



ASSEMBLY — 42ND SESSION

EXECUTIVE COMMITTEE

Agenda Item 13: Aviation Security — Policy

CREATION OF REGIONAL AVIATION CYBERSECURITY GROUPS IN THE REGIONAL OFFICES OF THE INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO)

(Presented by Venezuela (Bolivarian Republic of) and supported by 16 Member States of the Latin American Civil Aviation Commission (LACAC)²).

EXECUTIVE SUMMARY

The transnational nature of aviation and its rapid digitalization have turned the sector into a highly interconnected industry, dependent on diverse and complex IT networks that require the adoption of new and better technologies to optimize network efficiency and adapt to the new global aviation context. However, this dependence exposes the aviation sector to an increasingly broad spectrum of evolving and sustained cyber risks capable of compromising aviation safety and security. Cybersecurity is thus no longer an isolated concern but a challenge that demands a collective, coordinated response aimed at finding solutions based on the individual capabilities of States while bearing in mind regional realities, in order to deal with the growth in cyber threats.

Action: The Assembly is invited to:

- instruct the Council to request the Secretariat to design and set up regional aviation cybersecurity groups in ICAO's regions. This is an indispensable strategic step to safeguard the integrity, safety, security and continuity of air transport that will foster a more resilient and proactive attitude to cyber threats, as contemplated in ICAO's Cybersecurity Action Plan;
- ensure that these regional aviation cybersecurity groups are made up of professional cybersecurity experts who can draw up recommendations on protective measures and best practices in line with the work of the Cybersecurity Panel and regional needs; and
- recognize that aviation cybersecurity requires specific technical specialization, distinct from other fields, and coordination with other regional groups to ensure that the strategies developed by the Cybersecurity Panel are appropriately adopted in each region.

<i>Strategic Goals:</i>	This working paper relates to <i>Every Flight is Safe and Secure</i> Strategic Goal.
<i>Financial implications:</i>	It is proposed that the actions mentioned in this working paper be implemented with resources available in the regular programme budget of the current triennium and/or with extrabudgetary contributions.

¹ Spanish version provided by Venezuela (Bolivarian Republic of).

² Belize, Bolivia (Plurinational State of), Brazil, Colombia, Cuba, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay and Uruguay.

<i>References:</i>	Annex 17 – <i>Aviation Security</i> ICAO <i>Cybersecurity Action Plan</i> - 5.1.1; 5.8.1; 6.3.1; 9.3.1; 11.1.5. ICAO <i>Aviation Cybersecurity Strategy</i> (International Cooperation)
--------------------	---

1. INTRODUCTION

1.1 Civil aviation is a highly interconnected industry that relies on a range of technologies. A large proportion of the global aviation infrastructure now rests on complex IT networks that, while optimizing the sector's efficiency, also expose it to an increasingly broad spectrum of sophisticated and constantly evolving cyber threats with the ability to steal sensitive information, disrupt operations and critical navigation, communication and surveillance systems and inflict significant damage to the reputation of aviation and trust in its safety, to name only a few of the consequences.

1.2 It is therefore necessary to design efficient mechanisms and channels to mitigate or minimize cyber risks in the industry, since its transnational nature means that a cyber-attack in one country can have ripple effects or repercussions throughout a region or globally. Cybersecurity is thus no longer an isolated concern that relates only to aviation security but a challenge that demands a collective, coordinated response that transcends national borders and takes account of the realities and characteristics of each region.

1.3 Cyber threats have peculiar features that set them apart from traditional threats to aviation safety and security: they evolve at a significantly faster pace, as shown by the rapid emergence of new attack vectors and vulnerabilities, which can originate and be put into effect anywhere in the world; and it is generally difficult to identify the assailants and their attributes, as they may at times be anonymous. This is different from other threats or risks, which usually require physical presence or proximity, and it drastically changes the paradigms of detection, response and investigation.

1.4 ICAO has encouraged collaborative efforts, through cybersecurity discussions within regional groups or similar security initiatives; however, where cybersecurity is concerned, it is important to take a horizontal, intersectoral approach, incorporating it into various disciplines of aviation. Discussions about cybersecurity often involve complex technical details that require a thorough understanding of IT infrastructure and aviation operations.

1.5 All this implies a recognition that aviation cybersecurity has reached a level of complexity and criticality that requires specialized treatment and attention in a dedicated forum of professional specialists with a specific technical profile and coordinating their work with similar groups or initiatives in the field of aviation security and other regional groups where issues related to aviation cybersecurity are debated and discussed.

2. ANALYSIS

2.1 The proposed regional expert groups would basically act as a multiplier of the work of ICAO's Cybersecurity Panel (CYSECP), translating global strategy into practical action at the regional level, ensuring that aviation cybersecurity –a cross-cutting and multidisciplinary matter– is taken seriously in each region and dealt with appropriately and realistically. To that end, it is crucial to recognize and build on the hard groundwork accomplished by the Panel's experts, who have taken great pains to produce manuals, guidelines and best practices appropriate to the complex aviation environment.

2.2 The scope and application of CYSECP's work are often unknown or under-exploited by States. In that sense, the ICAO regional aviation cybersecurity groups would serve as a vital conduit to disseminate,

adapt and implement global guidelines in each regional context. States could thus benefit directly from the Panel's experience and the resources it develops, accelerating the maturity of each region's aviation cybersecurity posture.

2.3 The formal establishment of regional aviation cybersecurity groups is a pressing need. They would take inspiration from the Panel's structure, organization and purpose, replicating a model of cooperation that strengthens collective resilience, not only promoting the exchange of information and specialized training, but also making for coordinated and agile action. This will ensure a more focused and effective approach based on the protection of IT infrastructure and aviation operations and thus safeguarding the integrity, safety and continuity of aviation in our regions.

— END —