SNMC/27 WP18

INTERNATIONAL CIVIL AVIATION ORGANIZATION
WESTERN AND CENTRAL AFRICA OFFICE

Twenty-seventh Meeting of the AFI Satellite Network Management Committee (SNMC/27)
(Ghana, Accra, 25-29 November 2019)

Agenda item 5: Cyber Safety and Resilience

CYBER SAFETY AND RESILIENCE OF AFISNET

(Presented by Ghana Civil Aviation Authority)

SUMMARY

This paper seeks to discuss the issue of cybersecurity and resilience of AFISNET as an emerging critical issue.

Action by the meeting is at paragraph 3:

DISCUSSIONS:

(a) Gap analysis on AFISNET (cyber vulnerabilities and mitigation the related risks);

(b) The protection of AFISNET against cyber threat in technical specification

(c) Provision with support of ICAO, technical and operational personnel with the adequate education and training in the matter.

REFERENCES:

Annex 17 — *Security — Safeguarding International Civil Aviation against Acts of Unlawful Interference* to the *Convention on International Aviation*
Doc 9750, *Global Air Navigation Plan 5th Edition*
Doc. 9854, *Global Air Traffic Management Operational Concept*
Doc 8973–Restricted, *Aviation Security Manual*
Circ. 330, *Civil/Military Cooperation in Air Traffic Management*
Doc 9855, *Guidelines on the Use of the Public Internet for Aeronautical Applications*

1.0 INTRODUCTION

1.1 Cybersecurity, which may be defined as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment as well as organizations' and users' assets; encompasses the protection of electronic systems from malicious attacks and the means by which the consequences of such attacks should be handled.

1.2 Cybersecurity is a growing concern for civil aviation, as the industry increasingly relies on electronic systems for critical parts of its operations, including safety-critical functions.

1.3 Therefore, it is necessary for States in the AFI region to ensure that the risks and threats of cyber-attacks on air navigation systems are eliminated by developing an adequate regulatory framework and by identifying and enforcing appropriate actions by all parties involved in the provision or operation of air navigation services.

2.0 DISCUSSIONS

2.1 AFISNET cybersecurity vulnerabilities cover critical information systems within the aviation eco-system. These include but are not limited to:

a) **ATM Systems** (includes systems that manage communication with airplanes during flight/ landing and Information Systems within an airplane including its communication systems)

b) The AFISNET Network

c) Data to and from AFISNET member states

2.2 CURRENT GAP ANALYSIS ON AFISNET

AFISNET lacks sufficient integrated and scalable adoption and application of systemic risk assessment:

a) Maintenance Personnel has insufficient knowledge about the risks facing critical infrastructure networks as well as the frequency and impact of cyber-attacks on the cumulative components systems and associated data.

b) The same is true for risk and impact across the AFI Region (organizations and sectors) that share common cyber resources.
c) In addition to a limited understanding of the correlation of risk across the ecosystem, we have an imperfect view of where risk is concentrated.
d) There is little understanding of how to roll up to assess cybersecurity risk exposure at larger scales, up through a macroscopic level

2.3 AFISNET RELATED RISK MITIGATIONS

Cybersecurity risk has a direct impact across the entire aviation industry. The nature of these risks requires a new approach in terms of ***actions***, ***learning from the safety approach taking into account the similarities and differences***.

Since the risk assessment methodology might suffer from the uncertainty of hostile actors,' intent and capability measurement, its outcomes should be mostly qualitative and subjective:

a) Security management should not only be a matter of understanding threats but also realizing how internal vulnerabilities could be exploited, not only those related to hardware and software, but also human weaknesses. In this field, the emerging capability of antagonists should be better investigated.

b) A real-time adaptive response in terms of countermeasures and remediation processes in a very reliable, efficient and timely manner. This therefore requires:

"The key to managing the AFI region's cybersecurity risks within the aviation sector, is to develop a 360 degree approach, a comprehensive strategy capable of predicting cyber risks to the aviation ecosystem, identifying and implementing suitable controls to prevent cyber risks, the capability to monitor / detect attacks and the ability to respond and recover from successful attack" elaborated as follows:

Predict "Predictive" capabilities that will enable the ANSP's to learn from external events via external monitoring of the hacker underground to proactively anticipate new attack types against the current state of systems and information that it is protecting, and to proactively prioritize and address exposures. This intelligence is then used to feedback into the preventive and detective capabilities, thus closing the loop on the entire process.

Prevent: "Preventive" strategies include policies, products, and processes that are put in place to prevent a successful attack. The key goal of this category is to raise the bar for attackers by reducing their surface area for attack, and by blocking them and their attack methods before they impact the enterprise.

Detect: "Detective" capabilities designed to find attacks that have evaded the preventive category. The key goal of this category is to reduce the dwell time of threats and, thus, the potential damage they can cause. Detection capabilities are critical because the enterprise must assume that it is already compromised.

Respond: "Responsive" functions are required to investigate and remediate issues discovered by detective activities (or by outside services), to provide forensic analysis and root cause analysis, and to recommend new preventive measures to avoid future incidents.

2.4 AFISNET can be effectively protected from threats by taking into account the following in the ***technical specifications*****:**

a) Secured hardware

Hardware should be operated by the newest and most sophisticated types of cybersecurity software to prevent real threats.

All devices should have a complicated password (to be shared by device user only)

Effectiveness of physically attaching computers to desks to prevent intruders from walking away with company equipment and the sensitive data they hold.

"Find My Device" to be installed on all computers and related test gears so that equipment that is stolen can quickly be located by the authorities.

b) **Encryption and backup of all data.**

The capability of all data (including employee information and all business data) to be backup to prevent physical access to sensitive data and rendering that data useless if it falls into the wrong hands.

The software should be activated and updated on all company devices

All computers should have automatic hibernation time of 5 minutes by default

c) **Robust anti-malware and firewall software: -**

Provision of optimized firewalls from vendors to prevent malware from entering computer systems.

d) Investment in cybersecurity insurance: -

Provision of specialist advice for cybersecurity insurance

e) Creation of security-focused workplace culture: -

Education of staff on the dangers of unsecured networks and unsecured websites

2.5 Provision with support of ICAO, technical and operational personnel with adequate education and training in the matter.

In order to promote and attain technical and operational needs in Cybersecurity; ICAO has provided a vision of a global aviation Cybersecurity strategy which can be achieved through:

a) Member States recognizing their obligations under the *Convention on International Civil Aviation* (Chicago Convention) to ensure the safety, security, and continuity of civil aviation, taking into account Cybersecurity;

b) Coordination of aviation Cybersecurity among State authorities to ensure effective and efficient global management of Cybersecurity risks, and

c) All civil aviation stakeholders committing to further develop cyber resilience, protecting against cyber-attacks that might impact the safety, security, and continuity of the air transport system.

2.6 The Strategy aligns with other cyber-related ICAO initiatives and coordinated with corresponding safety and security management provisions. The Strategy's aims will be achieved through a series of principles, measures, and actions contained in a framework built on **seven pillars**:

a. International cooperation

b. Governance

c. Effective legislation and regulations

d. Cybersecurity policy

e. Information sharing

f. Incident management and emergency planning

g. Capacity building, training, and Cybersecurity culture

3.0 ACTIONS TO BE TAKEN:

1. Urgent technical training for Maintenance Personnel in this matter
2. Development of a template for cybersecurity risk assessment
3. Cybersecurity and safety resilience promotion awareness programs for Maintenance Personnel for counter- actions
4. Information sharing between all AFISNET members

--END--