Name: José María Peral Pecharromán
Position: Regional Officer, Aviation Security and Facilitation
International Civil Aviation Organization-ICAO

December 01, 2020
Global cyber-trends
Cybersecurity scope
Air transport ecosystem
Concerning scenarios
Acts of unlawful interference
Annex 17 SARPs and guidance material
Air Traffic Management Security Manual
More users and devices

Wider networks and faster connections

Easier data storage and new efficient data types

More usages and new services

Less isolated architectures

Quick adoption of new technologies
Physical Security

Data Security

Security roles, responsibilities, and accountabilities

Risk Management

Education and training

Monitoring

Recovery
 IT network crashes/lack of disaster recovery plans
 Confidentiality, integrity, and availability of data
 Cyber hygiene across entities
 Denial-of-service (network unavailable to its intended users)
 Precision navigation and timing disruption (e.g. jamming, spoofing)
 Lack of encryption or authentication
 Incident management across regions/borders
Acts of unlawful interference

- Unlawful seizure of aircraft,
- Destruction of an aircraft in service,
- Hostage-taking on board aircraft or on aerodromes,
- Forcible intrusion on board an aircraft, at an airport or on the premises of an aeronautical facility,
- Introduction on board an aircraft or at an airport of a weapon or hazardous device or material intended for criminal purposes,
- Use of an aircraft in service for the purpose of causing death, serious bodily injury, or serious damage to property or the environment,
- Communication of false information such as to jeopardize the safety of an aircraft in flight or on the ground, of passengers, crew, ground personnel on the general public, at an airport or on the premises of a civil aviation facility.
4.9.1 Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference.

4.9.2 Recommendation – Each Contracting State should ensure that measures implemented protect, as appropriate, the confidentiality, integrity and availability of the identified critical systems and/or data. The measures should include, inter alia, security by design, supply chain security, network separation, and the protection and/or limitation of any remote access capabilities, as appropriate and in accordance with the risk assessment carried out by its relevant national authorities.
ATM security definition

((ICAO Circular 330, Civil/Military Cooperation in Air Traffic Management)

The contribution of the ATM system to civil aviation security, national security and defense, and law enforcement; and the safeguarding of the ATM system from security threats and vulnerabilities.

ATM security has dual requirements of protection of the ATM system against threats and vulnerabilities and the provision of ATM security services in support of organizations and authorities engaged in aviation security, national security, defense, and law enforcement.
Facility physical security and access control (ATM facility design considerations, NAVAIDs, etc.)

Personnel security programme (position risk categorization, personnel screening and vetting, third-party personnel security, etc.)

Information and Communication Technology (ICT) system security (unauthorized access, tampering with the systems, attacks on the systems)

Contingency planning for ATM security (planning, system degradation to a safe/secure situation, service continuity, recovery, maintenance of plans)
❖ ATM contribution to safeguarding against unlawful interference

❖ ATM support for law enforcement (e.g. laser threats, man-portable air defence system threats)

❖ Disasters and public health emergencies (e.g. disaster response and recovery, communicable disease and other public health risks on board aircraft)

❖ Airspace management for ATM security (monitoring and reporting over security identification zones, emergency security control of air traffic, creation and monitoring of temporary airspace/flight restrictions)
THANK YOU!

2020-12-01 CANSO Cybersecurity webinar #1 - December 1st