ICAO

RECONNECTINGTHEWORLD

ADEQUACY OF EXISTING INTERNATIONAL AIR LAW INSTRUMENTS IN ADDRESSING CYBER THREATS AGAINST CIVIL AVIATION

LC/38-WP/2-2, PRESENTATION OF THE LEGAL WORK ON CYBERSECURITY

BACKGROUND

LC 37
2018

- Legal Committee included the issue of cyber threats to civil aviation to its Work Programme

A40
2019

- Legal Commission merged item 4: "Acts or offences of concern to the international aviation community, including cyber threats, that may not be adequately covered by existing air law instruments.
- A40-10 – calls for developing cybersecurity framework through a cross-cutting approach involving various aviation disciplines

C-222
2021

- approval of Cybersecurity Panel (CYSECP) reporting to the Aviation Security Committee (ASC) (SSGC to be dissolved)

09/2018 → 01/2022

Secretariat Study Group on Cybersecurity (**SSGC**) - Research Subgroup on Legal Aspects (**RSGLEG**)

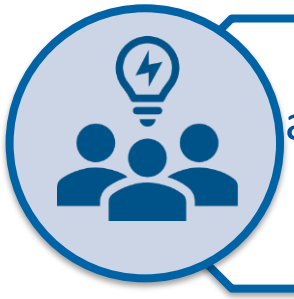
ESTABLISHMENT OF RSGLEG

- SSGC-RSGLEG/1 – held in Montréal on 22 November 2018, decided membership should be expanded to ensure wide geographical representation and diversity of legal systems.

- Participants included legal experts from **15 States** and **4 international organizations**.

- Study coordinated by Co-Rapporteurs: Ms. **Helena Hallauer** (Switzerland) and Dr. **Rebekah Tanti-Dougall** (Malta).

SCOPE OF WORK



3. Review and analyze (in relation to the identified threats, risks and actors) the adequacy of the current international legal framework as well as assess the need to reinterpret or amend the existing international air law instruments dealing with cyber threats or adoption of new instruments or SARPs

4. Analyze the State replies to ICAO State Letter AS 8/22-17/3 “Assembly Resolution A39-19 – Addressing Cybersecurity in Civil Aviation”

6. Identify aspects or matters to the ICAO Legal Committee/AVSEC Panel/other ICAO bodies.

STUDY BY RSGLEG

- RSGLEG met 10 times between 22 November 2018 and 21 January 2022
- Plenary meetings to consider the draft study presented by the co-Rapporteurs (first draft December 2020)
- Subgroup meetings on specific issues : scenarios, intent/effect/jurisdiction, 3 *bis*
- SSGC/10 delegated authority to RSGLEG to present the status of its work to LC/38
- RSGLEG did not conclude on finalizing the study, but agreed for the Secretariat to present a report based on the study and discussions among experts (Appendix A)

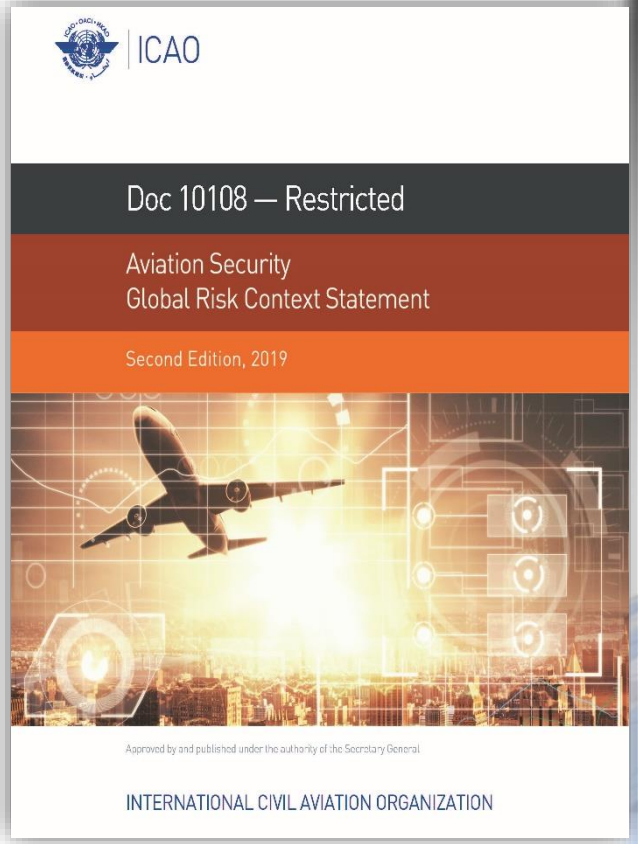
ADDITIONAL DETAILS OF THE DRAFT STUDY

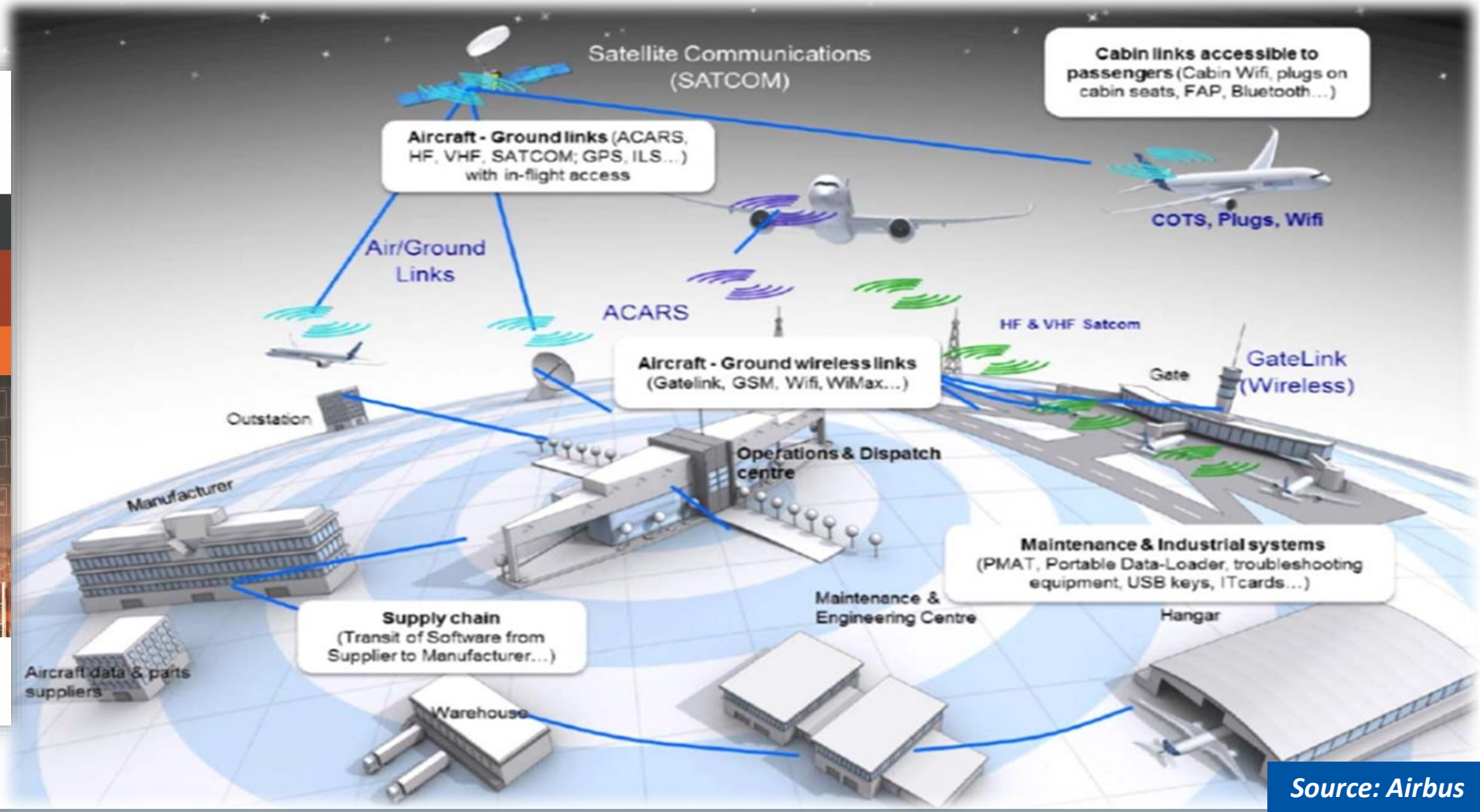
- The report of the Secretariat in Appendix A presents key elements of the Study and discussions from the RSGLEG
- The Study should be consulted for additional details on:
  - Definitions
  - Notion of intent
  - Cyber-attack methods and means
  - Variety of locations and attack paths
  - Effects of successful cyber-attacks
  - Overlap with cyber-specific instruments and deterrence
  - Attribution and jurisdiction
  - Detailed scenario analysis

ICAO

RECONNECTINGTHEWORLD

CYBERSECURITY ENVIRONMENT FOR CIVIL AVIATION





Source: Airbus

ANALYSIS OF INTERNATIONAL AIR LAW INSTRUMENTS

Tokyo Convention of 1963

Applicable to offences under **national penal law** and to a cyber-attack that may **jeopardize the safety** of an aircraft/person/property on board an aircraft

Requires the **perpetrator** to be **on-board the aircraft**

Montreal Protocol 2014

Expanded jurisdiction (State of landing and of the operator) expands scope to prosecute cyber-attacks when compared to Tokyo Convention 1963.

ANALYSIS OF INTERNATIONAL AIR LAW INSTRUMENTS

Hague Convention 1970

Requires that the cyber-attack resulted in **the control of the aircraft** + needs to be considered as a ***use of force***.

Requires the **perpetrator** to be **on-board the aircraft**

Beijing Protocol 2010

Broadens scope to aircraft **in service** instead of in flight, adds ***or by any technological means*** to Article 1.

No requirement for the offender to be on board.

Otherwise, same requirements as Hague Convention 1970.

ANALYSIS OF INTERNATIONAL AIR LAW INSTRUMENTS

Montreal Convention 1971 & VIA Protocol 1988

Broader application than Hague Convention 1970: no requirement for the perpetrator to be on-board, endangering flight or airport.

Further covers **air navigation facilities**, **provider of critical flight information** and **airport facilities**.

Beijing Convention 2010

Defines **air navigation facilities** to include **signals, data, information** or **systems**.

Such facilities could be directly applicable to cyber means of carrying an attack.

ANALYSIS OF INTERNATIONAL AIR LAW INSTRUMENTS

Article 3*bis*, Chicago Convention

May be applicable, requires the cyber means to be considered as a ***weapon*** and concerns **States**

Currently subject to debate between cybersecurity legal experts

Annex 17, Chicago Convention

Not an instrument for prosecution.

Standard 4.9.1 – *Measures relating to cyber threats* require States to develop and implement measures to protect critical information, ICT and data for civil aviation from unlawful interferences

Defines acts of unlawful interference to include unlawful seizure, misuse of aircraft, communication of false information.

POTENTIAL GAPS

- Fragmentation of the international air law framework (differences in ratification status of instruments and actors/attack/effect may include multiple jurisdictions).
- Interpretation of certain terms (e.g., “weapon”, “device”, “air navigation facilities”, “use of force”), may not be uniform throughout jurisdictions.
- Additional difficulties in applying older instruments to cyber threats due to the requirements to have the perpetrator on-board, the aircraft in flight, etc.
- Numerous cyber threats may not be covered by the current instruments as they may not *endanger the safety and security of a flight* (e.g., theft of passenger information).

CONCLUSIONS

- The air law framework is partially adequate in addressing cyber threats as certain gaps have been identified.
- While interpretation of certain terms may be required, the scope of the Beijing Instruments of 2010 seem to provide sufficient basis for prosecution of cyber-attacks.
- States urged to ratify the Beijing Instruments of 2010 in line with ICAO Assembly Resolutions A40-10 and A40-28.

APPENDIX B

Beijing Convention 2010

43 Parties*

Angola, Bahrain, Benin, Botswana, Burkina Faso, Cabo Verde, Congo, Côte d'Ivoire, Cuba, Cyprus, Czech Republic, Dominican Republic, Eswatini, Finland, France, Gabon, Gambia, Germany, Ghana, Guyana, Honduras, Kazakhstan, Kuwait, Luxembourg, Mali, Malta, Mozambique, Myanmar, Netherlands, Panama, Paraguay, Portugal, Romania, Rwanda, Saint Lucia, Seychelles, Sierra Leone, Sweden, Switzerland, Turkey, Turkmenistan, Uganda, Uruguay.

Beijing Protocol 2010

43 Parties*

Bahrain, Benin, Botswana, Burkina Faso, Cabo Verde, Congo, Côte d'Ivoire, Cuba, Cyprus, Czech Republic, Dominican Republic, Eswatini, Finland, France, Gabon, Gambia, Germany, Ghana, Guyana, Honduras, India, Kazakhstan, Kuwait, Luxembourg, Mali, Malta, Mozambique, Myanmar, Netherlands, Panama, Paraguay, Portugal, Romania, Rwanda, Saint Lucia, Saudi Arabia, Seychelles, Sierra Leone, Sweden, Switzerland, Turkey, Turkmenistan, Uganda.

*Germany deposited instruments of ratification on 21 March 2022; not included in Appendix B.

Thank You

ICAO