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

An overview and gap analysis of existing provisions

Note: This report presents key elements of the discussions by the experts in the RSGLEG on the draft study. The draft study maybe consulted for Definitions and additional material.

TABLE OF CONTENT

1. INTRODUCTION

The study on the applicability of international air law instruments to cyber threats against civil aviation was undertaken by the Research Subgroup on Legal Aspects ("RSGLEG") of the Secretariat Study Group on Cybersecurity ("SSGC"). The RSGLEG developed and reviewed the draft study on this topic over 10 meetings from November 2018 and reported its progress periodically to the SSGC. Experts from 15 States[1] and 4 organizations[2] participated one or more meetings of the group. This report presents key elements of the discussions and outcomes of the study by the Subgroup.

2. BACKGROUND

2.1. The cybersecurity environment for civil aviation

2.1.1. 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.

2.1.2. 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.

2.1.3. 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 cyber-attacks on civil aviation leading to an accident,[3] the consequences of a cyber-attack could be significant and should be taken into consideration when conducting the analysis of the applicable legal framework to cyber-attacks.

2.1.4. According to ICAO guidance, particularly ICAO Doc No. 10108 - Aviation Security Global Risk Context Statement (2nd Edition (2019 - Restricted), Appendix C and *Updated overview of threats and risks to civil aviation, September 2020 (Restricted)*, the current overall likelihood of a terrorist cyber-attack on civil aviation is currently assessed to be low but with high potential consequences.

2.2. ICAO's cybersecurity work

2.2.1. The SSGC was established following the 39th Session of the ICAO Assembly. During the fourth meeting of the SSGC (Montréal, 5 September 2018), the 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.

2.2.2. The issue of addressing cyber threats to civil aviation was 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

[1] Brazil, Canada, China, France, Israel, Kenya, Malta, Netherlands, Oman, Russian Federation, Singapore, South Africa, Switzerland, Turkey, and the United States.
[2] CANSO, EDA, IATA and ICCAIA.
[3] Incidents causing operational disruption have been reported.

Committee. The ICAO Assembly, during its 40th Session in 2019 further agreed to maintain this item on the work programme of the Legal Committee.

2.2.3. Furthermore, ICAO 40th Assembly adopted the ICAO Aviation Cybersecurity Strategy (A40-10) 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.

2.2.4. Following the adoption of the ICAO Aviation Cybersecurity Strategy by the Assembly, ICAO Council adopted the ICAO Cybersecurity Action Plan (C-DEC 219/2 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, investigation, and prosecution of cyber-attacks that impact the safety, security, efficiency, and/or continuity of civil aviation.

2.2.5. The analysis of the existing international air law instruments with respect to their applicability to cyber threats or cyber-attacks against civil aviation carried out within the RSGLEG is also timely in view of the "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" established under the UNGA which issued its conclusions and recommendations[4] for future work in July 2021. 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."*

3. OBJECTIVE AND SCOPE OF THE WORK

3.1.1. The objective of this work is to examine the adequacy of international air law instruments with regards to the 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; and

d) the best way to further promote the results thereof.

3.1.2. The general absence of explicit references to cyber threats in the framework requires analyzing whether the existing international air law instruments could be interpreted to cover such cyber threats or whether the instruments could be considered inapplicable. The following international air law instruments were discussed and analyzed in the study:

- Convention on International Civil Aviation (Chicago, 1944 – "Chicago Convention"); incl. *Annex 17 – Security — Safeguarding International Civil Aviation Against Acts of Unlawful Interference*

[4] 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.

- 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").

4. METHODOLOGY

4.1. General considerations

4.1.1. Cyber-attacks and their possible effects cover a vast range of possibilities that remains ever evolving with new systems and technologies, which present different concerns from traditional aviation security concerns (e.g., bomb threats, unruly passenger, etc.). As it is not possible to define cyber threats within a limited scope of potential scenarios, the analysis cannot simply assess whether all cyber threats scenarios would be covered by each instrument. Therefore, the analysis also considered the general applicability criteria of the air law instruments in order to circumscribe the extent of their coverage, highlight their limits and subsequently allow the analysis of whether any cyber threat situation could fall outside of the scope of each instrument.

4.1.2. As methods of conducting cyber-attacks evolve over time and can be carried out with various technical means, this analysis takes a "technology neutral" approach. As such, the technology used in conducting cyber-attacks will not be analyzed herein.

4.2. Applicability criteria - Actor

4.2.1. Various types of actors may be at the origin of a cyber-attack such as: individuals, State actors, groups, and legal entities. The type of actor requires to be analyzed as instruments are not equally applicable to all (e.g., Article *3bis* of the Chicago Convention only applies to State actors). The analysis below will therefore identify the actors for which they are applicable.

4.2.2. It will be appreciated that the actor criteria detailed herein is taken separately from any motive consideration which may be present in national laws and which may lead to different regimes being applicable. For example, certain national laws may provide different regimes for ethical hackers (e.g., "white hats" or security researchers) than illicit hackers, even if they each fall within the "individual" type of actors. Such considerations were not addressed in this analysis.

4.3. Applicability criteria - Intent (*mens rea*)

4.3.1. The various motives such as those mentioned above imply different levels of intent to harm civil aviation. 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 and relies on a factual assessment of the situation by the court. Providing an in-depth discussion of this topic is therefore beyond the scope of this study, which is limited to identifying whether an instrument requires intent or not.

4.4. Applicability criteria - Act (*actus reus*)

4.4.1. 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 the analysis of specific acts less relevant for this study.

4.4.2. As such, the applicability of international air law instruments, in terms of the act, will be herein analyzed by identifying all necessary elements, whether they are related to the impact on the safety of civil aviation, the location of the perpetrator, the timing of the attack or the effect of such attack.

4.5. Applicability criteria - Jurisdiction

4.5.1. The final air law instrument applicability criteria, necessary to ensure that alleged perpetrators are prosecuted, pertains to the jurisdiction provisions. The analysis will cover the bases for jurisdiction provided in each instrument, so as to allow the assessment of any potential gaps considering the particularities of cyber threat scenarios (e.g., perpetrator may act from a remote location in a different State that is otherwise not tied to a flight being attacked). While these particularities of cyber scenarios complicate, the analysis, compared to traditional attack scenarios, and prevents it from being exhaustive, it remains useful to identify any already existing potential gaps.

5. OVERVIEW OF THE INTERNATIONAL AIR LAW INSTRUMENTS

5.1. Chicago Convention, Article 3 *bis* and Annex 17

5.1.1. The present analysis 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;"*

5.1.2. The Chicago Convention and its Annexes provide a framework applicable to States that focuses on prevention and deterrence which sets the framework for the governance of international civil aviation with the objective to ensure safety and security. As it complements the offence-creating air law instruments with certain obligations for States, such as the provisions of Article 3 *bis* of the Chicago Convention, their analysis is of interest for the scope of the study.

5.1.3. 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"*.

5.1.4. 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.[5] 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".

Applicability Criteria			
Actors	**Act**	**Intent**	**Jurisdiction**
States	- Use of a weapon against civil aircraft - aircraft in flight	Not required	N/A

5.1.5. As for Annex 17 to the Chicago Convention, it includes Standards and Recommended Practices (SARPs) on preventive aviation security measures and more specifically includes a definition of acts of unlawful interference[6] which is relevant for this study. 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, which could include cyber threats.

5.2. Tokyo Convention 1963 and Montréal Protocol 2014

5.2.1. 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.[7] 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.[8]

[5] 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.
[6] Annex 17 to the Chicago Convention, "Security", Tenth Edition, 2017, Chapter 1 - Definitions.
[7] Convention on Offences and Certain Other Acts Committed on Board Aircraft, signed at Tokyo on 14 September 1963 [Tokyo Convention], Article 1(1).
[8] Tokyo Convention, Article 3.

Applicability Criteria			
Actors	**Act**	**Intent**	**Jurisdiction**
Not specified (applies to individuals and other non-State actors)	- offences against penal law, acts which may or do jeopardize safety of the aircraft/person/property or acts which jeopardize good order and discipline on board; - committed by a person on board the aircraft; - aircraft registered in a contracting State; - during flight (from power application for takeoff until the landing run ends) or in an area outside the territory of any State.	Not required	- State of Registration; - criminal jurisdiction in accordance with national law.

5.2.2. 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.[9]

Applicability Criteria			
Actors	**Act**	**Intent**	**Jurisdiction**
Not specified (applies to individuals and other non-State actors)	- offences against penal law, acts which may or do jeopardize safety of the aircraft/person/property or acts which jeopardize good order and discipline on board; - committed by a person on board the aircraft; - aircraft registered in a contracting State; - during flight (from external door closes after embarkation until such door opens for disembarkation) or in an area outside the territory of any State.	Not required	- State of Registration, State of Landing (alleged offender on board) or State of Operator (dry lease); - State of landing when safety/discipline is jeopardized - criminal jurisdiction in accordance with national law

5.3. Hague Convention 1970 and Beijing Protocol 2010

5.3.1. 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.[10] In addition to establishing the legal principle of "extradite or prosecute",[11] 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.[12]

[9] Montréal Protocol 2014, Article IV.
[10] Hague Convention, Article 1.
[11] Hague Convention, Article 7.
[12] Hague Convention, Article 4.

Applicability Criteria			
Actors	**Act**	**Intent**	**Jurisdiction**
Not specified (applies to individuals and other non-State actors)	- committed by a person on board the aircraft; - aircraft in flight (from external door closes after embarkation until such door opens for disembarkation); - unlawful use of force, threat or intimidation to exercise control of the aircraft.	Not required	- State of registration (or designated State of registration under Art. 5); - State of Landing or State of Operation (dry lease); - offender on territory and no extradition; - criminal jurisdiction in accordance with national law.

5.3.2. 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.[13] 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". 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.[14] Two optional bases are also included, when the offence is committed against a national or by a stateless person habitually resident in that State.[15] Both instruments require States to impose severe penalties for the offences.[16]

Applicability Criteria			
Actors	**Act**	**Intent**	**Jurisdiction**
Not specified, except addition of legal entities (applies to individuals and other non-State actors)	- unlawful act seizing or exercising control of an aircraft; - aircraft in service (from pre-flight preparations for a specific flight until 24h after landing); - perpetrated by any technological means.	Required	- on the State's territory; - State of Registration, State of Landing (alleged offender on board), State of Operator (dry lease); - offender is a national of that State; - offender on territory and no extradition; - criminal jurisdiction in accordance with national law. <u>Non mandatory:</u> - against a national of that State; - stateless offender residing on the territory of the State

5.4. Montréal Convention 1971 and VIA Protocol 1988

5.4.1. 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.[17] 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

[13] Beijing Protocol, Article II.
[14] Beijing Protocol, Article VII.
[15] Beijing Protocol, Article VII.
[16] Hague Convention Article 2 and Beijing Protocol, Article III
[17] Montreal Convention 1971, Article 1.

act. Furthermore, jurisdictional bases also include jurisdiction for offences committed "against or on board an aircraft registered in that State".

Applicability Criteria			
Actors	**Act**	**Intent**	**Jurisdiction**
Not specified (applies to individuals and other non-State actors)	- unlawful act likely to endanger the safety of aircraft in flight; - causes damage to the aircraft, places or causes to be placed a device, destroys/damages/interferes with operations of air navigation facilities or communicates false information (knowingly).	Required	- on the State's territory; - State of Registration, State of Landing (alleged offender on board) or State of Operation (dry lease); - offender on territory and no extradition; - criminal jurisdiction in accordance with national law.

5.4.2. 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.[18] 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.

Applicability Criteria			
Actors	**Act**	**Intent**	**Jurisdiction**
Not specified (applies to individuals and other non-State actors)	- unlawful act likely to endanger safety at the airport; - using any device/substance/weapon; - seriously damages airport facilities, seriously damages an aircraft not in service located at the airport or disrupts the services of the airport.	Required	- on the State's territory; - State of Registration, State of Landing (alleged offender on board) or State of Operation (dry lease); - offender on territory and no extradition; - criminal jurisdiction in accordance with national law.

5.5. Beijing Convention 2010

5.5.1. 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.[19] 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.[20] Furthermore, the Beijing Convention also broadens the scope of criminal liability to cover attempts, organizing, participating as accomplice, and conspiracy to commit,[21] and incorporates broader jurisdictional bases, including 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.[22]

[18] VIA Protocol, Article II.
[19] Beijing Convention, Article 1(1).
[20] Beijing Convention, Article 1(3).
[21] Beijing Convention, Article 1(4).
[22] Beijing Convention, Article 3.

Applicability Criteria			
Actors	**Act**	**Intent**	**Jurisdiction**
Not specified, except addition of legal entities (applies to individuals and other non-State actors)	- unlawful act likely to endanger the safety of aircraft in flight, to cause serious injury/death or likely to endanger safety at an airport serving international civil aviation; - causes damages to the aircraft, places or causes to be placed a device, destroys/damages/interferes with operations of air navigation facilities, communicates false information (knowingly), uses an aircraft in service to cause death/injury, causes serious damage to property or the environment, seriously damages airport facilities, seriously damages an aircraft not in service located at the airport or disrupts the services of the airport.	Required	- on the State's territory - State of Registration, State of Landing (alleged offender on board) or State of Operation (dry lease); - offender is a national of that State; - offender on territory and no extradition; - criminal jurisdiction in accordance with national law. <u>Non mandatory:</u> - against a national of that State; - stateless offender residing on the territory of the State.

6. ANALYSIS

6.1. Analysis of the applicability of the international air law instruments to cyber threats

6.1.1. As presented in the overview of the instruments section, the applicability requirements of each instrument were highlighted and summarized. The following section presents the analysis made of the particularities of each instrument, in relation to the aforementioned criteria and their relevance to cyber threats and attacks, in the same order as presented in the earlier sections.

6.1.2. **Article 3 *bis* of the Chicago Convention**, which only applies to State actors, requires the cyber threats and cyberattacks to 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.

6.1.3. 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. Within the context of cyber threats, the term "weapon" is being discussed, in current literature, as follows: *"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".*[23]

6.1.4. 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”.*[24]

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

[24] A_76_135-2104030E-1.pdf (un-arm.org), retrieved on 28 December 2021

6.1.5. **Annex 17 of the Chicago Convention** pertains to acts of unlawful interference as defined in Chapter 1 of the Annex, which may cover cyber-attacks when considered to have the effect of jeopardizing the safety of civil aviation. Furthermore, a 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, which reinforces the interpretation that Annex 17 can be applied to cyber threats.

6.1.6. The **Tokyo Convention of 1963** could be applicable to cyber threats in cases where 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 an aircraft. As such, the scope of application of the Tokyo Convention 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. However, as one of the applicability criteria requires the perpetrator to be on board the aircraft, the overall usefulness of the Tokyo Convention in addressing cyber threats may be limited, given that cyber threats can be carried out remotely.

6.1.7. The **Montreal Protocol of 2014** may improve the possibility of prosecuting a cyber-attack, in comparison to the Tokyo Convention of 1963, as it widens the scope of application of the Convention to include the State of landing as a valid jurisdiction. This new jurisdiction may help prosecuting the perpetrator of a cyber-attack that would be on board of the flight.

6.1.8. The **Hague Convention of 1970** requires that the specific effect of the cyber-attack be assessed, which necessitates a factual assessment that may be hard to conduct. As a matter of fact, to successfully apply the Hague Convention, it would need to be proven that the cyberattack, effected by a person on board the aircraft, effectively resulted in the control of the aircraft. Additionally, the cyber-attack would need to be considered as a "use of force", which could be interpreted differently depending on the jurisdiction in which a case is being prosecuted. Therefore, while remaining possible, it may be harder to prosecute a cyber-attack under the provisions of the Hague Convention than other instruments, for instance the Beijing Protocol.

6.1.9. The **Beijing Protocol of 2010**, amending the Hague Convention of 1970, broadens the timeframe for which unlawful acts are covered. This 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. Moreover, the Beijing Protocol adds the terms "or by any technological means" to Article 1, which seems indicative of the intent to clarify that the instrument does cover cyber acts. 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 it remains necessary to prove that the cyber-attack amounts to "seizing" or "exercising" control of an aircraft.

6.1.10. As for the **Montreal Convention of 1971** and its amending **VIA Protocol of 1988**, their scopes of application are broader, compared to the Hague Convention, that may provide easier prosecution of cyber-attacks. As a matter of fact, there is no requirement for the perpetrator to be on board the aircraft allows the coverage of remote cyber-attacks, the effect of the cyber-attack is limited to endangering the flight or the airport, and the cyber-attack can be covered not only when affecting an aircraft but also air navigation facilities, providers of critical flight information, or airport facilities.

6.1.11. Finally, the **Beijing Convention of 2010** introduces detailed provisions that facilitates the application of the instrument to cyber-attack scenarios, more so than any of the previous instruments. As such, the Convention includes a specific definition for "air navigation facilities" which incorporates

signals, data, information or systems necessary for the navigation of the aircraft.[25] This provides further clarity to the scope of acts that could cover attacks to such facilities and aircraft by cyber means.

6.1.12. In general, some additional considerations relevant to the applicability criteria and affecting all instruments should be noted. In the factual assessment of the intent, which may impact the prosecution of the cyber-attack perpetrator, the analysis does not include whether the attacker intended "only" the element of the attack with an impact on information security parameters, such as confidentiality, integrity, and 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.).

6.1.13. Due to the interconnectivity of systems, an intended cyber-attack could have consequences unintended by the attacker, which 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 by a more general, unspecific cyber-attack threat scenario that, while not targeted at civil aviation itself, 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).

6.1.14. Additionally, 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 from where the attack took place. 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 are able to 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.

6.1.15. 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. It is thus important to define the requirements for which an act could be considered as covered by the air law instruments.

6.1.16. A key characteristic of a cyber-attack is its lack of physicality (by the perpetrator at the time and location of the effect), which 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.

6.1.17. 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). 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.

6.1.18. Moreover, many instruments include terms that need to be interpreted broadly if the instrument is to be applied to cyber-attack scenarios. This may be an issue which applies differently in different jurisdiction, further causing a fragmentation of the application of the instruments. For example,

[25] Beijing Convention, Article 2(c).

while arguably being the easiest instrument to apply to cyber-attacks, the Beijing Convention of 2010 may require the interpretation of the following:

- 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 or 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?

6.1.19. 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 in the light of the current state of technology, and that the expanded definition in the Beijing Convention merely recognizes this fact.

6.2. Analysis of three sample cyber threat scenarios

6.2.1. In addition to the analysis 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 Appendix 3 of the draft study for the detailed scenarios and their analyses).

6.2.2. For the purpose of the scenario analysis, it was concluded that the hypothetical cyber-attack scenarios could be categorized in four categories[26], 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

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

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).

6.2.3. 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 and therefore be 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.

6.2.4. 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 cyber-attacks 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).

6.2.5. The scenarios provided were analyzed 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 analyzed against the legal aspects, including the type of actor, the act itself, the intention and the jurisdictional basis for prosecution.

6.2.6. Once all applicable instruments and provisions were identified, the second prong was then to analyze 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.

6.3. Results of the review of instruments and analysis of scenarios

6.3.1. 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.

6.3.2. Each of the instruments provides some useful basis to address cyber threat scenarios and their potential effects on civil aviation. However, certain more recent instruments, such as the Beijing instruments, provide clearer applicability or broader coverage, making them easier to address cyber threats. However, while these newer instruments might be easier to apply and require less judicial interpretation, all instruments could be found applicable in certain cases.

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

7.1.1. 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, a number of the recent aviation security instruments have a broader and more direct application.

7.1.2. 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.

7.1.3. 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.

7.1.4. 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.

7.1.5. 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.

7.1.6. 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.

8. CONCLUSIONS

8.1.1. 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);

8.1.2. 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;

8.1.3. Four broad categories of cyber-attacks were used:

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.

8.1.4. 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.

8.1.5. 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 attacks and where the attacks including their effects have potentially taken place or are regarded to have taken place (e.g., on board the aircraft);

8.1.6. 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.

8.1.7. 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 make reference to attacks by "any technological means".

8.1.8. The existing international air law instruments are considered partially adequate for identified cyber threat/attack scenarios, based on a case by case analysis. 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.

8.1.9. 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.

8.1.10. 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.

8.1.11. 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.