International Civil Aviation Organization

A40-WP/28
EX/13
25/6/19

WORKING PAPER

ASSEMBLY — 40TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 12: Aviation Security — Policy

ICAO CYBERSECURITY STRATEGY

(Presented by the Council of ICAO)

EXECUTIVE SUMMARY

This paper presents a comprehensive Cybersecurity Strategy and, to highlight its urgency and importance, includes an amended A39-19 *Addressing Cybersecurity in Civil Aviation* supporting its implementation by Member States. The Strategy is built on ICAO's vision for global cybersecurity – that the aviation sector should be resilient to cyber-attacks and remain safe and trusted globally, whilst continuing to innovate and grow. It will need to be supported by an action plan to be developed through appropriate mechanisms. The Strategy is the outcome of deliberations in the Secretariat Study Group on Cybersecurity.

Action: The Assembly is invited to:

a) adopt the proposed Assembly Resolution that supersedes Assembly Resolution A39-19 in Appendix A;
b) endorse the Cybersecurity Strategy in Appendix B; and
c) urge States to ratify the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* and *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft*.

Strategic Objectives:	This working paper relates to the following Strategic Objectives: *Capacity and Efficiency*, *Safety*, and *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:	Doc 10075, *Assembly Resolutions in Force* (as of 6 October 2016)

1. INTRODUCTION

1.1 The 39th Session of the ICAO Assembly reaffirmed the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyber-attacks and obtain global commitment for action by ICAO, its Member States and industry stakeholders, with a view to collaboratively and systemically addressing cybersecurity in civil aviation and mitigating the associated threats and risks. Resolution A39-19 *Addressing cybersecurity in civil aviation* identified the actions to be undertaken by States and other stakeholders in this regard. The 39th Session of the ICAO Assembly also instructed ICAO to develop a comprehensive cybersecurity work plan and governance structure.

1.2 To meet these objectives, ICAO established the Secretariat Study Group on Cybersecurity (SSGC) under the lead of the Deputy Director, Aviation Security and Facilitation (DD/ASF). The SSGC's membership consists of 20 States, 13 international organizations, and the ICAO Secretariat, and is monitored by the Secretariat Senior Management Group on Common Safety and Security Issues, chaired by the Secretary General of ICAO.

1.3 Since its inception in August 2017, the SSGC has met six times and developed a set of recommendations to address the emerging issue of cybersecurity in aviation. The principal outcome was the development of a comprehensive Cybersecurity Strategy. The Strategy aims to steer the work of States and ICAO with the aim of ensuring the safety, security and continuity of civil aviation through the application of a robust cybersecurity framework. The Council at its 217th Session approved the Aviation Cybersecurity Strategy in principle and agreed to present an amended A39-19 *Addressing Cybersecurity in Civil Aviation* to the 40th Session of the ICAO Assembly.

2. DISCUSSION

2.1 The Aviation Cybersecurity Strategy considers and complements other cybersecurity-related ICAO initiatives. It aligns with existing safety and security Standards and Recommended Practices (SARPs) related to cybersecurity and the protection of aviation critical information, in particular related to Annex 17 — *Security*.

2.2 The Strategy highlights the importance of recognizing cybersecurity as a cross-cutting issue that involves all domains of the aviation sector. It synthesizes existing provisions that relate to cybersecurity issues that are spread across the various Annexes into a single framework, focused on the management of cyber risk and improving cybersecurity as a whole. The Strategy provides States with a vision of the civil aviation sector as resilient to cyber-attacks, whilst continuing to innovate and grow.

2.3 The Strategy aims for:

a) the protection of civil aviation and the travelling public from cybersecurity threats that might affect the safety, security and trust of the air transport system;

b) maintaining or improving the safety and security of the aviation system in preserving the continuity of air transport services;

c) States to recognize their obligations under the *Convention on International Civil Aviation* (Chicago Convention) to ensure the safety, security and continuity of civil aviation, taking into account cybersecurity threats; and

d) coordination of cybersecurity measures among State authorities to ensure effective and efficient management of cybersecurity risks.

2.4 The Strategy's aims will be achieved through a series of principles, measures and actions contained in a framework built on seven pillars that include: international cooperation; governance; effective legislation and regulations; cybersecurity policy; information sharing; incident management and emergency planning; capacity building, training and cybersecurity culture.

2.5 A prerequisite for the implementation of the Strategy is that Member States ensure their national legislation and regulations are formulated and applied in accordance with ICAO provisions. This should include the consideration of whether national legislation requires an update or the adoption of new national legislation to allow for the prosecution of terrorist-related cyber threats as well as cyber-attacks negatively impacting civil aviation. The evaluation process and possible update of legislation at the State level may delay the effective implementation of the Strategy and pose a challenge for the harmonization of cybersecurity at the global level.

2.6 The Strategy addresses the need for capacity building and promotion of a cybersecurity culture. To this end, States will require appropriately-trained staff with cross-cutting expertise in aviation and cybersecurity. To achieve this goal, newly developed or updated academic curricula may be needed, and the time and resources for their development will need to be considered.

2.7 A comprehensive multi-disciplinary action plan will be required to ensure the orderly adoption and implementation of measures supporting the aims of the Strategy. ICAO, in cooperation with States and industry, should start the development of such a plan without delay through the appropriate mechanisms dealing with cybersecurity-related matters.

2.8 Cybersecurity is a fast-paced issue and needs to be addressed with a sense of urgency and importance. Therefore, and to highlight the responsibilities and obligations of States and ICAO to collaboratively address cybersecurity, an amended Assembly Resolution will highlight the achievements of States and ICAO in dealing with cybersecurity and the need to implement a Cybersecurity Strategy by adding to the existing A39-19, which was the starting point for ICAO's work on cybersecurity.

2.9 The amended Draft Assembly Resolution presented in the Appendix of this Working Paper further adds an element to the existing Cybersecurity Resolution by highlighting the need for global universal adoption and implementation of the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention) and *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* (Beijing Protocol) as a means for dealing with cyber-attacks against civil aviation.

2.10 It further recognizes the need to continue the work of the SSGC in a more formalized manner, allowing for the structured coordination with other expert groups of ICAO.

3. CONCLUSION

3.1 In the spirit of the Chicago Convention, the global ICAO Cybersecurity Strategy will provide a baseline going forward that is mutually acceptable to all States. It will serve to align international, regional and national cybersecurity frameworks, and promote appropriate information exchange mechanisms that will provide added benefits to cybersecurity risk management.

3.2 The Strategy will provide a flexible framework preparing civil aviation to effectively manage cybersecurity in the coming decades. The Strategy is structured in a modular manner that enables it to be adapted to emerging cyber threats to consider any future developments in civil aviation. It will ensure that all domains of the aviation sector are included and will consider issues in a cross-cutting multi-disciplinary manner.

3.3 The Cybersecurity Strategy will need to be supported by an action plan, including tangible steps to achieve a mature cybersecurity framework. The action plan will draw from guidance on how to implement existing cybersecurity-related SARPS, but will expand on and synthesize these to provide comprehensive guidance on how to achieve the highest degree of cybersecurity.

3.4 The Strategy takes account of existing global plans and further recognizes the need for trained and competent personnel with experience in both aviation and cybersecurity.

— — — — — — — —

APPENDIX A

DRAFT ASSEMBLY RESOLUTION
ADDRESSING CYBERSECURITY IN CIVIL AVIATION

Resolution A~~39-19~~ 40-XX *Addressing Cybersecurity in Civil Aviation*

Whereas the global aviation system is a highly complex and integrated system that comprises information and communications technology critical for the safety and security of civil aviation operations;

Noting that the aviation sector is increasingly reliant on the availability of information and communications technology systems, as well as on the integrity and confidentiality of data;

Mindful that the threat posed by cyber incidents on civil aviation is rapidly and continuously evolving, that threat actors are focused on malicious intent, disruption of business continuity and theft of information for political, financial or other motivations, and that the threat can easily evolve to affect critical civil aviation systems worldwide;

Recognizing that not all cybersecurity issues affecting the safety of civil aviation are unlawful and/or intentional, and should therefore be addressed through the application of safety management systems;

Recognizing the multi-faceted and multi-disciplinary nature of cybersecurity challenges and solutions and noting that cyber risks can simultaneously affect a wide range of areas and spread rapidly;

Reaffirming the obligations under the *Convention on International Civil Aviation* (Chicago Convention) to ensure the safety, security and continuity of civil aviation;

Considering that the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention) and *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* (Beijing Protocol) would enhance the global legal framework for dealing with cyberattacks on international civil aviation as crimes and therefore wide ratification by States of those instruments would ensure that such attacks would be deterred and punished wherever in the world they occur;

Reaffirming the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyber threats;

Considering the need to work collaboratively towards the development of an effective and coordinated global framework for civil aviation stakeholders to address the challenges of cybersecurity, along with short-term actions to increase the resilience of the global aviation system to cyber threats that may jeopardize the safety of civil aviation;

Recognizing the work of the Secretariat Study Group on Cybersecurity, which greatly contributed to the format of the Cybersecurity Strategy by linking safety and security characteristics of cybersecurity;

Recognizing that aviation cybersecurity needs to be harmonized at the global, regional and national levels in order to promote global coherence and to ensure full interoperability of protection measures and risk management systems; and

Acknowledging the value of relevant initiatives, action plans, publications and other media designed to address cybersecurity issues in a collaborative and comprehensive manner.

~~*Recalling* initiatives by the principals of Airports Council International (ACI), the Civil Air Navigation Services Organisation (CANSO), the International Air Transport Association (IATA) and the International Coordinating Council of Aerospace Industries Associations (ICCAIA) and ICAO that recognized the need to work together and be guided by a shared vision, strategy and roadmap to strengthen the global aviation system's protection from and resilience to cyber threats; and~~

The Assembly:

1. *Urges* Member States and ICAO to promote the universal adoption and implementation of the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention) and *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* (Beijing Protocol) as a means for dealing with cyberattacks against civil aviation;

2. *Calls upon* States and industry stakeholders to take the following actions to counter cyber threats to civil aviation*:*

   a) Implement the Cybersecurity Strategy at the Appendix;

   ~~a)~~b)Identify the threats and risks from possible cyber incidents on civil aviation operations and critical systems, and the serious consequences that can arise from such incidents;

   ~~b)~~ c) Define the responsibilities of national agencies and industry stakeholders with regard to cybersecurity in civil aviation;

   ~~c)~~ d) Encourage the development of a common understanding among Member States of cyber threats and risks, and of common criteria to determine the criticality of the assets and systems that need to be protected;

   ~~d)~~ e) Encourage government/industry coordination with regard to aviation cybersecurity strategies, policies, and plans, as well as sharing of information to help identify critical vulnerabilities that need to be addressed;

   ~~e)~~ f) Develop and participate in government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts;

   ~~f)~~ g) Based on a common understanding of cyber threats and risks, adopt a flexible, risk-based approach to protecting critical aviation systems through the implementation of cybersecurity management systems;

~~g)~~ h) Encourage a robust all-round cybersecurity culture within national agencies and across the aviation sector;

~~h)Determine legal consequences for activities that compromise aviation safety by exploiting cyber vulnerabilities;~~

i) Promote the development and implementation of international standards, strategies and best practices on the protection of critical information and communications technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation;

j) Establish policies and allocate resources when needed to ensure that, for critical aviation systems: system architectures are secure by design; systems are resilient; methods for data transfer are secured, ensuring integrity and confidentiality of data; system monitoring, and incident detection and reporting, methods are implemented; and forensic analysis of cyber incidents is carried out; and

k) Collaborate in the development of ICAO's cybersecurity framework according to a horizontal, cross-cutting and functional approach involving air navigation, communication, surveillance, aircraft operations and airworthiness and other relevant disciplines.

3. *Instructs* the Secretary General to:

a) develop an action plan to support States and industry in the adoption of the Cybersecurity Strategy; and ~~Assist and facilitate States and industry in taking these actions; and~~

b) continue to ensure that cybersecurity matters are considered and coordinated in a crosscutting manner through the appropriate mechanisms in the spirit of the Strategy.~~Ensure that cybersecurity matters are fully considered and coordinated across all relevant disciplines within ICAO.~~

— — — — — — — —

APPENDIX B

AVIATION CYBERSECURITY STRATEGY

1. THE VISION OF A GLOBAL AVIATION CYBERSECURITY STRATEGY

1.1 The civil aviation sector is increasingly reliant on the availability of information and communications technology systems, as well as on the integrity and confidentiality of data. The threat posed by possible cyber incidents to civil aviation is continuously evolving, with threat actors focusing on malicious intents, disruptions of business continuity and the theft of information for political, financial or other motivations.

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.

1.3 ICAO's vision for global cybersecurity is that the civil aviation sector is resilient to cyber-attacks and remains safe and trusted globally, whilst continuing to innovate and grow.

1.4 This can be achieved through:

- Member States recognizing their obligations under the *Convention on International Civil Aviation* (Chicago Convention) to ensure the safety, security and continuity of civil aviation, taking into account cybersecurity;
- coordination of aviation cybersecurity among State authorities to ensure effective and efficient global management of cybersecurity risks, and
- all civil aviation stakeholders committing to further develop cyber resilience, protecting against cyber-attacks that might impact the safety, security and continuity of the air transport system.

1.5 The Strategy aligns with other cyber-related ICAO initiatives, and coordinated with corresponding safety and security management provisions. The Strategy's aims will be achieved through a series of principles, measures and actions contained in a framework built on seven pillars:

I. International cooperation
II. Governance
III. Effective legislation and regulations
IV. Cybersecurity policy
V. Information sharing
VI. Incident management and emergency planning
VII. Capacity building, training and cybersecurity culture

2. INTERNATIONAL COOPERATION

2.1 Cybersecurity and aviation are both borderless in nature. Both require cooperation at the national and international level and call for a mutual recognition of efforts to develop, maintain and improve cybersecurity with the aim to protect the civil aviation sector from all cyber threats to safety and security.

2.2 Aviation cybersecurity needs to be harmonized at the global, regional and national levels in order to promote global coherence and to ensure full interoperability of protection measures and risk management systems.

2.3 ICAO is the appropriate global forum to engage States in addressing cybersecurity in international civil aviation. To this end, ICAO will organize, facilitate and promote international events that serve as a platform for knowledge exchange between States, international organizations and industry. States are encouraged to engage in discussions on cybersecurity in civil aviation.

3. GOVERNANCE

3.1 All ICAO Member States are encouraged to support and build upon the ICAO Aviation Cybersecurity Strategy, to ensure the safety, security and continuity of civil aviation in a world increasingly jeopardized by cybersecurity threats.

3.2 States are encouraged to develop clear national governance and accountability for civil aviation cybersecurity. Civil Aviation authorities are encouraged to ensure coordination with their competent national authority for cybersecurity, recognizing that the overall cybersecurity authority for all sectors may reside outside the responsibility of the civil aviation authority. It is also essential that appropriate coordination channels among various State authorities and industry stakeholders be established.

3.3 Furthermore, Member States are encouraged to include cybersecurity in their national civil aviation safety and security programmes. To this end, ICAO should also include cybersecurity in regional and global plans and work towards a common baseline for cybersecurity Standards and Recommended Practices (SARPs).

4. EFFECTIVE LEGISLATION AND REGULATION

4.1 The principal aim of international, regional and national legislation and regulation on cybersecurity for civil aviation is to support the implementation of a comprehensive Cybersecurity Strategy to protect civil aviation and the travelling public from the effects of cyber-attacks.

4.2 Member States must ensure that appropriate legislation and regulations are formulated and applied, in accordance with ICAO provisions, prior to implementing a national cybersecurity policy for civil aviation. Further development of appropriate guidance for States and industry in implementing cybersecurity related provisions is necessary. To this end, ICAO is committed to create, review and amend, as appropriate, guidance material relating to the inclusion of cybersecurity aspects to security and safety.

4.3 Relevant international legal instruments should be analysed to identify existing or missing key legal provisions in air law for the prevention, prosecution, and timely reaction to cyber-incidents in order to

form the basis for consistent and coherent implementation of cybersecurity legislation and regulations throughout the global aviation sector. In the meantime, States are encouraged to ratify ICAO instruments, including the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention) and *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* (Beijing Protocol).

4.4 States are encouraged to consider whether their national legislation requires an update or the adoption of new national legislation to allow for the prosecution of terrorist-related cyber threats as well as cyber-attacks negatively impacting civil aviation. In parallel, States are encouraged to set up appropriate mechanisms for cooperation with 'good faith' security research, which is research activity carried out in an environment designed to avoid affecting the safety, security and continuity of civil aviation.

5. CYBERSECURITY POLICY

5.1 Cybersecurity is to be included within a State's aviation security and safety oversight systems as part of a comprehensive risk management framework.

5.2 Recognizing there are different risk assessment methodologies, priority should be afforded to the amendment and possible development of guidance material related to cybersecurity threat and risk assessments, with the aim to achieve comparability of the outcomes of such assessments.

5.3 Across the civil aviation sector, cybersecurity policies may consider the complete life-cycle of the aviation system, and include elements such as: cybersecurity culture, promotion of security by design, supply chain security for software and hardware, data integrity, appropriate access control, pro-active vulnerability management, improving agility in security updates without compromising safety, as well as incorporating systems and processes to monitor cybersecurity relevant data.

6. INFORMATION SHARING

6.1 The civil aviation sector is a global, interdependent system with many common systems and cyber-attacks can easily spread and have global impact. The objective of information sharing is to allow for prevention, early detection and mitigation of relevant cybersecurity events before they lead to wider effects on aviation safety or security. A culture of information sharing will significantly reduce systemic cyber risk across the aviation sector, the value of which has already been proved across aviation safety and security.

6.2 The sharing of information on such aspects as vulnerabilities, threats, events and best practices, through established and trusted relations can reduce the impact of ongoing attacks. Appropriate information sharing mechanisms must be recognized, in line with existing ICAO provisions.

7. INCIDENT MANAGEMENT AND EMERGENCY PLANNING

7.1 There is a need, in line with existing incident management mechanisms, to have appropriate and scalable plans that provide for the continuity of air transport during cyber incidents. It is recommended that States and the aviation sector make use of existing contingency plans that are already developed and amend these to include provisions for cybersecurity.

7.2 Cybersecurity exercises are a useful tool to test existing cyber resilience and identify improvements, and are therefore highly encouraged. Such exercises can follow different formats (such as table-top exercises, simulations, or real-time exercises) and also vary in scale, (international, national, organizational).

8. CAPACITY BUILDING, TRAINING AND CYBERSECURITY CULTURE

8.1 The human element is at the core of cybersecurity. It is critically important that the civil aviation sector takes tangible steps to increase the number of personnel that are qualified and knowledgeable in both aviation and cybersecurity. This can be done by increasing awareness of cybersecurity, as well as education, recruitment and training. Curricula relevant to cybersecurity, and – where practical – aviation-specific cybersecurity at all levels should be included in the national educational framework as well as in relevant international training programmes. Innovative ways to merge and crosslink traditional information technology and cyber career paths with aviation relevant professionals should be pursued.

8.2 The support and stimulation of skills development in the existing and new workforce should lead to the fostering of cybersecurity innovation and appropriate research and design in the aviation sector. Appropriate job-related training should be provided on a continuous basis to support personnel in their daily roles.

8.3 Cybersecurity could be included in the strategy for the next generation of aviation professionals as ICAO is well-placed to work with States and industry to develop role-based competency requirements for aviation professionals.

8.4 The civil aviation sector has established an enviable safety record which is founded upon a pro-active safety culture which is seen as everybody’s responsibility. The principles of this safety culture are to be applied to develop and maintain a cybersecurity culture across the aviation sector.

— END —