International Civil Aviation Organization

WORKING PAPER

A42-WP/498
EX/224
28/8/25
(Information paper)
English only

ASSEMBLY — 42ND SESSION

EXECUTIVE COMMITTEE

Agenda Item 13: Aviation Security — Policy

STRENGTHENING CYBERSECURITY RESILIENCE IN CNS-ATM SYSTEMS

(Presented by Bangladesh)

EXECUTIVE SUMMARY

This paper highlights the growing need for robust cybersecurity in Communication, Navigation, and Surveillance / Air Traffic Management (CNS/ATM) systems across the Asia-Pacific region. As part of its modernization efforts, Bangladesh has implemented the Thales Seamless ATC TopSky system, including a new ATC tower and automated ATM center, significantly enhancing its air navigation capabilities.

Recognizing the cybersecurity risks associated with advanced digital infrastructure, Bangladesh has initiated several protective measures, including the integration of cybersecurity into system design, capacity building, governance reforms, and contingency planning. The paper emphasizes the importance of regional collaboration, proposing the creation of a coordinated cybersecurity framework under ICAO's guidance, and calls for shared policies, intelligence exchange, and joint training initiatives.

Strategic Goals:	This information paper relates to ICAO Strategic Goals: *Every Flight is Safe and Secure*.
Financial implications:	No significant financial implications are anticipated for States or ICAO.
References:	Annex 19 – *Safety Management* ICAO Global Air Navigation Plan (GANP) ICAO Global Aviation Safety Plan (GASP)

1. INTRODUCTION

1.1 With rapid advancements in aviation technology and increasing reliance on digital systems, maintaining cybersecurity in Communication, Navigation, and Surveillance / Air Traffic Management (CNS/ATM) has become a critical concern. The Asia-Pacific region, including Bangladesh, has witnessed significant modernization of ATM infrastructure to accommodate growing air traffic and to enhance safety and efficiency. However, these improvements also expose systems to heightened cyber threats.

1.2 This paper outlines the importance of strengthening cybersecurity resilience in CNS/ATM systems, highlights Bangladesh's initiatives including the adoption of Thales Seamless ATC TopSky and proposes a collaborative framework for cybersecurity preparedness and response across the region.

2. DISCUSSION

2.1 The modernization of ATM systems is crucial to meet ICAO's Global Air Navigation Plan (GANP) objectives. Bangladesh, in line with ICAO's Aviation System Block Upgrades (ASBU), has launched a comprehensive modernization programme involving the deployment of the Thales Seamless ATC TopSky system. This includes: a new 45-meter ATC tower at Hazrat Shahjalal International Airport (HSIA), a state-of-the-art ATM center equipped with automation facilities, and a Nationwide air surveillance and data communication enhancements.

2.2 While these advancements significantly improve air traffic services, they also expose the vulnerabilities of cyber-attacks that can disrupt operations, compromise safety, and affect national security.

2.3 **Cybersecurity Threat Landscape in Air Traffic Management (ATM)** ATM systems are deeply interconnected, relying on the seamless integration of data from radar systems, surveillance technologies, communication networks, and flight data processors. This intricate network is essential for maintaining safe and efficient airspace operations but also presents a significant cybersecurity challenge. As digital dependencies grow, so do the potential vulnerabilities. Potential cyber threats to ATM systems include:

a) *Unauthorized Access:* Intrusions into ATM systems or infrastructure by unauthorized entities may lead to information breaches, system manipulation, or service disruption.

b) *Data Corruption or Manipulation:* Altered or falsified flight or surveillance data can result in unsafe flight operations, navigational errors, or communication failures.

c) *Disruption of CNS Services:* Communication, Navigation, and Surveillance (CNS) services are critical to ATM. Malware infections or Denial-of-Service (DoS) attacks could degrade or disable these services, posing risks to flight safety.

d) *Compromised Communication Links:* Interference with communication between air traffic controllers and pilots can lead to miscommunication, delayed instructions, or complete communication blackouts—seriously endangering flight operations.

2.4 ***Evolving Digital Infrastructure in ATM*** As ATM services transition toward IP-based and cloud-enabled platforms, protecting the digital infrastructure becomes a shared responsibility among States. This migration increases the surface area for potential cyberattacks, making international cooperation,

standardized security frameworks, and robust cybersecurity strategies essential for maintaining safety and resilience in global air traffic management.

2.5 ***Bangladesh's Initiatives in Cybersecurity for CNS/ATM.*** Bangladesh has taken the following initiatives to secure its modernized air navigation systems:

a) *Deployment of Secure ATM Infrastructure:* Bangladesh has implemented the Thales TopSky Air Traffic Management (ATM) system as part of its efforts to establish a secure and resilient aviation infrastructure. This system is inherently equipped with robust cybersecurity features, including advanced firewalls, intrusion detection systems, and encryption mechanisms. These integrated safeguards are designed to protect critical ATM functions from cyber threats, ensuring the continuity and integrity of air traffic operations in compliance with international cybersecurity standards.

b) *Capacity Building:* Continuous efforts are being made to enhance the cybersecurity awareness and response capabilities of CNS/ATM technical personnel. These training programs are being continuously undertaken through collaborations with Thales and the Civil Aviation Authority of Bangladesh, ensuring that aviation professionals are equipped with the necessary skills to identify, prevent, and respond to cyber threats effectively.

c) *Incident Response Planning:* Development of an CNS/ATM-specific contingency plans, including cyber incident response protocols is underway.

3. REGIONAL AND INTERNATIONAL COLLABORATION NEEDS

3.1 The development of robust information-sharing platforms for cyber threat intelligence is crucial to enhance situational awareness, enable timely responses, and foster a culture of cooperation and trust among stakeholders. Bangladesh strongly advocates for the establishment of a Cybersecurity Coordination Group to facilitate collective efforts in addressing cyber risks within the regions. Bangladesh emphasizes the importance of developing comprehensive cybersecurity policies and guidelines to ensure consistency, foster harmonization, and strengthen alignment among Member States.

4. RECOMMENDATIONS

4.1 Bangladesh emphasizes the importance of tailored support from ICAO, particularly for States with limited technical capacity, to strengthen global aviation cybersecurity resilience. In this regard, Bangladesh encourages ICAO to enhance its guidance materials and provide customized assistance. It is recommended that Member States adopt a Cybersecurity Framework that aligns with ICAO's global cybersecurity strategy. To build sustainable capacity, national efforts should be supported through targeted training, technical assistance, and resource sharing. Additionally, integrating cybersecurity considerations into the State Safety Programme (SSP) and Safety Management Systems (SMS) for aviation service providers will ensure a holistic and proactive approach to aviation safety and security.

— END —