High Level Meeting
Cybersecurity in Civil Aviation

Bucharest, Romania, Palace of the Parliament, 8-9/11/2016

Bucharest Declaration

On 8 and 9 November 2016 a high level meeting took place in Bucharest, Romania, regrouping key stakeholders from industry, airspace users, Member States, European institutions, academia and cyber security institutions to discuss the aviation cybersecurity risk picture, actions already taken and ways forward.

Since a similar event, which took place in May 2015, a roadmap has been developed jointly by the Commission and EASA in close cooperation with EU Member States and Industry. Member States have embarked on the revision of the basic regulation, in which cybersecurity is addressed. EASA is in the process of implementing a European Centre for Cyber Security in Aviation. Collaboration with industry and regional and international organisations has gained momentum.

Context

Cyber security incidents are increasing in frequency, magnitude and complexity, and have no border. Civil aviation is an increasingly attractive target for adversaries. New technologies such as e-enabled aircraft, new generation CNS/ATM systems and drones are changing the risk landscape of the aviation system. At the same time, the rationalisation and concentration of the aviation IT infrastructure and the multiplication of network connexions will create new vulnerabilities.

There is a concern that the aviation system is insufficiently protected against cyber threats and that there is an urgent need to develop a holistic response. It is recognised that EASA should support any European initiative to develop such response but that the agency is not yet empowered to address cybersecurity across all aviation domains.

Enabling Objectives

In order to achieve a comprehensive, seamless and adaptive level of protection of the European aviation system against cyber threats, the HLM meeting participants agreed that a layered defence approach is necessary and identified the following enabling objectives:

Coordination

Although security threats may vary from one state to the other, it is necessary to have a European coordinated approach for cybersecurity in aviation, between industry and institutional stakeholders, and between aviation security (AVSEC) and aviation safety actors.

EASA will be tasked to facilitate a strategic EU coordination platform for cybersecurity in aviation, in order to avoid gaps and duplications in the efforts to be taken at European level, while ensuring also collaboration at regional and international level.

Bucharest Declaration

National aviation authorities are encouraged to organise coordination with organisations responsible for cybersecurity on their national level.

Sharing of Information and Reporting

The sharing of information about cyber threats, incidents and vulnerabilities is an essential element of the layered defence approach.

This sharing of information should be the combination of both mandatory reporting flows (e.g. of relevant incidents to NAAs) and of voluntary, trust based information sharing systems, which can be facilitated both by industry (e.g. EA-ISAC) and EASA (ECCSA).

In accordance with the intent of the NIS Directive, NAAs are encouraged to set up an aviation sector-specific Computer Security Incident Response Team, closely collaborating with ENISA and ECCSA on the European level, and to organise the sharing of information.

Member States should initiate the development of cyber intelligence information and establish secure dissemination of threat-related information, towards those stakeholders who need to know.

Regulations

In order to ensure both a level playing field and a balanced sharing of risk management, cybersecurity in aviation will require risk and performance based sectorial regulations that:

- Should allow for addressing the evolution of threats and technologies.
- Should be internationally harmonised
- Established as a solution compliant with the NIS directive and existing national regulations
- Should benefit from industry standards to the greatest extent possible.

Risk Assessments

Cybersecurity risk assessments should be coherent, their outputs should be comparable and the resulting decision making should be based on common risk acceptability criteria.

For this purpose common terminologies and risk assessment methodologies need to be developed or recognised, leveraging where possible the proven functional approach of safety assessments.

High Level Meeting
Cybersecurity in Civil Aviation

Bucharest, Romania, Palace of the Parliament, 8-9/11

Bucharest Declaration

Cybersecurity Promotion, Awareness and Preparedness

Cybersecurity is a mind-set that needs to be shared by all actors.

Stakeholders should endeavour to develop cybersecurity awareness and preparedness in their organisations, by means of awareness campaigns, skill development, trainings and exercises.

For this purpose training curricula should be made consistent and cross-domain exercises organised.

Knowledge and Foresight

Research and studies should be conducted to expand the collective knowledge on current and future cyber risks, and on the ability to protect civil aviation systems against cyber threats. This research activity should be adequately coordinated with the relevant national and European research programmes

Commitment and Resources

All stakeholders should endeavour to allocate the appropriate level of resources (human, financial and technical) for cyber security in aviation.

Next Steps

A European Strategic Coordination Platform will be set up in order to coordinate the definition and implementation of a European strategy for Cybersecurity in Aviation. This Platform will include representatives of key industry stakeholders, Member States, and EU institutions.
A first meeting will be scheduled early 2017 in Cologne.