2026

Committee on Aviation Security

Topic 2

Director – Sonia Hifdi

Conflict : Hybrid Threats to Civil Aviation — Safety, Capacity and Resilience.

A New Dimension of Conflict: The Hybrid Threat to Aviation.

Contemporary adversaries — whether non-State armed groups, or organized criminal networks — no longer rely solely on kinetic force. They deploy **hybrid strategies** combining conventional military action, cyber operations, electronic warfare, and deliberate manipulation of information systems. Civil aviation, as a globally interconnected and data-dependent industry, is one of the prime targets of this evolving threat landscape.

A single hybrid event can simultaneously compromise **safety** (by corrupting navigation or surveillance data), **capacity** (by disrupting ATM or airport operations), **efficiency** (by degrading communication systems), and **business continuity** (by destroying operational and commercial data). The GNSS spoofing campaigns over Eastern Europe and the Middle East and the sustained GNSS jamming over the Red Sea corridor illustrate how these threats have already materialized.

Key Information Security Threats.

GNSS RFI (Radio Frequency Interference) Spoofing and Jamming. Global Navigation Satellite System interference (particular RFI)— signal denial (jamming) or false signal injection (spoofing) — has emerged as the most acute hybrid threat to aviation. Covert, low-cost, and highly deniable, it can cause aircraft to navigate to incorrect positions, trigger false TCAS advisories, and compromise RNP approaches. ICAO has documented a sharp increase in interference events since 2022, concentrated in conflict-affected regions. Information on current interferences are available on different websites as https://gpswise.aero/map

Cyber Attacks on ATM and Airport Systems. ATM infrastructure, airport OT networks, and airline IT systems are high-value targets. A coordinated attack on a major ANSP can degrade surveillance, disrupt flight data processing, and impose flow restrictions across a wide area. In conflict-zone contexts, such attacks may be timed to amplify kinetic operations. The September 2025 Collins Aerospace ransomware attack illustrated the sector's vulnerability.

Disinformation and ADS-B Manipulation. The deliberate injection of false NOTAMs, SIGMET messages, or airspace status notifications can induce aircraft to enter dangerous airspace. Separately, ADS-B — which transmits position data on an unencrypted, unauthenticated basis — is inherently vulnerable to spoofing, enabling malicious actors to create phantom aircraft or mask real ones, generating confusion in ATM systems at critical moments. ADS-B spoofing is considered as a RFI spoofing.

Impact on Safety, Capacity, Efficiency and Business Continuity.

The convergence of these threats imposes cascading costs across the aviation system. On **safety**: GNSS spoofing can cause controlled flight into terrain or loss of separation; ATM Information Security attacks degrade controller situational awareness; corrupted maintenance data compromises airworthiness. On **capacity and efficiency**: RFI has already forced the closure of large volumes of airspace, compressing traffic into residual corridors and generating significant delays and fuel penalties. On **business continuity**: ransomware attacks disrupt check-in, boarding, and operational control with network-wide effects; prolonged recovery, reputational damage, and regulatory liability threaten smaller operators' viability. The interconnected nature of global aviation means that a local disruption can propagate across the entire network.

The International Legal and Institutional Framework.

The primary regulatory framework is provided by **Annex 17**, the provisions of Annex 10 and Annex 11 relating to system integrity, and ICAO's **Aviation Cybersecurity Strategy (2019)**. The Beijing Convention (2010) extends the definition of unlawful interference to include cyber-attacks, including

on ATM. UNSCR 2309 (2016) calls upon States to share threat information but provides no specific mechanism for information security events in conflict zones.

At the regional level, certain regulations such as EU PART-IS or NIS2 provide frameworks for reporting information security incidents and vulnerabilities. However, no equivalent global mechanism exists, and the attribution of hybrid attacks to specific actors — a precondition for legal remedy — remains exceptionally difficult.

Since the impacts can vary, an **Integrated Risk Management (IRM)** approach is desirable and relevant.

Analysis and Proposals for the Committee.

Considering the hybrid nature of contemporary threats to civil aviation in conflict zones and their potential impact on **safety, capacity, efficiency and business continuity**, you are invited to reflect on the respective roles of ICAO, Member States, military authorities, and industry in developing a resilient and coordinated response.

You will make recommendations to the Council, in the perspective of the 43rd ICAO Assembly, encouraging ICAO, States, military authorities, and industry to address the following matters:

- Considerations on the development of a common framework for classifying hybrid threats to civil aviation within ICAO's mandate, covering GNSS RFI, cyber attacks, ADS-B manipulation, and disinformation, and on the sharing of relevant findings with the UN Security Council;
- Establishment of a mandatory, standardized Integrated Risk Management approach by assessing impacts on **safety, capacity, efficiency and business continuity;**
- Considerations on the strengthening of civil-military coordination for information sharing in conflict-zone contexts, in line with Resolution A42-4, including real-time notification protocols between defence authorities and ANSPs;
- Considerations on international guidance for business continuity planning for ANSPs, airlines, and airport operators under hybrid conflict scenarios, drawing on existing frameworks;
- Targeted capacity-building programmes to enable States to detect, report, and mitigate hybrid information security threats to civil aviation, in coordination with ICAO Regional Offices and in the spirit of the ICAO Strategic Goal *No country left behind*; and
- Accelerating the development and adoption of authentication and integrity protection principles for safety-critical data links, including ADS-B and GNSS augmentation systems, and considerations on how progress should be reported to a subsequent Assembly.

Bibliography

ICAO. Risk Assessment Manual for Civil Aircraft Operations Over or Near Conflict Zones (Doc 10084). https://www.icao.int/sites/default/files/Security/SFP/Documents/Doc.10084.Third-edition.pdf

ICAO. Guidance on Operations Over Conflict Zones. https://www.icao.int/safety/conflictzones

Transport Canada. Safer Skies Initiative. https://tc.canada.ca/en/initiatives/safer-skies-initiative

EASA. Conflict Zone Information Bulletins (CZIB). https://www.easa.europa.eu/en/domains/air-operations/information-on-conflict-zones

ICAO. Assembly Resolution A42-4 – Addressing Risks to Civil Aviation from Conflict Zones.

https://www.icao.int/news/icao-statement-safety-and-security-aviation-operations