



ASSEMBLY — 42ND SESSION

EXECUTIVE COMMITTEE

Agenda Item 13: Aviation Security — Policy

**AVIATION CYBERSECURITY STRATEGY UNDER A COLLABORATIVE
WORK PLAN FOR THE PROTECTION OF CIVIL AVIATION**

(Presented by Colombia and supported by 16 LACAC Member States²)

EXECUTIVE SUMMARY

Aviation is undergoing an unprecedented digital transformation. Technologies such as digital communications, intelligent systems integration, data analytics, advanced surveillance, predictive ATM systems and cloud computing are reshaping the industry. However, this growing interconnectedness increases the cyber-attack surface and the vulnerability to cyber threats. Increasingly sophisticated attacks jeopardize safety, data privacy and confidence in the system.

To counter this challenge, it is crucial to strengthen industry cybersecurity. Member States should implement ICAO recommendations, such as the Aviation Cybersecurity Strategy and the Cybersecurity Action Plan, and tailor them to their national contexts, strengthening their organizational culture, technological infrastructure and cybersecurity regulations to meet specific cybersecurity-related challenges in civil aviation.

In addition, the transactional nature of cyberspace calls for dialogue and technical and operational cooperation mechanisms amongst Member States.

Action: The Assembly is invited to:

- a) request the ICAO Council to develop, as part of its 2026-2050 Strategic Plan, a self-assessment tool for States to measure their aviation cybersecurity maturity level.

*Strategic
Goals:*

This working paper relates to the following Strategic Goals:

- *Every Flight Is Safe and Secure*
- *Aviation Delivers Seamless, Accessible, and Reliable Mobility for All*
- *No Country Left Behind*

*Financial
implications:*

References:

- ICAO Annex 17 – *Aviation Security*
- ICAO document: *Aviation Cybersecurity Strategy*

¹ Spanish version provided by Colombia

² Belize, Bolivia (Plurinational State of), Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Uruguay, Venezuela (Bolivarian Republic of)

	- ICAO document: <i>Cybersecurity Policy Guidance</i> - <i>Resolution A41-19 on Addressing Cybersecurity in Civil Aviation</i> - ICAO document: <i>Cybersecurity Action Plan</i>
--	--

1. INTRODUCTION

1.1. Global aviation has undergone an unprecedented digital transformation, driven by advanced technologies. This digitalization, however, increases vulnerability to cyber-attacks, which can compromise security and confidence in the system. Strengthening cybersecurity is therefore crucial to protecting information and supporting continued air operations.

1.2. States have developed a comprehensive cybersecurity strategy that includes training human talent, strengthening security technologies, establishing a regulatory framework, public-private cooperation and international collaboration. This strategy aims to comprehensively improve State workforce training, technological infrastructure and risk management.

1.3. International cooperation is key to strengthening aviation against cyber threats. Information sharing, response coordination, and collaboration mechanisms – the importance of which was exemplified by the incident of 19 July 2024 that impacted airline management systems worldwide – help mitigate risks and ensure safety.

1.4. Digitalization has increased the vulnerability of civil aviation to cyber-attacks that jeopardize its safety and infrastructure. Strengthening cybersecurity is a strategic priority to ensure continuity and resilience.

1.5. ICAO's Aviation Cybersecurity Strategy and Cybersecurity Action Plan provide a solid framework for addressing these challenges. However, the effective implementation of these recommendations requires coordinated and sustained action at the regional level, as well as a strong commitment from all stakeholders, including Member States, industry and academia, as a catalyst for ICAO's Strategic Goals 2026–2050.

2. DISCUSSION

2.1. Digitalization has optimized civil aviation, improving processes and competitiveness. However, systems interconnectedness has increased cybersecurity risks, including unauthorized data access and tampering with critical systems. States must therefore strengthen their individual capabilities and cooperate to enhance safety and confidence in the sector.

2.2. Civil aviation faces the challenge of taking advantage of digitalization while ensuring cybersecurity. This requires the implementation of digital security technology, workforce training, experience sharing, and development of information and digital security policies and strategies for industry businesses.

2.3. ICAO views cybersecurity as a shared responsibility that calls for international cooperation. As cyber threats evolve rapidly and cross borders, States should respond in an agile and coordinated manner sharing information, best practices and technical resources.

2.4. Cyber-attacks against civil aviation are not a hypothetical threat but a real concern. Malicious actors can compromise critical systems such as air traffic control and navigation and flight management

systems, putting the safety of millions of passengers and crew members at risk. In addition, cyber-attacks can create significant disruptions to air operations, leading to millions in financial losses and damaging the industry's reputation.

2.5. Civil aviation faces cyber risks, including data theft, system tampering, disruption of critical services and loss of public confidence. Strengthening cybersecurity is key to ensuring safe and secure operations and preserving the stability of the sector.

2.6. With the growing threat of cyber-attacks, it is essential to take a comprehensive and collaborative approach to strengthen cybersecurity in civil aviation by creating a robust framework to guide States and stakeholders in the implementation of effective security measures. This framework should rely on the commitment of senior management, effective governance and clear cybersecurity policies for the protection of critical information and operations systems.

2.7. A process should be put in place to strengthen civil aviation cybersecurity capabilities. Its strategy should be built on four pillars: (i) workforce training; (ii) internal technological infrastructure strengthening; (iii) development of a regulatory framework to promote cybersecurity across civil aviation; and (iv) cooperation among entities.

2.8. This strategy aims to promote civil aviation security by managing information integrity, availability and confidentiality in critical systems, thus ensuring efficient service provision and protection of sensitive data with highly trained talent. A robust regulatory framework should also be implemented to boost cybersecurity at airlines, airports, suppliers and manufacturers, promoting robust security practices and a coordinated response to cyber incidents, in order to increase resilience and maintain user confidence in the face of growing digital threats.

2.9. In addition, it is essential to develop specialized talent through continuous cybersecurity training. The training of qualified professionals is key to ensuring safety and reducing the risks associated with staff turnover. There is also the need to consolidate a dedicated cybersecurity incident response center for civil aviation to enable a rapid and coordinated response to cyber incidents. This center should serve as a hub for incident management, coordination of efforts with industry stakeholders and its own team training.

2.10. International cooperation is another key element to information sharing and the development of joint simulation exercises to effectively respond to cross-border cyber threats. A single technological platform would foster the exchange of knowledge and best practices.

2.11. Ongoing dialogue should be maintained with authorities and industry businesses to coordinate a unified response to cyber threats. However, cyberspace knows no borders and therefore this dialogue should include States, which should develop efficient and robust mechanisms to share experiences and exchange recommendations on national cybersecurity strategies.

2.12. It is key for national cybersecurity strategies to be based on the laws and regulations of each State, but they should also be interoperable to ensure operational safety globally. Collaboration and information sharing among experts should be promoted to identify and address vulnerabilities and strengthen industry resilience to cyber-attacks. It is also important to create an ongoing forum where experts can provide feedback on local strategies and work jointly to close gaps that could be exploited by cybercriminals or cyber terrorists.

2.13. In this regard, it is considered necessary for ICAO to promote actions to strengthen the management of cybersecurity in civil aviation. The creation of a self-assessment tool integrated into the 2026–2050 Strategic Plan is justified insofar as it would allow States to identify policy, operational, and technical gaps early, facilitating proactive planning of mitigation measures and the development of national capacities. This would help to guarantee a more homogeneous level of protection between States, reducing asymmetries that currently generate vulnerabilities in the global aviation network.

2.14. Similarly, it is essential that ICAO promote more specific technical and policy guidelines on cybersecurity that guide States in the adoption of best practices and international standards. This would favor the construction of a common framework that allows facing digital threats more effectively, strengthening the resilience of the aeronautical system and preserving the safety and continuity of air operations at a global level.

3. **CONCLUSION**

3.1. Cybersecurity in civil aviation is a challenge that requires a global and coordinated response. ICAO, in collaboration with its Member States, should take the lead in making the industry more secure and resilient to cyber threats. The safety of millions of passengers and the stability of the global aviation system depend on it.

– END –