International Civil Aviation Organization

A41-WP/374
EX/170
2/8/22

WORKING PAPER

ASSEMBLY — 41ST SESSION

EXECUTIVE COMMITTEE

Agenda Item 14: Aviation Security — Policy

READINESS OF PERSONNEL FOR CYBERSECURITY IN AIR NAVIGATION SERVICES AT NORMAL AND CRISES TIMES

(Presented by the African Civil Aviation Commission (AFCAC) on behalf of 54 African States[1])

EXECUTIVE SUMMARY

The importance of cybersecurity and cyber resilience in the aviation dramatically increased with time, and this urgency of cybersecurity has been highlighted time and again due to subsequent attacks before and during the COVID-19 pandemic. Furthermore, in addition to the catastrophic impact of COVID-19 on the global economy in general, and on aviation in particular, the pandemic has showed increased levels of cyber-attacks. Considering the capacity building, training and cybersecurity culture as one of the main pillars of ICAO cybersecurity strategy and considering the significance of air navigation infrastructure in aviation sector. Therefore, this working paper highlights the importance of addressing the capacity building, training, and cybersecurity culture during the normal and crises times

Action: The Assembly is invited to:
a) take note of the information mentioned in the Working Paper; and
b) request ICAO to include, in the tasks of the Cybersecurity Panel, the development of capacity building, training, and cybersecurity culture initiatives during crisis times.

Strategic Objectives:	This working paper relates to the *Security and Facilitation* Strategic Objective
Financial implications:	
References:	*Aviation Cybersecurity Strategy* *Cybersecurity Action Plan* Assembly Resolution 40-10 – Addressing Cybersecurity in Civil Aviation Doc 9985, *Air Traffic Management Security Manual*

1

[1] Algeria, Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cabo Verde, Central African Republic, Chad, Comoros, Cote d'Ivoire, Democratic Republic of the Congo, 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, São Tomé and Príncipe, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, South Sudan, Sudan, Tanzania, Togo, Tunisia, Uganda, Zambia, Zimbabwe

1. INTRODUCTION

1.1 Technology and cyber systems have become essential to modern society and component of many activities that have become dependent on information technology. Therefore, the importance of cybersecurity and cyber resilience in the aviation dramatically increased with time, and this urgency of cybersecurity has been highlighted time and again due to subsequent attacks before and during the COVID-19 pandemic.

1.2 Recognizing the multi-faceted and multi-disciplinary nature of cybersecurity and noting that cyber-attacks can simultaneously affect a wide range of areas and spread rapidly, it is imperative to develop a common vision and define a global Cybersecurity Strategy. Therefore, ICAO developed and published Aviation Cybersecurity Strategy to enable a sustainable and strong cybersecurity framework.

1.3 The ICAO Cybersecurity Strategy comprises seven pillars: International cooperation, Governance, Effective legislation and regulations, Cybersecurity policy, Information sharing, Incident management and emergency planning, and **Capacity building, training, and cybersecurity culture.**

1.4 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 Cybersecurity Strategy.

1.5 The ICAO Cybersecurity Action Plan (CyAP) has been developed with the aim to propose a series of principles, measures and actions to achieve the objectives of the strategy's seven pillars. It provides the foundation for States, industry, stakeholders and ICAO to work together to develop the ability to identify, prevent, detect, respond to and recover from cyber-attacks on civil aviation as well as create a solid framework for cooperation.

1.6 Recently, the Cybersecurity Panel has been established, as part of the new governance mechanism to address cybersecurity in ICAO. The Terms of Reference of the Cybersecurity Panel includes work in line with the Aviation Cybersecurity Work Programme, with the objective of developing provisions that may include Standards and Recommended Practices (SARPs) and/or procedures for the purpose of safeguarding civil aviation against cyber threats while giving due consideration to economic, operational and other impacts of such provisions.

1.7 ICAO developed a guidance material for cybersecurity culture (The ICAO "Cybersecurity Culture in Civil Aviation).

2. DISCUSSION

2.1 The outbreak of the Coronavirus pandemic in 2019 (COVID-19) has changed our lifestyle irrevocably. Many actions have been taken by States to limit physical contact between people and thereby, control the spread of COVID-19, such as social distancing, remote learning, and remote working. This led to a spurt in telecommuting and video conferencing, digital transformation, innovation, and other online technologies, coming about in what came to be known as the "new normal". Besides the catastrophic impact of COVID-19 on the international economy and society, the pandemic showed increased levels of cyber-attacks, which also affected society and businesses.

2.2 The air navigation department is considered as one of the critical infrastructures in aviation domain and therefore, it must take significant attention with the shift of air navigation facilities from analogue ground-based systems to digital space-based systems to accommodate the tremendous growth in air traffic density.

2.3 The capacity building, training and cybersecurity culture is one of the main pillars of cybersecurity strategy that enable having cyber resilient aviation system. However, the existing ICAO framework does not address the cybersecurity during the times of crises, such as COVID-19 pandemic or other future pandemics or crises.

3. CONCLUSION

3.1 The capacity building, training and cybersecurity culture is considered as one of the main pillars to enable having cyber resilient aviation systems during normal and crises times. Therefore, ICAO resolution for cybersecurity should consider this important issue. Furthermore, the new established Cybersecurity Panel should consider also this issue in their tasks.

— END —