International Civil Aviation Organization
Latin American Civil Aviation Commission
ICAO/LACAC NAM/CAR/SAM Aviation Security and Facilitation Regional Group (AVSEC/FAL/RG)

WORKING PAPER

AVSEC/FAL/RG/9 — WP/23Rev.1
27/03/19

Ninth Meeting of the ICAO/LACAC NAM/CAR and SAM Aviation Security and Facilitation Regional Group (AVSEC/FAL/RG/9)
Santo Domingo, Dominican Republic, 25 to 29 March 2019

Agenda Item 7: **Training, Cooperation, and Assistance**
7.1 Implementation Support and Development Section – Security (ISD-SEC) Update

LESSONS LEARNED IN CYBERSECURITY

(Presented by the Secretariat)

EXECUTIVE SUMMARY

This Working Paper provides the latest ICAO developments in cybersecurity and the initiatives in this field in the NAM, CAR and SAM regions. The working paper also presents conclusions and recommendations extracted from the cybersecurity activities conducted for their consideration by the Regional Group and their possible presentation at the Aviation Security Panel (AVSECP).

Action:	Suggested action is presented in Section 5.
Strategic Objectives:	• Security & Facilitation
References:	• Resolutions adopted by the Assembly – 39th Session • Civil Aviation Cybersecurity Action Plan – 5 December 2014

1. Introduction

1.1 During the 39th ICAO Assembly Session there were two main resolutions related to Aviation Security (AVSEC). The first was the ICAO Assembly Resolution A39-18 "Consolidated AVSEC Policy", establishing AVSEC priority areas for the current triennium (2017-2019), which sets the basis for the development of the Global Aviation Security Plan (GASeP).

1.2 The second was ICAO Assembly Resolution A39-19, "Addressing cybersecurity in civil aviation", which recognized that *"…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*". The aviation sector is dependent on "*the availability of information and communications technology systems, as well as on the integrity and confidentiality of data*".

1.3 The rapid development of new technologies and an even more digitalized and connected world have not only created opportunities, but also a new area of threat. Cyber incidents/attacks are posing new threats which, if further evolved, can easily affect critical civil aviation systems all over the world. The cybersecurity declaration calls upon States and industry to develop a common understanding of the threat and a common strategy to combat this threat. This is yet another call for a global approach to a global problem, which can only be mitigated with joint efforts and collaboration.

2. ICAO developments in cybersecurity

2.1 The year 2018 was a major step forward towards promoting cybersecurity culture and collaboration between States and industry. After the work on cybersecurity coordinated by the Aviation Security Panel (AVSECP), the Amendment 16 to Annex 17, which became applicable on 16 November 2018, contains the first standard on measures relating to cybersecurity (4.9.1): *"Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference".*

2.2 Similarly, Recommended Practice 4.9.2 has been reworded and reads now: *"Each Contracting State should ensure that measures implemented protect, as appropriate, the confidentiality, integrity and availability of the identified critical systems and/or data. The measures should include, inter alia, security by design, supply chain security, network separation, and the protection and/or limitation of any remote access capabilities, as appropriate and in accordance with the risk assessment carried out by its relevant national authorities".*

2.3 Furthermore, ICAO established the Secretariat Study Group on Cybersecurity (SSGC), following the Assembly's instructions, to lead a comprehensive cybersecurity work plan. Among its main tasks are the drafting of an "ICAO Cybersecurity Strategy" and the feasibility study for a dedicated Cybersecurity Panel, both documents for consideration during the 216th ICAO Council Session (Montreal, from 18 February to 15 March 2019).

2.4 Within the SSGC the Cybersecurity Research Subgroup on Legal Aspects was also set up, whose objectives are the categorization of cyber threats and vulnerabilities and the analysis of the current international legal framework and States' legal provisions in cybersecurity.

3. Cybersecurity initiatives in the NAM, CAR and SAM regions

3.1 During the years 2018 and 2019, there were different activities addressing cybersecurity in the NAM, CAR and SAM regions, with the objectives of developing a common understanding of cyber threats and risks; share experiences and good practices among States and industry; and, ultimately, consistently apply mechanisms to coordinate, report and manage risks on cybersecurity.

3.2 The Jamaica Civil Aviation Authority (JCAA), in association with the Organization of American States Inter-American Committee against Terrorism and the NAM/CAR and SAM AVSEC/FAL Regional Group, hosted a Cybersecurity in Aviation Workshop, in Montego Bay, from 20 to 23 March 2018, with the aim of increasing awareness of cybersecurity threats within States and aviation industry and based on numerous real incidents that have occurred over the last years.

3.3 The Federal Aviation Administration (FAA) organized a Cybersecurity Tabletop Exercise in Washington D.C., from 17 to 19 July 2018, for Caribbean States. The exercise comprised two scenarios and a tour of the FAA Air Traffic Control System Command Centre and the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Centre (NCCIC), to observe how the United States handles cybersecurity and how it coordinates across the government.

3.4 From 4 to 6 December 2018, the ICAO NACC Regional Office organized the Workshop on Cybersecurity in Aviation, where States, industry and international organizations were brought together. The first session focused on the international initiatives and good practices applied not only in aviation; the rest of the sessions addressed cybersecurity for air navigation service providers (ANSPs), airlines and airports.

3.5 With the training material of Jamaica Workshop translated into Spanish, a new Cybersecurity on Civil Aviation Workshop was organized in Buenos, Aires, from 19 to 22 February 2019, aimed to raise cybersecurity awareness within States and industry.

4. Lessons learned and recommendations in cybersecurity

4.1 After the knowledge acquired and shared experiences during the activities previously mentioned, the present working paper tries to summarize the main conclusions and lessons learned by the States in implementing the Standard 4.9.1 and the Recommended Practice 4.9.2 for the consideration of the ICAO/LACAC NAM/CAR and SAM Aviation Security and Facilitation Regional Group (AVSEC/FAL/RG):

- Cyber threats in civil aviation and the challenges faced by the aviation industry (e.g. data confidentiality and integrity, systems availability, insider threat) are largely similar to the ones faced in other sectors (banking, insurance, government, entertainment). Therefore, many measures that civil aviation operators and entities should apply are similar to the measures already applied in other more experienced sectors and with more resources (e.g. financial sector).

- As cybersecurity is a transversal subject which affects different sectors and critical infrastructures of the States, policies and regulation on the protection of critical data and information and communications technology systems are established by specialized authorities (e.g. competent authorities in telecommunications) with little relation to civil aviation; therefore, it is recommended to check which general guidelines for cybersecurity already exist in each State.

- Several international and regional organizations develop cybersecurity guidance material and offer proven information on States' maturity level in cybersecurity (e.g. policy and strategy; legal frameworks; technologies):
  - The International Telecommunications Union (ITU) established in 2007 the Global Cybersecurity Agenda (GCA) which encompasses five pillars: legal measures; technical and procedural measures; organizational structure; capacity building; and international cooperation. ITU also offers technical assistance for critical infrastructure protection, training and organization of cybersecurity drills. Since the year 2014, ITU publishes the Global Cybersecurity Index (GCI) which measures the commitment of countries to the GCA (http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx).

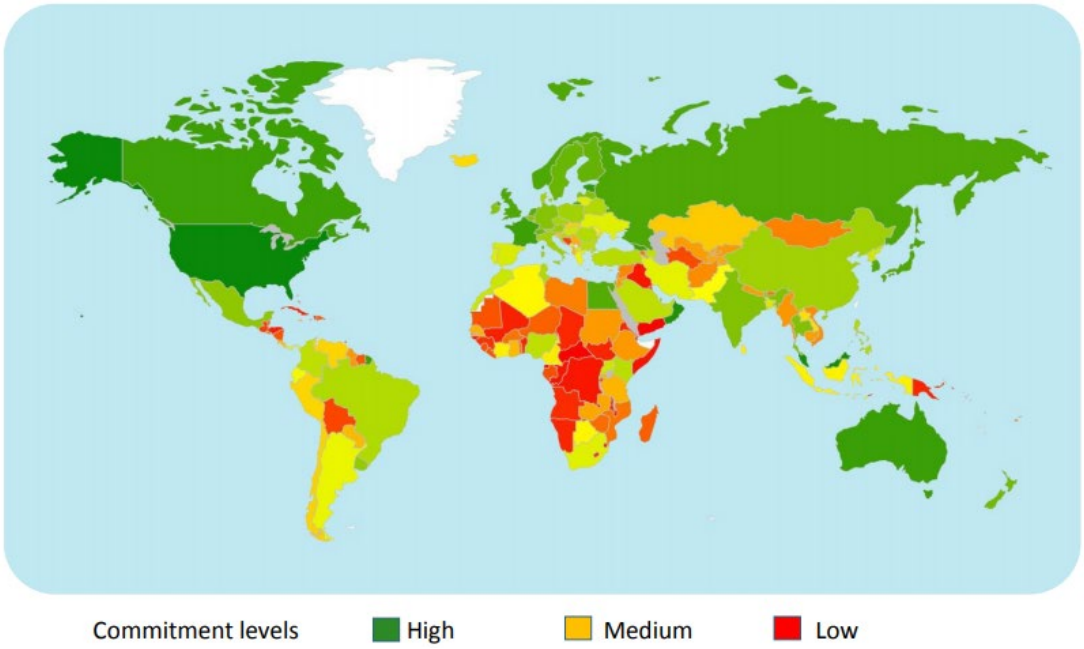

Figure 1. Global Cybersecurity Index (GCI) results in 2017

  - The Organization of American States (OAS) maintains an observatory on cybersecurity in Latin America and the Caribbean (http://observatoriociberseguridad.org) where it is possible to find statistics and a summary of cybersecurity initiatives for each of the OAS Member States. In addition, the OAS webpage dedicated to cybersecurity (www.sites.oas.org/cyber/EN/Pages/Directory/Default.aspx) keeps a repository with guidance documents (e.g. manual on managing cybersecurity incidents) and an updated list of States' CERTs/CIRTs/CSIRTs (Computer Emergency Response Team/Computer Incident Response Team/Computer Security Incident Response Team).

- Both, National AVSEC inspectors and ICAO AVSEC auditors should become aware and make use of the material and tools already available in order to undertake a first evaluation of the States in cybersecurity. The collected information should help determine whether a State has issued cybersecurity regulations and/or recommendations already applicable to civil aviation operators and entities which handle critical data and/or operate information and communications technology systems and infrastructures vital for the proper functioning of the air transport.
- In general, for those States with an established national CERT/CIRT/CSIRT it is assumed to have a basic capability to identify, defend, respond and manage cyber threats. Apart from reactive services, CERT/CIRT/CSIRT may also engage in proactive services such as vulnerability assessments and cybersecurity audits. However, it should be taken into consideration that there are different CERT/CIRT/CSIRT typologies: governmental (which only provide service to the public sector), sectorial (which are established for critical sectors such as healthcare or banking), academic, military.
- Civil Aviation operators and entities aware of handled data and operated systems criticality, usually externalize infrastructure monitoring and data protection to a Network Operations Centre/Security Operations Centre (NOC/SOC) specialized in the sector (e.g. Indra, Thales, SITA); however, big operators may choose to invest in equipment and staff training to build their own NOC/SOC. These NOC/SOCs centres conduct a study of customer's needs and offer architecture and security technology that covers customers' operational requirements, complying almost automatically with Recommended Practice 4.9.2.
- Current cybersecurity Standards and Recommended Practices (SARPs) contained in Annex 17 already take into account industry readiness and their developments in this field. In this respect, ICAO signed a Civil Aviation Cybersecurity Action Plan in December 2014, with the Airports Council International (ACI), the Civil Air Navigation Services Organization (CANSO), the International Air Transport Association (IATA) and the International Coordinating Council of Aerospace Industry Associations (ICCAIA), which included a clear roadmap and objectives that, at the present time, should have been fully achieved.

5. Suggested actions

5.1 The Meeting is invited to:

a) Review of the lessons learned and recommendations in cybersecurity and decide whether this working paper could be forwarded to the Aviation Security Panel (AVSECP) in order to gather other States' opinion on implementing cybersecurity SARPs and their supervision.

— END —