2024

Committee on Aviation Security– Topic 1

Director – Sylvain Lefoyer

CYBERSECURITY GOVERNANCE.

1. Historical background on cybersecurity governance in ICAO

1.1 In 2016, faced with growing concern about cyber-related risks to aviation, the 39th Session of the ICAO Assembly instructed ICAO to ensure that such matters were fully considered, and that States and industry were assisted in taking the necessary actions. The Secretariat Study Group on Cybersecurity (SSGC) was established in 2017 to drive this work forward, leading to adoption of the ICAO *Aviation Cybersecurity Strategy* at the 40th Session of the ICAO Assembly.

1.2 In 2018, the ICAO Council requested that the Secretariat conduct a feasibility study for the possible creation of a Cybersecurity Panel, a call repeated at the Second High-level Conference on Aviation Security (HLCAS/2). An initial outline for five possible scenarios was presented to the Council during its 217th Session in 2019. The methodology for the development of the feasibility study was approved by the Council during its 218th Session.

1.3 The 40th Session of the ICAO Assembly, in 2019, noted the multiple bodies involved in addressing cybersecurity in ICAO and expressed concern about the potential for gaps, duplication, inconsistency and loss of transparency. To address these concerns, the Assembly called on ICAO to bring the work of these groups under the aegis of an overarching structure; it discussed a set of criteria which could underpin a revised cybersecurity governance structure.

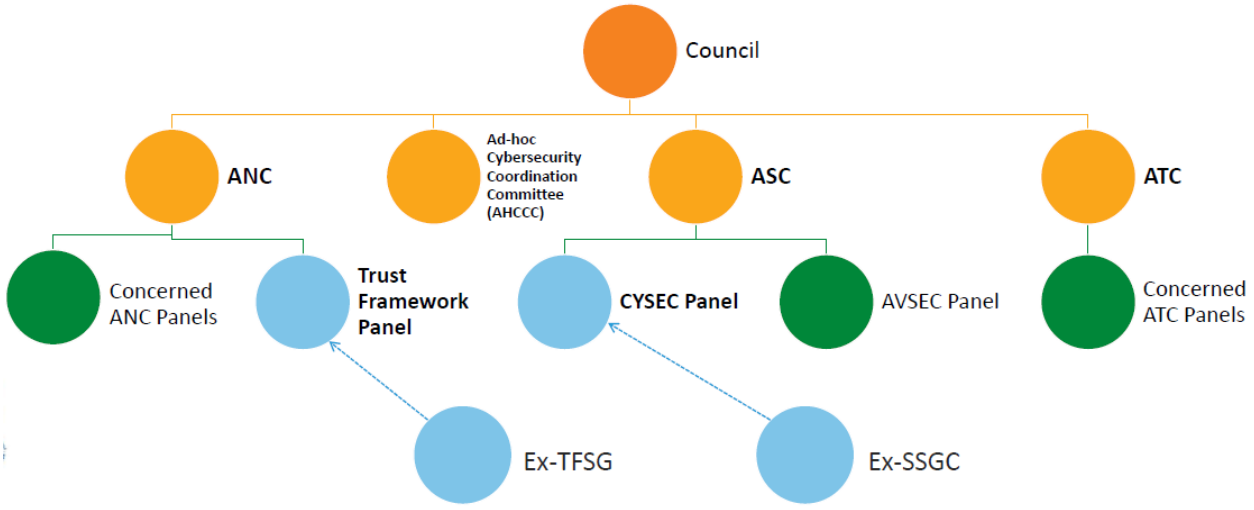
1.4 In 2020, the Council, during its 219th Session, reviewed the first two phases of the Feasibility Study and Gap Analysis on the Mechanisms to Address Cybersecurity, requested the Secretariat to further consider and update the feasibility study, and delegated authority to the President of the Council to establish a Small Working Group (SWG) composed of Council Representatives and Air Navigation Commission Members to further consider the work and present it to Council for further deliberation and decision making.

1.5 The Council, during its 222nd Session, considered the proposals presented by the SWG concerning an overarching governance mechanism to address cybersecurity in ICAO as well as the SWG's recommended solution. The Council approved a new governance structure for cybersecurity in ICAO comprising of a Technical Coordinating Committee of the Council on Cybersecurity (Cybersecurity Committee), a Cybersecurity Panel reporting to the Aviation Security Committee (ASC), and the integration of the Trust Framework Study Group (TFSG) into the ANC Panel structure.

1.6 During its 224th Session, the Council considered an overview of the progress made in developing the arrangements pertaining to the new cybersecurity governance structure of ICAO, in which the Council agreed to rename the Committee to "Ad Hoc Cybersecurity Coordination Committee" (AHCCC) and approved its Terms of Reference.

1.7 During the 229th Session, the Council approved the Secretariat's proposal to establish the AHCCC, delegated authority to the President of the Council to explore opportunities to enhance the composition of the AHCCC in this respect, and finalize the membership of the AHCCC, accordingly. Following extensive consultations with the President of the ANC and with the Secretariat, 13 Members were appointed to serve on the AHCCC and the first meeting of the AHCCC was convened in October 2023.

Fig.1: Cybersecurity Governance Structure



2. Achievements to date.

The work of ICAO on aviation cybersecurity covers many domains.

a. International Air Law instruments

First, the legal instruments that allow States to cooperate in order to bring perpetrators to justice. In that regard, the Beijing Convention and Protocol of 2010 are the most useful legal instruments to address cyber-attacks against civil aviation.

ICAO, in line with the last 3 Assembly Resolutions on Addressing Cybersecurity in Civil Aviation, encourages all Member States to adopt those instruments, which provide a framework to facilitate bringing cyber perpetrators to justice, and serve as a deterrent of cyber-attacks when perpetrators know that they can be brought to justice regardless of where they are located.

They are important instruments because:

- The Beijing Convention introduces detailed provisions that facilitate its application to cyber-attack scenarios, more so than any of the previous instruments. For example, it includes a specific definition for “air navigation facilities” which incorporates signals, data, information, or systems necessary for the navigation of the aircraft.

- The Beijing Protocol broadens the timeframe for which unlawful acts are covered. This is relevant to scenarios where cyber-attacks are conducted during pre-flight or post flight phases such flight calculations or maintenance activities. It also introduces the terms “or by any technological means”, which could used to cover cyber-attacks against civil aviation. It also does not require the perpetrator to be on-board the aircraft, which is a requirement in older security conventions, and which helps address the dimension of cyber threats to civil aviation.

b. Standards and Recommended Practices

The second area of ICAO's work is Standards and Recommended Practices for international civil aviation.

ICAO currently have one Standard, which is an obligation on States, and one Recommended Practice explicitly related to cybersecurity. Those provisions are in Annex 17 – Aviation Security.

The Standard requests States to ensure that entities under their supervision conduct a risk assessment, using which they identify their critical infrastructure, and take measures to protect it from cyber threats. The Recommended Practice on the other hand goes a little deeper and provides examples of techniques that can be used to ensure the confidentiality, integrity, and availability of aviation's critical systems, data, and information.

c. Assembly Resolutions

The third area related to ICAO's work is Assembly Resolutions which represent consensus among ICAO's 193 Member States to take actions.

In relation to cybersecurity, the latest 41st session of the ICAO Assembly adopted unanimously Resolution A41-19 on Addressing cybersecurity in civil aviation. The Resolution supersedes the previous Resolutions adopted at the previous two sessions of the ICAO Assembly.

In summary, the Resolution put a great focus on cooperation between States on the national, regional, and global levels, and also with industry on all levels too.

The Resolution also focuses on the importance of clear governance and accountability in terms of defining a point of convergence within the civil aviation ecosystem on the regulatory and oversight aspects related to aviation cybersecurity and their connection to aviation safety, security, and efficiency.

It further recognizes that aviation cybersecurity is a topic that affects all civil aviation domains as well as non-aviation domains, and therefore encourages States to address aviation cybersecurity in a holistic, harmonized, and cross-domain approach between all concerned within the State as well as on the regional and international levels.

ICAO 41st Assembly Resolution A41–19: *Addressing Cybersecurity in Civil Aviation*

- Highlights the need for global adoption of the Beijing Instruments
- Recognizes the need for aviation cybersecurity to be harmonized.
- Calls upon States to *(not an exhaustive list)*:
  - ✓ implement ICAO Aviation Cybersecurity Strategy, and make use of the ICAO Cybersecurity Action Plan
  - ✓ designate the authority competent for aviation cybersecurity, and define the interaction between that authority and concerned national agencies
  - ✓ define the responsibilities of national agencies and industry stakeholders with regard to cybersecurity in civil aviation
  - ✓ develop and implement a robust cybersecurity risk management framework that draws on relevant safety and security risk management practices, and adopt a risk-based approach to protecting critical civil aviation systems, information, and data from cyber threats.
  - ✓ design and implement a robust cybersecurity culture across the civil aviation sector

d. Aviation Cybersecurity Strategy

Developed in 2019 and endorsed by the 40th Session of the ICAO Assembly, it represents ICAO's vision for global aviation cybersecurity where the civil aviation sector is resilient to cyber-attacks and remains safe and trusted globally, whilst continuing to innovate and grow.

The Strategy comprises seven pillars:

1. The first pillar of the Strategy is international cooperation which recognizes the borderless nature of aviation and cybersecurity and calls for cooperation and harmonization between all stakeholders to address aviation cybersecurity.

2. The second pillar focuses on governance and accountability for civil aviation cybersecurity, also on including cybersecurity in States' civil aviation safety and security programmes, and on cooperation between civil aviation and cybersecurity competent authorities on the national levels.

3. The third pillar addresses effective legislation and regulation. It encourages States to review their national legislation to allow for the prosecution of cyber-attacks against civil aviation and encourages them to set up mechanisms for cooperation with "good faith" cybersecurity research.

4. The fourth pillar touches on cybersecurity policy, where it encourages States to include cybersecurity in their safety and security oversight systems as part of a comprehensive risk management framework.

5. The fifth pillar focuses on information sharing and it recognizes, through lessons learned from aviation safety and security management, that a culture of information sharing will significantly reduce systemic cyber risk in civil aviation.

6. The sixth pillar of the Strategy addresses incident management and emergency response, and focuses on formulating plans to ensure the continuity of operations during cyber incidents, and to test those plans and develop cyber response capabilities through exercises, while leveraging the existing crisis management frameworks related to safety and security incidents and accidents to support that work.

7. And last but not least, the seventh pillar of the Strategy focuses on the human element. Addressing aviation cybersecurity should be fostered through capacity building of the current aviation workforce, through including aviation cybersecurity in training programmes targeting the next generation of aviation professionals, and through developing and implementing a robust cybersecurity culture to fortify the sector's defenses against cyber threats.

3. Analysis and proposal for improvement.

Considering the role of ICAO as a forum for States to agree on global standards and the growing impact of cyber attacks, you are invited to reflect on the ICAO cybersecurity governance structure and its relevance and adequacy to the challenges faced by the aviation industry in cybersecurity.

You will also make recommendations, in the perspective of the 42nd ICAO Assembly in 2025, to raise States awareness and convince them to dedicate appropriate resources to address the matter nationally as well as to support ICAO.