International Civil Aviation Organization

Twenty Fifth Meeting of the Communications/ Navigation and Surveillance Sub-group (CNS SG/25) of APANPIRG

Video Tele-Conference, 18 – 22 October 2021

Agenda Item 11: Cybersecurity of CNS/ATM systems

11.2 Other Cybersecurity related issues

CYBERSECURITY IN AIR NAVIGATION ACTIVITIES

(Presented by the Secretariat)

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, as well as a summary about experience and activities development by ICAO NACC Regional Office to address and support Caribbean States in their air navigation cybersecurity approach.

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, aircrews, 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. DISCUSSION

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) Webinar in collaboration with Eurocontrol and the Industry: Cybersecurity Webinar on Air Traffic Management (ATM) and Communications, Navigation and Surveillance (CNS) Activities.
https://www.icao.int/NACC/Pages/meetings-2021-cswatm.aspx

d) Last phase of the ICAO NACC Cybersecurity initiative is direct support to States 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. ACTION BY THE MEETING

a) take note of the information presented in this working paper;

b) consider adopting multidisciplinary approaches to cybersecurity approach for all air navigation operations; and

c) any other activity that applies.

– – – – – – – – – – – – –