International Civil Aviation Organization

A42-WP/124
EX/60
29/7/25

WORKING PAPER

ASSEMBLY — 42ND SESSION

EXECUTIVE COMMITTEE

Agenda Item 13: Aviation Security — Policy

HOLISTIC APPROACH TO AVIATION CYBERSECURITY: FROM CONCEPT TO REALITY

(Presented by Denmark on behalf of the European Union and its Member States[1], the other Member States of the European Civil Aviation Conference[2] and by EUROCONTROL, and co-sponsored by Brazil, Kazakhstan and Peru)

EXECUTIVE SUMMARY

As civil aviation grows increasingly interconnected, cyber threats pose escalating risks to aviation security, safety and efficiency. This paper underlines the need for a holistic cybersecurity approach to overcome fragmented efforts to mitigate cybersecurity related risks.

This holistic approach should be applied to key cybersecurity principles such as establishing governance frameworks, embedding security-by-design in systems, proactive cyber risk management aligned with safety and security protocols, and competency-based training on cybersecurity across all aviation domains. The approach emphasizes lifecycle resilience, global coordination, and integration with existing strategies. ICAO is invited to update policies, foster collaboration and promote capacity-building initiatives to harmonize cybersecurity practices globally.

Action: The Assembly is invited to:

a) encourage ICAO to continue strengthening its policies and Standards and Recommended Practices to support a holistic cybersecurity approach and ensure all its working bodies collaborate to integrate cybersecurity with other regulatory frameworks, promoting a comprehensive and coordinated implementation of cybersecurity measures in civil aviation;

b) urge Member States and all relevant aviation stakeholders to adopt a holistic cybersecurity approach across the civil aviation ecosystem to ensure a harmonised, proactive, and lifecycle-driven approach to managing and mitigating cyber related risks;

c) encourage ICAO to promote capacity-building initiatives in order to support Member States in adopting a holistic cybersecurity approach, making best use of existing capacity-building activities and its own resources; and

d) recognize in Resolution A42-XX, that is proposed to update Assembly Resolution A41-19 on Addressing Cybersecurity in Civil Aviation the need to address cyber threats and risks to civil aviation in a holistic manner.

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

[2] Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Iceland, Monaco, Montenegro, North Macedonia, Norway, Republic of Moldova, San Marino, Serbia, Switzerland, Türkiye, Ukraine and United Kingdom

Strategic Goals:	This working paper relates to Strategic Goal of *Every Flight is Safe and Secure*.
Financial implications:	*The actions referred to in this paper will be subject to the resources available in the Regular Programme Budget and/or from extra budgetary contributions.*
References:	Assembly Resolution A41-19

1. INTRODUCTION

1.1 As civil aviation becomes increasingly interconnected and digitalized, cyber threats pose increasing risks to aviation safety, security and efficiency. This is exacerbated by the speed of development in big data and advanced data processing functions and services. In addition, as systems and applications, both advanced and legacy, become further integrated and interconnected through enhanced networking abilities and utilizing 'smart' components, civil aviation is evolving into a highly progressive, complex ecosystem.

1.2 These interlinkages pose new challenges to the protection of the confidentiality, integrity and availability of information. These challenges need to be addressed holistically, ensuring every aspect of the aviation ecosystem is secure from system design and operation to strategic management in a way that can be consistently applied across the globe.

1.3 To avoid fragmented and isolated efforts, a holistic approach expands cybersecurity concepts in every aspect of organizational practices, proactive and reactive measures, and capability across both authorities and industry. This comprehensive approach aligns cybersecurity efforts across all civil aviation activities enabling a consistent approach to risk management and resilience. Such an approach facilitates the integration of traditional aviation security and safety perspectives with cybersecurity in organizational management systems and strategies, improving their overall effectiveness and performance.

1.4 The establishment of the Ad Hoc Cybersecurity Coordination Committee (AHCCC) by the ICAO Council during the 2022–2025 triennium represents a positive and important step toward addressing cybersecurity in a more coordinated manner. Building on this initiative, there is a strong opportunity to further advance a truly holistic and integrated approach to cybersecurity. Embedding cybersecurity systematically across all ICAO activities, regulatory frameworks, and strategic priorities will strengthen global resilience and ensure that the aviation sector is well-prepared to meet the complex and evolving nature of cyber threats.

2. DISCUSSION

2.1 A holistic approach ensures cyber threats are assessed and risks are mitigated across the entire ecosystem rather than in isolated components. Embedding cybersecurity throughout system development and operations can allow Member States and aviation stakeholders to enhance resilience and contribute to a safe and secure, future-proof aviation sector.

This holistic approach should guide the application of the core cyber principles such as:

2.1.1 **Cybersecurity Governance**: A holistic approach to governance strengthens decision-making, resource allocation, and collaboration across aviation sectors. Effective governance aligns cyber objectives with strategic and operational goals, offering a structured framework for resource management.

It identifies key stakeholders, decision-making processes, legal frameworks, and policies to guide cybersecurity efforts, aiding in threat and risk identification. Furthermore, cybersecurity governance should integrate seamlessly with safety and security domains and business resilience.

2.1.2 **Cybersecurity-by-design**: A holistic "security-by-design" approach to cybersecurity integrates cybersecurity as a core element within the aviation ecosystem, rather than treating it as an add-on. This approach is beneficial as it allows organizations to proactively manage vulnerabilities and enhance resilience by embedding cybersecurity into every development phase. Coupled with a "security-by-default" methodology, it strengthens aviation infrastructure and processes from conception to operation. Effective implementation involves early-stage threat modelling, secure engineering principles, and lifecycle risk assessments to address vulnerabilities pre-emptively. Continuous monitoring, regular updates, and automated response mechanisms further enhance system agility against emerging cyber threats, fostering a robust cybersecurity posture across the aviation ecosystem.

2.1.3 **Managing Cyber Risks**: In the rapidly evolving landscape of technology and data processes within civil aviation, it is crucial to identify, protect and make resilient critical assets and infrastructures (e.g. ATM) from cyber attacks, including from emerging threats like AI. The interconnected nature of modern systems expands the cyber threat landscape, necessitating a holistic cyber risk management approach. By interconnecting cyber risk management with other risk management disciplines, aviation can create a comprehensive and resilient framework that balances safety, security, and efficiency. This strategy strengthens the ability to mitigate risks and enhances resilience against evolving cyber related threats.

2.1.4 **Cybersecurity Knowledge and Competencies:** Developing a holistic approach to cybersecurity training in aviation is essential for building robust competencies. This comprehensive strategy ensures individuals acquire the necessary skills to manage cybersecurity risks and measures effectively. Training should be practical, role-specific, and blend theoretical knowledge with hands-on experience. A culture of continuous learning helps aviation personnel stay updated on the latest practices and trends, apply good practices, enabling them to identify vulnerabilities and implement effective mitigation strategies. Regular programs, workshops, and simulations should target all levels, extending beyond IT personnel to include all staff. Such a training approach not only strengthens the overall cyber resilience of the aviation ecosystem but also equips all staff to better anticipate and respond to cyber threats, enhancing the sector's cybersecurity posture.

2.2 ICAO, as the global leader in promoting best practices for aviation, plays a crucial role in enhancing aviation cybersecurity. Given the varying levels of maturity and resources among States, ICAO should promote capacity-building initiatives in order to support Member States in adopting a holistic cybersecurity approach. By doing so, ICAO should make best use of existing capacity-building activities (e.g. Interregional Seminars on Innovation & Cybersecurity organised under the framework of the CASE Projects, which are financed by the European Commission and implemented by the European Civil Aviation Conference (ECAC), ECAC training courses on cyber security) and its own resources. These initiatives should promote a consistent and coordinated approach to strengthening cybersecurity capabilities while fostering international collaboration through the exchange of best practices.

2.3 Additionally, ICAO should ensure that its Standards and Recommended Practices, policies and tools remain up to date, providing Member States with the necessary frameworks to effectively manage cyber risks and adopt a holistic cybersecurity approach. Furthermore, ICAO’s working bodies should strengthen their collaboration to ensure that cybersecurity provisions are effectively integrated with other regulatory requirements. In this context, the Ad Hoc Cybersecurity Coordination Committee (AHCCC) has a role in facilitating and guiding this coordination, supporting a comprehensive and cohesive strategy across the aviation sector.

2.4 To advance this comprehensive approach, it is proposed that the 42nd ICAO Assembly recognize — through Resolution A42-XX, updating Assembly Resolution A41-19 — the need to address cyber threats and risks to civil aviation in a holistic manner. Embedding this recognition at the Assembly level will strengthen Member States' commitment to integrating cybersecurity systematically across all aviation activities, ensuring global alignment and enhancing the sector's collective resilience.

3. ACTIONS

The Assembly is invited to adopt the Actions presented above.

— END —