International Civil Aviation Organization

A39-WP/99
EX/45, TE/26
26/7/16

WORKING PAPER

ASSEMBLY — 39TH SESSION

EXECUTIVE COMMITTEE
TECHNICAL COMMISSION

Agenda Item 16 Aviation security
Agenda Item 36 : Aviation safety and air navigation implementation support

CYBER RESILIENCE IN CIVIL AVIATION

(Presented by the United States and by Slovakia on behalf of the European Union and its Member States[1], the other Member States of the European Civil Aviation Conference[2]; and EUROCONTROL)

EXECUTIVE SUMMARY

The civil aviation system consists of a patchwork of interconnected components, systems and networks. The potential for cyber incidents that could jeopardise communications and information exchanges between various aviation stakeholders, impact safety and security and damage aviation business continuity has increased over the years. While the importance of defining an appropriate cybersecurity approach in civil aviation has been recognised by ICAO, additional efforts are still required to increase global awareness and to further develop globally coherent cyber resilience approaches for the aviation system.

Action: The Assembly is invited to :

a) request that ICAO address cyber resilience in civil aviation in a comprehensive manner;
b) request that ICAO and its contracting States promote awareness on cyber threats and vulnerabilities in civil aviation notably through the inclusion of the cyber resilience dimension in relevant processes and activities such as system design, ATM procedures and safety management and aviation security;
c) request that ICAO facilitate, in a secure manner, information sharing between States and relevant stakeholders on cyber-threats, vulnerabilities and mitigating measures;
d) request that ICAO consider necessary steps for the development of guiding principles for managing current and future cyber-threats and vulnerabilities, from identification to mitigation taking into account relevant existing States' measures and industry standards; and
e) request that ICAO instruct existing panels and expert groups to take into account, where relevant, those guidelines, while performing their work.

Strategic Objectives:	This working paper relates to Strategic Objectives: Safety, Air Navigation Capacity and Efficiency, Security, and Facilitation.
Financial implications:	The activities referred to in the attached Assembly paper will be undertaken subject to the resources available in the 2017 – 2019 Regular Programme Budget and/or from extra budgetary contributions

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

[2] Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Iceland, Republic of Moldova, Monaco, Montenegro, Norway, San Marino, Serbia, Switzerland, The former Yugoslav Republic of Macedonia, Turkey and Ukraine.

References:	Doc 10022, *Assembly Resolutions in Force (as of 4 October 2013)* Annex 17 — *Security — Safeguarding International Civil Aviation against Acts of Unlawful Interference*

1. INTRODUCTION

1.1 The aviation system consists of a patchwork of interconnected components, systems and networks. New developments such as the progressive introduction of RPAS and the continuous evolution of the ATM system (e.g. SWIM) reinforce this inter-connectivity and integration of systems. Despite the preventive security measures taken so far, the exposure of the aviation system to cyber-incidents has increased.

1.2 The importance of an appropriate cybersecurity approach in aviation has been recognised at the global level. However, efforts to increase global awareness and to further develop globally coherent cyber-resilience approaches for the aviation system remain necessary.

1.3 Cyber-incidents can affect the global aviation community or individual systems at many levels. These incidents could jeopardise communications and information exchanges between various aviation stakeholders, impacting safety and security and damaging aviation business continuity. The ability to share cyber-related information and the application of strong standardized methods of securing data and information exchange, would enhance the aviation community's ability to protect itself and limit the impacts from cyber-incidents.

2. DISCUSSION

2.1 While a number of initiatives have been developed at local, national, regional and global levels, risks originating from the evolving cyber threat environment in aviation would benefit from a more standardized, consistent and coherent approach.

2.2 Promote global awareness on cyber resilience in aviation

2.2.1 In certain economic sectors such as banking, cyber-threats and vulnerabilities are well known and counter-measures have been implemented to mitigate identified risks. In the aviation domain however, cyber related risks are not always well understood by all States and stakeholders, nor are they addressed in a consistent and systematic manner.

2.2.2 There is a need to increase the awareness of cyber-threats and vulnerabilities in the aviation sector at the global level to ensure that all States and stakeholders identify risks that may arise, and mitigate them.

2.2.3 Such increased awareness could notably be formalised by adapting existing processes e.g. through the development of a security-by-design approach or the implementation of dedicated training. In addition and in coordination with the security related initiatives (e.g. Security Management Systems, where available, or National Civil Aviation Security Programmes), the cyber-resilience dimension should be taken into account in the context of safety management activities, at the organisation level (within its Safety Management System – SMS) as well as at the State or regional level (within State Safety Programme – SSP), and where relevant, in the context of a Regional Aviation Safety Programme.

2.3 Promote sharing of information on cyber-incidents, threats and standardised approaches

2.3.1 No single organisation or stakeholder group will be able to protect itself on its own from intentional unauthorised electronic interference. Furthermore cyber threats are constantly evolving and no one can pretend to be immune from all related possible risks. Effectively coping with cyber-incidents therefore requires States and stakeholders to share relevant information and harmonise how the integrity of data and information exchanges will be protected and maintained. Information sharing would help States and stakeholders to be better prepared to address cyber-incidents and take appropriate actions to mitigate them. Shared information may include occurrence of incidents, vulnerabilities, threats, trends and observed patterns, assessments of shared risks, risk treatment plans, successful mitigation means (technical, operational or organisational) or security assurance activities proven to demonstrate effective protections.

2.3.2 There are already a number of initiatives in aviation which promote sharing of security-related (and often sensitive) information, including at regional and global level, but this remains to be further developed and complemented to support the cyber-resilience of the overall aviation system. Such initiatives may be based on existing platforms for information sharing such as ISAC (information sharing and analysis centre) or CERT (computer emergency response team) and may require establishing common protocols for information sharing regarding cyber incidents, in line with national and regional rules on the protection of sensitive information.

2.3.3 There is also a need to improve the methods of protecting data and the exchange of information between all relevant stakeholders. The standardisation of technical controls that will provide stronger methods of authentication and data authorisation for the global aviation community should be encouraged.

2.4 Promote a "joint aviation risk management approach"

2.4.1 In aviation there are many methodologies to assess risks, most of which are focused on the characterisation and the evaluation of threats and vulnerabilities. While there may be agreement on which elements are needed to characterise risks (e.g. likelihood of occurrence and size of impact), the assessments of specific details are sufficiently diverse to achieve comparable, coherent or even consistent results. However when facing recurring cyber-incidents that may use similar patterns, there are benefits in defining "common principles" and methods to identify, assess, and mitigate the risks.

2.4.2 Such "common principles" should facilitate the identification of threats and vulnerabilities, allow assessing the risks and providing tools for mitigation. One example would be the formal definition of the security scope, describing the context in which risk assessments are performed, and the definition of this scope would assist in identifying critical aviation information systems as foreseen by existing ICAO Annex 17 provisions. Another example would be the consideration of end-to-end "Threat Scenarios", consisting of threats, the system architecture under review, and assets causing the unwanted effects to happen. It also includes known vulnerabilities within the threat scenario, which may need mitigation commensurate with the severity of the impact.

2.4.3 ‘Common principles" of risk assessment in aviation, once defined and adopted, would also ideally be applied in the ICAO framework when developing or amending the Standards and Recommended Practices (SARPs)

— END —