



ASSEMBLY — 42ND SESSION

EXECUTIVE COMMISSION

Agenda Item 18: Capacity Development and Implementation Support – Policy and Activities

DEVELOPING A CYBERSECURITY TRAINING PROGRAM ALIGNED WITH NEW GUIDELINES: A PROPOSAL

(Presented by the Republic of Korea)

EXECUTIVE SUMMARY

An analysis of recent aviation cyber incident statistics reveals that cyber threats have evolved into a **realistic danger**. In response, the Cybersecurity Panel is developing and publishing relevant guidance based on **ICAO Annex 17 – Security, para. 4.9**. However, there is currently only one official ICAO cybersecurity training course available. Building the capacity to counter these realistic threats requires education and training. Therefore, it's necessary to encourage member states to develop training programs based on the cybersecurity guidelines, and for ICAO to **standardize** these efforts.

Action: The Assembly is invited to:

- recognize the evolving nature of cyber threats to civil aviation;
- review the cybersecurity guidelines developed from the requirements in Annex 17 — *Aviation Security*, §4.9; and
- initiate the development of new ICAO Training programs, led by ICAO, based on these cybersecurity guidelines.

<i>Strategic Goals:</i>	This working paper relates to the Every Flight is Safe and Secure Strategic Goal.
<i>Financial implications:</i>	The ICAO activities referred to in this paper are expected to be undertaken within the resources available in the 2026-2028 Regular Budget and/or from extra-budgetary contributions as guided by the ICAO Business Plan 2026-2028.
<i>References:</i>	Doc 10184, <i>Assembly Resolutions in Force (as of 7 October 2022)</i> A42-WP/12 <i>Cybersecurity in Civil Aviation</i> A42-WP/13 <i>Outcome of the High-Level Ministerial</i> , Segment of the ICAO Security Week 2024 Held in Muscat, Oman

1. INTRODUCTION

1.1 Recently, the purpose of cyber-attacks has been changing. In the past, attackers focused on stealing personal information like passenger names, phone numbers, and credit cards. Now, their goal is shifting towards causing direct and tangible disruptions to civil aviation, such as paralyzing air transport services or disabling air navigation systems.

1.2 According to data released by EATM-CERT for the year leading up to the first half of 2025, the most common type of cyber-attack was ransomware, accounting for 15 out of a total of 33 incidents (approximately 45%), followed by hacking with 7 cases and DDoS with 5 cases. The primary targets were airlines with 16 incidents (approximately 48%), followed by airports with 7, the supply chain with 7, and Civil Aviation Authorities (CAAs) with 3.

1.3 It is anticipated that such cases will continue to increase, and considering the significant number of unreported incidents, cyber threats must now be recognized as a realistic and present danger to the aviation sector.

2. DISCUSSION

2.1 ICAO Annex 17 (Security) para. 4.9 requires the identification of critical information and communication technology systems and data used for civil aviation purposes and, where appropriate based on risk assessment, the development and implementation of measures to protect them from acts of unlawful interference.

2.2 The Republic of Korea satisfied the relevant required standards last year through the USAP-CMA (Universal Security Audit Programme - Continuous Monitoring Approach) with its national cybersecurity regulations, and it is expected that many member states will also be able to sufficiently meet these standards.

2.3 Furthermore, the Cybersecurity Panel has recently developed and partially published a number of guidance documents over the past four years to strengthen aviation cybersecurity capabilities, guiding member states to facilitate their application in civil aviation more easily.

2.4 From this perspective, it is judged to be the right time to parallelly develop ICAO Training for these guidelines, and there is a need to develop education and training programs for cybersecurity guidelines that are either under development or have already been published. (There is currently one cybersecurity program in ICAO Training).

3. CONCLUSION

3.1 An analysis of statistics from the last five years and recent data shows that we must recognize this is a time to proactively emphasize the strengthening of aviation cybersecurity resilience, as cyber threats to civil aviation have become a reality.

3.2 Cybersecurity guidelines that address the recommendations of Annex 17 (Security), §4.9 are being developed and published, led by the Cybersecurity Panel. It is necessary for all member states to identify these guidelines and prepare measures for institutional adjustment.

3.3 To achieve this, the most critical need is the development of cybersecurity education and training programs. Although training guidelines are being developed by the Cybersecurity Panel, there is only one official ICAO training course. ICAO should encourage many member states to develop cybersecurity training and then work to standardize it.

— END —