International Civil Aviation Organization

AN-Conf/14-WP/124[1]
29/6/24

WORKING PAPER

FOURTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 26 August to 6 September 2024

Agenda Item 4: Hyper-connectivity of air navigation system
4.2 Cybersecurity and information system resilience

REGULATORY CYBERSECURITY GUIDELINES FOR AIR TRAFFIC SERVICES (ATS)

(Presented by Argentina, co-sponsored by 19 Latin American Civil Aviation Commission (LACAC) Member States[2])

EXECUTIVE SUMMARY

This paper presents considerations for the harmonization of air traffic services (ATS) regulatory provisions, with the aim of including specifications, methods and procedures relating to possible malware attack scenarios against ATS, in order to ensure the continuous monitoring of initial and refresher training for personnel.

Action: The Conference is invited to:
a) support the initiatives presented in this working paper, while requesting an analysis of the utility of incorporating cybersecurity regulations and methods for ATS into the global aviation framework; and
b) encourage States to integrate their national cybersecurity strategies with ICAO civil aviation strategies in order to create a cybersecurity culture in the ATS, incorporating policies, strategies and mechanisms as safeguards through the development of the proposed regulatory provisions.

1. INTRODUCTION

1.1 The increasing use of state-of-the art, globally interconnected technology in civil aviation has led to a notable increase in the risk of cyber threats.

1.2 The 41st Session of the International Civil Aviation Organization (ICAO) Assembly recognized the importance of the issue by incorporating Assembly Resolution A41-19: *Addressing Cybersecurity in Civil Aviation* into *Assembly Resolutions in Force (as of 7 October 2022)* (Doc 10184), Part VII — *Unlawful interference; Other matters related to unlawful interference*. It calls upon States to take a number of actions; some of these actions should be approached using regulatory tools, thereby addressing current concerns in the aviation community about the efficacy of the existing standards,

[1] Spanish version provided by Argentina.
[2] Aruba (Kingdom of Netherlands), Belize, Chile, Colombia, Costa Rica, Cuba, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Uruguay, Venezuela (Bolivarian Republic of).

procedures and processes when it comes to maintaining an acceptable level of risk in a digitally connected environment.

1.3 According to an article published in 2019 by the ALLIANZ Group entitled "Risk Barometer: Top Business Risks*"* (quoted in the seventh edition of the Global Air Navigation Plan (GANP, Doc 9750)), the most dreaded types of *Business Interruption* (BI) are *ransomware* cyberattacks.[3] *WannaCry* and *Petya* are two examples of *ransomware* used to attack digital systems in the European Union. However, it is interesting to highlight that the article mentions that 12 per cent of cyber BIs occur as a result of criminal cyberattacks, whereas 88 per cent are due to technical breakdowns or errors caused by human interaction with the systems.

1.4 All of the civil aviation stakeholders have made great collaborative efforts to protect and safeguard the air navigation system against acts of unlawful interference, prioritizing risk management and system cyber resilience. In this context, the civil aviation regulatory bodies play a fundamental role that should keep evolving. That is to say, beyond the regulations currently in force, it would be beneficial to offer scalable, flexible innovations, especially in view of the new business models under development in which the focus should be business-to-business and/or business-to-consumer[4]. Accordingly, the regulations should set out the performance standards necessary for this new context rather than retaining their previous function of specifying individual technical components in great detail.

1.5 Therefore, the regulations should facilitate and promote innovation, fulfil the performance requirements and support the evolution of the air navigation system, while also ensuring monitoring and oversight. From this point of view, the new regulatory paradigm in many ways represents a transition from a centralized system designed for only two actors (the State regulatory body and the air navigation services provider (ANSP)) to a distributed, coordinated regulatory system that offers services adapted to the needs of a cyber-resilient infrastructure and the identified needs of users.

2. DISCUSSION

2.1 In view of the above, we present a number of considerations that promote the alignment and harmonization of the ATS regulatory provisions. Our aim is to analyze the proposal to include specifications and procedures relevant to possible *malware* attack scenarios against information systems, while addressing the needs of all involved stakeholders and providing continuous oversight of initial and refresher training to ensure that personnel maintain the necessary skills.

2.1.1 The scenario of a cyberattack against civil aviation is classified as unlawful interference in accordance with Assembly Resolution A41-19: *Addressing Cybersecurity in Civil Aviation* and because of its criminal nature.

2.1.2 Technological advances and the interconnection of air navigation systems are aimed at safety, but they potentially create the conditions under which unlawful interference can affect not only the aircraft, but also the ATS dependencies.

2.1.3 The Annex 11 — *Air Traffic Services* Standards and Recommended Practices (SARPs) and the methods set out in the *Procedures for Air Navigation Services — Air Traffic Management* (PANS-ATM

[3] *Ransomware is a type of malware that encrypts a user's archives and then demands a ransom in order to restore them.*
[4] *GANP Online. Emerging, new and adapted business models, ICAO: https://www4.icao.int/ganpportal/GanpDocument#/lessons/WWfUWzbjlhwCVRRkMTd9NRWaFjpHfZxp*

, Doc 4444) view unlawful interference through actions or procedures if an aircraft is, or is suspected to be, the object of unlawful interference.

2.1.4 The aforementioned documents do not address the case of a potential attack on the ATS dependency systems. Therefore, it may be essential to incorporate ICAO regulatory or technical guidance for the ATS dependencies affected by cyberattacks in order to provide adequate procedures for appropriate responses to such events. We propose to study the scenario of unlawful interference in ATS in order to develop specific measures for countering cyberattacks.

2.1.5 With this in mind, and in accordance with the ICAO Cybersecurity Action Plan, we suggest analyzing whether or not it is viable to incorporate specifications and/or procedures for informing the State-designated competent authority in cases where a cyberattack on an ATS dependency is suspected or confirmed, enabling a timely exchange of relevant information among all of the involved stakeholders, especially air operators.

2.1.6 Moreover, we believe it could be essential to establish mechanisms for the exchange of cybersecurity information between the military authorities and the ATS so that relevant information can be shared. Such a collaborative approach would contribute to mitigating the risk of cyberattacks in ATS.

2.2 Additionally, and on the basis that the Cybersecurity Action Plan indicates the need to "*pursue regulatory harmonization at the global, regional and national level in order to promote global coherence and ensure interoperability of protection measures*"[5], we note there is a need to include specific regulatory provisions, without prejudice to the adoption of other provisions related to the issue, including the following:

a) procedures addressing cyberthreat and cyberattack scenarios at the regional level, since this would provide a way to address the economic and technological differences that some States handle alone, especially considering that the impact of a cyberattack or cyberthreat usually goes beyond State borders;

b) adequate instruments to provide a link between the State cybersecurity strategy and the ICAO guidelines set out in the *Aviation Cybersecurity Strategy*, thereby ensuring that domestic civil aviation makes provision for a policy, strategy, training, and the costs associated with implementation of such strategy. Also included would be the designation of the competent authority for civil aviation cybersecurity and an indication of how this authority will interact with the national organizations and other interested stakeholders;

c) provisions concerning the security of the State air navigation systems, with architecture ensuring their integrity and protection. This could include methods for reporting, oversight and the conduct of forensic analyses[6] of cyber incidents specific to civil aviation;

d) provisions on training to promote a cybersecurity culture in the ATS and to provide adequate training to all personnel involved in the air navigation system. Along these lines, it would be essential to make provision for projects to train said personnel;

[5] *Cybersecurity Action Plan, Chapter 3, Strategic Action Plan, Pillar 1: International Cooperation, ICAO, 2022 edition*.

[6] Forensic cybersecurity analysis is a discipline used to investigate and analyze information security incidents. These include cyber-attacks, data theft and intrusions.

e) specific ATS contingency measures for handling these situations and ensuring a rapid recovery of operations, including recovery actions for cyber incidents and the identification of key stakeholders for effective communication and coordination during a crisis; and

f) protocols for detecting and notifying of cyber incidents establishing clear procedures for the early detection and timely notification of any cybersecurity incident affecting the ATS dependencies. This would ensure a rapid and coordinated response to any threat, thereby reducing the potential impact of cyberattacks on the safety and continuity of flight operations.

3. CONCLUSION

3.1 Cybersecurity in ATS is a concern necessitating coordinated actions at the national, regional and global levels. The uptake of the proposals set out in this paper represents a significant step towards enhancing the security of the service and the mitigation of risks associated with cyberattacks in ATS dependencies. In adopting these approaches, States would be better prepared to handle the emerging cybersecurity challenges, while simultaneously ensuring the continuity and integrity of flight operations. Additionally, international collaboration and regulatory harmonization would contribute to promoting a robust and resilient cybersecurity culture throughout the global aviation community.

3.2 Therefore, the Conference is invited to approve the following measures:

a) support the initiatives presented in this working paper while requesting an analysis of the utility of incorporating cybersecurity regulations and methods for air traffic services (ATS) into the global aviation framework; and

b) encourage States to integrate their national cybersecurity strategies with ICAO civil aviation strategies in order to create a cybersecurity culture in the ATS, incorporating policies, strategies and mechanisms as safeguards through the development of the proposed regulatory provisions.

— END —