Cyber Threat to Civil Aviation
– ECA Position Paper -

Background

The global aviation system and its critical elements are a potential target for cyber-attacks. 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. This risk increases with connectivity.

The purpose of this paper is to consider this threat and suggest measures that would contribute to best address it.

The reason for ECA concern: cyber risks

The typical commercial flight operation, whether passenger or cargo, generates and requires a large amount of data that is critical to the safe operation of the aircraft. Much of the technology currently in use was developed at a time when aircraft were not directly linked to the outside world, data input was completed manually, and therefore most of the systems were not designed to protect the information they carry. Furthermore, most communications between systems cannot be checked for integrity and completeness.

Cyber-attacks occur very frequently, one only needs to consider the number of phishing and scamming events that effect the general population to appreciate this global problem. They can be carried out from virtually anywhere and by anyone with sufficient knowledge, using low-budget methodologies.

The goal of these attacks can be to obtain confidential, critical or sensitive information, to manipulate or erase information and/or to control or destroy systems or services that could even result in uncontrollability of aircraft. In terms of extent of damage, they can result in local, limited perimeter or, worse, large scale cyber-attacks. In many cases, the compromised system may have not even been targeted but is taken down as a result of an attack elsewhere: in other words, it is a victim of “collateral damage”.

European Cockpit Association AISBL

Rue du Commerce 20-22, 1000 Brussels, Belgium I T +32 2 705 32 93 I F +32 2 705 08 77 I eca@eurocockpit.be I www.eurocockpit.be

Therefore, cyber security needs to be considered throughout all aviation communications pathways and applications. This cannot be done by single entities for their own systems only.

Due to the interdependencies in the realm of aviation, *cyber security is a shared responsibility* of authorities, aircraft manufacturers, airlines, airports and air traffic control organizations together with their suppliers.

Since public safety and security is at stake, it is the responsibility of States to ensure that all parties involved protect their part of the infrastructure and in coordination with all others. It is not acceptable to work in isolation and/or with the perspective that this is “someone else’s job”.

A regulatory response to cyber threat is needed

The European Commission should put forward regulation with the aim of setting the minimum requirements that the aviation industry must fulfill. These requirements could be specific technical cyber security measures but, preferably, they will be outcome-focused. Unlike physical security, cyber security techniques provide many ways to measure security performance; therefore, a risk-based strategy is definitely the way forward.

Such regulation should not only provide technical requirements. Proper training of all personnel is a significant factor in the mitigation of cyber risks. Contingency planning is a key aspect as well, and therefore all personnel that use safety critical systems, including flight deck crew, should also be adequately trained to detect actual cyber-attacks and act accordingly. This has to be addressed at regular intervals and compliance should be audited by the Authorities.

ECA believes the topic would be best addressed by requiring the National Civil Aviation Security Programmes (NCASPs) to contain a mandatory chapter on Cyber Security dealing with the issue in a comprehensive and holistic manner.

The European Commission should define the minimum requirements that would cover at least the issues of governance, risk assessment and testing/auditing.

Information sharing is paramount

The importance of an appropriate cyber security approach in aviation has been recognized at the global level. However, efforts to increase awareness and to further develop consistent cyber-resilience approaches for the aviation system remains essential.

In other industries – such as banking - information sharing has proven to be vital in the protection of critical infrastructure. In aviation, the sharing of information is greatly lacking and cyber risks are not always understood by States and relevant stakeholders. If parties were to share information on security breaches, detected attacks and best practices, the total (global) security performance of the system

would benefit significantly. To achieve this goal/objective, confidentiality is key. Partners must be able to trust that the information will not be made public, until appropriate countermeasures have been implemented.

Considering that the voluntary approach to reporting and sharing of information has been in place for several years now but with limited results, it is time for the EU and its Member States to seriously consider establishing a *mandatory reporting system for aviation-related cyber security incidents*, as well as proactively looking for evidence of such incidents (logs collection and analysis, monitoring, audits, etc.).

This would help in finding trends in threats, so to take appropriate action when appropriate. It would also help making sure all players in the aviation industry participate in the information sharing effort.

In this respect, ECA particularly welcomes the EASA's initiative to team up with CERT-EU[1] to cooperate in the establishment of a European Centre for Cyber Security in Aviation (ECCSA)[2]. Nevertheless, ECA is of the opinion that for the ECCSA to become an effective tool, a gradual shift to a model of mandatory reporting of cyber security incidents will be necessary.

More crucial, given the sensitivity and importance of the issue at stake, ECA believes that cyber security in civil aviation would be best dealt with by a single body/entity. This would also entail the requirement to ensure that the body in question is equipped with adequate resources. This should be a pre-requisite for any entity willing to take over this important task.

ECA recommendations

ECA considers cyber to be a significant threat to the safety of aviation. Therefore, ECA firmly believes it should be addressed in a coordinated manner and without delay, both by industry and regulators. In particular, ECA supports a holistic approach to this particular threat since addressing the issue purely on a technical level is insufficient. Institutional policies, human factors (training, expertise, security culture, etc.) and pan-organisational processes would need to be part of this effort.

To conclude, ECA strongly recommends to:

- Include a mandatory chapter on cyber security in all NCASPs;
- Establish a mandatory reporting of cyber security incidents.
- Set up dedicated and specific training for all personnel that use safety critical systems, incl. flight crew.
- Enhance cooperation between industry, IT and avionics specialists.
- Guarantee data protection and confidentiality in the exchange of information amongst all relevant stakeholders.

Brussels, 28.04.2017

[1] Computer Emergency Response Team of the EU Institutions (CERT-EU).
[2] https://www.easa.europa.eu/newsroom-and-events/news/easa-cooperate-cert-eu-cybersecurity