International Civil Aviation Organization

A41-WP/151
EX/66
2/8/22

WORKING PAPER

ASSEMBLY — 41ST SESSION

EXECUTIVE COMMITTEE

Agenda Item 14: Aviation Security — Policy

THE COMPLEXITY OF ADDRESSING CYBERSECURITY IN CIVIL AVIATION

(Presented by the United Arab Emirates)

EXECUTIVE SUMMARY

The aviation industry relies more and more on digitalization and cybersecurity became an essential component of a resilient civil aviation system. This paper outlines a complex and cross-cutting domain of cybersecurity that involves all aspects of civil aviation, including aviation safety, aviation security, and air navigation capacity and efficiency. It also extends to commercial and economic interests of States and stakeholders to ensure business continuity of air transport operations. This paper presents the deliberations of the Cybersecurity Forum, held under the "World Government Summit 2022" and the High-level International Programme for Civil Aviation Leaders from 28 to 30 March 2022, at Expo 2020 Dubai, United Arab Emirates.

Action: The Assembly is invited to:

a) recognize the need for ICAO, Member States and all relevant stakeholders to continue to address collaboratively complex cybersecurity domain in civil aviation; and
b) encourage aviation cybersecurity stakeholders to further develop capacity building strategies in order to enhance human resources' competences and proficiency to ensure sufficient expertise in both cybersecurity and civil aviation fields.

Strategic Objectives:	This working paper relates to Strategic Objectives: *Air Navigation Capacity and Efficiency, Safety, and Security and Facilitation.*
Financial implications:	This working paper has no direct financial implications.
References:	Annex 17 – *Aviation Security* Doc 10118. *Global Aviation Security Plan* *Aviation Cybersecurity Strategy* *Cybersecurity Action Plan* Cybersecurity Policy Guidance Cybersecurity Culture in Civil Aviation Guidance on Traffic Light Protocol (TLP) A40-10, *Addressing Cybersecurity in Civil Aviation*

1. INTRODUCTION

1.1 Aviation cybersecurity is a global and cross-cutting domain that involves all aspects of civil aviation, including aviation safety, aviation security, and air navigation capacity and efficiency. It also extends to commercial and economic interests of States and civil aviation stakeholders to ensure business continuity of air transport operations. Concerns about cybersecurity in civil aviation have increased as the number and the severity of the attacks have risen, not necessarily in civil aviation sector, but in various sectors at the global level, and for the reason that the aviation industry relies more and more on digitalization. Therefore, cybersecurity has become an essential component of a resilient civil aviation system.

1.2 In order to support States and stakeholders in addressing aviation cybersecurity ICAO developed the Aviation Cybersecurity Strategy; Cybersecurity Action Plan; Cybersecurity Policy Guidance; Cybersecurity Culture in Civil Aviation; ICAO Guidance on Traffic Light Protocol (TLP). However due to complexity of cybersecurity there are many challenges on the national, regional, and global levels, to be further addressed in order to ensure a holistic, harmonized, and consistent approach to aviation cybersecurity across the civil aviation sector.

2. DISCUSSION

2.1 In order to better understand the current challenges related to cybersecurity in civil aviation, the General Civil Aviation Authority of the United Arab Emirates organized the Cybersecurity Forum which was held under the "World Government Summit 2022" under the High-level International Programme for Civil Aviation Leaders from 28 to 30 March 2022, at Expo 2020 Dubai, United Arab Emirates. It should be noted that this Cybersecurity Forum was held prior to the first meeting of the ICAO Cybersecurity Panel, which was held in May 2022.

2.2 This Cybersecurity event included the Round Table Discussion: "A Globally Harmonized Approach to Aviation Cybersecurity" and the High Level Civil Aviation Cybersecurity Forum: "The Importance of Cybersecurity in Civil Aviation". High officials and subject matter experts on cybersecurity represented: numerous States (including Ministers, Directors of CAA and/or appropriate sectors, Heads of Cybersecurity Departments etc.), ICAO, regional civil aviation organizations (including African Civil Aviation Commission (AFCAC), Arab Civil Aviation Organization (ACAO), European Civil Aviation Conference (ECAC), etc.), international organizations (including Airports Council International (ACI), etc.), industry and other important stakeholders, in the round table discussion and high level forum.

2.3 Various challenges were considered and discussed at the strategic level, such as: complexity of cybersecurity in civil aviation; digitalisation and dynamic environment due to technical developments; limitations of traditional approach and need to change mind-set in addressing cybersecurity in civil aviation; constraints on international and national levels related to legal provisions for the prevention, prosecution, and timely reaction to cyber incidents; actions to be taken by governments as cybersecurity overarches all sectors at the national level, including civil aviation; proper allocations of roles and responsibilities for various government entities related to complex cybersecurity domain, including civil aviation aspect and coordination; civil aviation cybersecurity governance; development of a national civil aviation cybersecurity strategy as a part of national cybersecurity strategy; the evolution of aviation cybersecurity threats and risks mitigations; cybersecurity incident response on national, regional and international levels; the importance of development of cybersecurity culture; sharing of information and cybersecurity threats between States and stakeholders (including aircraft manufactures); the importance of

partnership, capacity building, training and human resources development; designing and implementing aviation cybersecurity oversight obligations and capacity; etc.

2.4 Participants shared their achievements, experiences, approaches, views, concerns and proposals for way forward. It was emphasized that a holistic, harmonized and consistent approach to cybersecurity in civil aviation remain a challenge to many civil aviation stakeholders, including government entities, authorities, industry and stakeholders. In order to enhance collaboration and partnership, holistically address complex cybersecurity cross-cutting domain and further develop capacity and human resources proficiency, more work and coordination are required to be done in the civil aviation sector, for achieving a consistent and harmonized protection against, mitigation of, and response to, cyber threats to civil aviation as well as in order to ensure cyber resilience of civil aviation system.

3. CONCLUSION

3.1 It is important for all stakeholders to continue to collaboratively address cybersecurity in civil aviation. The aviation cybersecurity matters are to be considered and coordinated in a cross-cutting manner. The complex nature of aviation cybersecurity requires extensive collaboration between: ICAO, States, organizations, industry and stakeholders in all relevant aviation disciplines to safeguard civil aviation against cyber threats. States should be further supported to continue the work in developing national aviation cybersecurity strategies based on the ICAO Aviation Cybersecurity Strategy and national cybersecurity context. These cannot be achieved without developing capacity building strategies and sufficient human resources' competences and proficiency in both cybersecurity and civil aviation fields.

— END —