EASA
European Union Aviation Safety Agency

Workshop 1: “Cybersecurity from the global aviation perspective”

Juan Anton

Cybersecurity in Aviation & Emerging Risks Section Manager

5th – 7th February 2020

Workshop on Cybersecurity in Aviation

Aviation Partnership Project

Sri Lanka

Your safety is our mission.

An Agency of the European Union

Cybersecurity risks are a global challenge

Elements driving the cybersecurity risks

Aviation is a “System of Systems”, covering all aviation domains, and where products, services and organisations are increasingly interconnected.

Cybersecurity risks have no borders and are driven by the notion of malicious intent, where vulnerabilities are exploited and an accident is not a fortuitous event.

Cybersecurity risks evolve very quickly, which requires industry and authorities to do business differently.

The role of ICAO

The role of ICAO

- **In 2016, ICAO Assembly Resolution A39-19 instructed ICAO to develop a comprehensive cybersecurity work plan and governance structure;**

- **As a result, the SSGC (Secretariat Study Group for Cybersecurity) was established** under the authority of the Secretary General, being chaired by the Deputy Director for Aviation Security and Facilitation. **The SSGC is structured in four working groups:**
  - Working Group on Flight Safety (ANB lead)
  - Working Group on Air Navigation Systems (ANB lead)
  - Working Group on Airlines and Aerodromes (ATB lead)
  - Research Sub-Group on Legal Aspects (ATB/LEB lead)

The role of ICAO

- **Significant outcomes of the work of the SSGC:**
  - **Development of ICAO Cybersecurity Strategy**
    - Endorsed by ICAO 40th Assembly in October 2019
  - **Development of ICAO Cybersecurity Action Plan**
    - Presented to the SSGC for discussion and approval in December 2019.
    - Defines the cybersecurity programme for the next triennium.
    - Needs to be endorsed by the ICAO Council.

The ICAO Strategy: Main pillars

- **Cybersecurity Strategy – Main pillars**
  - International Cooperation
  - Governance
  - Effective Legislation and Regulation
  - Cybersecurity Policy
  - Information Sharing
  - Incident Management and Emergency Planning
  - Capacity Building, Training and Cybersecurity Culture

The ICAO Strategy: Main pillars

- **International cooperation:**
  - ICAO is the appropriate global forum to engage States in addressing cybersecurity in international civil aviation;
  - ICAO to facilitate and promote international events in the cybersecurity field.
- **Governance:**
  - States encouraged to support and build upon the ICAO Cybersecurity Strategy;
  - States to develop clear national governance and accountability for civil aviation cybersecurity;
  - States to include cybersecurity in their national civil aviation safety and security programmes.

The ICAO Strategy: Main pillars

- **Effective legislation and regulation:**
  - ICAO to provide States the basis for the development of appropriate legislation and regulation needed for the comprehensive implementation of the Cybersecurity Strategy;
  - ICAO to create, review and amend guidance material relating to the inclusion of cybersecurity aspects to safety and security.

- **Cybersecurity Policy:**
  - States to ensure that cybersecurity is a part of aviation security and safety systems and comprehensive risk management framework.

The ICAO Strategy: Main pillars

- **Information Sharing:**
  - ICAO to develop the Cybersecurity Repository and Point of Contact Network for sharing information on aspects such as vulnerabilities, threats, events and best practices.

- **Incident Management and Emergency Planning:**
  - States to amend existing contingency plans, include provisions for cybersecurity and conduct exercises to test cyber resilience.

The ICAO Strategy: Main pillars

- **Capacity Building, Training and Cybersecurity Culture:**
  - States to ensure that qualified personnel are hired, that there is increased cybersecurity awareness and training, and that cybersecurity innovation and research are promoted, along with cybersecurity culture – understanding the responsibility.

ICAO: Next steps

→ States to implement the Cybersecurity Strategy;

→ ICAO Council to endorse the Cybersecurity Strategy Action Plan;

→ ICAO to promote the Cybersecurity Strategy and the Action Plan;

→ States to develop their own action plan for the implementation of the Cybersecurity Strategy;

→ ICAO to start the implementation of the Action Plan and to monitor its implementation by States.

The creation of Regional Platforms and the experience of the European case

Background information on EASA involvement on cybersecurity

- **EASA has been working on cybersecurity matters for a long time:**
  - **Initially, only for the certification of aircraft and engines (since 2003)**
  - **Later (after 2011), introducing certain cyber requirements for organisations involved in *Air Traffic Management, Air Navigation Services and Aerodrome operations***

- **In May 2015, the European Commission tasked EASA to develop an Action Plan to:**
  - **Develop a coordinated defense against cyber threats**
  - **Minimize duplication and remove loopholes in regulation**

As a result, EASA started working on a *"Comprehensive EU Cybersecurity Strategy for Aviation"* in coordination with EU Institutions and Agencies, States and stakeholders.

1. The importance of involving all the affected parties

The European Strategic Coordination Platform (ESCP)

- **Members:**
  - European Commission *(DG-MOVE, DG-CNECT, DG-GROW and DG-HOME)*
  - Other EU Agencies and Organisations *(EEAS, EUROPOL, EASA, ENISA, CERT-EU, EUROCONTROL, SESAR)*
  - European Defence Agency
  - States *(ECAC plus 6 EU individual Member States: Finland, France, Poland, Romania, Sweden, UK)*
  - EU relevant Aviation industry associations: *Aircraft/Engine manufacturers (ASD), Airlines (A4E, IATA, ERAA), Helicopter Operators (EHA), Aerodromes (ACI), Air Navigation Services (CANSO), Air Crew and maintenance personnel (ECA, ETF), Maintenance Organisations (EIMG), General Aviation (GAMA).*
- **Observers:**
  - ICAO (International Civil Aviation Organisation), FAA (US aviation authority), TCCA (Canada aviation authority), AIA (US manufacturers), AIAC (Canada manufacturers), NATO

The European Strategic Coordination Platform (ESCP)

- **The ESCP has been meeting regularly for more almost 3 years.**

- **The ESCP has been discussing, among other aspects:**
  - The development of an EU aviation cybersecurity strategy and action plan.
  - The approaches to take in order to coordinate this strategy at global level.
  - The development of common regulations for the management of cybersecurity risks.
  - The development of common methodologies for the risk assessments performed by different organisations.

2. The importance of developing a common EU cybersecurity strategy

The Strategy for Cybersecurity in Aviation

- **Developed by the European Strategic Coordination Platform (ESCP) and published on the EASA website on 10th September 2019**
- **According to this strategy, the future aviation systems needs to be:**
  - **A trustworthy and dependable environment,** where the different organisations can rely on the services and information provided by others
  - **A system-of-systems capable to adapt and to withstand new threats without significant disruptions,** following a systemic approach for current and legacy systems.
- **And the effort is focused on two aspects:**
  - **Making Aviation an evolutionary cyber-resilient system**, which, under attack, can maintain its essential functionalities.
  - **Making Aviation self-strengthening by adopting a "built-in security" approach** developed since the systems' conception.
- **The strategy also contains objectives to achieve "cyber resiliency" and "built-in security".**
- **The ESCP is working on the associated Implementation Plan**

3. The importance of global coordination

International Cooperation and Harmonization

ICAO SSGC (Secretariat Study Group on Cybersecurity)

- This is where all cybersecurity activities are coordinated at ICAO level.
- One of the activities has been the development of a global ICAO cyber strategy and action plan.
  - Members from EASA and from the ESCP have participated to ensure a coordinated approach between the global ICAO cyber strategy and the EU cyber strategy, as well as the associated action plans.

Other initiatives

- **FAA (ederal Aviation Administration):** Mainly on regulatory activities and standards.
- **Military Sector:** Since both civil and military share the same airspace.
- **Other EU Agencies:** Covering other transportation modes (ERA, EMSA).

4. The importance of developing an EU regulatory framework consistent with other EU cyber requirements

Common rules for the management of cybersecurity risks:

- → **Introducing common requirements for Information Security Management Systems and reporting of incidents.**

- → **Covering all aviation domains and interfaces, and applicable to organisations and authorities** *(aviation is a system-of systems).*

- → **Consistent with other EU requirements** such as NIS Directive 2016/1148 and Aviation Security Regulation 2015/1998 *(no gaps, loopholes or duplications).*

5. The importance of facilitating the coordination between the different authorities within each Member State

Coordination between authorities within the Member States

- **Essential because:**
  - **Cybersecurity is just at the interface between security and safety.**
  - In most cases, **there are different authorities within the Member States responsible for safety and security**:
    - National Aviation Authorities, Ministries, Cybersecurity Agencies, etc.
  - **There are different EU regulatory frameworks including cybersecurity requirements, with possible different authorities responsible for each one of them:**
    - Directive 2016/1148 (NIS Directive for essential services)
    - Regulation 2015/1998 (Aviation security)
    - Future EASA rules (currently under development)

  It is important to align regulatory requirements and inspection regimes.

6. The importance of promoting and facilitating the collaboration and information sharing between different parties, supported by adequate research initiatives

Collaboration and Information Sharing

ECCSA (European Centre for Cybersecurity in Aviation)

- **Objectives:**
  - Promote networking and information sharing among organisations and authorities, promoting a cybersecurity culture and trust environment.
  - Increase the understanding of risks and threats, and overall situational awareness.
- **Currently implemented with the support of CERT-EU (Computer Emergency Response Team of the European Union)**
- **Currently around 25 members.**

EASA
European Union Aviation Safety Agency

Questions

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union