International Civil Aviation Organization

A40-WP/427
EX/176
2/8/19

WORKING PAPER

ASSEMBLY — 40TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 12: Aviation Security Policy

PROPOSAL FOR ICAO GOVERNANCE OF CYBERSECURITY AND RESILIENCY

(Presented by the United States)

EXECUTIVE SUMMARY

Cybersecurity and resiliency in the aviation ecosystem is a multidisciplinary issue that affects or will affect nearly every aspect of global aviation. Due to the complexities and the reliance on shared digital information and communication, the need for cybersecurity and resiliency becomes more vital with every advancement in technology and the continuous modernization of the aviation ecosystem.

While ICAO, Member States and industry are diligently working to address cybersecurity and resiliency issues, the current approach at ICAO lacks appropriate governance and focuses on individual sectors and varying expertise instead of reflecting the holistic global aviation ecosystem.

To address these issues, the United States recommends that ICAO establish a Council Technical Committee on Cybersecurity and Resiliency to centralize governance and properly address cybersecurity and resiliency in a holistic approach. The Committee will manage policy and integration of industry standards while evaluating potential development of technical Standards and Recommended Practices.

Action: The Assembly is invited to:

a) Request that the ICAO Council establish a new Council Technical Committee on Cybersecurity and Resiliency as proposed in this paper;
b) Urge States to support the proposed ICAO Cybersecurity Strategy developed by the Secretariat Study Group on Cybersecurity; and
c) Urge States to support the work of the Trust Framework Study Group.

Strategic Objectives:	This working paper relates to Strategic Objectives: Security and Facilitation, Air Navigation Capacity and Efficiency
Financial implications:	None
References:	Doc 10075, *Assembly Resolutions in Force*, A39-18 and A39-19 ICAO 13th Air Navigation Conference Recommendation 5.4/1 A40-WP/28 *ICAO Cybersecurity Strategy* Doc 7559/10 *Rules of the Council*, Section III, Rule 17 a)

1. INTRODUCTION

1.1 Cybersecurity and resiliency in the aviation ecosystem is a multidisciplinary issue that affects or will affect nearly every aspect of global aviation. As recognized by the 39th Session of the ICAO Assembly in Resolutions A39-18 and A39-19, the global aviation system is becoming more complex and integrated through information and communication technology. Due to these complexities and reliance on shared digital information and communication, the need for cybersecurity and resiliency becomes more vital with every advancement in technology and the continuous modernization of the aviation ecosystem.

1.2 The importance of cybersecurity and resiliency is further evidenced by Recommendation 5.4/1 resulting from the ICAO 13th Air Navigation Conference, which calls for States and ICAO to, inter alia, work together along with industry to become more aware of threats and undertake cooperative means to mitigate threats. The ICAO Second High-level Conference on Aviation Security also recommended that ICAO develop a comprehensive cybersecurity strategy and undertake a feasibility study for a Cybersecurity Panel.

1.3 While ICAO is making progress in creating the ICAO Cybersecurity Strategy (A40-WP/28 refers), the governance of cybersecurity and resiliency within the Organization is still insufficient. The lack of appropriate governance creates inefficiencies and results in a lack of information sharing, making it impossible to properly address cybersecurity and resiliency in a holistic approach that centrally manages policy, integration of industry standards, and potential development of technical Standards and Recommended Practices (SARPs).

2. DISCUSSION

2.1 The current ICAO governance of cyber-related issues divides activities between the Air Transport Bureau (ATB), which oversees cybersecurity while, and the Air Navigation Bureau (ANB), which oversees cyber resiliency.

2.2 The ATB is responsible for developing SARPs and amending Annex 17 – *Security*. The ATB also supports the work of the Aviation Security Panel and the Committee on Unlawful Interference (UIC), including the formation of the Secretariat Study Group on Cybersecurity (SSGC). The SSGC serves as a focal point for cybersecurity work; reviews such as review of ICAO Annexes to consolidate SARPs related to cybersecurity, and engages in general promotion of information sharing throughout the aviation community.

2.3 The approach of the ATB works well when cybersecurity is considered as a singular topic focused on protecting critical systems from unlawful interference as defined in section 4.9 of Annex 17. However, global aviation is a holistic ecosystem including many interconnecting systems that directly affect operations, which are not included in the remit of the ATB and UIC to address cybersecurity.

2.4 The ANB is responsible for developing and amending SARPs in 17 different Annexes addressing safety and air navigation capacity and efficiency. The ANB also supports the work of the Air Navigation Commission and its technical panels, including the formation of the INNOVA Working Group and the Trust Framework Study Group. The Trust Framework Study Group serves as the focal point for developing cyber resilient network interconnections through a trusted framework to enable global transfer of aviation data and information vital to operations.

2.5 The approach of the ANB works well when only considering operational data and information transfer. However, it does not take into account the security of systems not connected to the operational network, but which may have an impact in other areas affecting safety or efficiency.

2.6 While it is clear that ICAO is addressing both cybersecurity and resiliency, the current governance structure creates a division between security and resiliency that negatively affects the holistic aviation ecosystem. Member States and industry have recognized this problem and have submitted recommendations to establish a new 'Panel' on cyber. However, an ICAO Panel has a specific purpose to advance solutions to specialized problems or to develop SARPs (Doc 7984, *Directives for Panels of the Air Navigation Commission* refers). Cybersecurity and resiliency is more multidisciplinary and comprehensive than a 'specialized problem' and at this time industry based standards for cyber should be used instead of developing new ICAO SARPs or a new ICAO Annex.

2.7 With this in mind, cybersecurity and resiliency should be recognized for the impact to the entire aviation ecosystem and therefore be elevated and centrally managed by the ICAO Council under a Technical Committee established for this purpose.

2.8 In accordance with Section III, Rule 17 a) of Doc 7559/10, *Rules of the Council*, the United States proposes forming a Council Technical Committee on Cybersecurity and Resiliency. Doc 7559/10 states that the Council may establish other Commissions, Committees or Working Groups, either Standing or Temporary. A new Committee of the Council may be devised to deal with problems involving technical, economic, social and legal aspects of international civil aviation, which, for the advancement or resolution thereof, require expertise, which is not available to the Council through other means.

2.9 The proposed Technical Committee will work under the direct control of the Council, which will also develop the proposed Committee's Terms of Reference and membership through the "*Directives for the Committee on Cybersecurity and Resiliency"*. The SSGC and Trust Framework Study Group will reorganize under the new Technical Committee in full consideration of the tasks, efforts, and costs involved to ensure proper management of the new Committee. Through this approach, the proposed Committee will properly utilize subject matter experts from various disciplines, including from within the ICAO working structure, while avoiding inefficiencies and communication challenges produced by distributing complex, inter-related issues among multiple bureaus and offices with varying priorities.

3. CONCLUSION

3.1 Cybersecurity and resiliency greatly affect the entire global aviation ecosystem. The proposed approach discussed in this paper will elevate this critical issue to a Council Technical Committee that can work through multidisciplinary measures and leverage expertise from within multiple ICAO Bureaus and across the aviation community, while maintaining the pace of innovation in the face of ever-increasing threats.

3.2 The Assembly is invited to endorse the actions in the Executive Summary.

— END —