CYBER THREAT TO CIVIL AVIATION

– ECA Position Paper –

Background

Global aviation connectivity is ramping up with the generalization of non-aviation specific technology such as big data, cloud-based infrastructures, mobile networks, electronic flight bags, onboard internet, satellite communications and navigation. The typical commercial and cargo flight now generates and requires a large amount of data that is critical to the safe operation of the aircraft.The abundance of legacy aircraft, dated technology and unencrypted data transfer protocols pose their own challenges and add to the complexity.

ECA has identified that aircraft, ground facilities, and other critical infrastructures are vulnerable to cyber-attacks and therefore are at significant risk of unsafe situations that may, ultimately, even cause loss of life.

The reason for ECA concern: cyber risks

In this respect, aviation is not different from other industry sectors. Cyber-attacks occur and are increasing. Over 200 incidents/events have been identified by EATM-CERT alone in 2019[1]. Depending on attacker profile - state-sponsored, cyber-crime, hacktivism, or isolated individuals - the goal of these attacks can range from simple system reconnaissance or confidential data leakage to sensitive information tampering, or even to full system takeover and/or destruction.

Facing such a constantly evolving threat, the aviation sector cannot claim to be cyber secure, it should develop and maintain cyber resilience instead.

A regulatory response to cyber threat is needed

This is more than ever a shared responsibility of authorities, aircraft manufacturers, airlines, airports, pilots and air traffic control organizations together with their suppliers. An ‘isolationist’ approach will not work and considering that a system or service could manage or survive a cyber-attack because "nothing" happened in the past is an illusion.

The EU Commission has already put forward an ambitious rule-making process.

ECA particularly welcomes the EASA’s European Strategic Coordination Platform (ESCP) and the European Plan for Aviation Safety (EPAS). The definition of an

[1] 2020 Report on cyber in aviation, EATM-CERT, EUROCONTROL, 10 June 2020

European Cockpit Association AISBL

Rue du Commerce 20-22, 1000 Brussels, Belgium I T +32 2 705 32 93 I eca@eurocockpit.be I www.eurocockpit.be

Information Security Management System scheme on the same model as SMS for Aviation Safety, with mandatory reporting of aviation cyber events is a good example and can be positively quoted.

ECA encourages the growth and development of the European Centre for Cyber Security in Aviation (ECCSA) and promotes similar frameworks at the global level (ICAO).

Training, Information Sharing, Accident Investigations

All these new regulations should not only provide technical requirements. Proper training of all personnel including flight deck crew is of paramount importance in the mitigation of cyber risks.

Like other industries, such as banking, information sharing has also proven to be vital in the protection of critical infrastructure. In aviation, the sharing of information is greatly lacking. If parties were to share information confidentially – e.g. on security breaches, detected attack patterns and best practices – the security performance of the system would benefit significantly.

Moreover, ECA underlines that the multiplication of local/national initiatives and instances can be deleterious. A comprehensive and coordinated global response should be promoted.

Finally, regarding incident and accident investigations, cyber-attacks should be considered as a potential contributory factor and included in any accident root cause analysis.

ECA recommendations

ECA considers cyber threats to be a significant and increasing threat to the safety of aviation. Therefore, ECA firmly believes it should be addressed in a coordinated and timely manner both by industry and regulators. ECA strongly recommends to:

- Ensure all steps are taken to reach the highest level of information security to promote confidentiality, integrity and availability of information exchange in the aviation sector;
- Ensure that aviation personnel are trained to recognize and manage cybersecurity risks: a mandatory chapter on cybersecurity could be included in all NCASPs;
- Promote mandatory reporting of cybersecurity incidents and ensure clear reporting lines and protocols;
- Enhance cooperation between industry, IT, and avionics specialists: apply proven means that other domains have adopted for many years;
- Assess cyber-attack as a potential contributory factor in root-cause analysis in aviation incident/accident investigations.

European Cockpit Association AISBL
Rue du Commerce 20-22, 1000 Brussels, Belgium I T +32 2 705 32 93 I eca@eurocockpit.be I www.eurocockpit.be