International Civil Aviation Organization

WORKING PAPER

A40-WP/283
EX/114
5/8/19

ASSEMBLY — 40TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 12 : Aviation Security — Policy

STRATEGIC APPROACH TO AVIATION CYBERSECURITY

(Presented by France)

EXECUTIVE SUMMARY

Given the growing importance of cyber threats, many States have already developed a strategic and sovereign trans-sectorial approach. At the same time, specific aviation cybersecurity approaches are or should be developed for ensuring the safety, the security and the continuity of air transport. These two approaches should not contradict each other; on the contrary, they should contribute to each other.

Moreover, in order to effectively implement the aviation cybersecurity strategy, it is of utmost importance that cybersecurity activities do not transform in a disciplinary silo which would eventually create potential redundancies, duplications, or inconsistencies.

For example, to ensure this effective coordination, France has created the Air Transport Cybersecurity Council which provides already key outputs to protect civil aviation against cyber-attacks.

ICAO's strategy on this subject should be welcomed and encouraged in this spirit, with the creation of a dedicated collaborative and transversal body.

Action: The Assembly is invited to:

a) recommend all States to establish an efficient national coordination between their civil aviation authority and their relevant agencies in charge of cybersecurity comprising coordination mechanisms at both strategic and operational levels with all service providers and industry stakeholders;

b) emphasize the importance of effective cross-domain work and coordination between the Security and Safety branches of the ICAO Secretariat, and their associated groups and panels; and

c) urge the ICAO Council to define and create a cross-domain civil aviation cybersecurity body within ICAO, such as a panel established following the Directives for Panels Doc 9482, to consolidate and harmonize all cybersecurity related activities and documentation, including the Trust Framework.

Strategic Objectives:	This working paper relates to Strategic Objectives: *Safety, Air Navigation Capacity and Efficiency, Security and Facilitation*
Financial implications:	The activities referred to in this paper will be undertaken subject to the resources available in the 2020 - 2022 Regular Programme Budget and/or from extra-budgetary contributions.
References:	A40-WP/28 EX/13 *ICAO Cybersecurity Strategy*

1. BACKGROUND

1.1. At the national level, Member States have the responsibility to ensure the safety, security, and continuity of civil aviation, taking into account cybersecurity, as already requested by ICAO Annex 17 — *Security*. However, preserving Air Transport from cyber-attacks covers a very wide spectrum of themes and requests assets of different nature. Therefore, it is of the utmost importance to scope the action of civil aviation authorities and as a consequence the role of ICAO in this domain.

1.2. Cybersecurity is not specific to aviation and many States have already developed strategic and sovereign trans-sectorial approach and regulations. They very often manage cybersecurity at an inter-ministerial level either through a specialized agency or a dedicated body within a ministry. This regulatory or "sovereign approach" addresses aviation among all sectors of vital importance.

1.3. Simultaneously, and especially in International Civil Aviation, various States impose protection measures to aviation operators (Airports, Airlines, ANSP,…) and manufacturers trying to keep them interoperable, balanced and consistent with the overall safety and security management processes. This is the objective of the "aviation cybersecurity approach".

1.4. At its level, in order to address the cybersecurity issues in aviation and mitigating associated threats and risks, ICAO established the Secretariat Study Group on Cybersecurity (SSGC), set up the Trust Framework and defined a robust aviation cybersecurity strategy.

2. DISCUSSION

2.1. Aviation cybersecurity could lead to consider all aspects of air transport activities including potential economic, reputational, environmental and privacy aspects. Several of them do not present any specificity in the aviation domain and are regulated by other authorities, according to different frameworks. Thus, it is necessary to not create an additional disciplinary silo which would eventually create potential redundancies or inconsistencies but to focus on security and safety management, which is already significant and will involve extensive resources. Other aspects of cybersecurity in aviation should then be driven by a national regulatory approach or be managed internally by the industry.

2.2. Aviation cybersecurity approaches need to articulate properly at a national level with sovereign approaches and ensure a homogeneous and consistent implementation. Feedback from the aviation sector should be used to amend sovereign cybersecurity provisions and activities if needed. Reciprocally, cybersecurity information and data originating from other sectors may assist in identifying potential threats to aviation.

2.3. Finally, at a national level, aviation cybersecurity approach should consider the entire aviation system and manage exhaustively all cyber risks inherent to aviation activities, not setting aside small aerodromes or operators, while keeping requirements proportionate to the risk incurred. It could therefore be considered as the way to achieve sovereign approach objectives throughout the entire national aviation sector.

2.4. At global level, ICAO should aim to create the necessary framework that ensures this proper articulation between sovereign and aviation approaches. In line with the priorities defined above for civil aviation authorities, this ICAO framework should preserve the qualities of the global aviation system, especially safety, security, and interoperability. It should lead to a systemic approach to cybersecurity in synergy with existing safety management processes in place worldwide.

2.5. ICAO should represent the aviation sector in UN fora dealing with the sovereign approaches to cybersecurity in order to avoid that non-coordinated national cybersecurity measures be detrimental to the performance of the overall aviation system.

3. AN EXPERIENCE OF COORDINATION: THE CASE OF FRANCE

3.1. France established in April 2018 the Council for Cybersecurity in Air Transport (CCTA). Chaired by the director general of the civil aviation with a representation of all public and private stakeholders (i.e. the national agency in charge of cybersecurity, ministerial departments in charge of defense and home affairs, aircraft and electronic equipment manufacturers, as well as service providers for airports, airlines, navigation), it is the competent body to handle all exchanges about cybersecurity in civil aviation.

3.2. In this context, it appeared clearly that aviation cybersecurity should be apprehended in a holistic and integrated way, regardless of the classic boundaries between security and safety, in order to get all the possible synergies and work through possible contradictions.

3.3. Integrated CCTA work also showed the importance to precisely define a common vocabulary and a shared methodology in order to assess the different scenario. These scenarios are expressed as classic cybersecurity goals (availability, integrity, authenticity and confidentiality) applied to critical aviation assets and are assessed on a 4-level scale, compatible with safety risks assessment.

3.4. Based on risk analysis, the mapping of information flows irrigating all the operations (aircraft on maintenance, airport operation, aircraft in flight operations, aircraft on ground operations…), is currently worked on. This systemic mapping will enable the CCTA to identify critical information flows, information systems and information system boundaries relevant to each scenario. An important expected output is to establish a shared hierarchy of the importance of the scenarios.

3.5. The next steps will be to evaluate mitigation and/or remediation measures in order to collectively choose the most efficient way to tackle the threat a particular scenario represents.

4. CONCLUSION

4.1. National and ICAO aviation Cybersecurity strategies should focus on improving the safety and security of the Aviation System and preserving the continuity of air transport services.

4.2. At the national level, all States should coordinate Aviation Cybersecurity management and corresponding regulatory frameworks and management processes with security and safety ones. An efficient national coordination should be organized between their civil aviation authority and their relevant agencies in charge of cybersecurity, as well as coordination mechanisms at strategic and operational levels with all aviation service providers and industry stakeholders.

4.3. Aviation cybersecurity approaches need to articulate properly at a global, regional and national level with sovereign approaches in order to ensure full interoperability of protection and mitigation measures and risk management systems.

4.4. At the international level, it seems necessary to create a cross-domain civil aviation cybersecurity body within ICAO, such as a panel established following Doc 9482 — *Directives for Panels of the Air Transport Committee and the Committee on Unlawful Interference*. In coordination with the Security and Safety branches of the ICAO Secretariat, it could work across all ICAO domains to consolidate and harmonize all cybersecurity related activities and documentation, including the Trust Framework. In the interim, the Secretariat Study Group on Cybersecurity should continue working on the subject.

— END —