International Civil Aviation Organization

MIDANPIRG Communication, Navigation and Surveillance Sub-Group

Fourteenth Meeting (CNS SG/14)
(Abu Dhabi, UAE, 19 – 23 October 2025)

Agenda Item 3: CNS Planning and Implementation Framework in the MID Region

CYBERSECURITY THREATS TO CNS INFRASTRUCTURE

(Presented by UAE)

SUMMARY

This paper highlights the growing cybersecurity threats to Communication, Navigation, and Surveillance (CNS) systems resulting from increased interconnectivity, digitalization, and IP-based architectures. It outlines key vulnerabilities such as weak access controls, inadequate network segmentation, and insufficient monitoring, and discusses operational, safety, and financial impacts.

In addition, the paper integrates UAE's national aviation cybersecurity framework, notably the GCAA National Civil Aviation Cybersecurity Strategy, Policy, Guidelines, and the Reporting of Security Breaches (ROSB) mechanism, as a foundational example for harmonizing state-level governance with ICAO's Cybersecurity Action Plan (CyAP). It proposes that MID States adopt or adapt such national structures and collaborate on a CNS-specific awareness toolkit and reporting framework.

Action by the meeting is at paragraph 4.

REFERENCES

- ICAO Cybersecurity Policy Guidance (January 2022)
- ICAO Cybersecurity Action Plan (Second Edition, January 2022)
- ICAO Aviation Cybersecurity Strategy (Assembly Resolution A40-10)
- ICAO Doc 10097 – Manual on Cybersecurity
- GCAA National Civil Aviation Cybersecurity Strategy (UAE)
- GCAA Civil Aviation Cybersecurity Policy & Guidelines
- GCAA Reporting of Security Breaches (ROSB) mechanism
- MIDANPIRG/19 Conclusion 19/16 – Aviation Cybersecurity Coordination

1. INTRODUCTION

1.1 The modernization and digital transformation of CNS systems—including integration of IP networks, remote maintenance access, data exchange links, and shared infrastructure—has introduced new cyber risk vectors that must be managed proactively.

1.2 The United Arab Emirates, through the General Civil Aviation Authority (GCAA), has established a National Civil Aviation Cybersecurity Strategy, aligned with the UAE National Cybersecurity Strategy, to strengthen cyber resilience in aviation systems. This includes a Civil

Aviation Cybersecurity Policy, supporting guidelines, and a Reporting of Security Breaches (ROSB) portal for aviation stakeholders to report incidents securely.

1.3 This paper aims to raise awareness in the MID Region of cybersecurity threats specific to CNS infrastructure, to align national cyber governance models with ICAO's Cybersecurity Action Plan (CyAP), and to propose regionally harmonized awareness, reporting, and resilience-building measures.

2. DISCUSSION

2.1 The migration of CNS functions to networked, IP-based architectures (e.g., ADS-B over IP, digital ATC automation, remote system management interfaces) offers efficiency, scalability, and operational flexibility. However, such interconnectivity opens up exposure to network-level intrusions, malware deployment, supply-chain attacks, and insider misuse. Typical vulnerabilities include default system credentials, poor network segregation (flat networks), delayed patching, insecure remote connections, and lack of continuous monitoring.

2.2 In the UAE, the GCAA strategy establishes a governance model coordinating civil aviation cybersecurity efforts with national authorities (National Cybersecurity Council, State Security, Ministry of Interior, Ministry of Defense). This ensures that aviation systems are part of the national cybersecurity posture and that relevant agencies collaborate on threat intelligence and incident response.

2.3 The GCAA policy and guidelines promote security-by-design, defense-in-depth, and risk-based controls in civil aviation systems, including CNS components.

2.4 Another key element is the ROSB (Reporting of Security Breaches) portal, which GCAA provides to support timely, confidential reporting of cybersecurity incidents by aviation stakeholders. This mechanism encourages early detection, sharing of indicators of compromise, and coordinated response. For CNS systems, integrating ROSB or equivalent incident reporting channels is critical to build collective awareness and facilitate cross-State cooperation.

2.5 In line with ICAO's CyAP, the UAE's approach emphasizes governance, incident management, and cybersecurity culture. For CNS systems, that means ensuring that states adopt clear cybersecurity roles and responsibilities, integrate CNS cyber risk into national aviation safety and security programs, and establish incident response capabilities aligned with civil aviation and national cyber frameworks.

2.6 From a technical and operational standpoint, CNS systems should adopt strong identity and access management (IAM), network segmentation (e.g., separating maintenance networks from operational CNS networks), intrusion detection and prevention systems (IDS/IPS), secure remote access (e.g., VPNs with multi-factor authentication), endpoint protection, and regular vulnerability scanning and patch management. CNS operators should also conduct regular penetration testing and audits of network and system architectures.

2.7 Further, in CNS-specific context, achieving high integrity of data paths is crucial: encrypted data flows, integrity checks, and logging must be enforced to detect tampering or replay attacks. State and ANSP-level fusion systems (e.g., combining radar and ADS-B feeds) should include anomaly detection, cross-checking among sensors, and fail-safe modes when suspicious data entered.

2.8 Perhaps most importantly, cybersecurity culture and awareness must be embedded across all roles. In the UAE, GCAA encourages operators and stakeholders to adopt cybersecurity training, including phishing awareness, password hygiene, handling removable media, secure configuration, and reporting of anomalies through ROSB. For CNS personnel (operations, engineering, maintenance), dedicated, role-based training should be mandated, along with periodic drills and simulated cyber-incident tabletop exercises.

2.9 Regional collaboration is essential. Sharing anonymized incident summaries, threat intelligence, and lessons learned among MID States (via ICAO/ MID Office, CNS SG channels) fosters a stronger regional posture. States are encouraged to adopt or reference national cybersecurity strategies (such as the UAE's GCAA model) and align CNS cybersecurity governance with national frameworks and ICAO CyAP.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the enhanced national cyber framework of UAE including GCAA's cybersecurity strategy, guidelines, and ROSB portal, and consider their applicability to CNS infrastructure in the MID Region;

b) encourage MID States and ANSPs to develop or strengthen national civil aviation cybersecurity strategies, policies, and guidelines, aligned with ICAO's Cybersecurity Policy Guidance, and incorporating CNS cyber risk;

c) promote the deployment of secure and confidential cybersecurity incident reporting mechanisms (similar to ROSB) for CNS and aviation stakeholders, with mutual information-sharing among States for trend analysis;

d) initiate MID Regional Cybersecurity Awareness Toolkit for CNS systems, containing role-based training modules, phishing simulations, and best practices tailored to CNS operations; and

e) recommend States integrate CNS cybersecurity governance within their national aviation safety and security oversight systems, and align with states national cyber authority structures as exemplified by the UAE approach.

-- END --