A40-10: Addressing Cybersecurity in Civil Aviation

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

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

Mindful that the threat posed by cyber incidents on civil aviation is rapidly and continuously evolving, that threat actors are focused on malicious intent, disruption of business continuity and theft of information for political, financial or other motivations, and that the threat can easily evolve to affect critical civil aviation systems worldwide;

Recognizing that not all cybersecurity issues affecting the safety of civil aviation are unlawful and/or intentional, and should therefore be addressed through the application of safety management systems;

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 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 cyberattacks 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 protecting civil aviation's critical infrastructure systems and data against cyber threats;

Considering the need to work collaboratively towards the development of an effective and coordinated global framework for civil aviation stakeholders to address the challenges of cybersecurity, along with short-term actions to increase the resilience of the global aviation system to cyber threats that may jeopardize the safety of civil aviation;

Recognizing the work of the Secretariat Study Group on Cybersecurity, which greatly contributed to the format of the Cybersecurity Strategy by linking safety and security characteristics of cybersecurity;

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

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

The Assembly:

1. *Urges* Member States and ICAO to promote the universal adoption and implementation 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) as a means for dealing with cyberattacks against civil aviation;

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

a) Implement the Cybersecurity Strategy;

b) Identify the threats and risks from possible cyber incidents on civil aviation operations and critical systems, and the serious consequences that can arise from such incidents;

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

d) Encourage the development of a common understanding among Member States of cyber threats and risks, and of common criteria to determine the criticality of the assets and systems that need to be protected;

e) 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;

f) 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;

g) Based on a common understanding of cyber threats and risks, adopt a flexible, risk-based approach to protecting critical aviation systems through the implementation of cybersecurity management systems;

h) Encourage a robust all-round cybersecurity culture within national agencies and across the aviation sector;

i) Promote the development and implementation of international standards, strategies and best practices on the protection of critical information and communications technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation;

j) Establish policies and allocate resources when needed to ensure that, for critical aviation systems: system architectures are secure by design; systems are resilient; methods for data transfer are secured, ensuring integrity and confidentiality of data; system monitoring, and incident detection and reporting, methods are implemented; and forensic analysis of cyber incidents is carried out; and

k) Collaborate in the development of ICAO's cybersecurity framework according to a horizontal, cross-cutting and functional approach involving air navigation, communication, surveillance, aircraft operations and airworthiness and other relevant disciplines.

3. Instructs the Secretary General to:

a) develop an action plan to support States and industry in the adoption of the Cybersecurity Strategy; and

b) continue to ensure that cybersecurity matters are considered and coordinated in a crosscutting manner through the appropriate mechanisms in the spirit of the Strategy.

— END —