



WORKING PAPER

ASSEMBLY — 40TH SESSION

EXECUTIVE COMMISSION

Agenda Item 12: Aviation Security — Policy

CYBER-SECURITY

(Presented by United Arab Emirates)

EXECUTIVE SUMMARY

Cyber-security remains a threat to civil aviation. ICAO and other international organisations are actively working to ensure that the likelihoods and consequences of a cyber-attack are reduced to the minimum.

However, the aviation community needs to work hand in hand to address this developing threat to our civil aviation system. Industry is partially aware of the cyber security issue when it comes to safety. The ICAO Cyber Summit hosted by the UAE in April 2017 was a demonstration of this lack of awareness in the aviation safety world. Attendees believed that the Cyber event was having an orientation more towards aviation security than safety.

Action: The Assembly is invited to:

- a) Acknowledge that Assembly A39 and Dubai Declaration on cyber security in civil aviation have been key in the design of the Cybersecurity Strategy and the amended Assembly Resolution A39-19 “Addressing Cybersecurity in Civil Aviation” which is brought before this Assembly under WP 28;
- b) Instruct ICAO to ensure that SARPs are developed for each Annex about Cyber-security and actively engage experts from Aviation Safety; and
- c) Encourage States to participate in information sharing frameworks as outlined in the ICAO CYBERSECURITY STRATEGY presented by ICAO Council under WP 28.

<i>Strategic Objectives:</i>	This working paper relates to Strategic Objectives: Safety, Air Navigation Capacity and Efficiency, and Economic Development of Air Transport
<i>Financial implications:</i>	
<i>References:</i>	

1. INTRODUCTION

1.1 Cyber-security remains a major threat to civil aviation.

1.2 ICAO and other international organisations are actively working to ensure that the likelihoods and consequences of a cyberattack are reduced to the minimum.

1.3 However, the aviation community needs to work hand in hand to address this developing threat to our civil aviation system.

2. DISCUSSION

2.1 Annex 17 contains few measures relating to cyber threats.

2.2 Cybersecurity is multidimensional and affects ALL annexes. Therefore, an appropriate mechanism for the coordination between all aviation domains (safety, security etc) needs to be found.

2.3 It would be advisable if ICAO addresses the multidimensional aspect of cybersecurity with the establishment of an appropriate structure for cybersecurity – in line with the Council instructions to conduct a feasibility study and gap analysis for the future structure of the ICAO cybersecurity work program.

2.4 The new structure should aim at fostering a cyber resilience across all domains of air transport: safety, security and economy.

2.5 We need to remember the cyber-attacks which affected airlines in past years. Their consequence is not safety nor security but they can play a negative role on air transport since they can lead to loose of trust from the travelling public and bring unnecessarily attention/concern on air transport.

— — — — —

APPENDIX

DUBAI DECLARATION

DECLARATION ON CYBERSECURITY IN CIVIL AVIATION DUBAI, UNITED ARAB EMIRATES 4 TO 6 APRIL 2017

We, the Officials and representatives from the States and regional and international organizations participating in the summit on cybersecurity in civil aviation convened by the International Civil Aviation Organization (ICAO) in Dubai, United Arab Emirates from 4 to 6 April 2017, to address challenges to aviation resulting from cyber threats;

Recalling the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation*, and the *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* done at Beijing on 10 September 2010 (Beijing Instruments);

Recalling further the ICAO Assembly Resolution A39-19: Addressing Cybersecurity in Civil Aviation, and the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyber-threats by, inter alia:

- a) implementing global, regional and State-level strategies on cybersecurity in civil aviation based on a shared vision;
- b) increasing the resilience of the global aviation system against cyber-threats that may jeopardize the safety, security and efficiency of civil aviation; and
- c) reaffirming the prominent role of ICAO as aviation's highest-level forum for addressing collaboratively cybersecurity in civil aviation;

Mindful of the challenges in safeguarding civil aviation against cyber-threats in a demanding and continuously evolving aviation cybersecurity environment;

Noting that in many cyber incidents affecting the safety and security of civil aviation, their actors are focused on malicious intent, disruption of business continuity and theft of information for political, financial or other motivations;

Recognizing that cyber incidents can affect critical civil aviation systems worldwide with catastrophic consequences, including the availability of information and communications technology systems, and the integrity and confidentiality of data, all of which the aviation sector is increasingly reliant on; and

Considering the need to facilitate and encourage initiatives worldwide aimed at addressing cybersecurity in a collaborative, comprehensive and cross-cutting manner;

Declare that:

1. It is the responsibility of States to act in such a way as to mitigate the risk posed by cyber threats, to build their capability and capacity to address such threats in civil aviation, and to ensure their legislative framework is appropriately established to take action against actors of cyber-attacks;
2. Cyber capabilities applied to aviation should be used exclusively for peaceful purposes and only for the benefit of improving safety, efficiency and security;
3. Collaboration and exchange between States and other stakeholders is the sine qua non for the development of an effective and coordinated global framework to address the challenges of cybersecurity in civil aviation;
4. Cybersecurity matters must be fully considered and coordinated across all relevant disciplines within State aviation authorities;
5. Cyber-attacks against civil aviation must be considered an offense against the principles and arrangement for the safe and orderly development of the international civil aviation; and
6. The ratification and entry into force of the Beijing Instruments would ensure that a cyber-attack on international civil aviation is considered an offence, would serve as an important deterrent against activities that compromise aviation safety by exploiting cyber vulnerabilities, and therefore it is imperative that all States and ICAO work to ensure the early entry into force and universal adoption of the Beijing Instruments, as called for in ICAO Assembly Resolution A39-10: Promotion of the Beijing Convention and Beijing Protocol of 2010; and

Reiterate our commitment to the development of a robust, efficient and sustainable civil aviation system.

Done in Dubai, United Arab Emirates, on this 5th day of April 2017.

— END —