International Civil Aviation Organization

A41-WP/22
EX/10
7/7/22

WORKING PAPER

ASSEMBLY — 41ST SESSION

EXECUTIVE COMMITTEE

Agenda Item 14: Aviation Security — Policy

CYBERSECURITY IN CIVIL AVIATION

(Presented by the Council of ICAO)

EXECUTIVE SUMMARY

The civil aviation sector's awareness of the importance of addressing cyber threats to civil aviation has been steadily increasing over the years, despite some challenges mainly attributed, directly and indirectly, to the COVID-19 pandemic crisis. Although many developments have been taking place on the national, regional, and global levels, 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 a review of activities related to aviation cybersecurity, including those mandated by the Assembly, and proposes an update to Resolution A40-10 on *Addressing Cybersecurity in Civil Aviation* to emphasize the importance of improving the cybersecurity and cyber resilience of the civil aviation sector.

Action: The Assembly is invited to:
a) note the developments in aviation cybersecurity activities; and
b) adopt the revised Assembly Resolution on *Addressing Cybersecurity in Civil Aviation*, presented in the Appendix, to supersede Assembly Resolution A40-10.

Strategic Objectives:	This working paper relates to the following Strategic Objectives: *Air Navigation Capacity and Efficiency*, *Safety,* and *Security and Facilitation.*
Financial implications:	The ICAO activities referred to in this paper are expected to be undertaken within the resources available in the 2023-2025 Regular Budget and/or from extra-budgetary contributions as guided by the ICAO Business Plan 2023-2025.
References:	Doc 10140, *Assembly Resolutions in Force* (as of 4 October 2019) Doc 10118, *Global Aviation Security Plan* Doc 9750, *Global Air Navigation Plan* *Aviation Cybersecurity Strategy* *Cybersecurity Action Plan*

1. INTRODUCTION

1.1 The 39th Session of the ICAO Assembly instructed ICAO to ensure that cyber threats to civil aviation are 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.

1.2 The 40th Session of the ICAO Assembly reaffirmed the importance and urgency of global commitment for action by all stakeholders to collaboratively address cybersecurity in civil aviation, and adopted the Aviation Cybersecurity Strategy. It also called on ICAO to develop an Action Plan to support the implementation of the Aviation Cybersecurity Strategy, and to continue to ensure that cybersecurity matters are considered and coordinated in a cross-cutting manner. Moreover, it noted some gaps in the structure addressing cybersecurity in ICAO and discussed a set of criteria which could underpin a revised cybersecurity structure.

1.3 It is worth noting that the COVID-19 pandemic affected the progress of ICAO's work on aviation cybersecurity due to resources being redirected to support critical tasks in managing the crisis and in supporting the restart and recovery of civil aviation, as well as financial constraints faced by the Organization during the first eight months of 2020, resulting in the loss of cybersecurity resources.

2. DISCUSSION

2.1 Cybersecurity Action Plan

2.1.1 In line with the Assembly Resolution A40-10, ICAO developed and published in November 2020 the Cybersecurity Action Plan (CyAP) to support States and stakeholders in implementing the Aviation Cybersecurity Strategy. The CyAP provides the foundation for ICAO, States and stakeholders to work together, and proposes a series of principles, measures, and actions to achieve the objectives of the Cybersecurity Strategy's seven pillars (International cooperation; Governance; Effective legislation and regulations; Cybersecurity policy; Information sharing; Incident management and emergency planning; Capacity building, training and cybersecurity culture).

2.1.2 Taking into account the changing priorities of Member States due to the ongoing COVID-19 pandemic, and the experience of States and stakeholders in implementing aviation cybersecurity initiatives in their States and organizations, ICAO conducted a revision of the CyAP and published the second edition of the document in January 2022. The review included streamlining the document to be more concise and clearer and the action items were clarified in terms of actions, indicators, and initiation time.

2.2 Strengthening the Mechanism to Address Cybersecurity in ICAO

2.2.1 The 40th Session of the ICAO Assembly 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, and discussed a set of criteria which could underpin a revised cybersecurity governance structure.

2.2.2 The Council, during its 218th Session, endorsed the methodology for the development of the Feasibility Study and Gap Analysis on the Mechanism to Address Cybersecurity. The first two phases of the study were presented during the 219th Session. The Council requested the Secretariat to further consider and update the feasibility study, and delegated authority to the President of the Council to consider the establishment of a small working group composed of Council Representatives and Air Navigation Commission (ANC) Members to develop Phase 3 of the feasibility study with the assistance of the Secretariat. The Small Working Group met extensively between November 2020 and January 2021,

considered several governance options and recommended a solution which was approved by the Council during its 222th Session. The new governance structure for cybersecurity in ICAO includes:

a) evolving the Secretariat Study Group on Cybersecurity to become a Cybersecurity Panel reporting to the Aviation Security Committee of the ICAO Council;

b) evolving the Trust Framework Study Group to be integrated within the ANC Panel structure; and

c) establishing an Ad-Hoc Cybersecurity Coordination Committee (AHCCC) under the Council. The Committee membership comprises one member from each of the Air Transport Committee, Aviation Security Committee, Air Navigation Commission, and every ICAO Panel and expert group addressing elements of cybersecurity in their work programme. The Committee is expected to offer the Council, and everyone involved in cybersecurity-related activities in ICAO, a single focal point for all ICAO cybersecurity-related activities, hence enhancing the accountability, transparency, efficiency, and coordination of ICAO's work on aviation cybersecurity and cyber resilience. The Council, during its 224th Session, approved the Terms of Reference of the AHCCC.

2.2.3 Following the Council's decision on the new governance structure, the Cybersecurity Panel was established during the 225th Session and held its first meeting in May 2022. The ANC, during its 219th Session, approved the evolution of the Trust Framework Study Group into a new ANC Panel to continue the work on the International Aviation Trust Framework.

2.3 Development of an International Aviation Trust Framework

2.3.1 Since its 223rd Session, the Council has discussed the development of an International Aviation Trust Framework. It will continue to progress this work, including the concept of operations and the governance of such framework.

2.4 Adequacy of international air law instruments to address cyber-attacks on civil aviation

2.4.1 The Aviation Cybersecurity Strategy calls for the analysis of the relevant international legal instruments, in order to identify existing or missing key legal provisions for the prevention, prosecution, and timely reaction to cyber incidents. This task was accordingly reflected in the Cybersecurity Action Plan as an action item for ICAO. As such, the SSGC established the Research Sub-Group on Legal Aspects (RSGLEG). The Sub-Group comprised of legal and cybersecurity experts to ensure that all expertise required to address its objectives are available. As agreed by the RSGLEG at its last meeting in January 2022, the Secretariat reported on the work conducted by the Sub-Group to the 38th Session of the Legal Committee which was held in March 2022.

2.5 Guidance Material

2.5.1 In line with the Cybersecurity Action Plan, ICAO developed guidance material to support States and stakeholders to address cybersecurity in civil aviation which includes the following (published on ICAO-NET under "Publications" and "Others"):

a) Guidance on Traffic Light Protocol (TLP), which provides States and stakeholders with guidance on using TLP in order to facilitate cybersecurity information sharing;

b) Cybersecurity Policy Guidance, which addresses the protection and resilience of international civil aviation's critical infrastructure against cyber threats, and the multilateral cooperation requirement within civil aviation as well as with external

authorities. The guidance also addresses the need to designate the authority competent for aviation cybersecurity, and includes a template to support States and stakeholders to develop a Cybersecurity Policy; and

c) Cybersecurity Culture in Civil Aviation, which supports the design and implementation of a robust cybersecurity culture, building on civil aviation's success in implementing safety and security cultures.

2.6 Capacity Building

2.6.1 In 2020, ICAO developed a Cybersecurity Training Roadmap to support the Organization's efforts to build the capability to deliver appropriate, coherent and relevant aviation cybersecurity training to States and stakeholders. The Cybersecurity Training Roadmap supports the Aviation Cybersecurity Strategy and the Cybersecurity Action Plan. Its development also supports Assembly Resolution A40-25: *Implementing Aviation Training and Capacity Building Strategies*, which lays out how ICAO, through training activities, shall assist and support States with the development of sufficient human resources and capacity. Following the Training Roadmap, ICAO began building a cybersecurity training portfolio which includes to-date the following courses:

2.6.1.1 Foundations of Aviation Cybersecurity Leadership and Technical Management: The course was developed 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.

2.6.1.2 Managing Security Risk in Air Traffic Management (ATM): The course was developed in partnership with EUROCONTROL. It covers ATM security including both physical and cybersecurity elements. The first session of the course will be delivered in November 2022.

2.6.1.3 Cybersecurity Oversight in Civil Aviation: The course is being developed in partnership with the United Kingdom's Civil Aviation Authority. It will cover key aspects that would support States in designing and implementing their oversight obligations for aviation cybersecurity.

2.7 Raising Awareness and Outreach Activities

2.7.1 Raising awareness of States and stakeholders to the importance of addressing cybersecurity in civil aviation has been a core activity of ICAO. The Organization continues to be heavily involved in the organization, and/or participation in, national, regional, and international conferences, meetings, and webinars in order to promote cooperation between all stakeholders in the cybersecurity and cyber resilience field, as well as promote the implementation of the Aviation Cybersecurity Strategy and the Cybersecurity Action Plan.

2.8 Audit of Cybersecurity Obligations under the (USAP-CMA)

2.8.1 The objective of the Universal Security Audit Programme – Continuous Monitoring Approach (USAP-CMA) is to improve global aviation security through auditing and continuous monitoring of the aviation security performance of Member States. Auditors identify the documentation in which the requirement is established for operators or entities to identify their critical information and communications technology systems and data used for civil aviation purposes. They also ensure this requirement covers the assessment, development and implementation of measures to protect such information and systems from unlawful interference. Once the requirement is identified, auditors ensure that responsibilities for cybersecurity measures are clearly allocated.

2.8.2 Of the 136 States audited as at 31 December 2021, documentation-related aspects of cybersecurity preparedness were audited in 54 States. The audit results from these States indicate the following:

a) fifteen per cent of States had not established a requirement for operators or entities to identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference;

b) twenty-six per cent of States had not defined the responsibilities of operators or entities with regard to cybersecurity in civil aviation; and

c) forty-one per cent of States had not developed criteria for the protection of critical information and communications technology systems and data used for civil aviation purposes from unlawful interference.

2.8.3 These results are not necessarily indicative of the global picture in relation to safeguarding aviation against cyber threats, as some States were audited remotely due to the pandemic and their results are incomplete. Moreover, the overall sample size is not representative enough to provide a high degree of confidence. However, these results clearly show that the civil aviation sector needs to enhance its efforts to address cyber threats to a baseline that allows for a consistent and harmonized protection against, mitigation of, and response to, cyber threats to civil aviation.

— — — — — — — —

APPENDIX

DRAFT ASSEMBLY RESOLUTION
ADDRESSING CYBERSECURITY IN CIVIL AVIATION

~~A40-10~~ A41-xx: Addressing Cybersecurity in Civil Aviation

Whereas the global aviation system is a highly complex and integrated system that comprises ~~information and communications technology~~ systems that are critical for the safety and security of civil aviation operations;

Noting that the aviation sector is increasingly reliant on the availability, integrity and confidentiality of information, data, and ~~communications technology~~ systems~~, as well as on the integrity and confidentiality of data~~;

Mindful that ~~the threat posed by~~ cyber ~~incidents on~~threats to civil aviation ~~is~~ are rapidly and continuously evolving, that ~~threat actors are focused on malicious intent, disruption of business continuity and theft of information for political, financial or other motivations~~ aviation continues to be a target for perpetrators in the cyber domain as in the physical one, and that ~~the~~ cyber threats can ~~easily~~ evolve to affect critical civil aviation systems worldwide;

Recognizing that not all cybersecurity ~~issues~~ events affecting the safety of civil aviation are unlawful and/or intentional~~, and should therefore be addressed through the application of safety management systems~~;

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

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 dealing with cyber-attacks on international civil aviation as crimes and therefore wide ratification by States of those instruments would ensure that such attacks would be deterred and punished wherever in the world they occur;

Reaffirming the importance and urgency of ~~protecting~~ addressing the cybersecurity and cyber resilience of civil aviation's critical ~~infrastructure~~ systems, ~~and~~ data, and information against cyber threats and hazards, including common interfaces between civil and military aviation;

Considering the need to work collaboratively towards the development of an effective and coordinated global framework ~~for civil aviation stakeholders to address the challenges of~~ to address aviation cybersecurity~~, along with short-term actions~~ and to ~~increase~~ support the cybersecurity and cyber resilience of the global aviation system to cyber threats that may jeopardize the safety and/or security of civil aviation;

Recognizing ~~the~~ ICAO's leadership and work in the fields of ~~the Secretariat Study Group on Cybersecurity~~ aviation cybersecurity and cyber resilience~~, which greatly contributed to the format of the Cybersecurity~~

~~Strategy by linking safety and security characteristics of cybersecurity~~ across the different aviation disciplines;

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

Recognizing the importance of developing clear national governance and accountability 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 initiatives, action plans, publications and other media designed to address cybersecurity issues in a collaborative and ~~comprehensive~~ holistic manner.

The Assembly:

1. *Urges* Member States ~~and ICAO to promote the universal adoption and implementation of~~ to adopt and ratify 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) as a means for dealing with cyberattacks against civil aviation;

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

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

b) designate the authority competent for aviation cybersecurity, and define the interaction between that authority and concerned national agencies;

~~c) Identify the threats and risks from possible cyber incidents on civil aviation operations and critical systems, and the serious consequences that can arise from such incidents;~~

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

d) 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;

~~j~~e) ~~E~~establish policies and instruments, and allocate resources ~~when needed~~ 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 transfer ~~methods for data transfer are secured, ensuring integrity and confidentiality of data~~; system monitoring, and incident detection and reporting, methods are implemented; incident recovery plans are developed and practiced; and forensic analysis of cyber incidents is carried out; ~~and~~

~~d) Encourage the development of a common understanding among Member States of cyber threats and risks, and of common criteria to determine the criticality of the assets and systems that need to be protected;~~

~~e~~f) ~~E~~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;

g) encourage civil/military cooperation with regard to identifying, protecting, and monitoring common vulnerabilities and data flows at interfaces between civil and military aviation systems, and collaborate in response to common cyber threats and recovery from cyber incidents;

~~f~~h) ~~D~~develop and participate in government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts;

~~g) Based on a common understanding of cyber threats and risks, adopt a flexible, risk-based approach to protecting critical aviation systems through the implementation of cybersecurity management systems;~~

~~h~~i) ~~Encourage~~ design and implement a robust ~~all-round~~ cybersecurity culture ~~within national agencies and~~ across the civil aviation sector;

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

~~i) Promote the development and implementation of international standards, strategies and best practices on the protection of critical information and communications technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation;~~

k) ~~Collaborate~~ continue collaborating in the development of ICAO's 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, ~~and~~ airworthiness, and other relevant disciplines.

3. *Instructs* ~~the Secretary General~~ 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) and Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing Protocol); and

~~a) develop an action plan to support States and industry in the adoption of the Cybersecurity Strategy; and~~

b) continue to ensure that cybersecurity and cyber resilience matters are considered and coordinated in a cross-cutting manner through the ~~appropriate mechanisms in the spirit of the Strategy~~ new mechanism in ICAO to address aviation cybersecurity.

— END —