MINISTRY
OF INFRASTRUCTURE
AND CONSTRUCTION

EASA
European Aviation Safety Agency

Civil Aviation Authority

High Level Conference Cybersecurity in Civil Aviation

Krakow Declaration

8-9 November 2017, Kraków, Poland

The Krakow Conference has been built on the discussion held during the High Level Meeting on Cybersecurity in Civil Aviation held in Bucharest on 8-9 November 2016 and the High Level Conference on Drones held in Warsaw on 23-24 November 2016.

Subsequent to these two Conferences, the European Strategic Coordination Platform (ESCP) has been established and initiated its Engagement Phase. It is developing its Charter until end of 2017 and coordinates the work on the Cybersecurity in Aviation horizontal rule EASA is proposing to address objectives common to all aviation stakeholders. The objective is to engage all stakeholders in a fair and non-discriminatory fashion in establishing a resilient European civil aviation system, creating the largest level playing field in the world.

The Conference discussed the progress achieved for aviation ground systems so far, including institutional set-up, legislation advancement, risk assessment methodology, cybersecurity promotion, research activities, commitments and resources devoted to cybersecurity and to establish a ground for the future European strategy for Cybersecurity in Aviation and the Cybersecurity Road Map that will define the future actions that have to be undertaken at European level in order to ensure a secure environment for aviation covering the cyber-space.

The Conference:

- called upon the Council and the European Parliament to conclude the negotiations on the revision of Regulation 216/2008 namely to clarify the role of EASA within cybersecurity,
- called upon the European Commission and the European Aviation Safety Agency to develop and adopt Implementing Regulations addressing Cybersecurity in Aviation with harmonised common objectives but tailored requirements for subjects and sub-sectors, assuring commensurate responses to risks,
- called on the Member States of the European Union to address cybersecurity nationally, in line with Directive 2016/1148 (NIS Directive),
- recognised the need that the safety critical elements of aviation flow in a consistent and coordinated way with the existing EU NIS Directive ground base,
- acknowledged the role of the European Union Agency for Network and Information Security (ENISA) in aligning the responses of cyber threats against essential services, including civil aviation, at European level,
- acknowledged the importance of the European Strategic Coordination Platform (ESCP[1]) to coordinate the European approach to Cybersecurity in Aviation in Europe,

[1] Members: ACI Europe, Aerospace Industries Association of America Inc.- AIA (Boeing), Airlines for Europe - A4E (Lufthansa), ASD, CANSO (ENAV), CERT-EU, DG CNECT, DG Move, ECA, ECAC (FOCA), ENISA, EUROCONTROL NM, European Defence Agency, European Independent Maintenance Group – EIMG, GAMA, IATA, ICAO, SESAR Deployment Manager, SESAR Joint Undertaking, Member States (Poland), Member States (UK), Member States (Finland), EASA.

- called upon the European Commission, the European Aviation Safety Agency (EASA) and the National Aviation Authorities to take the next steps in their System-of-Systems approach in order to create a level playing field in Cybersecurity in Aviation among all stakeholders relevant for European aviation,
- encouraged the European Aviation Safety Agency (EASA) to ensure that the European Plan for Aviation Safety (EPAS) reflects all efforts required at European level,
- acknowledged the role of the European Centre for Cyber Security in Aviation (ECCSA) to facilitate information sharing among aviation stakeholders including the drone industry and to coordinate the response to cyber-threats,
- supported the international commitment of EASA to support other Regional Safety Oversight Organisations (RSOOs) with its experience related to concepts, rulemaking, and training for oversight,
- called upon the continuation of the research and development activities for Cybersecurity as part of the overall Cybersecurity strategy of the European Union, e.g. to find solutions resolving the “stability/agility” dilemma,
- suggested to invite EU institutions to ensure a high level of priority of aviation-relevant subjects in the next Research Framework Programme (FP9),
- invite all relevant research actors including SESAR Joint Undertaking, Shift2Rail, national research institutions, industry, etc. to join efforts,
- acknowledged the objective to secure the use of solely digital information from the origin of the Definition of Need to its fulfilment in aviation, in response to the benefits possible by the emergence of new digital technologies,
- recognized the valuable contribution on Cybersecurity in Aviation from the European Civil Aviation Conference (ECAC), notably the works of its Study Group on Cyber Security in Civil Aviation, including the updated ECAC Doc 30 Recommendations on cyber security and supporting Guidance Material and invite ECAC and EASA to join efforts,
- called on airports, Ground Handling Operators, maintenance organizations, air navigation service providers to develop information security management systems in accordance with specific procedures and appropriate standards,
- recommended to harmonise the security risk assessment methodologies,
- recognised that cybersecurity is an interdisciplinary problem in transport that has its challenges in aviation, but also in shipping, rail and road transport,
- called upon a stronger partnership between regulators, operators, service providers, and manufacturing industry, in particular within the ESCP, where EASA welcomes and supports the Industry to come with standards,
- stressed the need to conclude the ESCP engagement phase before end of 2018 with:
    - the signing of the partnership Charter,
    - the adoption of the Aviation Cybersecurity Strategy, including its Roadmap,

  and underlined the importance to start immediately afterwards the operational phase,
- welcomed the joint EASA / Computer Emergency Response Team (CERT-EU) initiative to inform on a regular basis the transport community on the cyber situation an threats.
- acknowledged the need to evaluate the progress made together with ESCP within 12 months.