limited to the perpetrator being on board the aircraft and therefore renders this Convention inapplicable in a cyber-attack wherein the perpetrator is not on board the aircraft.

3. Scenario B

3.1. Scenario Description

3.1.1. A major maintenance organization was infiltrated by a cyber-attack over the period of 6 to 12 months. Eventually, a malware was introduced into an update to the fuel computer that relays fuel information to the cockpit flight displays.

3.1.2. The malware affects the displayed amount of fuel available on-board, where the fuel is shown to be 10% lower than the actual remaining fuel. The malware only modifies the displayed fuel values when the aircraft is in flight, such that it is not discernable when fueling the aircraft. The infected update was installed on 5 trans-continental aircraft belonging to 5 different operators in 5 different countries.

3.1.3. The next day, all five aircraft were conducting long haul flights ranging between 7 to 12 hours flight time. Ultimately, all 5 aircraft pilots noticed differences in remaining fuel at specified waypoints compared with their pre-flight calculations and decided to divert their aircraft to different airports around the world, causing disruption of air traffic across 3 major aviation regions.

3.1.4. Additional aircraft were impacted by the malware and more diversions took place around the world and the same issue continued for 4 days until the reason behind this phenomenon was identified.

3.1.5. Once a malware in the fuel computer was identified, all States decided to ground their operators' aircraft of the same type pending a full scan of their systems. As a result, several hundred people were misplaced around the world, there was a serious mistrust in the civil aviation system by the public. The attack eventually resulted in several airline bankruptcies as well as serious repercussions for traffic around the world which lasted for several months.

3.2. Scenario Analysis

1.	**Scenario Category**	The Scenario Category has been identified as falling under 2 and 4.
2.	**Type of act/attack**	The type of act/attack has been identified as a malware attack.
3.	**Assumptions**	N/A
4.	**Type of actor**	The type of actor has not been identified.
5.	**Intent**	The intent behind the act/attack is unknown.
6.	**Method used**	The method used has also been identified as a malware attack.
7.	**Location of actor**	The location of the actor is unknown.
8.	**Path**	Regarding the vector, it has been identified via the maintenance organization and the fuel computer.
9.	**Location of potential device/weapon**	The location of the potential device/weapon has on the one hand been unidentified but on the other, has been identified as each aircraft affected as well as the maintenance organization.

10.	**Location of the effect**	The location of the effect has been identified as multiple aircraft as well as the maintenance organization.
11.	**Potential impact(s) on information security (IT/OT technical impact) Potential impact(s) on information and information systems used in civil aviation (on confidentiality/integrity/availability):**	Regarding the potential impact(s) on information security (IT/OT technical impact); potential impact(s) on information and information systems used in civil aviation (on confidentiality/integrity/availability), it has been noted that the fuel level information was displayed as incorrect and therefore the integrity of fuel level information was compromised
12.	**Consequences on civil aviation (safety and security)**	The consequence on civil aviation and potential impact(s) on aviation safety and security are the potential impact on safety due to tampering with fuel levels; however, there was no actual impact on safety because the tampered fuel level displayed was lower than the real fuel level. Had it been higher, it would have caused an actual impact on safety.
13.	**Consequences on civil aviation (other than above)**	Regarding potential impact(s) on civil aviation other than the above, they include grounding of aircraft, diversions, lack of trust by travelling public as well as bankruptcies. The consequences broader than civil aviation have been identified as lack of trust by the travelling public and bankruptcies.
14.	**Jurisdiction**	With regard to Jurisdiction, the following have been identified: a) Maintenance organization location, b) location of effect c) State of registration of the aircraft d) State of operator e) nationality principle f) where the effect was felt
15.	**The potential applicable air law instruments have been identified as the following:**	**a) The Beijing Convention 2010** *1(1). Any person commits an offence if that person unlawfully and intentionally:* *(d) destroys or damages air navigation facilities or interferes with their operation, if any such act is likely to endanger the safety of aircraft in flight;* *(e) communicates information which that person knows to be false, thereby endangering the safety of an aircraft in flight;* It is worth noting that further to various discussions, the Beijing Convention has been deemed inapplicable due to the fact that there is no actual

safety impact in this scenario. However, would the tampering have indicated higher fuel levels, thereby leading to an actual safety impact, Article 1(1) e could be reconsidered as being applicable.

b) The Beijing Protocol 2010

Article 1

(1) Any person commits an offence if that person unlawfully and intentionally seizes or exercises control of an aircraft in service by force or threat thereof, or by coercion, or by any other form of intimidation, or by any technological means

The Convention for Suppression of Unlawful Seizure of Aircraft (the Hague Convention), as amended by Beijing Supplementary Protocol, has been deemed not applicable since the element of 'seizure' is not applicable in this scenario.

c) The Montreal Convention 1971

1. Any person commits an offence if he unlawfully and intentionally:

(e) communicates information which he knows to be false, thereby endangering the safety of an aircraft in flight.

However, in view of 2.11, it is debateable to what extent the safety of an aircraft has been affected. As with the Beijing Convention, this analysis could change if there was an actual safety effect. Moreover, discussion was also held about the intent.

4. Scenario C

4.1. Scenario Description

4.1.1. An aircraft wi-fi signal was hacked while in-flight using a ground-based station. The intruders took control of the aircraft In-Flight Entertainment system (IFE) and showed a video that tells passengers that the aircraft will explode in 60 minutes through a bomb planted on-board.

4.1.2. The airline analyzed the situation and decided that the bomb threat was not credible. However, and despite the efforts of the flight crew to calm down the passengers, the act resulted in unruly behavior on-board that developed to violent behavior. By then 20 minutes would have passed since the warning video was broadcast.

4.1.3. Given the extreme behavior on-board, the pilot decided to divert the flight to the nearest airport which was 45 minutes of flight time. Although the flight landed safely at the alternate airport,

the unrest on-board led to severe injuries for 2 cabin crew members who were trying to prevent passengers from attacking the cockpit door. Assume any relevant State is a party to all instruments.

4.2. Scenario Analysis

1.	**Scenario Category**	The Scenario Category has been deemed to fall under 2.
2.	**Type of act/attack**	The type of act/attack has been identified as taking control of the IFE.
3.	**Assumptions**	N/A
4.	**Type of actor**	The type of actor is unknown, however in view of the bomb threat, it may be deemed to be a terrorist.
5.	**Intent**	The intent behind the act / attack has been deemed as terror in view of the threat.
6.	**Method used**	The method used has been identified as hacking of wi-fi to take control of the IFE
7.	**Location of actor**	The location of the actor has not been identified.
8.	**Path**	The vector has been classified as ground-based, through the wi-fi, and leading to in-flight.
9.	**Location of potential device/weapon**	The location of the potential device/weapon has been deemed to be the aircraft in-flight.
10.	**Location of the effect**	The location of the effect has been identified as the aircraft in-flight.
11.	**Potential impact(s) on information security (IT/OT technical impact) Potential impact(s) on information and information systems used in civil aviation (on confidentiality/integrity/availability):**	The potential impact(s) on information security (IT/OT technical impact); and the potential impact(s) on information and information systems used in civil aviation (on information security parameters confidentiality/integrity/availability) resulted in the integrity of IFE being compromised and used to convey a bomb threat.
12.	**Consequences on civil aviation (safety and security)**	The consequence on civil aviation and the potential impact(s) on aviation safety and security are that although the flight landed safely at the alternate airport, the unrest on-board caused by the bomb threat, led to severe injuries for 2 cabin crew members who were trying to prevent passengers from attacking the cockpit door.
13.	**Consequences on civil aviation (other than above)**	N/A
14.	**Jurisdiction**	The jurisdiction has been identified as the State of registration of the aircraft and the State of operator. Moreover, it may be noted that the State of landing could also be a possibility, however, most air law instruments require the perpetrator to be on board, which is not the case in this scenario.

15.	**The potential applicable air law instruments have been identified as the following:**	**a) The Beijing Convention 2010 (and Montreal Convention 1971)** Article 1 *1(1) Any person commits an offence if that person unlawfully and intentionally:* *(e) communicates information which that person knows to be false, thereby endangering the safety of an aircraft in flight;* It is noteworthy to mention that whereas there was information communicated, which the person knew to be false, it was deemed by the cabin crew as not credible, and in fact, it was the reaction of the passengers that endangered the safety of the aircraft due to them being unruly. Therefore, it may be argued whether the false information resulted in a direct effect endangering the safety of the aircraft, or whether it was done indirectly. As an opinion, it is debateable whether the correlation between the false information being communicated and the endangering the safety of the aircraft are to be a direct cause and effect, or a by-product of the false information. **b) The Beijing Protocol 2010** *Article 1* *1. Any person commits an offence if that person unlawfully and intentionally seizes or exercises control of an aircraft in service by force or threat thereof, or by coercion, or by any other form of intimidation, or by any technological means.* *2. Any person also commits an offence if that person:* *(a) makes a threat to commit the offence set forth in paragraph 1 of this Article; or* *(b) unlawfully and intentionally causes any person to receive such a threat, under circumstances which indicate that the threat is credible.*

It has been noted that the Beijing Protocol might not find applicability since it would not be deemed a 'credible' threat. Albeit that people on the aircraft in the scenario did believe that the threat was believable, and resulted with the behavior that ensued, as well as the diversion. Moreover, a similar argument but forward under the Hague Convention regarding the interpretation of article 1as referring to the bomb threat, even if through technological means, as 'seizing or exercising control' of that aircraft.

c) The Hague Convention 1970

Article 1

(1) Any person who on board an aircraft in flight:

(a) unlawfully, by force or threat thereof, or by any other form of intimidation, seizes, or exercises control of, that aircraft, or attempts to perform any such act, or

This Convention would not be applicable as it necessitates the perpetrator being on board the aircraft. Moreover, it would be difficult to interpret 1(a) as referring to the bomb threat as 'seizing or exercising control' of that aircraft.

d) The Tokyo Convention 1963

Article 1 (1)(b)

acts which, whether or not they are offences, may or do jeopardize the safety of the aircraft or of persons or property therein or which jeopardize good order and discipline on board.

However, the Convention requires that the perpetrator would be on board and therefore would not be rendered applicable, as mentioned under Article 1(2): ''Except as provided in Chapter III, this Convention shall apply in respect of offences committed or acts done by a person on board any aircraft registered in a Contracting State, while that aircraft is in flight or on the surface of the high seas or of any other area outside the territory of any State.''