58th CONFERENCE OF DIRECTORS GENERAL OF CIVIL AVIATION ASIA AND PACIFIC REGIONS

Dhaka, Bangladesh
15 to 19 October 2023

AGENDA ITEM 5: AVIATION SECURIY AND FACILITATION

CREATING A CRISIS RESPONSE MANUAL FOR ADVANCED AVIATION SECURITY EQUIPMENT IN RESPONSE TO CYBER ATTACKS

(Presented by the Republic of Korea)

SUMMARY

Cyber attacks, including advanced threats like hacking, pose a significant threat to the civil aviation sector. With the proliferation of advanced aviation security equipment such as AI-based detection systems and remote central monitoring, vulnerabilities to cyber attacks have increased. This DP aims to suggest the development of operational guidelines for advanced security equipment and crisis-specific manuals on the ICAO level.

CREATING A CRISIS RESPONSE MANUAL FOR ADVANCED AVIATIN SECURITY EQUIPMENT IN RESPONSE TO CYBER ATTACKS

1. INTRODUCTION

1.1 During the COVID-19 pandemic, the aviation security field witnessed an increase in the use of non-contact and remote aviation security equipment. With the coming of endemic era, there has been a rise in the adoption of advanced aviation security equipment that can maximize operational efficiency, such as reducing passenger screening times, to cope with the surge in passengers.

1.2 Especially, advanced aviation security equipment such as AI-based detection systems and remote centralized screening systems operate on network-based systems. In the event of a cyber attack that disrupts the system, it can lead to the paralysis of the entire screening system, resulting in significant damage including passenger inconvenience and flight delays.

1.3 Furthermore, a possible hacking of advanced aviation security equipment could result in the screening images being manipulated, which could potentially allow prohibited items such as explosives to be brought onboard, posing a serious threat to security and safety of passengers.

1.4 Despite such far-reaching implications expected, the section 4.9 of ICAO Annex 17 mandates that each Contracting State identify and assess cybersecurity threats based on domestic standards. Therefore, there is a pressing need to establish internationally unified criteria to enhance the level of cyber security and strengthen the overall aviation security.

2. DISCUSSION

2.1 Currently, the sections 18.1 and 18.2 in ICAO's Aviation Security Manual Doc. 8973, provide definitions and protection guidelines for critical aeronautical information and communication technology systems, as well as a common framework for responding to cyber attacks. However, these sections do not adequately consider the physical and electronic characteristics of security screening equipment, which could lead to the application of varying standards by different countries.

2.2 Therefore, in order to enhance the international cyber security standards for aviation security screening, it is necessary to establish a new section "18.3 Security Protection of Aviation Security Equipment" that takes into account the characteristics and operational environment of security screening equipment. This new section will help develop cyber security standards for evolving security screening equipment while ensuring its cyber resilience.

2.3 For example, in the Republic of Korea, airport operators conduct their own security assessment when introducing advanced aviation security equipment. Additionally, the national cyber security oversight authority performs security suitability validation[1] based on internationally recognized common assessment criteria[2] (Common Criteria, ISO/IEC 5408), followed by Cryptographic Module verification[3].

2.4 Taking inspiration from such instances, incorporating the establishment and application of criteria for aviation security equipment and related devices, as well as security audit standards for

[1] "Security Suitability validation" refers to a system that verifies the safety of systems containing security functions, such as information protection systems and network equipment.

[2] "Common Criteria" refers to international standards for security certifications that outline common requirements for security features in various types of equipment.

[3] "Cryptographic Module verification" refers to the system verifying the safety and suitability of cryptographic modules introduced to protect business data in information and communication networks.

aviation security equipment, could be included in the cyber security standards.

18.3 Protection of Security Screening Equipment

18.3.X. Security screening equipment must adhere to the procedures outlined in section 18.2, taking into account their physical and electronic characteristics, as well as the operational environment specific to each airport. (Further development may be required)

18.3.X. Security screening equipment used in security screening areas must ensure cyber resilience through the following verifications

a. Appropriateness verification based on common criteria

b. Verification of cryptographic modules when the modules are included

18.3.X. The developed verification standards for security screening equipment and related to international cyber security management levels should be shared among contracting states.

18.3.X. Security screening equipment must undergo regular and irregular security audits, and the criteria necessary for security audits are referenced in Appendix X. (Development of Appendix X is required in the future.)

2.5 Furthermore, it is necessary to response measures and crisis-specific scenarios developed for a possible occurrence of a cyber attack on advanced equipment in ICAO's 'Cybersecurity Action Plan (CyAP).'

2.6 With the publication of the second edition of ICAO's 'Cybersecurity Strategy and Action Plan' in 2022, strategic objectives and detailed action items for aviation cyber security have been established at a higher level.

2.7 However, advanced aviation security equipment is rapidly evolving, and correspondingly, cybersecurity threats are also becoming more sophisticated. In response to this, there is a need for threat analysis and the development of crisis-specific response scenarios to address these challenges.

2.8 In the Republic of Korea, a cybersecurity crisis response system is being established, and regular trainings for cyber security crisis response at airports are being conducted.

2.9 Utilizing these validated systems, it is necessary to incorporate the development of scenarios for continued operation or operational recovery in the event of a cyber attack on advanced aviation security equipment as a new action item[4] under "Strategic Objective 6: Incident Management and Emergency Response Plans."

3. ACTION BY THE CONFERENCE

3.1 The Conference is invited to:

a) Propose reaffirming the support for ICAO's leadership on cybersecurity at the 58th DGCA, with a unified stance among Member States;

b) Propose the establishment of an ad-hoc group within ICAO CYSECP to discuss

[4] CyAP 6.X.
Identify cyber threat scenarios for advanced equipment that has already been introduced or is planned to be introduced and develop corresponding crisis response procedures.

topics such as developing operational guidelines and crisis response manuals for advanced equipment in preparation for cyber attacks; and

c) Propose that the Cybersecurity Ad-hoc group discuss the following cybersecurity response measures:

a. Propose the addition of section "18.3 Security Protection for Screening Equipment" in Doc. 8973, incorporating the following measures:

i) When introducing security screening equipment, perform security suitability verification and cryptographic module validation based on the international cyber security standards, the Common Criteria;

ii) During the operation of security screening equipment, conduct regular and irregular security audits, including software updates, to ensure continuous compliance with cybersecurity standards.

b. In the context of CyAP's "Strategic Objective 6: Incident Management and Emergency Response Plan," propose the development of a new sub-item "6.X: Identification of Cyber threat Scenarios and Corresponding Crisis Response Procedures."

— END —