International Civil Aviation Organization

AN-Conf/14-WP/14
11/4/24

WORKING PAPER

FOURTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 26 August to 6 September 2024

Agenda Item 4: Hyper-connectivity of air navigation system
4.2: Cybersecurity and information system resilience

IMPLEMENTATION OF CORE ELEMENTS OF AN AVIATION CYBERSECURITY FRAMEWORK

(Presented by the Secretariat)

EXECUTIVE SUMMARY

The digital transformation of the civil aviation sector across all aviation domains is accelerating the need to address cybersecurity in civil aviation to ensure the safety, security, capacity and efficiency of the sector. This paper presents a number of high-level core elements that should be considered by States and stakeholders to address aviation cybersecurity in a holistic and harmonized manner across all relevant domains. It also identifies the need for additional ICAO guidance to support States and stakeholders to enhance the protection and resilience of the sector to cyber threats and risks. It further provides recommendations that allow further harmonization and consistency at the regional level.

Action: The Conference is invited to agree to Recommendation 4.2/x — Aviation cybersecurity in paragraph 3.

Strategic Objectives:	This working paper relates to the Safety, Air Navigation Capacity and Efficiency, and Security and Facilitation Strategic Objectives
Financial implications:	*Impact for the aviation community:* There will be costs involved in implementing the areas addressed by this paper. However, this implementation will provide the opportunity for a clear approach to aviation cybersecurity with well-defined roles and responsibilities for all stakeholders involved. *Impact for ICAO (relative to the current Regular Programme Budget resource levels):* The ICAO activities referred to in this working paper will continue over the next triennia. Additional resources will be required to support the development of these activities as well as conducting awareness campaigns and providing implementation support.
References:	Doc 8973, *Aviation Security Manual (Restricted)* Doc 9750, *Global Air Navigation Plan* Doc 10004, *Global Aviation Safety Plan* Doc 10118, *Global Aviation Security Plan* Doc 10184, *Assembly Resolutions in Force (as of 7 October 2022)* ICAO Aviation Cybersecurity Strategy

	Cybersecurity Action Plan Cybersecurity Policy Guidance Cybersecurity Culture in Civil Aviation

1. INTRODUCTION

1.1 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, through adoption of resolution A40-10: *Addressing Cybersecurity in Civil Aviation* and endorsement of the ICAO Aviation Cybersecurity Strategy[1]. The 41st Session of the ICAO Assembly reiterated the importance to address cybersecurity in civil aviation through the updated resolution A41-19.

1.2 The Assembly also called on ICAO to develop an Action Plan to support States' and stakeholders' implementation of the Aviation Cybersecurity Strategy. The second edition of the Cybersecurity Action Plan[2], published in January 2022, 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[3].

1.3 In line with the Cybersecurity Action Plan, ICAO already published guidance material on topics related to aviation cybersecurity. ICAO's work also included initiatives related to research into the adequacy of international legal instruments to address cyber-attacks against civil aviation, research into the need for aviation cybersecurity Standards and Recommended Practices in the Annexes to the Convention on International Civil Aviation (Chicago Convention), development of materials to facilitate interoperable trust in different aviation domains, raising awareness on the importance of addressing cyber threats and risks to civil aviation, development of aviation cybersecurity capacity building initiatives and conducting international aviation cybersecurity table-top exercises.

2. DISCUSSION

2.1 As the civil aviation sector continues to benefit from technological innovations to enhance its capacity and efficiency, while maintaining agreed levels of safety and security, cybersecurity has been considered in each aviation domain separately. Over the years, this has led to aviation becoming a System of Systems (SoS) where controls and processes for cyber protection and resilience were not designed, nor implemented, holistically, leading to potential gaps on the macro-level.

2.2 In that regard, it is important that aviation cybersecurity is integrated in civil aviation domains at the national, regional and international levels in a coordinated, harmonized and holistic manner. This would support addressing cyber threats and risks to civil aviation, without potentially jeopardizing safety, security, capacity and efficiency requirements.

2.3 Significant progress has been made to address cybersecurity in civil aviation, but there is a need for additional guidance to support States' integration of aviation cybersecurity into their existing

[1] https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx
[2] https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx
[3] The pillars of the ICAO Aviation Cybersecurity Strategy are: International Cooperation, Governance, Effective Legislation and Regulations, Cybersecurity Policy, Information Sharing, Incident Management and Emergency Planning, and Capacity Building, Training and Cybersecurity Culture.

regulatory and oversight systems, as well as in their regional and national plans related to the relevant civil aviation domains, primarily aviation safety, aviation security and facilitation, and air navigation.

2.4 Moreover, both the United Nations Security Council Resolution 2341 (2017) on protection of critical infrastructure against terrorist acts, and the UN General Assembly Resolution (A/RES/77/298) on the eighth review of the United Nations Global Counter-Terrorism Strategy (A/RES/60/288), stress the importance of a multi-stakeholder, cross domain cooperation in addressing cybersecurity, among international, regional and subregional organizations, the private sector and civil society.

2.5 As such, and in line with the ICAO Assembly Resolutions in force, the Aviation Cybersecurity Strategy, its Action Plan, and the various guidance materials developed by ICAO, this paper proposes baseline core elements that should be considered by States and stakeholders to address cyber threats and risks to civil aviation. These core elements should include:

a) State-level regulatory aspects:

1) **Aviation cybersecurity governance on the State level**: This element includes, but is not limited to, aspects related to identifying a competent authority for aviation cybersecurity, integrating aviation cybersecurity in States' safety programmes and national civil aviation security programmes, identifying the roles and responsibilities of aviation and non-aviation authorities (e.g. national cybersecurity authorities) and coordinating their activities in relation to regulation and oversight of cybersecurity in civil aviation, leveraging national cybersecurity resources to support organizations in monitoring, detecting, responding to, and recovering from cyber incidents.

2) **National legal framework**: This element includes aspects related to States' national legal frameworks to allow for prosecution of cyber-attacks against civil aviation. It also includes aspects related to the ratification of the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing, 2010) and *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* (Beijing, 2010) as means for dealing with cyber-attacks against civil aviation globally.

3) **Aviation cybersecurity policy**: This element includes aspects related to State-level aviation cybersecurity policy.

4) **Oversight functions**: This element includes aspects related to States' oversight capabilities in aviation cybersecurity, which can be implemented through the existing aviation safety and aviation security oversight mechanisms in a coordinated manner.

b) State and stakeholders' aspects:

1) **Cyber risk management**: This element includes aspects related to identifying aviation critical infrastructure and integrating cyber risk assessment into existing safety and security risk assessments of that infrastructure.

2) **Cyber incident reporting**: This element includes aspects related to implementing a cyber incident reporting mechanism from entities to their authorities, which can be done separately or through existing reporting mechanisms for aviation safety or security.

3) **Cyber information sharing**: This element includes aspects related to the implementation of information sharing mechanisms among States and stakeholders on the national, regional and international levels.

4) **Cyber incident response and recovery**: This element includes aspects related to the implementation of cyber incident response and recovery plans and capabilities. It also includes aspects related to integrating those plans with aviation emergency response/crisis management plans.

5) **Cyber supply chain management**: This element includes aspects related to managing cyber risks from the aviation and non-aviation supply chains. This includes several types of supply chain, e.g. aviation-certified equipment/systems, aviation system services (e.g. flight planning systems, airport networks), non-aviation service providers (e.g. cloud service providers, satellite communication providers).

6) **Cybersecurity culture**: This element includes aspects related to the implementation of a robust cybersecurity culture in civil aviation, that leverages the experience of the sector in implementing safety and security cultures.

7) **Aviation cybersecurity training programmes**: This element includes aspects related to the development and deployment of aviation cybersecurity training programmes that address the different types of audiences (e.g. general awareness versus role-based training).

2.6 Given that the aviation sector is identified as a national critical infrastructure in many States, a progressive and multi-layered approach to address the cybersecurity protection and resilience of the sector is necessary. The objective is to implement a defense in depth strategy[4] that includes all stakeholders either directly or indirectly involved in addressing cyber threats and risks to civil aviation. The elements outlined above are not the full list of areas that should be addressed in the scope of aviation cybersecurity; however, they provide a foundation that allows for the robust and effective management of aviation cybersecurity, including the protection and resilience of aviation assets managed by States and stakeholders.

2.7 Cybersecurity groups are being established in ICAO Regions to support regional discussions of cyber protection and resilience in the different aviation domains. Those activities are very relevant to address specific areas related to each region in relation to cyber threats and risks, however, there is a potential risk of duplication and even conflict if those activities are not coordinated across the different regional groups and plans. Such coordination will allow for a holistic, harmonized and coordinated approach to addressing cyber threats and risks in the different regions, and will ensure consistency and complementarity in regional plans for air navigation, safety, and security and facilitation with regard to aviation cybersecurity, which will further positively impact Member States' planning and implementation activities at the national levels. States may also utilize those forums to report back to ICAO on the challenges they are facing to address cybersecurity in civil aviation, which would inform ICAO's activities related to the development of provisions and guidance material.

[4] Defense in depth, is the application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. The methodology involves layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another (ISO/IEC 62443 1-1 refers).

3. CONCLUSION

3.1 The digital transformation of the civil aviation sector across all aviation domains highlights the need to address cybersecurity in civil aviation to ensure the safety, security, capacity and efficiency of the sector. While recognizing the challenges associated with aviation cybersecurity, baseline core elements need to be considered by States and stakeholders on the regulatory and operational levels.

3.2 In light of the above, the Conference is invited to agree to the following recommendation:

Recommendation 4.2/x — Aviation cybersecurity

That States:

a) develop and implement a national plan to address cyber threats and risks to civil aviation in a holistic manner across all aviation domains, and in coordination with relevant non-aviation stakeholders using the core elements as a reference;

b) align aviation cybersecurity activities in the regional air navigation, safety, and security and facilitation plans through the coordination processes of the Planning and Implementation Regional Groups (PIRGs), Regional Aviation Safety Groups (RASGs) and Regional Aviation Security and Facilitation (AVSEC/FAL) Groups;

c) report to ICAO their experience in implementing ICAO provisions and guidance material related to aviation cybersecurity, through the appropriate expert groups or through the processes of the PIRGs, RASGs and Regional AVSEC/FAL Groups; and

that ICAO:

d) provide guidance on the core elements to support States and stakeholders in addressing aviation cybersecurity, and integrate all aviation cybersecurity activities holistically in a consistent and coordinated manner.

— END —