



ASSEMBLY — 42ND SESSION

EXECUTIVE COMMITTEE

Agenda Item 13: Aviation Security – Policy

CONTINGENCY PLANS AND CYBER EXERCISES AS MEANS OF INCREASING RESILIENCE TO CYBER THREATS

(Presented by Brazil)

EXECUTIVE SUMMARY

The working paper emphasizes the need to establish contingency plans for critical systems used by civil aviation, as outlined in ICAO Cybersecurity Action Plan corresponding to Pillar 6 of the ICAO Aviation Cybersecurity Strategy, as well as the improvement of plans as a result of simulated cyber-attack training exercises based on real characteristics of the systems and on facts already observed that could lead to such attacks, as outlined in ICAO Cybersecurity Action Plan corresponding to Pillar 7 of the Strategy. It highlights the evolution of cyber-attacks in civil aviation as well as the importance of related exercises and contingency plans.

Action: The Assembly is invited to encourage Member States to:

- foster the establishment of cyber incident management plans dealing with the aviation critical infrastructure; and
- establish regular cyber drills, with the participation of government and private stakeholders.

<i>Strategic Goals:</i>	This working paper relates to Strategic Goal <i>Every Flight is Safe and Secure</i>
<i>Financial implications:</i>	Not applicable.
<i>References:</i>	Pillar 6 (Incident Management and Emergency Planning) and Pillar 7 (Capacity Building, Training and Cybersecurity Culture) of ICAO Aviation Cybersecurity Strategy.

1. INTRODUCTION

1.1 Cyber threats represent a significant and growing challenge for the civil aviation sector, an inherently interconnected global system where vulnerabilities can contribute to the rapid spread of malware, causing widespread and global impacts. While technological advances have brought numerous benefits to aviation, they have also introduced an evolving cyber threat landscape due to the deep reliance on digital infrastructures. Recognizing this urgent need for cyber protection and resilience for critical aviation systems, the ICAO Aviation Cybersecurity Strategy outlines principles, measures and actions based on seven fundamental pillars.

1.2 This working paper therefore proposes to outline some actions taken by Brazil to achieve greater cyber resilience in situations where pillars 6 (Incident Management and Emergency Planning) and 7 (Capacity Building, Training, and Cybersecurity Culture) of the ICAO Aviation Cybersecurity Strategy can support the cyber protection of important assets used in air traffic control. By integrating these two pillars, civil aviation can build a comprehensive and adaptable defence, not just reacting to threats but proactively preventing and mitigating their impact, ensuring the continued safety and reliability of air travel.

1.3 Pillar 6 includes robust recovery procedures, having clear and tested contingency plans to immediately initiate the procedures to restore compromised systems and data, ensuring minimal disruption to air traffic control, ground operations, and passenger services. This includes backups, alternate systems, and detailed recovery steps.

1.4 Pillar 7 addresses awareness and training for all stakeholders involved in air traffic control, empowering everyone from air traffic controllers to ground maintenance staff on how to respond to a cyber incident and their role in maintaining a safe and secure environment. A strong cybersecurity culture means everyone understands that they are a potential first line of defence. Similarly, continuous learning and adaptation are important, recognizing that the cyber threat landscape is constantly evolving and committing to adapting to new cybersecurity strategies and technologies. This means never getting complacent and always striving to improve.

1.5 These principles are essential to enhance collaboration between civil aviation cybersecurity authorities and other stakeholders to respond to cyber-attacks, establishing a robust scenario in which contingency plans are a way to respond to these malicious actions. Coordination between all actors should be addressed in the document, showing all the mechanisms that will be available to restore normal operations following a compromise of each system, highlighting the critical requirements for implementing response actions, contributing to a safer and more resilient global aviation ecosystem.

2. DISCUSSION

2.1 Every day, the media reports on attempted cyber-attacks, some of which are successful and others that are not even reported because they were contained by the various protective measures that companies and organizations implement to deal with these daily attacks. The reality is not different in the aviation sector. Attackers mainly look for unpatched vulnerabilities to try to invade and steal information and modify systems, generally seeking financial gain.

2.2 Brazil, through DECEA, has been working on measures to make the Brazilian airspace control system more resilient in the context of cyber threats, which are growing every day. Thus, corroborating ICAO's understanding of the topic and reflecting two of the pillars cited in the organization's cybersecurity strategy, DECEA has been promoting exercises to train incident response teams from airspace

control agencies. In addition to contributing to team training, these exercises also help identify cybersecurity gaps resulting from combinations of systems and applications developed to meet the demands of air traffic control operations. The results of these training exercises are compiled in reports that are addressed to the teams responsible for improving the systems and the contingency plan.

2.3 In relation to the exercises, each simulated situation is accompanied by details provided by the experts in the maintenance of each system to obtain reliability of the situations that are based on real occurrences. As a result, the actions become closer to a real situation and allow a more accurate assessment to extract effective improvements for the actions adopted, for each system (gaps identified), and for the plan itself.

2.4 Another pillar of ICAO's cybersecurity strategy, which concerns incident management and emergency plans, serves as a basis for the preparation of contingency plans associated with each critical system used in the control of Brazilian airspace. All the information necessary to direct actions towards the reestablishment of the functionalities offered by each system at the different levels of air traffic control is described in the document, as well as the various actors involved in the responses with due coordination to minimize unavailability and the impact caused to air transport users.

2.5 Contingency plans are developed based on international standards, such as ISO/IEC 27031, and are adjusted to the specificities of each location. This makes it possible to aggregate details of the systems' functionalities in each location to maintain these functionalities even in the event of cyber-attacks, keeping the environment resilient and controlled.

2.6 It is important to clarify that DECEA also participates in the Brazilian national cybersecurity exercise, under the responsibility of the Ministry of Defence, which aims to protect the country's critical systems. In this national exercise, DECEA contributes the expertise developed within its airspace control units to air transport security and receives information from other areas that also have critical systems and require protection and resilience measures. The activities developed in this major national exercise help to corroborate and improve contingency plans, which need to be constantly updated in the face of daily new threats.

2.7 Brazil calls on ICAO Member States and the aviation industry to support and organize cybersecurity exercises to bring together government and industry experts to share best practices and knowledge in training cyber experts in responding to cyber-attacks and building more reliable cyber contingency plans to protect aviation critical infrastructure and systems.

3. CONCLUSION

3.1 Cyber threats are an ever-present challenge, and the civil aviation sector, with its intricate global network, is also vulnerable. Brazil's proactive stance, as demonstrated by DECEA's initiatives, aligns with ICAO's Aviation Cybersecurity Strategy, particularly Pillars 6 and 7. The emphasis on robust contingency plans, informed by international standards like ISO/IEC 27031 and tailored to local specificities, coupled with regular, realistic cyber exercises, significantly enhances cyber resilience. These efforts not only train incident response teams and identify vulnerabilities but also foster a strong cybersecurity culture across all stakeholders. By sharing expertise and collaborating in national and international exercises, Brazil underscores the critical need for continuous adaptation and collective action to safeguard the global aviation ecosystem from evolving cyber risks.