International Civil Aviation Organization
CAR/SAM Regional Planning and Implementation Group (GREPECAS)

WORKING PAPER

PPRC/5 — WP/26
11/07/19

Fifth Meeting of the Programmes and Projects Review Committee (PPRC/5)
Mexico City, Mexico, 16 to 18 July 2019

Agenda Item 7: Analysis of the Emerging Threats to Air Navigation
7.1 ICAO's perspective on cyber-security and cyber-resilience

ACTIVITIES OF THE ICAO CAR/SAM REGIONS ON CYBER-SECURITY AND CYBER-RESILIENCE

(Presented by the Secretariat)

EXECUTIVE SUMMARY

This Working Paper shows the activities carried out by CAR and SAM regions to provide their States with information to develop a correct implementation of mechanisms to support the security of aeronautical information.

Action:	Suggested actions are presented in Section 3.
Strategic Objectives:	• Air Navigation Capacity and Efficiency
References:	• A39-19 Assembly Resolution on Cyber-security in civil aviation • NAM/CAR/SAM Meeting for the AIDC implementation, Lima, Peru, April 2018 • ICAO NAM/CAR/SAM Workshop on Cyber-security in aviation, Mexico City, Mexico, from 4 to 6 December 2018.

1. Introduction

1.1 This Working Paper shows the activities carried out by CAR/SAM regions during 2018 to support A39-19 Assembly Resolution addressed to the States to encourage them in the promotion of legal provisions on cyber-security to be applied within their territory.

1.2 Cyber-security has been tracked from a security approach, however, during the NAM/CAR/SAM Meeting for the AIDC implementation, held in Lima, Peru, in April 2018, the States indicated the need to broaden this cyber-security vision to the air navigation systems, taking into account the ADS-B systems, aeronautical information systems and air traffic control systems that can be vulnerable to cyber-attacks.

1.3 In this Meeting was analysed that, in addition to information protection, there are other aspects that the States must assure for the protection of their operations, internally and externally, for which it was necessary to implement security mechanisms in all aspects.

1.4 Due to a request of the States, ICAO NACC and SAM Regional Offices coordinated a cyber-security workshop in Mexico City in December 2018, in which the following sessions were developed:

1. Session I: International Initiatives and legal provisions regarding Cybersecurity. This session focused on the work done on cybersecurity by international organisations, and presented existing structures for coordination on cybersecurity issues and current guidance material and provisions on the subject concerning international civil aviation.
2. Session II: Air Navigation Services (ANS) Cybersecurity. This session focused on ANS, the area in which the concept of operations and supporting technology is probably changing more rapidly and where the framework of Cybersecurity recommendations is more developed.
3. Session III: Cybersecurity and airlines. The airline industry relies on computer systems extensively in their ground and flight operations. This session covered how airlines implement automation and new technologies and protect their systems against cyber-threats.
4. Session IV: Cybersecurity at airports. This session focused on securing airport systems and protecting the increasing amount of information and data that these systems manage.
5. Finally, there was also a breakout session in order to provoke the exchange of ideas and discuss the current regulatory framework on cybersecurity, potential initiatives in the NAM/CAR and SAM regions and the role that ICAO could play.

2. Discussion

2.1 As a result of the discussions it was concluded that cyber-security must be included in the security culture through training of air transport personnel (Air navigation services provider [ANSP], airlines and airports). Technology and Internet are affecting all type of non-suspicious equipment. The application of good basic practices can obstruct cyber-attacks that, although they represent minimal risks in security, can affect public confidence.

2.2 While new equipment may be better prepared for cyber-attacks, older equipment is still in use at airports, airlines and ANSP. Cyber-security is an interrelated matter that not only should be considered under Annex 17 – Security, because it also affects aerodromes, airworthiness or air navigation.

2.3 ICAO Regional Offices play a key role in cyber-security promotion among the States. They can facilitate the interaction of the States with programmes and initiatives on cyber-security of other international organizations, that can help building capacity (e. g. development of a national strategy on cyber-security), to coordinate the participation of the States in cyber-security exercises, or assisting carrying out risk assessments on cybersecurity.

2.4 The Meeting also provided a series of recommendations “Air navigation services provider (ANSP)” that are attached in the Appendix A to this Working Paper.

2.5 In this regard, the NACC and SAM Regional Offices have incorporated these activities in the following way:

1. NAM/CAR Region: has integrated all cybersecurity development and subjects in all the ANI/WG tasks forces as a complementary task to the terms of reference of these groups. Furthermore, the MEVA/TMG works on the development of a new MEVA phase that integrates security requirements, aeronautical databases interconnection and information security.

2. SAM Region: addressed this matter more specifically for the SAM States during the Twenty Second Meeting or the Coordination Committee (RCC/22) of the Regional Project RLA/06/901, in Lima, Peru, 5 to 7 March 2019, in which was adopted the following conclusion:

<table>
<tr><td colspan="2">Conclusion
RCC/22-4 ACQUISITION OF FIREWALL EQUIPMENT FOR REDDIG II</td></tr>
<tr><td>That the Secretariat:
a) At the request of REDDIG member States, and together with the ICAO TCB, purchase firewall equipment for REDDIG II;
b) The initial budget assigned for this acquisition would be USD 375,000.00.</td><td>Expected impact:
☐ Politician / Global
☐ Inter-regional
☐ Economic
☐ Environmental
☒ Technical/Operational</td></tr>
<tr><td colspan="2">Why:
To better protect the network against cyber attacks and unauthorised access.</td></tr>
<tr><td>When:
2019/2020</td><td>Status:
Underway</td></tr>
<tr><td colspan="2">Why:
RCC/22 Secretariat</td></tr>
</table>

2.6 Both regions have adopted carrying out activities through their aeronautical communication groups, but it is necessary to boost safety in every area that are part of the information and aeronautical services chain.

2.7 The need for States to implement mechanisms to allow the assurance of aeronautical operations now are necessary and it is required that the States of our regions start to work on this matter to face current menaces and to be prepare for future ones, in order to always assure continuous operation of activities. In this regard, NAM/CAR/SAM Regions propose the Regional Project of **Appendix B** to this Working Paper.

3. Suggested actions

3.1 The Meeting is invited to:

a) take note of this information

b) analyse the recommendations provided in Appendix A to this Working Paper; and

c) review and approve the proposal of the project in the Appendix B to this Working Paper.

— — — — — — — — — — —

APPENDIX A
AIR NAVIGATION SERVICES (ANS) RECOMMENDATIONS

1. States need to identify their communications, navigation and surveillance infrastructure that supports their air traffic services and, accordingly, identify their critical infrastructure vulnerable to cyber-attacks. Protect critical infrastructure must be a priority for States.

2. Automated systems such as Air Traffic Control (ATC) centres or aeronautical information systems, among others, base their operation on databases that support decisions based in real time information. These systems should be adequately protected to ensure the confidentiality, integrity and availability of the information.

3. The risk analysis on cybersecurity should encompass air traffic services and be carried out on a continuous basis, in order to provide States with a complete view of risks and threats on cybersecurity in air transport operations.

4. The new technologies implemented on air traffic services provide greater efficiency and simplify operations management. However, they could be vulnerable to new cyber threats and in order to mitigate this and ensure redundancy, States should review and update the technical and operational specifications of their systems.

5. Monitoring and analysing the exchange of information and the connections are essential to identify cyber-attacks and establish the adequate protection measures for air traffic systems.

6. States and industry should partner in order to adapt technical requirements to the development pace of new technologies and to ensure that hardware and software of air traffic systems are updated and prepared against cyber threats. Also, all interested parties (i.e. States, ANSPs and industry) need to collaborate in the design of the Standard Operating Procedures (SOPs) for ensuring an adequate protection of the operations.

7. The qualification and the adequate training of the personnel that manages ANS technical and operational areas are essential for a correct provision of the services. Staff should be knowledgeable and need to have the skills to carry out recovery plans in the event of a cyber incident.

— — — — — — — — — — —

CAR/SAM CYBER-SECURITY PROJECT PROPOSAL

CAR/SAM Region	PROJECT DESCRIPTION (PD)	PD N° C	
Programme	**Project Title**	**Starting Date**	**Ending Date**
New Programme (ICAO Coordinator: CAR Region: Mayda Ávila SAM Region: Francisco Almeida)	**Implementation of Cyber-security and Cyber-resilience mechanisms for Air navigation services** **Project proposal** Project coordinators: To be defined Experts supporting the Project: To be defined	September 2019	August 2020
Project objectives	1. To stablish the implementation status of **Cyber-security and Cyber-resilience** measures **of air navigation services of the States.** 2. To stablish a regional approach for the understanding of this matter. 3. To develop an analysis and implementation mechanism of **Cyber-security and Cyber-resilience** measures of air navigation services.		
Scope	The scope of the Project includes the assessment and identification of the principal service levels, establishment of databases and of all the equipment and services that are vulnerable to cyber-attacks internally and externally in the institutions and that is part of the air navigation services chain in the CAR/SAM States. To stablish a regional analysis mechanism that provides to the States information to identify risks and stablish necessary mechanisms to minimize or limit risks and assure the continuity of the service.		
Metrics	• The analysis of the 20 CAR States regarding their air navigation services. 14 States of the SAM region. • To stablish an action plan for each State. • To stablish a regional action plan.		
Goals	• The identification of risks regarding cyber-security and cyber-resilience for air navigation services of the CAR/NAM States. • To obtain regional statistics of identified threats. • To stablish regional training needs. • To stablish a regional action plan to support the national action plan on this matter. • To identify technical and operational requirements for the functioning of MEVA and REDDIG communication networks.		

CAR/SAM Region	PROJECT DESCRIPTION (PD)	PD N° C	
Programme	Project Title	Starting Date	Ending Date
Strategy	• The execution of the Project activities will be coordinated among members of the Project, the Project coordinator en the programme coordinator, primarily through teleconferences and eventual meetings that can be carried out according to the work plan. • The Project coordinator will coordinate as appropriate, with the programme coordinator, the requirements of other projects and of other information of the NAM/CAR implementation Tasks Forces. Additional expert would be included to the tasks and specialized works.		
Justification	• Nowadays, Air traffic control services demand a wider data sharing, not only between specific control centres but through an information cloud that could be access with a user-number to get or provide information in an unlimited number of virtual connections. Although the increase of information to create a better situational awareness also increases the risk of a cyber-attack. Increasing the use of technology increases the risk of cyber-attacks. • Today, the States require assuring that the systems that provide air navigation services, either with equipment, systems, or databases, have the necessary mechanisms to warranty their continuous operation based in its correct operation, quality of information, and harmonized interoperability with the operational requirements. To do so, the States must make a risk analysis identifying possible risks to their operations internally and externally, and having developed mechanisms to face these threats and reduce the risks. In this analysis the States must incorporate diverse aspects such as human resources, natural disasters, vulnerabilities and other threats within each State. • According with Doc 9854 “Global ATM Operational Concept”, the States must take action regarding aviation security and safety with the objective to eliminate intentional or no intentional threats, hackers, criminal acts, human resources errors, service interference and other possible threats. • The States must analyse and identify their threats, implement protection processes and how to response to these threats to define contingency processes to assure the continuity of their operations. • Facing this threat process, this project looks to support the States in the process to identify and analyse their threat and risks, supporting the development of the required action plans to eliminate or reduce their impact.		
Related Projects	This process is related to Programme D (ATN and their Ground-ground applications and Air-ground ATN), Phase IV of the MEVA network.		

— END —