



WORKING PAPER

THIRTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 9 to 19 October 2018

COMMITTEE A

Agenda Item 5: Emerging issues

5.4: Cyber resilience

CYBER RESILIENCE

(Presented by the Secretariat)

EXECUTIVE SUMMARY

The importance of an appropriate approach to cyber resilience in civil aviation has been recognized at the global level and is a crucial matter to be dealt with in the 2019 edition of the *Global Air Navigation Plan (GANP)* (Doc 9750). Successfully managing cyber resilience in an increasingly interconnected aviation system requires a globally harmonized approach between all stakeholders. Without a globally coordinated trust framework to secure ground-ground, air-ground and air-air exchange of information and commitment to building a culture of trust leading to the sharing of cyber-related incident information, cyber resilience may not be assured. It is also recognized that despite the increasing level of reliance on information technology, human involvement is simultaneously a leading cause of, and the first line of defence against, cyber threats and for this reason operational staff should be trained to recognize general aspects of cyber threats and to report any suspected cyber threat or incident.

Action: The Conference is invited to agree to Recommendation 5.4/x – Cyber resilience, in paragraph 3.

<i>Strategic Objectives:</i>	This working paper relates to the Safety and Air Navigation Capacity and Efficiency Strategic Objectives.
<i>Financial implications:</i>	<i>Impact for the aviation community:</i> The introduction of policy, technologies and procedures to guarantee cyber resilience may have significant financial impact for some stakeholders. The impact, however, will depend on the size of the aviation activity and the supporting infrastructure. Safety, efficiency, financial and reputational impacts may also exist if the cyber resilience of the air navigation system cannot be assured. <i>Impact for ICAO (relative to the current Regular Programme Budget resource levels):</i> Since the planning, development and State-level implementation of a global trust framework and further cyber resilience awareness activities will continue over the next triennia, additional resources are required, both financial and human, to support ICAO's efforts in the highly specialized areas associated with cyber resilience and trust framework.

<i>References:</i>	<i>Annex 1 — Personnel Licensing</i> <i>Annex 6 — Operation of aircraft</i> <i>Annex 8 — Airworthiness of Aircraft</i> <i>Annex 10 — Aeronautical telecommunications</i> <i>Annex 11 — Air Traffic Services</i> <i>Annex 14 — Aerodromes</i> <i>Annex 15 — Aeronautical Information Services</i> <i>Annex 17 — Security — Safeguarding International Civil Aviation against Acts of Unlawful Interference</i> <i>Annex 19 — Safety Management</i> <i>Doc 9854 — Global Air Traffic Management Operational Concept</i> <i>Doc 9750 — Global Air Navigation Plan</i> <i>Doc 9896, Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols</i> <i>Doc 10022, Assembly Resolutions in Force (as of 4 October 2013)</i> <i>Doc 10039, Manual on System Wide Information Management (SWIM) Concept</i>
--------------------	--

1. INTRODUCTION

1.1 Aviation is a complex system, made up of a variety of networks and devices that are becoming increasingly connected and mutually dependent for the exchange of digital data and information. Aviation stakeholders such as States, aircraft and aerodrome operators, air navigation service providers (ANSPs) and others have come to rely on interconnected and interoperating information and communications technology (ICT) systems for their day-to-day operations and have become part of a digital civil aviation ecosystem. Developments such as system-wide information management (SWIM), the introduction of remotely piloted aircraft systems (RPAS) and the emergence of future airspace users and stakeholders that are not yet operational only reinforce this interdependency.

1.2 The evolution towards interconnected and interoperating information systems mentioned above brings also new vulnerabilities. Cyber-related events can impact aviation on many levels and can jeopardize the performance of the air navigation system. These events can influence information exchanges between stakeholders, directly affecting safety, capacity and efficiency with potentially severe repercussions.

1.3 In a fully interconnected aviation environment, cyber resilience becomes critical to the safety of operations. The aviation system therefore needs to improve its resilience to cyber threats. Cyber resilience can be defined as the ability of the aviation system to endure and recover from a reduced-performance state resulting from cyber-related threats and incidents, including but not limited to data loss or corruption and system disruptions such as loss of connectivity or interoperability.

1.4 Cyber resilience can be achieved through a combination of standards, procedures and methods that help mitigate cyber threats involving systems critical to the safety and efficiency of aviation.

1.5 The importance of an appropriate cyber resilience approach in civil aviation will be included in the 2019 edition of the *Global Air Navigation Plan* (Doc 9750) and is a key component to realizing the vision outlined in the *Global Air Traffic Management Operational Concept* (Doc 9854). Accordingly, increased stakeholder awareness of cyber threats, vulnerabilities and risks to the aviation system is required to further develop a set of globally coherent cyber resilience approaches for civil aviation.

1.6 In acknowledging the urgency and importance of protecting civil aviation's critical infrastructure, information and communication technology systems against cyber threats, the 39th Session of the ICAO Assembly called for a coordinated approach to achieve an acceptable and commensurate cyber resilience capability on a global scale. In this respect and to promote cyber resilience awareness throughout the aviation community, ICAO established the Secretariat Study Group on Cybersecurity (SSGC) to address aspects of the international aviation system that may be affected by cyber incidents.

2. DISCUSSION

2.1 A cyber-resilient system is necessary to ensure an information-rich environment with real-time data that enables predictive analysis and modelling. Together with a range of automated decision-making and supporting tools, it will enable the evolution of services as envisioned in Doc 9854.

2.2 System interconnectivity and cyber resilience through trust framework

2.2.1 Successfully managing cyber resilience requires a globally harmonized approach amongst all stakeholders. Agreement is needed on how digital information systems should interoperate to provide a shared information-rich environment for the aviation community as a whole. The secure and resilient exchange of information required to cope with the needs of evolving aviation activities can be enabled through a trust framework which consists of coordinated standards, procedures, methods and agreements for the digital exchange of information between ground-ground, air-ground and air-air systems and to regulate an identity system.

2.2.2 Improving the protection of information exchanges amongst stakeholders and from system to system is also required to enhance cyber resilience. Models adopted by other industries and based on open and proven information and communication technology standards such as the concept of trust frameworks, digital certificates and virtual private networking over public internet infrastructure, can serve as an example of how global civil aviation information exchange may be protected.

2.2.3 Ultimately, safety-critical systems and channels used for the exchange of digital information need to be developed and continuously reviewed using a secure-by-design approach where cyber resilience is ensured through both technological and procedural methods.

2.2.4 A global trust framework allows for increased digital systems interoperability and connectivity and therefore increases cyber resilience. The development of an aviation trust framework at a global level should focus on governance, policy and overall technical performance requirements that would be implemented by aviation stakeholders wishing to exchange digital information. Fragmented and uncoordinated approaches at the State or regional level would be ineffective, result in higher costs for all stakeholders and ultimately limit digital systems from connecting and interoperating as well as reduce the cyber resilience of the aviation system.

2.2.5 A global trust framework can only be realized by a standardizing body that has acquired the trust of a sufficient majority of aviation stakeholders and that can intrinsically be relied on for the global coordination of policy, procedures and methods to ensure the safety and efficiency of civil aviation.

2.2.6 A draft concept of operations for a trust framework to support a secure exchange of information is available at (<https://www4.icao.int/ganportal/trustframework>). This preliminary draft serves to provide more information on a trust framework and will be further developed.

2.3 **Information sharing and cyber awareness**

2.3.1 No individual aviation stakeholder can protect itself from all cyber threats on their own. Information sharing would help all aviation stakeholders to be better prepared to address a broader set of cyber-related incidents and increase their ability to mitigate such incidents and reduce risks. Sharing cyber-related information affecting operational safety would further develop a culture of trust between aviation stakeholders that ultimately increases the cyber resilience of the aviation system and increases the awareness of cyber threats for all stakeholders.

2.3.2 All stakeholders are also urged to recognize that despite the increasing level of reliance on information technology, human involvement is simultaneously a leading cause of, and the first line of defence against, cyber threats. Operational staff at all levels should be trained to recognize general aspects of cyber threats and to report any suspected cyber threat or incident, no matter how trivial they may be.

3. **CONCLUSION**

3.1 Aviation systems will continue to be connected at an ever-increasing rate and the digital aviation system will continue to expand. Without a globally coordinated trust framework consisting of governance, policy and overall technical performance requirements for system interconnectivity and interoperability, aviation cyber resilience cannot be assured. The sharing of cyber-related threats and incident information, coupled with appropriate staff training, further enhances cyber resilience. The ongoing safety and efficiency of aviation in an increasingly connected and interoperable digital aviation system demands harmonized cyber resilience approaches at multiple levels that directly benefit all stakeholders now and in the future.

3.2 Considering the importance of addressing cyber-related threats and acknowledging their impact on the resilience of the aviation system, the Conference is invited to agree to the following recommendation:

Recommendation 5.4/x – Cyber resilience

That the Conference:

- a) request ICAO to work with States, industry and international organizations to develop a globally harmonized aviation trust framework including governance, policy, training and overall technical performance requirements to allow the realization of an information-rich and resilient aviation system;
- b) request ICAO to work with States, industry and international organizations to promote the trust framework, explain its benefits and raise awareness of how it enhances cyber resilience; and
- c) urge States, industry and international organizations to work with ICAO to increase the awareness of cyber threats and system resilience processes, and to coordinate cyber-related incident information sharing and training activities.

— END —