International Civil Aviation Organization

A39-WP/187[1]
EX/72
10/08/16

WORKING PAPER

ASSEMBLY — 39TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 16: Aviation Security – Policy

CYBER SECURITY DEFENSE STRATEGY

(Presented by the Civil Air Navigation Services Organisation (CANSO))

EXECUTIVE SUMMARY

Cybersecurity is one of the most relevant issues and the most debated topics in civil aviation. The evolution of aviation systems poses new risks, relevant for impact on safety and continuity due to the increasing dependence on information technology. Air Traffic Management (ATM) systems but also aircraft systems, airport management systems, booking systems, aeronautical information and weather information could be equally affected by cyber incidents, which are not only related to confidentiality, but mainly on availability and continuity.

Action: The Assembly is invited to agree on the recommendation contained in paragraph 5

Strategic Objectives:	This working paper relates to Strategic Objective C — *Security and Facilitation*.
Financial implications:	Reduction of insurance costs; mitigation of threats and hazards in the light of resilience and safety and minimization of costs related to crisis management and social implications.
References:	Annex 17 – *Security* to Chicago Convention; Doc. 8973; Doc. 9985; Doc 9854; CANSO Cyber Security Risk Assessment Guide

1. INTRODUCTION

1.1 Civil aviation remains a potential high level target for criminals and terrorists. The obligation to protect civil aviation against acts of unlawful interference must cope with sophisticated threats, including those of a technological nature. Society will always expect zero accidents and incidents due to breaches of security to the aviation industry as a whole. This perspective will set the end-customer's confidence in air transport. The air transport network is essential to the global economy and fundamental to international trade, tourism, investment and prosperity. Any disruptions to its efficiency can result in significant economic and social disruption worldwide. The development of complex systems, by their nature

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

interoperable, in a global and international environment, requires a methodological approach of the security governance to enable the constant monitoring of resources, process integration between Information Technology (IT), logical and physical security. This has to be done by continuously evaluating the threat level and the potential vulnerability, with the aim to prevent, react and responding to acts of unlawful interference. This also requires a close coordination between all the actors of the aviation system, the States and the relevant Stakeholders. Mere compliance with regulations is not enough, while it is always necessary to demonstrate due diligence for the protection of human lives in the air and on the ground and to ensure security, continuity, resilience and regularity of the system. ICAOs Threat and Risk Working Group (TRWG) also underlined that the global aviation system in its information and communication complexity, is certainly a potential target for serious cyber-attacks. The interoperability objective and the opening of networks to a network centric operation concept enabled by real-time sharing of information and operational data are opening the system for more vulnerabilities.

1.2 ICAO has already raised the concern that cyber security could be an impediment for the implementation of the Global Air Navigation Plan (GANP) and supported joint initiative with major aviation Stakeholders, in order to assess systematically the existing cyber framework (Industry High Level Group Cyber [IHLG] signed at Montréal, 5 December 2014).

1.3 During the ICAO Aviation Security Panel (AVSECP/27) held in March 2016 a large number of Member States highlighted the need of upgrading the current Recommended Practice in Annex 17 (Security) regarding cyber security into a Standard. However, the majority of Members held the view that cybersecurity is not limited to the aviation security system alone. Members underscored the critical need to ensure appropriate coordination, including alignment with other Annexes, namely Annex 3, 6, 10, 11, 14 and 15. Furthermore, coordination with other relevant Panels is necessary before upgrading the current Recommended Practices into Standards, and there is a clear need for the ICAO Air Navigation Commission (ANC) to be consulted.

1.4 CANSO wants to underline the importance of the protection of all digital information and systems within the aviation system. This is vital to assure the protection and safety of the general public, passengers, crew, ground personnel, aircraft and aviation facilities against acts of unlawful interference perpetrated either on the ground or in flight. Specific actions could be required to enhance this concept in less developed States, as encompassed under the ICAO “No Country Left Behind (NCLB)” initiative.

2. THE NEED OF A CLARIFICATION ON CYBERSECURITY

2.1 CANSO notes that there is a certain grade of confusion regarding the term “Cybersecurity”. It is used for the threat posed by antagonists, as well for the need to assess and fix vulnerabilities in IT systems. Further, it is used to describe how to implement effective contingency planning in the light of resilience.

2.2 CANSO emphasizes that a sound security strategy for civil aviation should consider not only the technological level of maturity, but mainly a methodological protective approach to reach the primary objective of aviation security. This can only be achieved by a bottom up approach, including the whole organisation, taking into account human factors.

2.3 This objective is clearly stated in the *Global Air Traffic Management Operational Concept* (ICAO Doc. 9854) in which the role of security is definitely depicted as essential and presented in a very innovative way:

"Security refers to the protection against threats that stem from intentional acts (e.g., terrorism) or unintentional acts (e.g., human error, natural disaster) affecting aircraft, people or installations on the ground. Adequate security is a major expectation of the ATM community. The ATM system should therefore contribute to security, and the ATM system, as well as ATM-related information, should be protected against security threats.".

2.4 From this perspective – related to major standards in IT Security – the aim of providing availability, integrity and confidentiality refers to the general obligation for Contracting States to ensure the protection of the main constituents of the civil aviation, pursuant in the Chicago Convention and especially in ICAO Annex 17 (Security).

3. A NEW APPROACH

3.1 CANSO highlights that the protection of relevant assets, essential for the safety of civil aviation may differ between Aviation Stakeholders based on their goals; e.g. governments, ANSP's, airlines, airports, manufacturers, military, etc. It is possible to identify some of the cyber security topics for aviation, common for all members of the community, defined with specific needs:

a) to ensure that critical information is accessible only to those authorized, in order to prevent acts of unlawful interference by insider threats, independently on the operator's core service

b) to fulfil the obligation, based on common sense and *bona fide*, to identify and address vulnerabilities on critical systems, to identify with the ordinary diligence and prudence;

c) to extend risk management, to the risk deriving from the increasing dependence on IT resources owned by the single operator;

d) to have in place an appropriate response management for incident handling and crisis management, including contingency planning; and,

e) to assess impacts deriving from (cyber)security breaches not only on the single operator but also on the overall industry, in the framework of the National Civil Aviation Security Programme.

3.2 In other terms, cybersecurity is not different from the traditional aviation security approach, but it is just a natural extension of the basic principles contained in Annex 17 (Security) and the guidance material, addressing the most common threats and vulnerabilities referred to physical security.

3.3 Cyber threat to aviation will most likely be one of the main security issues in any new modernisation programmes, being the Single European Sky (SES), SES ATM Research (SESAR), Next Generation (NEXTGEN) and others that are developed on a regional level. It appears to be one of the most relevant drivers in other parts of the aviation industry. As a critical resource, information must be treated like any other asset essential to the survivability and success of ATM systems. All those programmes, not limited to the ATM but also involving aircraft operators, airports, military and others, will be based on the System Wide Information Management (SWIM) concept, facilitating the net-centric operational exchange of information and services across the entire system. The SWIM concept will improve the collaborative decision-making, providing better quality of required information on need to know basis at the right time to the right recipient. SWIM is the key enabler for the future technological

environment for aviation and its associated infrastructure should be considered as critical infrastructure for which security should be considered as a key requirement by design.

3.4 In this regard, while the general security remains an obligation on the Contracting States with implications of national sovereignty, defence, intelligence and law enforcement, the need to consider the specificity of the aviation environment urges to a more effective action.

3.4.1 Relevant initiatives at regional level are ongoing or already implemented. Just to mention some recent outcomes: The European Union position on cyber in ATM clearly states in the released issue of EC Regulation (Reg. 1035/2011) a clear relationship between security vulnerabilities and prescribes binding requirements for cybersecurity. The Federal Aviation Administration of the United States (FAA) in its offer presented to the US Senate declares a relevant objective for cybersecurity (Sec. 4109) aimed at challenging objectives, including a wide set of actions for coping with cyber issues. Other States are also focusing their regulatory effort on aviation cybersecurity in a similar way.

3.4.2 Due to the importance of cybersecurity for the civil aviation, CANSO fully supports any initiative aimed at realizing a full integration of cybersecurity theme within national and regional aviation security programmes and declares its full availability to actively participate.

4. CONCLUSION

4.1 Cybersecurity in aviation is a topic to be addressed methodologically and in a realistic way, considering implications and impacts on the overall industry and on the confidence of general public.

4.2 CANSO promotes a renewed international initiative under leadership from ICAO and in an effective and sustainable way under the “No Country Left Behind” principle.

4.3 The Industry High Level Group (Cyber) initiative, following the Cybersecurity Action Plan signed on December 2014, is developing a framework to enhance voluntary cooperation in this field. This industry led programme should be complemented and supported by a regulatory endorsement and a more in-depth consideration of the cross-cutting issue in civil aviation represented by cybersecurity.

5. RECOMMENDATIONS

5.1 The Assembly is invited to task the ICAO Secretariat as a matter of urgency to make cybersecurity an actual part of aviation security in a sound, sustainable, and effective way. The Assembly is invited to agree on the following recommendations:

That the Assembly:

a) consider the content of the paper and endorses it, recognizing the relevance and the possible impact to civil aviation;

b) agree that ICAO develop a new strategy on aviation cybersecurity as a vertical domain within aviation security and issue guidance material, aimed at harmonization of the current initiatives both at regional and national level;

c) recommend Member States to focus their attention on vulnerabilities in systems and networks rather than on threats and to consider the implications on the entire civil aviation industry;

d) recommend that a forum is set up for aviation firms to share best practices in a secure/trusted environment so that effective tools and techniques that enhance security in the current and future technology estates can be shared;

e) recommends Member States to review recent initiatives presented during AVSECP/27 in order to elevate to a Standard the current Recommended Practices 4.9.1 and 4.9.2 of Annex 17.; and

f) take note of the *CANSO "Cyber Security and Risk Assessment Guide"*[2].

—END—

[2] https://www.canso.org/canso-cyber-security-and-risk-assessment-guide