International Civil Aviation Organization

A42-WP/165[1]
EX/83
24/7/25

WORKING PAPER

ASSEMBLY — 42ND SESSION

EXECUTIVE COMMITTEE

Agenda Item 13: Aviation Security — Policy

STRENGTHENING GOVERNANCE AND MANAGEMENT OF DIGITAL AND CYBERSECURITY THREATS TO CIVIL AVIATION

(Presented by the International Coordinating Council of Aerospace Industries Associations (ICCAIA) and International Federation of Air Line Pilots' Associations (IFALPA))

EXECUTIVE SUMMARY

Civil aviation increasingly relies on interconnected digital technologies and systems, including those that directly control or influence physical and operational processes. Although these technologies bring major benefits, they also expose the sector to intentional, unintentional and natural digital threats, as well as vulnerabilities that can amplify such threats and endanger critical operations.

Most ICAO frameworks — whether in safety, security, or operational domains — were not originally designed to address the systemic and cross-cutting nature of digital threats, which now span across emerging digital capabilities and interdependencies. The most pressing gap concerns intentional and malicious acts that straddle the boundaries of Security and Safety.

This paper invites ICAO, as a first step, to establish an internal, coordinated governance and management framework on digital threats, aligning its safety, security, and operational domains, with an initial focus on intentional and malicious threats. As a complementary step, it encourages ICAO to accelerate the development of guidance and global standards necessary to achieve a coherent and effective level of security performance across the aviation ecosystem.

Action: The Assembly is invited to:

a) Acknowledge that all categories of digital threats — whether intentional, unintentional, or natural — pose risks to civil aviation and must be addressed through a comprehensive governance approach, to be first established within ICAO to ensure coherence and effective support to States and Industry;

b) Request the ICAO Council, to initiate the establishment of an internal multi-domain and multidisciplinary governance framework for digital threats within ICAO;

c) Encourage ICAO to accelerate the development of guidance and, where appropriate, Standards and Recommended Practices (SARPs) to establish a systemic, harmonized, and adaptive baseline of digital security for all States and stakeholders; and

d) Recommend that ICAO strengthen awareness and communication on the coordinated treatment of digital threats through its regional networks, to support harmonized action and globally effective security performance.

[1] English, Arabic, Chinese, French, Russian and Spanish versions provided by ICCAIA and IFALPA.

Strategic Goals:	This working paper relates to Strategic Goal of *Every Flight is Safe and Secure*.
Financial implications:	None.
References:	A41-19 Addressing Cybersecurity in Civil Aviation Annex 17 — *Aviation Security* Annex 19 — *Safety Management*

1. INTRODUCTION

1.1 Digital transformation has enhanced civil aviation performance. Yet greater digital dependency reveals—and creates—vulnerabilities driven by rising interconnectivity and systemic complexity.

1.2 This evolution creates organizational and governance challenges due to responsibilities shared across ICAO domains, including safety, security, capacity, and efficiency, illustrating a broader need for holistic and coordinated governance.

1.3 Among the various categories of digital threats, intentional and malicious acts - commonly referred to as cybersecurity attacks - are particularly urgent to address due to their potential to disrupt critical aviation systems and the current uncertainty regarding responsibilities across safety and security domains.

1.4 This shift also highlights the absence of a global framework for systematically implementing a "security by design" and threat-informed approach through dedicated guidance and standards across all domains. In the absence of harmonised approaches, interim coordination mechanisms may be needed to support early action, especially in high-risk operational contexts.

1.5 Digital threats—defined as any potential or actual harmful event originating from or facilitated by digital capabilities—have begun to receive attention within ICAO panels and working groups. However, many of these threats remain insufficiently addressed, particularly when they do not align with conventional definitions of unlawful interference or safety hazards. This is particularly true for intentional and malicious threats that fall at the intersection of ICAO domains, leading to uncertainty regarding accountability, oversight, and coordinated response.

2. DISCUSSION

2.1 Digital threats to civil aviation encompass a wide range of events. These threats can be intentional (malicious or not), unintentional (human error, misconfiguration), or natural (environmental events). They can originate from digital, physical, or hybrid vectors and affect both digital elements and the physical systems that rely on them, thereby compromising aviation safety, security, and operational continuity. Understanding these broad categories is only the first step; the sector must also confront how the ongoing digital transformation amplifies their complexity.

2.2 Digital transformation is reshaping the aviation ecosystem by introducing not only new technologies but also new modes of failure, exposure, and dependency. Many of these risks are not adequately captured by traditional ICAO domain frameworks — starting with, but not limited to, those related to safety and security. The absence of a global structure leads to uneven responses, fragmented responsibilities, and a lack of shared understanding—conditions which undermine protection and resilience.

2.3 Beyond increasing exposure to malicious acts, digital transformation introduces structural complexities that challenge existing governance and risk/event management frameworks. It creates opaque

Information Technology (IT)/ Operational Technology (OT) interdependencies, supply-chain exposures and a pace of change that outstrips certification cycles. Legacy avionics now depend on cloud, Artificial Intelligence (AI) and Internet-Protocol (IP) links whose third-party components update monthly, injecting vulnerabilities beyond traditional controls. Innovation advances in months, whereas regulation evolves over years, making mitigations obsolete and widening State-level divergence. Lacking a shared taxonomy and incident-sharing mechanism, the community sees only fragments of the problem, delaying proportionate safeguards.

2.4 The absence of dedicated global guidance and SARPs founded on a "security by design" and threat-informed philosophy means there is no harmonized, systemic approach to addressing digital threats across all domains. This lack of a common performance baseline for States creates a vulnerable systemic context, setting the stage for threats deliberately engineered to exploit this very complexity.

2.5 Against this backdrop, intentional and malicious threats warrant special attention. Often complex, dynamic, and difficult to attribute, these threats are designed to exploit digital dependencies to cause operational degradation or disruption. Their unique characteristics may place them within, across, or beyond traditional aviation classifications, creating challenges for detection, reporting, and response.

2.6 Operational experience shows that some malicious digital interference does not fall clearly within existing domains' frameworks. A notable example is the intentional GNSS signal spoofing, which involves broadcasting counterfeit positioning signals that mislead an aircraft's navigation systems without requiring physical access or visible intrusion. Although intentional and capable of directly affecting flight operations, such actions may not meet the criteria for unlawful interference as defined in Annex 17, nor trigger a mandatory safety occurrence report under Annex 19.

2.7 This regulatory blind spot not only limits situational awareness and coordinated response but, more importantly, demonstrates the compelling need for a governance and management framework that integrates these new forms of digital interference, establishes clear reporting thresholds, and unambiguously defines institutional roles between the safety and security domains.

2.8 In the current absence of a coordinated international framework, States and regional authorities have begun to adopt diverse regulatory approaches. This growing divergence introduces complexity for aviation stakeholders, including manufacturers (OEMs), suppliers, and service providers, who must navigate heterogeneous compliance environments.

To meet this challenge, a dual approach is necessary:

- A comprehensive and holistic strategy capable of covering the full spectrum of digital threats—intentional, unintentional, and natural.
- A focused and prioritized effort on intentional and malicious threats, given their urgency, potential severity, and current regulatory misalignment.

3. CONCLUSION

3.1 Strengthening protection against digital threats is essential to sustaining the safety, security, capacity and efficiency of civil aviation. As digital dependencies continue to grow across systems and domains, so too does the need for coordinated, forward-looking governance.

3.2 To meet this challenge, ICAO and its stakeholders must pursue a clear dual objective:

- Adopt a holistic approach that addresses the full spectrum of digital threats—whether intentional, unintentional, or natural.
- Prioritise the treatment of intentional and malicious threats, which currently pose the greatest risk of uncertainty regarding roles and coordination among relevant ICAO domains.

3.3 By fostering alignment across domains, advancing interim instruments, and building a common understanding, ICAO can play a central role in ensuring a coherent, adaptive, and globally consistent response to evolving digital risks.

3.4 This effort could be directed by the existing Ad Hoc Cybersecurity Coordination Committee (AHCCC), by assigning it a specific governance mandate—a role it currently lacks.

— END —