International Civil Aviation Organization

AN-Conf/14-WP/125[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

CYBERSECURITY IN THE PROVISION OF AIR TRAFFIC SERVICES (ATS)

(Presented by Argentina and supported by 19 members of Latin American Civil Aviation Commission (LACAC)[2])

EXECUTIVE SUMMARY

This paper offers thoughts on the design of mechanisms to support air traffic services (ATS) providers in managing cyberthreats and cyber events, and in developing efficient mitigation strategies.

Action: The Conference is invited to:
a) develop guidance mechanisms to assist air traffic service providers in managing safety-related cyber risks as part of their safety management system;
b) develop and/or implement technologies, procedures and arrangements that enable controllers to provide air traffic services (ATS) safely and recover operations promptly in the case of a cyber event; and
c) define the competencies and skills that air traffic controllers need in order to assess and address cyber events and their impacts on ATS provision, so as to achieve cyber-resilience.

1. INTRODUCTION

1.1 In view of the rise in cyber threats and cyberattacks in the aviation industry, and recalling that one of the seven pillars of the ICAO *Aviation Cybersecurity Strategy* and underlying *Cybersecurity Policy* is the incorporation of *cybersecurity* into aviation risk management, it is more important than ever to identify and measure the impact that such events have on the provision of air traffic services (ATS), notwithstanding the fact that emerging technologies in air navigation are evolving to better handle *cyber events*.

1.2 Because aviation systems are intricately connected to one another and to other external systems, cyber events have become more far-reaching and impactful, with the potential to create global *disruptive events*[3]. It is therefore important to consider *cyber events* as safety hazards, or at least as

[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).
[3] Disruptive event: An unusual and serious occurrence on a national, regional or global scale that adversely affects aviation. Such events do not normally arise from aviation activities, but can nevertheless have a significant impact on operations.

precursors and contributing factors to the global high-risk category (G-HRC) occurrences described in the *Global Aviation Safety Plan 2023-2025* (Doc 10004, GASP). Moreover, the *ATM Operational Concept* (Doc 9854) warns that decisions are often taken on the basis of varying criteria, including for safety. This situation calls for action to achieve one of the expected benefits cited in Appendix E of Doc 9854: […] *expanding the definition of hazards will enable more stable user trajectories*.

1.3 Air traffic services are being provided in a more automated, digitalized and interconnected environment that makes them more vulnerable to *cyberthreats* and *cyberattacks*. The use of controller-pilot data link communications (CPDLC), the integration of unmanned aircraft in controlled airspace, remote digital towers, and aerodrome automated flight information systems (A-AFIS) are just a few of the developments that argue in favour of greater awareness and actions to address the impact of *cyber events* in the provision of ATS.

1.4 There have indeed been major advances in preventing and/or mitigating *cyber events*. However, by definition, such events directly involve air traffic management/communications, navigation and surveillance (ATM/CNS) and information systems, and so more work is needed to urgently address the impact of cyber events on ATM.

1.5 If ATS units do not have adequate risk controls and defensive barriers in place, they may experience a partial disruption of services, ZERO air traffic control (ATC) conditions, or even safety incidents such as loss of separation between aircraft in flight potentially causing a mid-air collision (MAC), one of the five global high-risk categories of occurrence.

1.6 Section 4 – *Developing a Cybersecurity Policy* of the *Cybersecurity Action Plan* (CyAP) developed by the ICAO Secretariat Study Group on Cybersecurity (SSGC) proposes actions for managing cyber risks. On this basis, it is worth rethinking the ways in which safety risks are managed as part of ATS in a global context that is described as volatile, uncertain, complex and ambiguous, and increasingly brittle and non-linear[4].

2. DISCUSSION

2.1 In light of the foregoing, it is essential to identify opportunities to improve predictive capabilities and actions for promoting *cybersecurity* in the provision of ATS.

2.2 First, it is important to take another look at the growing complexity of the operational context in which air traffic services are provided, and redefine the role and functions of ATS units, especially at the intersection of four comprehensive management systems where action is required: cyber risk management, safety risk management, security management, and information security management.

2.3 Further, there are three aspects relating to ATS for which *cyber event* mitigating measures need to be designed and implemented:

a) Safety risk management in relation to ATS provision;

b) Technical/operational tools[5] used by ATS units to provide services; and

[4] This description is taken from the social science models known as *VUCA* (volatile, uncertain, complex, ambiguous) and *BANI* (brittle, anxious, non-linear, incomprehensible) that are used to explain current global circumstances and that may be applied to all fields of study.

[5] These include operational procedures, computer systems and other ICTs, ATS surveillance, communications, etc.

c) The skills and competencies that air traffic controllers (ATCOs) need to achieve cyber-resilience in their ATS units.

2.4 Concerning ATS safety risk management, *cyberthreats* and *cyberattacks* should be incorporated into the safety management system (SMS) of the air traffic services provider (ATSP). Component 2 of an SMS naturally takes on particular relevance insofar as the hazards must logically be identified in order to manage the associated risks. Consequently, it is fundamental to understand that *cyberthreats* and *cyberattacks* must be identified as such as a first step in recording their occurrence, measuring their ATS impacts, and evaluating their risks.

2.5 This approach should not be limited to the identification of hazards traditionally associated with ATS but should expand to cover hazards relating to information technology (IT) such as the network supporting the ATM/CNS systems of an ATS unit, the software, server and hardware used, and other relevant elements. With technology changing by leaps and bounds, this approach must absolutely not be considered as static, but rather dynamic and adaptive. This will entail constant revision and adjustment to keep up with the rapid technological developments not just in the operational domain, but in the overall environment. It must therefore be understood that both a cyber event and an incident may evolve into a safety occurrence in ATS provision and flight operations.

2.6 As for the operational tools used by ATS units, these are understood as the technologies, procedures and arrangements that controllers need to provide ATS safely, and to achieve cyber-resilience and prompt recovery of operations in response to a cyber event. For this reason, it is vitally important to develop mechanisms to assist controllers in quickly identifying cyberthreats and taking appropriate action.

2.7 The role of air traffic controllers has changed, and the way they interact with the elements of the SHELL model is shifting in response to the new normal. Symbiosis between humans, hardware and software has intensified and heightened exposure to *cyber events*. The necessary competencies and skills must therefore be developed so that controllers in ATS units can achieve cyber-resilience and be able to handle different *cyber event* scenarios.

3. CONCLUSION

3.1 In view of the foregoing and bearing in mind the cross-cutting nature of cybersecurity in ATS provision, there is a need for mechanisms to provide guidance to ATSPs in incorporating *cyberthreats* and *cyber event* management into their SMS, and also acquire the analytical tools for designing mitigation strategies and early detection procedures as well as instruments to help controllers take immediate decisions in response to cyber occurrences.

3.2 It is also appropriate to define competencies and skills for air traffic controllers to be able to assess and respond to a cybersecurity event that may impact ATS provision, and also enhance their situational awareness of the possible consequences and human factors involved.

3.3 The Conference is invited to consider:

a) develop guidance mechanisms to assist air traffic service providers in managing safety-related cyber risks as part of their safety management system;

b) develop and/or implement technologies, procedures and arrangements that enable controllers to provide air traffic services (ATS) safely and recover operations promptly in the case of a cyber event; and

c) define the competencies and skills that air traffic controllers need in order to assess and address cyber events and their impacts on ATS provision, so as to achieve cyber-resilience.

— END —