International Civil Aviation Organization
North American, Central American and Caribbean Office

WORKING PAPER

NACC/WG/6 — WP/20
23/08/21

Sixth North American, Central American and Caribbean Working Group Meeting (NACC/WG/6)

On-line, 25 to 27 August 2021, 09:00 to 13:00 (UTC-5)

Agenda Item 4: Implementation of Air Navigation Issues
4.8 Emerging technologies and new regional challenges

CYBERSECURITY IN AIR NAVIGATION ACTIVITIES

(Presented by the Secretariat)

EXECUTIVE SUMMARY	
This working paper provides information of one relevant and emergent challenge that must be taken into account as an integral part of air navigation activities.	
Action:	Suggested actions are provided in Section 4.
Strategic Objectives:	• Air Navigation Capacity and Efficiency • Economic Development of Air Transport
References:	• Global Air Navigation Plan version 6, October 2019. • Assembly Resolution A40-10: Addressing Cybersecurity in Civil Aviation, October 2019

1. Introduction

1.1 Technology and cyber-systems have become essential for modern society, we depend even more on technology, which provide greater efficiency to all activities that are carried out day to day. Along with the benefit of cyber technologies, insecurities arise that affect all systems and infrastructures. Cyber-threat and cyber-attack have a transnational component and effect, as global systems are interconnected. Furthermore, the complexity of the action has implications for various actors at the national, regional and international levels.

1.2 The Aviation Cybersecurity Strategy developed by ICAO indicates that the civil aviation sector is increasingly dependent on the availability of information and communication technology systems, as well as the integrity and confidentiality of data. The threat of potential cyber incidents to civil aviation is constantly evolving, with perpetrators acting maliciously to disrupt operations and steal information for political, financial and other reasons.

1.3 Operational personnel, air crews, air traffic controllers, CNS infrastructures, will depend more and more on the management and technical capacity to face threats in terms of cyber-attacks in order to guarantee operational security.

1.4 The obligation of the States to identify critical infrastructures and establish adequate mechanisms to face these new challenges, as well as to establish the mechanisms for restoring a cyber-attack and the mechanisms for business continuity.

2. Analysis

2.1 ICAO, through Resolution ***A40-10: Addressing Cybersecurity in Civil Aviation***, of Assembly 40, developed in 2019, established the necessary recommendations for the issue of cybersecurity to be established as an integral part of aviation operations. Resolution A40-10 can be found in the **Appendix** to this working paper.

2.2 ICAO has established the cybersecurity strategy based on seven important pillars for the implementation of cybersecurity:

https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.SP.pdf

2.3 Air Navigation operations are supported by state-of-the-art technology, both at the level of the equipment on the ground and the avionics on board the aircraft. Facilities such as aeronautical information exchange, automated protocols between control centers, ATFM, A-CDM, among others, require that the data have quality, availability and certification measures, this information is the basis for decision-making in real time.

2.4 Aviation includes airspace users, air navigation providers, airport operators, civil aviation authorities and equipment manufacturers, among others. In this sense, it is necessary to carry out an analysis of the aviation system integrating all the interested parties that are part of the system.

2.5 Cybersecurity requires a holistic approach, the interfaces between aviation security components deserve special attention, such as Air Traffic Management (ATM) security, the security of Communication, Navigation and Surveillance (CNS) components and operations (ADS-B, GNSS, data Link), airspace security and airport security. Air traffic management security must be an integral part of the aviation security system.

2.6 The ICAO NACC Regional Office, through the cybersecurity initiative for air traffic services in collaboration with Industry and Organizations, as recommended by ICAO Resolution A40-10, has developed in collaboration with CANSO and AIRBUS the Project for the CAR region that aims to support the States in the establishment of their first *Cybersecurity Policy Manual*.

2.7 The project has successfully developed the following activities:

a) Basic cybersecurity workshop: covering general cybersecurity guidelines, ICAO documentation and best practices.
https://www.icao.int/NACC/Pages/meetings-2020-aci.aspx

b) Workshop on the template for Cybersecurity Manual for air navigation, which includes a document developed within this initiative, by ICAO/NACC, CANSO and AIRBUS that provides recommendations so that States can begin to work on their Manual of Policies of Cybersecurity.
https://www.icao.int/NACC/Pages/meetings-2021-canso02.aspx

c) Third stage under development, where within the initiative the States are directly supported in the development of their cybersecurity policy manual according to their aviation system, their ATM/CNS infrastructure and to their operations.

3. Conclusions

3.1 Cybersecurity challenges require joint work by all areas of the Civil Aviation system, integrating both internal areas and parts of the system, as well as external stakeholders to civil aviation operations.

3.2 Cyber-attacks have been increasing in recent years, aviation did not think that it could be a target of this type of threats, but the use of cutting-edge technology, regional and global interconnectivity, as well as other interests make our sector vulnerable to this threat.

3.3 Cybersecurity needs a job that includes all aviation disciplines and requires seeing the system as a whole and not by parts.

4. Suggested actions

4.1 The Meeting is invited:

a) take note of the information presented in this working paper;
b) consider adopting multidisciplinary approaches to cybersecurity approach for all air navigation operations;
c) the adoption of corresponding tasks for all Task Groups part of the ANI/WG (NACC / WG);
d) take advantage of the ICAO/NACC-CANSO-AIRBUS cybersecurity initiative for the specific support of the activities of their States; and
e) any other activity that applies.

— — — — — — — — — — —

APPENDIX
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, crosscutting 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 —