International Civil Aviation Organization

A40-WP/172[1]
EX/70
1/8/19

WORKING PAPER

ASSEMBLY — 40TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 12: Aviation Security — Policy

CYBER-RESILIENCE

(Presented by the Civil Air Navigation Services Organisation (CANSO))

EXECUTIVE SUMMARY

Cyber-security is a critical issue for aviation and becoming more so as various initiatives, such as system wide information management (SWIM), result in systems becoming more interoperable and open. Currently, the examination of what actions ICAO should take to ensure cyber-resilience, is evaluated by the ICAO Secretariat Study Group for Cybersecurity (SSGC). The lead is with the ICAO Air Transport Bureau (ATB) and supported by the ICAO Air Navigation Bureau (ANB).

This results in little governance from States, Air Navigation Commission (ANC) and the ICAO Council. The SSGC is currently comprised of around 50 participants. The process appears to lack speediness, because of the fact that a Secretariat Study Group (SSG) is unable propose SARPs and has no mandate to coordinate the activity of all the panels or working groups related to cyber-security. The SSGC is established to provide advice and the follow-up is left to the consideration of the Secretariat General.

Given the importance of cyber-resilience and the need for quick action, there is a need for a more effective way of addressing the issue. To obtain better governance and accelerate the process for the introduction of guidance material and, if necessary, SARPs, the current SSGC should be upgraded to an ICAO Panel under the ICAO Council. The newly formed "Trust Framework Study Group" should be placed under this new Panel as a WG.

A new Cyber Resilience, Safety and Security Panel (CRSSP) should discuss and propose any new or adapted SARPs and guidance material to ensure the consistency and coherency of all aviation cyber related activities in ICAO Panels and various experts groups.

Action: The Assembly is invited to:

a) Recognize the need for a speedy, well governed multi-disciplinary approach to cyber-security;
b) Urge the ICAO Council to create a "Cyber Resilience, Safety and Security Panel" (CRSSP) under governance of the ICAO Council and the Air transport Committee (ATC); and
c) Urge the ICAO Council to create a Working Group under the newly formed CRSSP for the establishment of a framework for an aviation Trust Framework.

Strategic Objectives:	This working paper relates to Strategic Objectives: *Safety*; *Air Navigation Capacity and Efficiency*; *Security and Facilitation.*
Financial implications:	
References:	

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

1. INTRODUCTION

1.1 Similar to other industries that embraced “the digital revolution”, aviation has to maintain trust from stakeholders by accurately perceiving vulnerabilities and opportunities as well as understanding adversary threats. The following are the challenges facing a connected and digitalised civil aviation:

1.2 As the aviation industry increasingly connects systems and services, the potential attack surface of systems that an adversary could engage with is growing larger and more complex, resulting in a bigger target and threat.

1.3 Since the aviation industry relies heavily on technology and enters more and more a cyber-environment, understanding and overcoming the cultural differences between the two industries will require global reform. Developing a shared culture, viewing the challenges and potential solutions together will require cross-disciplinary cooperation.

1.4 Perception of the threat posed by a digital environment is going to be critical in understanding and managing risk. It is necessary that everyone in the aviation industry attain the same level of perception and understanding in order to address the potential risk and promote a collaborative dialogue that values multiple perspectives.

1.5 The aviation industry has decades of experience in addressing safety and security issues, but the cyber-security challenge is comparatively new. It may take longer to develop and replace aviation systems than it does for perpetrators to develop capabilities, creating a challenge in accurate risk assessment and threat models.

1.6 Investments in Air Traffic Management (ATM) are already providing significant benefits but using advanced technologies such as Global Positioning Systems (GPS), digital communication and Automatic Dependent Surveillance-Broadcast (ADS-B) means we have to manage the vulnerabilities that arise from these technologies and encourage cyber resilience.

2. DISCUSSION

2.1 For the last several years, ICAO has researched cyber-security and cyber-resilience in different fora. The Aviation Security Panel (AVSECP) has been looking at the vulnerabilities to the aviation system by act of unlawful interference. The Threat and Risk WG of the AVSECP has stated several times that the risk of cyber acts of unlawful interference is low.

2.2 To research the possibility of an aviation trusted network the ICAO Secretariat set up the “INNOVA” discovery team. This group of experts created a Concept of Operations (CONOPS) for a global resilient aviation interoperable network. As of May 2019 the INNOVA group has been transformed in the Trust Framework Study Group (TFSG). This group is expanding its work in different working groups defining identification requirements, current and future needs for such a network. Another working group under the TFSG is developing a vision on a common digital trust framework and is tasked to guide the evolution to facilitate a secure, resilient and seamless exchange of information in a digitally connected environment in support of current and future operations.

2.3 ICAO established the Secretariat Study Group on Cybersecurity (SSGC) under the lead of the Deputy Director, Aviation Security and Facilitation (DD/ASF). The SSGC is monitored by the Secretariat Senior Management Group on Common Safety and Security Issues, chaired by the Secretary General of ICAO.

2.4 The current approach within ICAO does not allow for an efficient and holistic approach. A Secretariat Study Group has to forward its finding to separate ICAO Panels, who will evaluate and decide if it is necessary to create a SARP on the issue. Further, all information technology (IT) related SARPs are divided over almost all of the 19 ICAO Annexes. The establishment of a Cyber Resilience, Safety and Security Panel (CRSSP), reporting through the Air Transport Committee (ATC) and Committee on Unlawful Interference (UIC), directly to the ICAO Council would be more efficient. This new Panel would create a multidisciplinary, holistic approach throughout ICAO and consolidate all work within ICAO on cyber related issues.

2.5 The CRSSP should consider and advice on the development of a dedicated Annex for Cyber-Resilience, Safety and Security related issues within the aviation sector. The benefit of a dedicated Annex would be that all cyber related issues are clustered together like in Annex 19 for Security Management. Another benefit will be that States can directly forward all SARPs and changes to SARPs to IT experts. It would also show the importance of Cyber-Resilience, Safety and Security in the further digitalising aviation world.

2.6 The current TFSG should work directly under the CRSSP as a separate working group.

3. CONCLUSION

3.1 The current work method of ICAO to address Cyber-Resilience, Safety and Security related issues is not sufficiently coordinated and not efficient.

3.2 Creating a multidisciplinary Panel on all cyber-resilience, cyber-safety and cyber-security would enhance the coordination and efficiency of investigating and countering Cyber Resilience, Safety and Security related issues in the aviation system. To make sure there is efficient oversight and a multidisciplinary approach the Panel should be directly under the ICAO Council, the ATC and the UIC. The outcomes of the Panel should be discussed during the combined meetings between the ATC and the UIC to create holistic coordination.

3.3 The creation of a separate Annex for Cyber Resilience, Safety and Security related issues will show the importance of Cyber Resilience, Safety and Security in the digitalising aviation system and create a comprehensive oversight of all Cyber Resilience, Safety and Security SARPS through the ICAO Annexes.

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

— END —