International Civil Aviation Organization

WORKING PAPER

A41-WP/74
EX/36
26/7/22

ASSEMBLY — 41ST SESSION

EXECUTIVE COMMITTEE

Agenda Item 14: Aviation Security — Policy

DEVELOPMENT OF A FRAMEWORK FOR CYBERSECURITY

(Presented by Czechia on behalf of the European Union and its Member States[1] and the other Member States of the European Civil Aviation Conference[2], the Member States of the African Civil Aviation Commission[3], and EUROCONTROL)

EXECUTIVE SUMMARY

Cybersecurity continues to develop in importance as new technologies and aviation's greater reliance on information technology and digital operational systems create new vulnerabilities as well as new opportunities. An increased understanding of the cyber domain further points to a number of specific challenges, highlighting the need to promote and make progress towards a distinct approach to the mitigation of risk. Its growing importance further underscores the critical need for States and ICAO to step-up efforts in support of the development of a cybersecurity framework, as well as cybersecurity culture and training.

[1] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden.

[2] Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Iceland, Moldova, Monaco, Montenegro, North Macedonia, Norway, San Marino, Serbia, Switzerland, Türkiye, Ukraine, and the United Kingdom.

[3] Algeria, Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cabo Verde, Central African Republic, Chad, Comoros, Congo, Cote d'Ivoire, Democratic Republic of the Congo, Djibouti, Egypt, Equatorial Guinea, Eritrea, Eswatini, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau, Kenya, Lesotho, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Rwanda, Sao Tome and Principe, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, South Sudan, Sudan, Togo, Tunisia, Uganda, United Republic of Tanzania, Zambia and Zimbabwe.

Action: The Assembly is invited to: a) Request that ICAO consider the necessary steps to make progress towards guidance on the assessment of aviation cybersecurity risks, taking into account the actors involved, the need for a holistic cross-cutting perspective and the distinctive factors described in this Working Paper; b) Request that ICAO finalize the compilation of relevant existing Standards and Recommended Practices (SARPs) and other international legal bases that States and organizations can build upon to include cyber risks within their aviation frameworks; c) Request that ICAO and its contracting states intensify efforts to promote a dedicated cybersecurity culture and activities to support the development of sufficient human resources and capacity to manage cybersecurity and cyber resilience in civil aviation; and d) Request that ICAO consider the organisation of cybersecurity exercises at global and regional levels.	
Strategic Objectives:	This working paper relates to the *Security and Facilitation* Strategic Objective.
Financial implications:	
References:	

1. INTRODUCTION

1.1 The 40th Session of the ICAO Assembly adopted Assembly Resolution A40-10 – *Addressing Cybersecurity in Civil Aviation*. The resolution addresses cybersecurity through a horizontal, cross-cutting and functional approach, reaffirming the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyber threats and calls upon States to implement the ICAO Aviation Cybersecurity Strategy (October 2019). The Strategy is implemented via the Cybersecurity Action Plan (CyAP) and with the support of the newly established Cybersecurity Panel, which will build upon the work of the Secretariat Study Group on Cybersecurity.

1.2 As digitalisation profoundly impacts economies and reshapes the aviation sector, the issue of cybersecurity becomes ever more critical. Cybersecurity also continues to pose a challenge to all sectors during the COVID-19 pandemic recovery phase. Businesses are employing more virtual means of working, which may increase their vulnerability to cyber threats. This requires stepping-up efforts in the development of a cybersecurity framework while taking into account its specificities.

2. THE CYBERSECURITY LANDSCAPE PRESENTS DISTINCTIVE ELEMENTS IN DEFINING A RISK MANAGEMENT APPROACH

2.1 The cybersecurity domain presents a unique threat picture. It must focus not only on terrorist groups seeking direct attacks and mass casualties, but also an array of possible other actors and motivations. These could include large organised entities, activists, and criminal hackers, seeking, for example, disruption, coercion, a show of strength, media attention, or financial gain. Attacks may also intentionally, or not, affect civil aviation, potentially even endangering safety, and impact the sector either directly or indirectly.

2.2 Other elements that would need to be taken into account in cyber risk management include the significant number of non-aviation specific service providers to the aviation system, and which may have a different understanding of cybersecurity needs and risks.

2.3 The cyber sphere is further characterised by State regulation that may operate across sectors, without a distinctive aviation element.

2.4 The above points to the need to define a specific approach to cybersecurity risk assessment where:

a) the expertise required, particularly in relation to vulnerabilities and mitigation measures, has to combine aviation and IT knowledge and experience;
b) the scope of the assessment needs to be clearly defined, focusing on safety, security and resilience of critical functions cutting across individual operators/entities and domains; and
c) the risk assessment can identify potential single points of failure from a (global) information security perspective in order to address them appropriately.

3. DEVELOPING A CYBERSECURITY FRAMEWORK THAT TAKE SPECIFICITIES INTO ACCOUNT

3.1 In developing a cybersecurity framework, the aviation sector must develop approaches that not only cross traditional boundaries of aviation domains (such as the need for both a macro perspective (e.g. ATM) and an individual flight perspective), but that also take into account the different positioning of non-

aviation sectors and horizontal (non-aviation specific) State regulation as described in 2.2 and 2.3 above. It is imperative to ensure consistency, as well as avoid duplication, gaps, and unnecessary regulatory or oversight burden on States and operators in the implementation of a cybersecurity framework.

3.2 The aviation sector is well placed to benefit from and build upon existing international aviation roles and responsibilities and procedures. ICAO aviation security and safety SARPS provide a firm foundation and can be built upon, both at government and organisational level. The same holds true for information sharing and reporting mechanisms. There are also existing international air law instruments for the criminalization of acts that jeopardize safety and which should be used to the extent possible.

3.3 States and organizations are encouraged to review and consider relevant ICAO cybersecurity documents and implement existing cybersecurity relevant SARPs. It is also important for States and organizations to re-think existing aviation security and safety, as well as aviation criminal law structures from a digital perspective to ensure that roles and responsibilities remain current and are properly coordinated.

4. THE CRITICALITY OF THE HUMAN ELEMENT IN CYBERSECURITY

4.1 The human element is at the core of cybersecurity, as recognised by the ICAO Aviation Cybersecurity Strategy (2019).

4.2 The increasing digitalisation and interconnectivity of the aviation system calls for stepping-up efforts to meet the growing demands for and in support of awareness raising, training, updated academic curricula, and appropriately-trained staff with cross-cutting expertise in aviation and cybersecurity.

4.3 The ICAO Secretariat has launched a first ICAO course on cybersecurity and cyber resilience, “Foundations of Aviation Cybersecurity Leadership and Technical Management”, as well as a course on “Managing Security Risk in ATM”, developed in partnership with EUROCONTROL. It would be important to build upon these welcome efforts and lessons learned.

4.4 As noted in the ICAO Aviation Cybersecurity Strategy, cybersecurity exercises are a useful tool to test existing cyber resilience and identify improvements, and are therefore highly encouraged. In addition to exercises at individual European State level, Europe has regional experience to share in this area to the benefit of the international aviation community.[4] ICAO is encouraged to explore possibilities for hosting such exercises.

4.5 As highlighted during the ICAO *Year of Security Culture* (YOSC), it is vital to extend the notion of security and safety culture beyond the physical realm. States and organisations are encouraged to build upon the achievements of the YOSC by promoting a cybersecurity culture, and to share best practices. ICAO should foster efforts towards this end, including by developing appropriate guidance material.

— END —

[4] “Cyber Europe 2018” organised by The European Union Agency for Network and Information Security (ENISA) target audience was comprised of professionals and organisations involved in information security activities in the Aviation sector; the European Aviation Crisis Coordination Cell (EACCC) organised a crisis management exercise in 2018 as a result of a cyber-attack on surveillance tracker software and is preparing a crisis management exercise in 2022 simulating the large scale outage of a European digital network infrastructure as a result of a cyber-attack; the European Union Aviation Safety Agency has also organised cybersecurity exercises.