International Civil Aviation Organization

LC/40-WP/2-7
12/9/26

WORKING PAPER

LEGAL COMMITTEE – 40TH SESSION

(Montréal, 26 – 30 October 2026)

Agenda Item 2 Consideration of the General Work Programme of the Legal Committee

CYBER SECURITY VULNERABILITIES OUTSIDE THE SCOPE OF CURRENT AIR LAW

(Presented by South Africa)

1. INTRODUCTION

1.1 Considering the rise of cybersecurity attacks, associated threats towards civil aviation, and complexities around management, enforceability, and applicability of the current international legal instruments, it is critical that States increase their paces to examine current legal international instruments and close legal gaps that are hindering effectiveness of measures that can be taken to enforce and deter cyber security related offences.

1.2 While cybersecurity attacks are prevalent, there are several complexities that make it difficult to identify, deter, and prevent perpetrators and take necessary legal action. This paper examines those complexities which will require multi prompt approach and commitment from States to avail resources to resolve.

2. DISCUSSION

2.1 International aviation law framework is being tested by threats it was not originally designed to manage. The issue is not that international aviation law has become irrelevant; rather, there are identifiable gaps in attribution, jurisdiction, enforcement, liability, information-sharing, and treatment of cyber security attacks. This is based on the increasing exposure to a combined threat environment involving the following:

a) Sponsored cyber operations and politically motivated disruption;
b) Ransomware and attacks against airport check-in, baggage, airline, and ground-handling systems;
c) Global Navigation Satellite System (GNSS) interference and spoofing;
d) Drones, missiles and air-defence systems operating near civil air routes;
e) Disruption of air-navigation services, communications, and aviation supply chains;
f) Hacktivist and proxy activity where the sponsors may be difficult to prove; and
g) Rapid changes to airspace availability during times of crisis.

2.2 ICAO treats these risks as interconnected rather than as separate “safety”, “security” and “cybersecurity” matters. The interlinking of this risk is well articulated through the ICAO Global Cyber Risk Considerations (Doc 10213).

2.3 The wider legal concern is also reflected in ICAO's recent recognition as contained in the Gap Analysis on the Need for Aviation Cybersecurity Standards and Recommended Practices report which gives recognition to the work and findings of the Task Force on Cybersecurity Standards and Recommended Practices stating that existing legal protection has not been sufficient by itself to protect civil aircraft during times of cyber-attack related crisis. This is underpinned by an urgent need for rapid-information sharing, stronger risk assessment, and coordination amongst various stakeholders at national and international level when a cyber-attack event ensues.

2.4 **Identified Gaps**

2.4.1 Cyberattacks are not always clearly classified based on international legal instruments as acts of unlawful interference. Cyberattacks that impact civil aviation safety and security often raise the following questions:

a) When does disruption of air-navigation or airport systems amount to an attack on civil aviation rather than ordinary cybercrime?
b) What level of disruption constitutes a threat to aviation safety and security?
c) How should a cyberattack be treated when it causes economic disruption but no physical damage or aircraft accidents?

2.5 The current international legal framework is defined around traditional physical acts such as hijacking, destruction of aircraft, or attacks against aviation facilities than for cyberattacks that may initially affect data integrity or passenger processing.

2.6 **Attribution remains the central weakness**

2.6.1 While investigators may identify the infrastructure, malware family, or operational pattern used in an attack, proving who is the party responsible for the attack is more complex and difficult. This creates a practical accountability gap where:

a) A proxy group conducts the operation;
b) Infrastructure is located in several countries;
c) The group uses compromised systems belonging to innocent third parties;
d) A State provides support but does not openly direct the specific operation;
e) The victim's State cannot publicly disclose intelligence supporting its conclusion; and
f) The attacker denies involvement and benefits.

2.7 Cyberattacks are sophisticated, and they do not conform to the conventional ways of safety and security forms of attack.

2.8 **Jurisdiction is fragmented**

2.8.1 A single aviation cyber incident may involve the following:

a) The airport or airline in different affected States;
b) A cloud provider in another country;
c) A software or equipment supplier in a different country;
d) Attack infrastructure in several jurisdictions;
e) Passengers from numerous nationalities; and
f) An attacker or proxy group operating from a State unwilling to cooperate

2.9 **Liability and compensation**

2.9.1 While the *Convention for the Unification of Certain Rules for International Carriage by Air* (Montreal, 1999) establishes important airline liability rules, it was not designed as a comprehensive cyber-risk allocation instrument. Difficult questions that arise from a cyberattack include the following:

a) Who pays for passenger losses caused by a cyberattack on an airport?
b) Is flight cancellation caused by ransomware treated as an extraordinary circumstance?
c) When is an airline liable for failure to maintain cyber resilience?
d) What responsibility does an airport, air-navigation service provider, cloud provider, or equipment supplier carry?
e) How should liability be allocated when several organisations contributed to vulnerability?
f) Does a cyber-attack affecting baggage or check-in systems create the same legal consequences as an attack affecting aircraft safety systems?

2.10 The absence of a harmonised international legal framework that covers issues relating to supply-chain liability and cyber-related operational disruption can lead to inconsistent outcomes between jurisdictions.

3. CONCLUSION

3.1 Existing international civil aviation instruments do not create a complete, centralized jurisdictional system for investigation, prosecution and compensation of victims for cross-border aviation cyber incidents. In practice, responsibility may be divided between national criminal law, aviation regulation, data-protection law, telecommunications law, contract law, and international law.

3.2 It is necessary for ICAO to take steps to galvanise resources through States in order to develop a comprehensive legal framework that will consider all permutations and challenges that are associated with cyber security incidents.

4. ACTION BY THE COMMITTEE

4.1 The Legal Committee is invited to:

a) Acknowledge the work currently undertaken to analyse the applicability of the current international legal instruments to address challenges associated with cyber security incidents that affect civil aviation safety and security; and

b) continue the work towards assessment of an international legal framework that will cover not only the traditional safety and security threats but also consider the less visible and increasingly complex risks associated with cyberattacks

— END —