Resolution A41-19: Addressing Cybersecurity in Civil Aviation

Whereas the global aviation system is a highly complex and integrated system that comprises systems that are critical for the safety and security of civil aviation operations;

Noting that the aviation sector is increasingly reliant on the availability, integrity and confidentiality of information, data, and systems;

Mindful that cyber threats to civil aviation are rapidly and continuously evolving, that aviation continues to be a target for perpetrators in the cyber domain as in the physical one, and that cyber threats can evolve to affect critical civil aviation systems worldwide;

Recognizing that not all cybersecurity events affecting the safety of civil aviation are unlawful and/or intentional;

Recognizing the multi-faceted and multi-disciplinary nature of cybersecurity challenges and solutions and noting that cyber risks can simultaneously affect a wide range of aviation areas and spread rapidly;

Reaffirming the obligations under the *Convention on International Civil Aviation* (Chicago Convention) to ensure the safety, security and continuity of civil aviation;

Considering that the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention) and Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing Protocol) would enhance the global legal framework for dealing with cyber-attacks on international civil aviation as crimes and therefore wide ratification by States of those instruments would ensure that such attacks would be deterred and punished wherever in the world they occur;

Reaffirming the importance and urgency of addressing the cybersecurity and cyber resilience of civil aviation's critical systems, data, and information against cyber threats and hazards, including common interfaces between civil and military aviation;

Considering the need to work collaboratively towards the development of an effective and coordinated global framework to address aviation cybersecurity and to support the cybersecurity and cyber resilience of the global aviation system to cyber threats that may jeopardize the safety and/or security of civil aviation;

Recognizing ICAO's leadership and work in the fields of aviation cybersecurity and cyber resilience across the different aviation disciplines;

Recognizing that aviation cybersecurity needs to be harmonized at the global, regional and national levels in order to ensure the consistency and full interoperability of protection measures and risk management systems;

Recognizing the importance of developing clear national governance and accountability for civil aviation cybersecurity, including the designation of a competent national authority responsible for aviation cybersecurity in coordination with concerned national authorities and agencies; and

Acknowledging the value of relevant initiatives, action plans, publications and other media designed to address cybersecurity issues in a collaborative and holistic manner.

The Assembly:

1. *Urges* Member States to adopt and ratify the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention) and *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* (Beijing Protocol) as a means for dealing with cyberattacks against civil aviation;

2. *Calls upon* States and industry stakeholders to take the following actions to address cyber threats to civil aviation:

a) implement the ICAO Aviation Cybersecurity Strategy, and make use of the ICAO Cybersecurity Action Plan as a tool to support the implementation of the Aviation Cybersecurity Strategy;

b) designate the authority competent for aviation cybersecurity, and define the interaction between that authority and concerned national agencies;

c) define the responsibilities of national agencies and industry stakeholders with regard to cybersecurity in civil aviation;

d) develop and implement a robust cybersecurity risk management framework that draws on relevant safety and security risk management practices, and adopt a risk-based approach to protecting critical civil aviation systems, information, and data from cyber threats;

e) establish policies and instruments, and allocate resources to ensure that, for critical aviation systems: system architectures are secure by design; systems are protected and resilient; data is secured and available in storage and while in transfer; system monitoring, and incident detection and reporting, methods are implemented; incident recovery plans are developed and practiced; and forensic analysis of cyber incidents is carried out;

f) encourage government/industry coordination with regard to aviation cybersecurity strategies, policies, and plans, as well as sharing of information to help identify critical vulnerabilities that need to be addressed;

g) encourage civil/military cooperation with regard to identifying, protecting, and monitoring common vulnerabilities and data flows at interfaces between civil and military aviation systems, and collaborate in response to common cyber threats and recovery from cyber incidents;

h) develop and participate in government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts;

i) design and implement a robust cybersecurity culture across the civil aviation sector;

j) encourage States to continue contributing to ICAO in the development of international Standards, strategies, and best practices to support advancing aviation cybersecurity and cyber resilience; and

k) continue collaborating in the development of ICAO's cybersecurity framework according to a horizontal, cross-cutting and functional approach involving aviation safety, aviation security, facilitation, air navigation, communication, surveillance, air traffic management, aircraft operations, airworthiness, and other relevant disciplines.

3. *Instructs* ICAO to:

a) continue to promote the universal adoption and ratification of the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention) and *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* (Beijing Protocol); and

b) continue to ensure that cybersecurity and cyber resilience matters are considered and coordinated in a cross-cutting manner through the new mechanism in ICAO to address aviation cybersecurity.

— END —