Dossier 45 – Cyberattacks targeting air transport
Executive Summary and Recommendations

The Working Group of the Air and Space Academy focused its thinking on the following theme:

Cyberattacks may cause accidents or create serious incidents that endanger passengers and crews.
How to reduce the risks of occurrence and avert their consequences?

In order to understand the subject as a whole, it should be noted that the world of commercial air transport forms an ecosystem or system of systems (SoS) composed of the following elements:

- airliners
- airlines
- manufacturers, suppliers and subcontractors
- air traffic management (ATM)
- airports
- access and service providers[1]
- maintenance companies

and all associated personnel.

Civil aviation is increasingly **connected** thanks to modern communications means (Internet, etc.) that allow high flow rates for passengers and crews. Ground systems connectivity is also improving with the development of new air traffic management systems (notably SESAR[2] in Europe and NextGen[3] in the USA).

The openness of the systems in question significantly increases the attack surfaces of air transport. Consequently, in this digital transformation, **safety and security models** must rapidly evolve to demonstrate that **cybersecurity[4]** has been taken into consideration. The plane and its crew can no longer be "isolated" during the flight but must be capable of being autonomous, while being both connected and cyber-resilient.

[1] Among other aspects, service providers manage ground-to-air links and make data available.

[2] The SESAR (Single European Sky Air Traffic Management Research) programme is designed to update current systems to provide Europe with efficient air traffic management systems.

[3] Next Generation Air Transportation System is the new US ATM system currently under development. Designed to replace the National Airspace System, it is due to be deployed in the country between 2012 and 2025.

[4] The term “cybersecurity” includes the notions both of security against cyberattacks and their impact on the safety of people and goods.

2.1 Risks

Attacks against air transport can take the form of "denial-of-service" or **jamming** to block the incoming communication signals. Other possible attacks on communication links include **spoofing** (i.e. the transmission of **false data**), on the ground or on board aircraft. Depending on the corruption of such data, the consequences can be serious if there is no means of verifying the **availability**, **authenticity**, **integrity**, **confidentiality** and **traceability** of the information provided. Attacks may also target **operational software**, on board or on the ground. The presence of **malicious codes** (malware), programmed to trigger harmful actions at a specific time, is obviously a significant threat. Such malware may have been integrated at manufacturing stage of the aircraft by an agent of the manufacturer, an equipment manufacturer or a subcontractor, or may also have been inserted during maintenance operations or regular data updates.

2.2 Risk management

As with risks involving hostile humans, it is necessary not only to provide fixed or adaptable protections, but also to set up organisational and human processes to fight against the attack with tools suited to the threat.

Cyber-attackers are able to find flaws in practically all fixed defences of systems, including firewalls and other protections. The only real protection would be physical, with no wired or wireless communication and no possibility to transmit data by USB stick or other, but this type of protection is no longer practicable in a digitised, connected world. However, some relatively simple measures can slow down most attackers.

The high level coordination entity must ensure that all players comply with a predefined **security policy** (as recommended in ISO 270001 Standard[5]). When effective defence procedures are used, the different players' responsibilities must be clear at all times:

• In defence actions, make the distinction between detection/identification of attacks and their consequences, in order to optimise action

• Be capable of deceiving the attacker to direct them to less dangerous actions

• Be able to map threats and attackers.

2.3 Recommendations

Vis-à-vis the industrialists

Engineering, **production**, **operations** and **maintenance** activities must be screened to identify, address and prevent potential vulnerabilities.

Recommendation R1: Processes and techniques to protect manufacturers', suppliers' and subcontractors' industrial resources against cyberattacks shall be set up and monitored in order to achieve the same level of security as the Information System of the prime contractor. Action: Manufacturers, equipment suppliers and subcontractors.

[5] https://www.iso.org/isoiec-27001-information-security.html

Recommendation R2: All operators (including their freight forwarders) involved in the maintenance of onboard and ground equipment shall be certified, trained in cybersecurity procedures and regularly audited[6].
Action: Manufacturers, equipment suppliers and subcontractors.

Recommendation R3: A policy for updating operational software and data shall be defined and implemented by all actors, with **authorised personnel**, **dedicated and safe means** and **secure procedures**. In particular, this includes regular implementation of software protection patches.
Action: Airlines, manufacturers, equipment manufacturers, maintenance companies and service providers.

At design stage

Although cabins are still vulnerable to possible breaches of security, aircraft cockpits are well protected, especially on most recent aircraft, thanks to successive barriers and anti-intrusion filters. **Multimedia entertainment systems,** though, are much more open to cyberattacks.

Recommendation R4: Onboard **multimedia entertainment systems** for passengers shall comply with cybersecurity rules to protect system operation and passengers' data; it must be possible to **shut them down quickly**. Because of their rate of evolution, their security condition readiness shall be regularly controlled.
Action: Airlines, IFE[7] suppliers and maintenance companies.

Tablets and Electronic Flight Bags

Recommendation R5: Software, data and Internet connection of **Electronic Flight Bags (EFB)** and other electronic cockpit tablets shall **imperatively be secured**. Safety demonstrations - including technical checks by specialised cybersecurity empowered personnel - **are mandatory**.
Action: FAA, EASA and National Authorities.

Communications

Digital technology is everywhere: in voice and datalink communications, in navigation, surveillance and anti-collision systems.

Recommendation R6: Ground communications between air and ground shall be **segregated between different users (pilots, cabin crew and passengers)**. A risk reduction analysis based on the technical impacts and costs of the various solutions[8] is to be carried out.
Action: Manufacturers and airlines.

Radionavigation and positioning data

Recommendation R7: To counter the non-availability or non-integrity of GNSS[9] satellite

[6] At least as often as stipulated in the ISO 9001 et 27001 standards

[7] IFE: In-Flight Entertainment

[8] This separation can be achieved either by using distinct communication terminals, or a single terminal, separating links by frequency, or again by multiplexing links on the same frequency but separating them logically (use of a virtual private network , VPN, for critical links).

[9] GNSS: Global Navigation Satellite System, which includes the satellite constellations GPS, Galileo, Glonass, Beidou.

location information, **SBAS** and **GBAS**[10] systems shall evolve and **redundancy of ground-based radio-navigation means shall be maintained** in order to keep degraded mode air traffic flowing.
Action: EASA[11], National Authorities and Air Navigation Services.

Surveillance: ADS / B

An important potential vulnerability concerns **ADS/B**[12], a means of **surveillance** to identify and locate aircraft. Currently under deployment in the United States and Europe, ADS/B is a pillar of the air traffic management system renovation programmes SESAR and NextGen. ADS/B data is continuously transmitted by the transponder of the aircraft without the latter needing to be interrogated by the secondary radars on the ground.

ADS/B allows anyone to constantly monitor planes trajectories. Attackers using ADS/B protocol are potentially capable of generating information on "false aircraft" or transmitting false locations to the ground. Ground controllers and the crew then have to manage these false aircraft and remove doubts, which can lead to a degraded safety level. ICAO[13] (in a June 2017 document), and the US GAO[14] alert on the vulnerabilities of ADS/B and recommend that States take risk reduction measures.

With ADS/B data issued by aircraft, mainstream sites (such as Flight Radar 24 and others) broadcast real-time information on the tracking of commercial flights.

Recommendation R8: Before switching to the use of ADS/B as the primary means of surveillance, a **risk analysis** shall be carried out, which may lead to the setting up of additional monitoring means. The ADS/B standard should evolve to improve its level of cyber-security protection (i.e. with data authentication and/or encryption)[15].
Action: ICAO, FAA[16] and EASA.

Protections, human factors, supervision and control
There can be no total protection; there will always be flaws in connected aeronautical infrastructures: the question is not **whether** there will be attacks, but rather **when** they will be. Air transport must therefore be more **cyber-resilient**, to ensure that aircraft remain safe and reliable, regardless of the type of attack. To this end, it is essential that **systems** and **personnel** develop **control** capabilities, recognise precisely what to do when an incident occurs, and of course, react immediately. It is also vital to detect "weak signals" that may precede cyber-incidents, denial-of-service or other attacks.

Recommendation R9: Personnel at risk of **cyberattacks** on air transport shall be **trained** in the methods and practices for detecting, countering or limiting a possible cyberattack.
Action: All actors.

Feared events are not necessarily plane crashes, but potential disorganisation or panic, whether on board, in control centres or in terminals. These events can have significant

[10] SBAS: Satellite Based Augmentation System. GBAS: Ground Based Augmentation System.

[11] EASA: European Aviation Safety Agency - www.easa.europa.eu

[12] ADS/B: Automatic Dependant Surveillance – Broadcast. The aircraft periodically sends its position and other information to ground stations and other aircraft in the zone equipped with ADS-B. It emits on the 1090 MHz frequency.

[13] ICAO: International Civil Aviation Organization - www.icao.int

[14] Government Accountability Office report, January 2018: www.gao.gov/assets/690/689478.pdf

[15] Authentication and encryption means are widely used, for instance in banking and the judiciary system.

[16] FAA: Federal Aviation Administration - www.faa.gov

media, economic and social repercussions leading to loss of confidence in air transport. There can also be theft of commercial information, data or files, or disorganisation of the “Supply Chain” with manufacturing blockages at subcontractor level. All these **feared events** shall be **analysed** in order to assess on the one hand the probabilities of occurrence, depending on the criteria of **ease, attractiveness and impunity,** and on the other hand the potential gravity of the consequences.
With regard to **flight safety**, the basic principle is that the crew shall ensure data consistency relating to the trajectory and energy status of the aircraft in the short term (heading, vertical and horizontal speeds, altitude, thrust) and medium term (programmed waypoints, altitude constraints, approach and programmed track, etc.).
The aircraft must also be "transparent" and the crew should on the one hand have easy access to all information in autopilot mode and, on the other, have at their disposal tools and procedures to rapidly validate this data before its activation: one must not believe any uploaded data to be true without verifying it.
In case of doubt, the proposed data must be refused and other modes used as needed.

What solutions?
Technical solutions exist, but **flaws** are also often of **human** origin. It is therefore important to create devices with improved resistance to unsafe human intervention, with "deep defences" or successive barriers to be crossed before reaching the data. In addition, long-term actions should be carried out to raise the **awareness** of the personnel, not limited to crisis periods, and not overlooking aspects such as organisation, empowerment and training of personnel.

Each actor in the air transport industry (large airline or small service provider) shall exercise monitoring, supervision and control through regular audits. In particular, the online and offline update and maintenance operations of the aircraft are to be monitored very closely, as they are an easy gateway to human interventions that can corrupt both the hardware and the data, and introduce malware.

Crisis management

When a cyber-attack is declared during operation, despite implementation and monitoring of the previous preventive measures, then action must be taken by the concerned entities, on ground and on board, in a coherent manner at national, European, or even worldwide level when necessary.
The procedures and rules to be used by crews to thwart threats will only be effective if the time required to implement them is compatible with the time available to correct the corrupt situation. However, these can be complex, risky unexpected situations, during take-off or landing phases for instance. This available time parameter shall be taken into account in the definition of corrective actions.
Similarly to organisation of the civil or defence security forces of each country, each actor involved in air transport must comply with a **safety policy** precisely defining the operating modes to be used when faced with the different types of attack, whether observed or anticipated.

Recommendation R10: Crisis management procedures shall be elaborated to deal with cyber incidents and shared with all actors.
Action: all air transport stakeholders.

Management of cybersecurity and lessons learned

A cybersecurity management system should exist for all air transport stakeholders, and should include a verification that the rules of IT health are properly applied and are accompanied by measures for the prevention and treatment of incidents.

Incidents will occur. Unfortunately, the player on the receiving end of the attack tends not to divulge the information - and it is difficult, even after much digging, to find the real causes of incidents and to distinguish between failures, bugs, false manipulations or real acts of malicious intent.

As with the analyses conducted into air incidents and accidents, the human factors that cause cyber-incidents should be systematically examined and exploited. These include not only the decisions and actions that have been used to detect and counter a threat in due time, but also those that have resulted in a "successful" attack.

Key Recommendation R11: All certified air transport actors shall **mandatorily report, share and then systematically process cyber-incidents** in the same way as air accidents and incidents are reported, shared and analysed in a process that has lead to a significant increase in air transport safety.
Action: ICAO, FAA, EASA and National Authorities.

Public actors have assumed their responsibilities. The US Department of Homeland Security holds briefings for cybersecurity professionals to share information about potential threats, new tools used by perpetrators and how they work.
The French Agency for Security Information Systems (ANSSI) and the European Centre for Cybersecurity in Aviation (ECCSA, created in 2017 under an EASA initiative) are aware of the threats related to air transport and analyse, characterise and share them (in a secure way) with the concerned actors. These agencies have yet to reach full capacity.

Industrialists in the United States have set up Information Sharing and Analysis Centers (ISACs). The same kind of centres are in the process of being created in Europe.

Standards, certification and regulatory aspects

With regard to **regulation and certification**, some standards exist but remain to be applied, and their implementation must then be regularly monitored by audits conducted by certified authorities or laboratories. There is, however, no coordination and harmonisation of regulations at worldwide level.

Key Recommendation R12: There is an **urgent** need to develop **a harmonised worldwide regulatory framework** for cybersecurity in civil aviation, within a global management system (integrating security and safety) and to ensure its implementation and compliance **through qualified cybersecurity entities**.
Action: ICAO.

The example of the security standards of the payment card industry is an interesting one. Set up in the 2000s, a standard was created to increase control over cardholder information in order to reduce the fraudulent use of various payment instruments. Banking authorities - while retaining their role of certification - delegated responsibility for the technical evaluation to qualified trusted third parties to enable an efficient industrial response internationally.

The certification of interbank exchanges for credit cards, as well as procedures for updating Internet “boxes”, should serve as examples in order to develop a system of **cyber-certification** in the area of air transport and to ensure the security condition readiness.

Recommendation R13: Certification and authentication processes for sensitive data exchanges based on industry standards shall be developed or adapted and implemented. Action: Industry.

Governance

The real difficulties concern **governance and responsibility**, complex problems linked to different legal regimes, to public and private actors and to different links in the supply chain. The chain of **cyber-trust** in civil aviation needs to be strengthened.

International organisations such as ICAO, IATA, CANSO, EASA, etc. are aware of cyber threats and risks to air transport. As emanations of States and of the involved actors, instead of limiting themselves to understanding, acknowledging, recognising, encouraging, promoting, supporting, welcoming, ... they should obtain **mandates from them to act quickly**.

Key Recommendation R14: ICAO shall lead and coordinate at worldwide level all activities contributing to enhancing cybersecurity in civil aviation. EASA and national authorities shall be **given a mandate** to **define and decide on cyber action plans** and quickly put in place **roadmaps** with associated **resources and timelines** together with minimum short term measures.

Of course, the above recommendations can only be adopted and implemented by means of close coordination, harmonisation and collaboration between all air transport stakeholders.