International Civil Aviation Organization

WORKING PAPER

A42-WP/12
EX/4
21/7/25

ASSEMBLY — 42ND SESSION

EXECUTIVE COMMITTEE

Agenda Item 13: Aviation Security — Policy

CYBERSECURITY IN CIVIL AVIATION

(Presented by the Council of ICAO)

EXECUTIVE SUMMARY

The civil aviation sector's awareness and actions to address cyber threats and risks to civil aviation has been steadily increasing. Many developments have been taking place during the past triennium in ICAO as well as in States on the national, regional, and global levels. However, more work needs to be initiated, especially on the national levels, to ensure a holistic, harmonized, and consistent approach to aviation cybersecurity across the civil aviation sector.

This paper presents an overview of activities related to aviation cybersecurity, including those mandated by the Assembly, and proposes an update to Resolution A41-19 on *Addressing Cybersecurity in Civil Aviation* to emphasize the importance of improving the protection and resilience of the civil aviation sector to cyber threats and risks, while taking into account the development of ICAO's work on this topic.

Action: The Assembly is invited to:
a) note the developments in aviation cybersecurity activities; and
b) adopt the Assembly Resolution on *Addressing Cybersecurity in Civil Aviation* in the Appendix.

Strategic Goals:	This working paper relates to the Strategic Goals: *Every Flight is Safe and Secure* and the *Aviation Delivers Seamless, Accessible and Reliable Mobility for All*.
Financial implications:	The activities referred to in this paper will be undertaken subject to the resources available in the 2026 - 2028 Regular Budget and/or from extra budgetary contributions as guided by the ICAO Business Plan 2026 – 2028.
References:	Doc 10184, Assembly Resolutions in Force (as of 7 October 2022) *Aviation Cybersecurity Strategy* *Cybersecurity Action Plan*

1. INTRODUCTION

1.1 The civil aviation sector has been witnessing a rapid evolution in the use of information and new technologies to support its needs for automation, interconnectivity and interoperability as well as the deployment of new operational concepts on the ground and in the air and integrate new entrants, such as unmanned aircraft systems (UAS), into the air transport system. The ultimate objective of these developments is to support the growth of the civil aviation sector while ensuring its safety, security, efficiency, capacity and sustainability.

1.2 However, this trend has led to the increase of cyber threats to operational systems, data and information. This increase is further exacerbated by the geopolitical tensions taking place around the world. Although there have been no reports of cyber-attacks leading to significant impacts on aviation safety or security, the sector is witnessing an upward trend in reporting cyber incidents, which, to-date, seem to be mostly motivated by financial gain, theft of information or hacktivism.[1]

1.3 The increasing complexity of cyber threats and their potential impacts on civil aviation underscore the need for a global, robust and harmonized approach to enhance the protection and resilience of civil aviation to cyber threats. In that regard, ICAO continues to work with Member States, international organizations and industry, supporting them in mitigating cyber risks to the civil aviation sector.

1.4 The 41st Session of the ICAO Assembly noted with satisfaction the development of ICAO's work on aviation cybersecurity during the past triennium (2019 – 2022), and commended ICAO and its groups of experts on their work. In particular, the Assembly welcomed the adoption and implementation of an enhanced internal governance structure for aviation cybersecurity in ICAO, as well as the continuous development of aviation cybersecurity policies, provisions, guidance, capacity-building, and awareness initiatives. The 41st Session of the ICAO Assembly also adopted Assembly Resolution A41-19 on *Addressing Cybersecurity in Civil Aviation*, which superseded Assembly Resolution A40–10.

2. DISCUSSION

2.1 Aviation Cybersecurity Standards and Recommended Practices

2.1.1 In response to action item CyAP3.4 in the Cybersecurity Action Plan (CyAP) which requests ICAO to "Review existing ICAO Standards and Recommended Practices (SARPs) to identify the need for potential cybersecurity updates.", in 2022, ICAO conducted an in-depth individual analysis of sixteen Annexes to the *Convention on International Civil Aviation* (Chicago Convention), with the objective to identify potential areas of interest in ICAO SARPs related to aviation cybersecurity, in support of a holistic and cross-cutting approach to aviation cybersecurity in ICAO provisions.

2.1.2 The analysis was delivered to the Cybersecurity Panel, which established a Task Force on Cybersecurity Standards and Recommended Practices (TF-CYSARPS) to continue the work by cross-referencing the potential areas of interest across aviation disciplines as reflected in the relevant Annexes. The Task Force's work aims at investigating whether aviation cybersecurity is adequately covered by existing SARPs (whether explicitly or implicitly), identifying potential gaps in ICAO SARPs framework, and coordinating with relevant expert groups to address those gaps as appropriate. The work on this topic is ongoing and is expected to continue throughout the upcoming triennium.

2.2 International Legal Instruments

2.2.1 The "Study on the Applicability of International Air Law Instruments to Cyber Threats against Civil Aviation" that was submitted to the 38th Session of the Legal Committee concluded that the *Convention on*

[1] Further information on cyber threats and risks to the civil aviation sector can be found in ICAO Global Cyber Risk Considerations (*Doc 10213 – Restricted*).

the Suppression of Unlawful Acts Relating to International Civil Aviation[2] (Beijing, 2010 – "Beijing Convention 2010") and the Protocol Supplementary to the *Convention for the Suppression of Unlawful Seizure of Aircraft*[3] (Beijing, 2010 – "Beijing Protocol 2010"), contain important enhancements over older instruments, thus providing a sufficient basis for States to deal with cyber-attacks against civil aviation as crimes.

2.2.2 As of 1 April 2024, 53 Member States have ratified the Beijing Convention 2010, and 54 Member States have ratified the Beijing Protocol 2010. Given that these instruments introduce provisions that are relevant to address cyber-attacks against civil aviation, wide adoption and ratification of those instruments by Member States, as emphasized in the Assembly Resolutions on addressing cybersecurity in civil aviation, is highly recommended to support the deterrence of cyber threats to civil aviation and the prosecution of cyber-attacks against the sector.

2.3 Second Edition of the Global Aviation Security Plan (GASeP)

2.3.1 In line with the Cybersecurity Plan's action item CyAP2.5 which requests ICAO to "include cybersecurity in regional and global plans to ensure the safety, security, and resilience of aviation", and benefiting from the update of the GASeP of which the Second Edition was published in June 2024 (https://www.icao.int/Security/Pages/Global-Aviation-Security-Plan.aspx), ICAO included aviation cybersecurity in the plan's provisions under Global Priorities 1, 2 and 4.

2.4 Guidance Material

2.4.1 In line with the Cybersecurity Action Plan, ICAO developed guidance material[4] to support States and stakeholders to address cybersecurity in civil aviation which includes guidance on aviation cybersecurity governance and policy at State-level, cybersecurity culture in civil aviation, and cyber information sharing planning and implementation. ICAO also published the *Global Cyber Risk Considerations* (*Doc10213 – Restricted*), a guidance document that provides a methodology to integrate cyber risk management into aviation safety, aviation security, and air navigation efficiency and capacity risk management processes, as well as includes a high-level global cyber threat and risk landscape overview:

2.4.2 In line with Recommendation 4.2/1 of the 14th Air Navigation Conference on aviation cybersecurity, ongoing work on guidance material includes the development of a comprehensive set of guidance documents to address different aspects of aviation cybersecurity. It also includes a plan to compile all guidance material into *an Aviation Cybersecurity Manual* that covers all aspects related to the protection and resilience of critical aviation infrastructure and services to cyber threats and risks.

2.5 Trust Frameworks

2.5.1 During its 220th Session in June 2022, the Air Navigation Commission approved the establishment of the Trust Framework Panel (TFP). Since then, the TFP has been supporting the development of guidance materials for the establishment of interoperable trust frameworks:

a) technical guidance for interoperable trust and identity assurance for operational contexts has been developed, including guidance on information security (*Doc 10204 – Manual on Aviation Information Security*);

b) an Aviation Common Certificate Policy to support interoperable digital identities, information authenticity and assurance in civil aviation, including, inter alia, supporting

[2] Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation
[3] Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft
[4] https://www.icao.int/aviationcybersecurity/Pages/Guidance-material.aspx

authentication of Satellite-Based Augmentation Systems (SBAS) for Global Navigation Satellite Systems (GNSS);

c) a list of operational use-cases where trust frameworks would be beneficial is developed and maintained. Work has recently begun on guidance to support aviation stakeholders in establishing trust framework instances; and

d) guidance material for secure air/ground communications via the Aeronautical Telecommunications Network over Internet Protocol Suite (ATN/IPS) is being finalized in close coordination between the relevant groups of experts to directly support Amendment 93 to Annex 10 Volume III – Aeronautical Communications, Communication Systems.

2.6 ICAO Aviation Cybersecurity Work Programme

2.6.1 The Council, during its 228th Session in 2023, approved the establishment, membership and Terms of Reference of the AHCCC, following identification of adequate Secretariat resources to support its functioning. The AHCCC comprises of one Member from each of the Air Transport Committee (ATC), the Aviation Security Committee (ASC) and the Air Navigation Commission (ANC), and eleven Members from each expert group regularly addressing cybersecurity in its work programme.

2.6.2 The Committee's main functions are to coordinate aviation cybersecurity-related work across ICAO through the development and maintenance of a comprehensive ICAO Aviation Cybersecurity Work Programme. It also serves as the main advisory body of the Council on prioritization of work elements in line with the Work Programme.

2.6.3 The AHCCC met three times since its establishment and continues to refine the ICAO Aviation Cybersecurity Work Programme as the work on cybersecurity evolves, serving as a collaboration platform for expert groups to share information and support a harmonized and consistent approach to aviation cybersecurity in the context of their respective work areas.

2.7 Training and Capacity Building

2.7.1 ICAO's cybersecurity training portfolio includes to-date two aviation cybersecurity courses:

a) Foundations of Aviation Cybersecurity Leadership and Technical Management: The course was developed by ICAO in partnership with Embry-Riddle Aeronautical University and began delivery in October 2021. It is a comprehensive awareness course that covers all aspects of cybersecurity addressed in the Aviation Cybersecurity Strategy. During the previous triennium, the course was delivered to 88 participants between September 2022 and April 2025; and

b) Cybersecurity Oversight in Civil Aviation: The course was developed by ICAO in partnership with the United Kingdom's Civil Aviation Authority and began delivery in March 2023. It covers key aspects that would support States in developing and implementing an oversight framework for aviation cybersecurity, taking the experience of the United Kingdom as an example. During the previous triennium, the course was delivered to 34 participants between March 2023 and April 2025.

2.8 **Raising Awareness and Outreach Activities**

2.8.1 In line with the calls of the 41st Session of the Assembly for ICAO to intensify its awareness campaigns and to conduct aviation cybersecurity table-top exercises, the Organization benefited from kind voluntary contributions from Portugal and Singapore to the aviation cybersecurity programme, which allowed the development and delivery during the triennium of a series of five regional aviation cybersecurity seminars.

2.8.2 The seminars gathered participants from all aviation and non-aviation relevant disciplines (aviation safety, aviation security, air navigation, cybersecurity, national CERTs/CSIRTS, national cybersecurity authorities, law enforcement, military, etc.). Overall, the seminars were attended by more than 450 participants.

2.8.3 In addition to the table-top exercises (TTX) delivered as part of the regional aviation cybersecurity seminars, ICAO conducted a TTX on the side of the Fourth Meeting of the Cybersecurity Panel (CYSECP/4) on 5 June 2025, during its Security Week in 2023 as well as four stand-alone TTX's, bringing the overall number of international TTX's conducted by ICAO during the triennium to ten aviation cybersecurity exercises.

3. **Revision of Assembly Resolution A41-19**

3.1 Following the adoption of the Muscat Declaration and considering the outcomes of the 14th Air Navigation Conference, the proposed updates to Assembly Resolution A41-19 can be found in the attached Appendix. The updated Resolution was coordinated with the ICAO Cybersecurity Panel to align it with the content of the Declaration and the outcomes of the Conference in relation to aviation cybersecurity, as well as with the definitions of aviation cybersecurity terms endorsed by the Third Meeting of the Cybersecurity Panel, and with the evolution of ICAO's work on the topic.

— — — — — — — —

APPENDIX

Resolution ~~A41-19~~ A42-XX: Addressing Cybersecurity in Civil Aviation

Whereas the global aviation system is a highly complex and ~~integrated~~ interconnected one ~~system~~ that comprises data, information and systems which are ~~information and communications technology~~ critical for the safety, ~~and~~ security, efficiency and capacity of civil aviation operations;

Noting that the aviation sector is increasingly reliant on the availability~~,~~ and integrity ~~and confidentiality~~ of data, information, ~~data,~~ and systems, and in certain circumstances, their confidentiality;

Recognizing that aviation cybersecurity is critical for the sustainable and efficient development of air transport and therefore should be prioritized and appropriately resourced;

~~*Recognizing* that not all cybersecurity events cyber incidents affecting the safety, security, efficiency or capacity of civil aviation are unlawful and/or intentionally targeting civil aviation;~~

Mindful that cyber threats to civil aviation are ~~rapidly and~~ continuously evolving and growing in scale, sophistication and frequency, that aviation continues to be a target for malicious actors ~~perpetrators~~ in both the cyber ~~domain as in the~~ and physical domains ~~one~~, and that cyber threats ~~can affect~~ could pose significant risks to ~~critical~~ civil aviation's critical infrastructure, potentially jeopardizing aviation ~~systems worldwide~~ safety, security, efficiency or capacity;

Recognizing the multi-faceted and multi-disciplinary nature of cybersecurity challenges and solutions and noting that cyber risks can simultaneously affect, and spread through, a wide range of aviation areas ~~and spread rapidly~~;

Recognizing that not all ~~cybersecurity events~~ cyber incidents affecting the safety, security, efficiency or capacity of civil aviation are unlawful ~~and/~~or intentionally targeting civil aviation;

Reaffirming the obligations under the *Convention on International Civil Aviation* (Chicago Convention) to ensure the safety, security and continuity of civil aviation;

Considering that the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention) and Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing Protocol) would enhance the global legal framework for criminalizing ~~dealing with~~ cyber-attacks on international civil aviation ~~as crimes~~ and therefore wide ratification and implementation ~~by States~~ of those instruments by Member States would ensure that such attacks would be deterred and punished wherever ~~in the world~~ they occur;

Reaffirming the importance and urgency of ~~addressing~~ enhancing the ~~cybersecurity and cyber~~ protection and resilience of civil aviation's critical ~~systems, data, and information against~~ data, information and systems to cyber threats and risks ~~hazards~~, including common interfaces between civil ~~and military~~ aviation and other connected sectors;

Considering the need to work collaboratively towards the development of an effective and coordinated global ~~framework to address~~ aviation cybersecurity framework ~~and~~ to address ~~support the cybersecurity and cyber resilience of the global aviation system to~~ the protection and resilience of the sector to cyber threats and risks in a harmonized and consistent manner ~~that may jeopardize the safety and/or security of civil aviation~~;

Recognizing ICAO's leadership and work in ~~the fields of~~ aviation cybersecurity ~~and cyber resilience~~ across ~~the different~~ aviation disciplines;

Recognizing that aviation cybersecurity needs to be harmonized at the global, regional and national levels in order to support ~~ensure~~ the consistency and ~~full~~ interoperability of protection and resilience measures and processes ~~risk management systems~~;

Recognizing the importance for States ~~of~~ to develop~~ing~~ and implement clear and comprehensive aviation cybersecurity plans, that address ~~national governance and accountability~~ laws, regulations, policies, procedures and measures for civil aviation cybersecurity, including the designation of a competent national authority responsible for aviation cybersecurity in coordination with concerned national authorities and agencies; ~~and~~

Acknowledging the value of relevant provisions, guidance material and initiatives~~, action plans, publications and other media~~ designed to address cybersecurity issues in a collaborative and holistic manner~~.~~; and

Considering the outcomes of the 14th Air Navigation Conference held in Montréal from 26 August to 6 September 2024, as well as the provisions of the Muscat Declaration on Aviation Security and Aviation Cybersecurity which was adopted in Muscat – Oman on 11 December 2024.

The Assembly:

1. *Urges* Member States to ~~adopt and~~ ratify and implement the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing Convention) of 2010 and Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing Protocol) of 2010 as a means for dealing with cyber-attacks against civil aviation;

2. *Calls upon* States and industry stakeholders to take the following actions to address cyber threats to civil aviation:

a) implement the ICAO Aviation Cybersecurity Strategy, and make use of the ICAO Cybersecurity Action Plan as a tool to support its ~~the~~ implementation;

b) develop and implement national aviation cybersecurity plans that address strategic aviation cybersecurity objectives, governance and responsibilities, policies, communications, cyber risk management, incident response and recovery, capacity building and training, regulatory compliance and audits, monitoring and continuous improvement, documentation and record keeping, with the objective to address cyber threats and risks to civil aviation in a holistic manner across all aviation disciplines;

c) develop and implement processes and tools that support the implementation and monitoring of aviation cybersecurity plans;

d) ~~b)~~ designate the authority competent for aviation cybersecurity as part of the national aviation cybersecurity plan, and define the interaction between that authority and concerned national aviation and non-aviation agencies;

e) ~~c)~~ define the responsibilities of national agencies and industry stakeholders with regard to cybersecurity in civil aviation;

f) secure sufficient resources to ensure the availability and continuous training of qualified and competent aviation and cybersecurity professionals who would be able to regulate, operate, manage, maintain, and oversee the effective implementation of relevant aviation cybersecurity laws, regulations, policies, procedures and measures;

g) ~~d)~~ develop and implement a robust cyber~~security~~ risk management framework that integrates cyber risk management into ~~draws on~~ relevant safety, ~~and~~ security, efficiency and capacity risk management practices, and adopt a risk-based approach to enhance the protection and resilience of critical civil aviation data, information and systems~~, information, and data from~~ to cyber threats and risks;

h) ~~e)~~ establish laws, regulations, policies, procedures and measures ~~instruments~~, as appropriate, and allocate adequate resources to ensure that, for critical aviation systems: system architectures are secure by design; systems are protected and resilient; data is secured and available in storage and while in use or in transfer; system monitoring, and cyber incident detection and reporting, methods are implemented; cyber incident response and recovery plans are developed and practiced in coordination with established emergency response and crisis management plans; and forensic analysis of cyber incidents is carried out;

i) ~~design and implement a robust~~ develop and implement practical actions to enhance cybersecurity culture across all civil aviation entities ~~across the civil aviation sector~~;

~~f) encourage government/industry coordination with regard to aviation cybersecurity strategies, policies, and plans, as well as sharing of information to help identify critical vulnerabilities that need to be addressed;~~

j) ~~h)~~ develop and participate in government/government and government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, vulnerabilities, indicators of compromise, trends, ~~and~~ mitigations, best practices and lessons learned ~~efforts~~;

k) ~~g) encourage~~ develop ~~civil/military~~ cooperation mechanisms with relevant national entities, including but not limited to military, law enforcement and cybersecurity authorities, with regard to identifying, protecting, and monitoring common vulnerabilities and ~~data~~ information flows ~~at interfaces between civil and military~~ that may affect civil aviation systems, and collaborate in the mitigation of, and preparedness for ~~response to~~, common cyber threats, and in response and recovery from cyber incidents;

~~a. encourage States to continue contributing to ICAO in the development of international Standards, strategies, guidance and best practices to support advancing aviation cybersecurity and cyber resilience; and~~

l) ~~k)~~ continue collaborating and contributing to ICAO in the development of ICAO's aviation cybersecurity framework according to a horizontal, cross-cutting and functional approach

involving ~~aviation safety, aviation security, facilitation, air navigation, communication, surveillance, air traffic management, aircraft operations, airworthiness, and other~~ all relevant aviation disciplines, in order to holistically address cyber threats and risks to aviation safety, security, efficiency and capacity.

3. *Instructs* ICAO to:

a) continue to promote the universal ~~adoption and~~ ratification of the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention) of 2010 and *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* (Beijing Protocol) of 2010; and

b) continue to ensure that aviation cybersecurity ~~and cyber resilience~~ matters are considered and coordinated in a cross-cutting and holistic manner through collaboration between all relevant ICAO bodies ~~the new mechanism in ICAO to address aviation cybersecurity~~.

— END —