International Civil Aviation Organization

WORKING PAPER

A40-WP/243[1]
EX/95
5/8/19

ASSEMBLY — 40TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 12: Aviation Security — Policy

CYBERSECURITY

(Presented by Airports Council International (ACI))

EXECUTIVE SUMMARY

Cybersecurity threats have become real risks for the aviation sector and these risks are expected to increase in number and impact for the foreseeable future. Thus, it is essential that aviation stakeholders establish a programme of cyber resilience and maintain robust and efficient cybersecurity defences. All businesses, including airports, are at risk from cyber threats, from businesses with a straightforward set of systems to those with the most sophisticated IT digital transformation programs.

There is a clear need for international cooperation, joined up governance, and coherent and practical policies to address cybersecurity, coupled with practical solutions for information sharing, oversight, capacity building and training. The current siloed approach does not effectively address the issue; a clear ICAO vision and strategy and joint working across all disciplines is needed that considers safety, security, operations and resilience.

Action: The Assembly is invited to:

a) Support the ICAO Aviation Cybersecurity Strategy and require that ICAO work with States and Industry to develop an action plan in support of the Strategy;

b) Recognise the immediate need for a multi-disciplinary approach to cybersecurity;

c) Request that ICAO rapidly complete an assessment of the current governance structure for cybersecurity, with serious consideration for a Panel responsible for cybersecurity that considers security, safety, resilience and operational continuity issues together. The Panel must include appropriate skilled resource from States and industry to progress the work identified in the "Cybersecurity Strategy" and should be jointly governed by the Air Navigation Commission and either the Unlawful Interference Committee or the Air Transport Committee.; and

d) Request that Council involve the industry as well as States when defining policy, a strategy, plans and standards for aviation cybersecurity.

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 would be undertaken within the resources available in the 2020 - 2022 Regular Programme Budget and/or from extra-budgetary contributions.
References:	A40-WP/28 EX/13 *ICAO Cybersecurity Strategy* Annex 17 – *Security*, Doc 8973, *Aviation Security Manual*

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

1. INTRODUCTION

1.1 Aviation systems are increasingly connected; the systems of airports, aircraft operators, ANSPs, ground handlers and passenger systems are mutually dependent for the exchange of digital information.

1.2 Cybersecurity threats have materialised into real risks for the aviation sector and these risks will likely continue to grow in number and impact for the foreseeable future. Thus, it is vitally important for aviation stakeholders to establish robust and efficient cybersecurity defences and maintain a program of cyber resilience. All businesses, including airports, are at risk from cybersecurity threats, from businesses with a straightforward set of systems to those with the most sophisticated IT digital transformation programs.

1.3 Most importantly, it must be emphasized that cybersecurity is not "only" an Information and Communication Technology (ICT) issue. Cybersecurity is the responsibility of the entire organization and an effective cyber resilience relies on the support of everyone, strong quality assurance and oversight, clear policy frameworks and effective collaboration between stakeholders. It is essential that a strong information security culture develops in the aviation sector.

1.4 Cyber-related threats and incidents can affect the entire air transport system, and can cause safety concerns, security concerns, operational disruption and financial loss, with impacts that can rapidly span boundaries and affect globally.

1.5 Understanding of cybersecurity threats will be critical in understanding and managing risk. It is necessary that everyone in the aviation industry collaborates in order to promote a dialogue that values multiple perspectives and agrees a common set of actions.

1.6 The aviation industry has decades of experience in addressing safety and security issues, but the cybersecurity challenge is comparatively new. The aviation and the airport industry are gaining experience in addressing cyber-security risks. As such, the industry should be associated equally with States on decision making, but also policy and standards developments at the ICAO appropriate bodies. It may take longer to develop and replace aviation systems than it does for perpetrators to develop capabilities, so an approach is needed that enables industry to continue to implement best practices according to existing international standards such as ISO, while promoting greater implementation globally.

1.7 A comprehensive approach is needed that addresses security, safety, resilience of the air transport system, protective measures, response mechanisms, information sharing, capacity building and oversight.

2. DISCUSSION

2.1 For the last several years, ICAO has dealt with cybersecurity and resilience to cybersecurity attacks in different fora.

2.2 The AVSEC Panel currently considers cybersecurity from an aviation security perspective and has focused mainly on the use of cybersecurity with terrorist intent to harm aviation. Three working groups of the panel have addressed the topic in some detail.

2.3 The Working Group on Threat and Risk has conducted (in 2015) an analysis of risk from a deliberate cybersecurity attack that might affect airline, airport and air navigation systems. In particular, for airports, the focus has been on deliberate tampering with security systems such as access control systems and security screening equipment.

2.4 The AVSEC Panel's Working Group on Guidance Material (WGGM) has produced a chapter on cybersecurity for the ICAO *Security Manual* (Doc 8973). This chapter covers, at a high level, background for States, guidance on creating a risk assessment and policy, a suggested framework, governance, training, design practices, procurement, detection, incident response and recovery and reporting.

2.5 The AVSEC Panel's Working Group on Annex 17 has discussed SARPs at length, culminating in the AVSEC Panel's support initially for two recommended practices in Annex 17 amendment 15, replaced by a standard and recommended practice included in Annex 17 amendment 16, November 2018.

2.6 To research the possibility of an trusted network for air navigation, the ICAO Secretariat set up the "INNOVA" team within the Air Navigation Bureau, aiming to define a means of facilitating a secure, resilient and seamless exchange of information in a digitally connected environment in support of current and future operations. To pursue this aim, the Trust Framework Study Group (TFSG) was constituted under the Air Navigation Bureau to develop a common set of principles, policy, and guidance, and a transition strategy for a globally harmonized framework that will enable trusted ground-ground, air-ground and air-air exchange of data and information among relevant aviation stakeholders with the level of resilience and interoperability needed to support increased capacity and efficiency for the continued safe operation of the civil aviation system.

2.7 ICAO established the Secretariat Study Group on Cybersecurity (SSGC) under the lead of the Deputy Director, Aviation Security and Facilitation (DD/ASF). This group has been working on recommendations for ICAO on strategy, legal policy and overall needs of States and Industry in relation to cybersecurity but is limited in scope and participation.

2.8 The Remotely Piloted Aircraft Systems (RPAS) Panel has developed standards for information exchange between remotely-piloted aircraft and remote pilot stations to minimize the potential for and mitigate the impacts of any unauthorized control.

2.9 The Legal Committee considers the adequacy of existing international air law instruments in addressing cyber threats against civil aviation.

2.10 ACI recognises ICAO as the most appropriate organisation to drive action on cybersecurity for aviation. However, the current split of cybersecurity activities within ICAO described above does not allow for an efficient and holistic approach.

2.11 ACI does not believe that there need to be detailed or prescriptive standards for cybersecurity. Indeed, these may be counterproductive since it is a fast paced, volatile issue where responses need to be flexible and agile. Different States also have different approaches, with different responsibilities across multiple agencies. This makes a set of standards purely for aviation difficult and complex to implement.

2.12 However, there is a clear need for international cooperation, joined up governance and coherent and practical policies to address these issues. Coupled with practical solutions for information sharing, oversight, capacity building and training, there is an urgent need for a strategy and action plan for civil aviation.

2.13 This action plan should promote and facilitate the development of common guidelines, standards, metrics, awareness and knowledge exchange on cyber security for the aviation ecosystem. In addition, awareness initiatives and the cross-exchange of know-how and practices among aviation stakeholders should be supported to leverage lessons learned and existing good practices.

3. **CONCLUSION**

3.1 ACI fully supports the ICAO Secretariat's working paper regarding Cybersecurity Strategy and will continue to play an active role in its further development and implementation.

3.2 It is critical that ICAO, States and industry accelerate work in this area, and work together across all disciplines to address cybersecurity. It is not an issue that can be separated naturally into safety, security, operations, air navigation and facilitation since it cuts across all areas; risk assessment, guidance material, policy development and oversight will apply to all areas.

3.3 A Cybersecurity Panel, if correctly resourced, could potentially address some of the issues identified above by bringing:

a) A greater range of expertise and experience in membership of the panel specifically on the topic of cybersecurity;

b) A holistic approach to risk assessment with methodologies agreed and mutually understood by all stakeholders, drawing on regional and national experience;

c) The ability to create working groups to dedicate more time and resource to the development of guidance materials, programmes, capacity building, assistance and training, as required; and,

d) Consideration of air navigation, safety and security issues in a single place.

— END —