International Civil Aviation Organization

HLCAS/2-WP/18
16/10/18

WORKING PAPER

SECOND HIGH-LEVEL CONFERENCE ON AVIATION SECURITY (HLCAS/2)

Montréal, 29 to 30 November 2018

Agenda Item 2: Future approaches to managing aviation security risks

DEVELOPMENT OF A GLOBAL CYBERSECURITY STRATEGY

(Presented by Romania)

SUMMARY

This paper presents recommendations for States and industry that should actively support the development of a global cybersecurity strategy in civil aviation.

Action by the High-level Conference on Aviation Security is in paragraph 4.

1. INTRODUCTION

1.1 The Europe, Middle East and Africa (EMEA) Cybersecurity in Civil Aviation Summit was held in Bucharest, Romania from 7 to 9 May 2018. The Summit was attended by 416 delegates from fifty-five States and nineteen International organizations. The Summit discussed how to harmonize and promote cybersecurity frameworks.

1.2 The Summit recalled the *Dubai Declaration on Cybersecurity in Civil Aviation*, initially presented in Dubai on 5 April 2017. Furthermore, it recognized the work of the ICAO Secretariat Study Group on Cybersecurity (SSGC) and its ongoing work with a view to addressing all elements of the international aviation framework that may be affected by cyber incidents.

2. DISCUSSION

2.1 A decade ago, cybersecurity received little attention as an international issue in the aviation industry. From the beginning of the current decade, aviation experts have warned that a malicious cyber-attack on civil aviation operations could potentially be catastrophic. As technology radically transforms design, production, operation and maintenance, models of safety and security must adapt.

2.2 The cyber space became a vital substrate for economic, social, and political interactions. Along with rising interdependence and economic opportunity, however, came vulnerability and insecurity. With big data, machine learning, and the “Internet of Things,” some experts anticipate that the number of Internet connections may grow to nearly a trillion by 2035. The number of potential targets for attack, by both private and state actors, will expand dramatically, and include everything from industrial control systems to heart pacemakers, self-driving cars, drones and last but not least civil aviation.

2.3 Similar to other industries that embraced “the digital revolution”, aviation has to maintain trust from stakeholders by accurately perceiving vulnerabilities and opportunities as well as understanding adversary threats. The following are the challenges facing a connected and digitalized civil aviation:

2.3.1 As the aviation industry increasingly connects systems and services, the potential attack surface of systems that an adversary could engage with is growing larger and more complex, resulting in a bigger target.

2.3.2 Since the aviation industry relies heavily on technology, more and more on cyber environment, understanding and overcoming the cultural differences between the two industries will require global reform. Developing a shared culture, viewing the challenges and potential solutions together will require cross-disciplinary cooperation.

2.3.3 Perception of the threat posed by digital power is going to be critical in understanding and managing the risk. It is necessary that everyone in the industry attains the same level of perception and understanding in order to address the potential risk and promote a collaborative dialogue that values multiple perspectives.

2.3.4 The aviation industry has decades of experience in addressing safety and security issues, but the cybersecurity challenge is comparatively new. It may take longer to develop and replace aviation systems than it does for perpetrators to develop capabilities, creating a challenge in accurate risk assessment and threat models.

2.3.5 Investments in Air Traffic Management (ATM) are already paying dividends, but using advanced technologies such as Global Positioning Systems (GPS), digital communication and Automatic Dependent Surveillance-Broadcast (ADS-B) means we have to manage the vulnerabilities that arise from these technologies and encourage cyber resilience.

2.3.6 Airports are federations of several distinct organizations with potentially different approaches and the cyber vulnerability of one can affect all others. Appropriate protection of physical security systems from cyber threats at airports is critical.

2.3.7 National and international policies and regulations are agreed and understood for safety and physical security, but it is yet unclear how aviation cybersecurity can achieve the same maturity and clarity. That is why ICAO, EASA, EUROCONTROL, ECAC, as well as other multilateral entities, must stay shoulder to shoulder for developing policy and regulation, coherent systems thinking, governance and accountability, resilient trust and secured human decision-making process in a shared, cross-functional and cross-border cyber environment.

2.3.8 ICAO is in a strong position to draw together the numerous global aviation cyber security initiatives and bring coherence, leadership, and set Standards. In order to promote coherency in developing cybersecurity standards among nations, and promote dialogue and collaboration among disparate stakeholders there is a need of a critical assessment of the Annexes (8, 10, 17, 18, etc.) of the Chicago Convention and they have to be amended accordingly from the cyber security standpoint. There is a real need to recognize that unlawful interference through cyber means is now a reality, as well as incorporating cyber perspectives with many parallels to the current physical focus.

2.3.9 Developing cybersecurity capabilities – the synergy among people, technology and processes – using an information network-based operation approach and being able to detect, protect, defend, analyze, decide and react, as well as restore, will ensure the resilience of civil aviation in the foreseeable future.

2.3.10 Comprehensive and timely information sharing will minimize risks, and the added value of such collaborative work is a better management of cybersecurity for stakeholders. The newly established European Center for Cybersecurity in Aviation with links into the CERT EU, Aviation-Information Sharing and Analysis Center or Security Operations Centers are cybersecurity force multipliers for Member States.

2.3.11 Civil-military information sharing is also important. How the military perceives and approaches the challenge of securing aircraft and systems within environments that face radio frequency jamming and spoofing, and cyber threats may have lessons for civil aviation.

2.3.12 EASA produced the "Bucharest Declaration on high-level efforts in civil aviation cybersecurity" with a focus on several objectives, such as coordination at a European level, international cooperation, risk assessments, increasing awareness, information sharing and research and development. There was also a desire for the regulations to be internationally harmonized because the challenges need a wider holistic approach.

3. CONCLUSION

3.1 Considering that in order to develop a cybersecurity life cycle, cyber risk management stretches from concept, design, assurance, supply, construction, delivery, operations and maintenance; there is therefore a need for an overarching, comprehensive and integrating approach. In order to bridge the gap between the present status and the desired outcome there is a need to act for countering the risks and threats in the new cyber environment sooner rather than later.

3.2 The Officials and representatives from States, regional and international organizations, and industries participating in the ICAO Europe, Middle East, and Africa Cybersecurity Summit in Civil Aviation convened in Bucharest, Romania from 7 to 9 May 2018, to address challenges to international civil aviation from cyber threats.

3.3 Mindful of the need to ensure the safety, security and continuity of civil aviation in an orderly manner we recommend that:

3.3.1 State and industry cybersecurity frameworks be developed in a harmonized way to the maximum extent possible;

3.3.2 States and industry foster regional cooperation in the definition of common strategies, exchange of information and best practices, following the example of already existing initiatives;

3.3.3 Trust frameworks to enable secure information sharing where appropriate are being promoted;

3.3.4 States and industry collaborate to identify long-term human resource needs and establish strategies to attract, education, and retain the next generation of aviation professionals; and

3.3.5 States and industry actively support the development of a global cybersecurity strategy, under the auspices of the International Civil Aviation Organization.

4. ACTION BY THE HIGH-LEVEL CONFERENCE

4.1 The High-level Conference on Aviation Security is invited to endorse the conclusions and to support the need for an overarching, comprehensive and integrating approach in the cybersecurity area.

— END —