International Civil Aviation Organization

A40-WP/219[1]
EX/82
5/8/19

WORKING PAPER

ASSEMBLY — 40TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 12: Aviation Security - Policy

PROPOSAL REGARDING ICAO GOVERNANCE STRUCTURE FOR CYBERSECURITY

(Presented by the International Coordinating Council of Aerospace Industries Associations (ICCAIA))

EXECUTIVE SUMMARY

Civil aviation cybersecurity is a broad, complex and multi-disciplinary field which encompasses aspects of information technology, traditional aviation security, safety management and impacts to aviation operations. Because cybersecurity is transversal, ICAO's current panels and study groups are not effective at coordinating activities like cybersecurity. There is a need to establish an ICAO entity, governed by member States with the support from industry, which is not constrained by the existing ICAO organizational structure. This entity should have the ability to ensure that all cybersecurity activities are effectively coordinated across ICAO and that interfaces of cybersecurity with other disciplines are appropriately managed. This entity should be responsible for a common ICAO strategy for cybersecurity and to align and orientate work being performed by existing panels and study groups.

Action: The Assembly is invited to:

a) request the Council establish a civil aviation cybersecurity entity, governed by member States with the support from industry, that can work transversally to consolidate and harmonize cybersecurity related activities across ICAO;
b) request the Council to approve the cybersecurity strategy developed by the SSGC, while recognizing that the SSGC was not structured to address the horizontal and crosscutting nature of cybersecurity;
c) instruct the Secretary general to coordinate with States and industry to harmonize the cybersecurity risk management processes, taking into account the harmonization work already done at regional or national levels; and
d) request the Council to urge States of various regions to develop cybersecurity crisis management capacities and to coordinate at the international level to prevent the loss of passengers trust due to a local aviation cybersecurity incident.

Strategic Objectives:	This working paper relates to Strategic Objectives: Safety; Air Navigation Capacity and Efficiency; Security and Facilitation
Financial implications:	The activities referred to in this paper will be subject to the resources available in the 2020-2022 Regular Programme Budget and/or from extra budgetary contributions.
References:	Doc 10075, Assembly Resolutions in Force (as of 6 October 2016)

[1] English, Arabic, Chinese, French, Russian and Spanish versions provided by ICCAIA.

1. INTRODUCTION

1.1 Civil aviation cybersecurity is a broad, complex and multi-disciplinary field which encompasses aspects of information technology management, traditional aviation security, safety management and impacts to aviation operations.

1.2 Cybersecurity activities have typically been initiated on a case by case and local basis and there is now a need for re-enforced overall coordination to ensure that all aspects are considered without any gaps and overlaps. Furthermore, given the fact that cybersecurity intersects with many activities within ICAO it is necessary to ensure that proper coordination between all the disciplines is put in place to enforce the definition and operation of an integral design and decision-making process taking into consideration, among other things, aviation safety, aviation physical and cybersecurity.

1.3 Because cybersecurity is transversal, ICAO's current panels and study groups are not effective at coordinating activities like cybersecurity. There is a need to establish an ICAO entity, governed by member States with support from the industry, which is not constrained by the existing ICAO organizational and political structure. This entity should have the ability to ensure that all cybersecurity activities are effectively coordinated across ICAO and that interfaces of cybersecurity with other disciplines are appropriately managed. This entity should be responsible for a common ICAO strategy for cybersecurity and to align and orientate work being performed by existing panels and study groups.

1.4 The intent would be to minimize overhead and impacts to the organization and leverage as much as possible the existing structures to perform the work, and be viewed as an entity for setting the strategy and vision and providing leadership and guidance. It would be made up of both ICAO member States representatives, industry and individual cybersecurity experts that, all together, carry out the work and propose jointly agreed recommendations for decision.

2. DISCUSSION

2.1 A centralized cybersecurity entity has the potential to address some of the issues identified in the introduction as it could help support the need for global aviation cross-domain governance of cybersecurity activities within ICAO. The type of ICAO entity needs to be carefully considered so as to successfully achieve the needs and objectives of the global civil aviation community. The pros and cons of the different organizations (such as a Panel or Council Committee) should be weighed carefully against the needs and objective outlined here.

2.2 This centralized cybersecurity entity, if correctly resourced, could bring:

- a greater range of membership experience and industry expertise specifically on the topic of cybersecurity in civil aviation;
- a harmonized approach to risk management with a set of methodologies agreed by all stakeholders, drawing on regional and national experience;
- the ability to create working groups or allocate work to existing entities with the aim of focussing effort on the development of Standards and Recommended Practices, guidance materials, programmes, capacity building, assistance and training, as required;

- consideration of all cybersecurity issues (Cybersecurity for flight safety, operations, maintenance, cybercrime…) in a single entity; and

- a team of mixed cybersecurity experts, and safety and operations specialists representing all the concerned stakeholders across governments and industry. At a minimum this should include aerodromes, airlines, aircraft manufacturers and suppliers, maintenance operators, and navigation service providers.

2.3 Given the cross-cutting and multi-discipline nature of cybersecurity, the development of extensive coordination with aviation safety and aviation security disciplines through strong links between the Air Navigation Commission, Unlawful Interference Committee, Study Groups and Panels is recommended. Understanding the rapidly evolving nature of cybersecurity and interactions with new technologies, this cybersecurity entity must be able to leverage participation from all global experts, including individuals and organizations beyond the list of current "invited organizations" (https://www.icao.int/about-icao/Pages/Invited-Organizations.aspx).

2.4 Acknowledging that the concepts presented within the cybersecurity strategy developed by the Secretariat Study Group for Cybersecurity (SSGC) are an appropriate baseline to build upon, this cybersecurity entity should be tasked to develop and operate an action plan for all matters related to all cybersecurity civil aviation domains and to maintain the ICAO cybersecurity vision, scope and strategy. The ICAO cybersecurity entity should leverage from the numerous and already engaged cybersecurity initiatives engaged at regional and national levels as a means to accelerate the definition and adoption of standards and guidance. This cybersecurity entity should also, among other things:

2.4.1 Consolidate the SSGC strategy and harmonize the work being performed by groups and panels (i.e. TFSG, AVSEC Panel, etc.) to develop sets of cybersecurity principles, measures and actions contained in a framework built on eight pillars:

- International cooperation
- Governance
- Effective legislation and regulations
- Policies
- Information sharing
- Global risk statement relating to cybersecurity in aviation
- Incident management, and operational impact and continuity
- Capacity building, training and cybersecurity secure culture

2.4.2 Take forward the Working Group on Threat and Risks (WGTR), work on assessing civil aviation cybersecurity risks, possibly as a working group of this new entity or allocated appropriately within the bureaus. There is a strong need to establish guidance and criteria to ensure comparable analysis results when utilized by different member states and organizations.

2.4.3 Work with the Trust Framework Study Group to help develop the work outcomes and after its 2-year period of existence, continue to harmonize and evolve the outcomes and appropriately allocate the continued work within the bureaus or as appropriate.

3. CONCLUSION

3.1 International cooperation and coordination are necessary so as to harmonize policies and regulations to enable worldwide cybersecurity interoperability and continuity in operations. ICAO's current panels and study groups are not effective at coordinating activities like cybersecurity. There is a need to establish an ICAO entity, governed by member States with the support from industry, which is not constrained by the existing ICAO organizational structure. This entity should have the ability to ensure that all cybersecurity activities are effectively coordinated across ICAO and that interfaces of cybersecurity with other disciplines are appropriately managed.

— END —