ICAO

RECONNECTINGTHEWORLD

ICAO Global Aviation Cybersecurity Framework

Rashad Karaky
Aviation Cybersecurity Officer
International Civil Aviation Organization

Agenda

- ICAO's Work on Cybersecurity & Cyber Resilience
- The Aviation Cybersecurity Strategy and Action Plan
- Capacity Building Initiatives
- Cybersecurity Guidance Material
- ICAO Universal Security Audit Programme

ICAO's Work on Cybersecurity & Cyber Resilience

- **Legal Instruments:**
  - The Beijing Convention and The Beijing Protocol of 2010

ICAO's Work on Cybersecurity & Cyber Resilience

Governments' Adoption of the Beijing Instruments is an Important **DETERRENT of Cyber-Attacks** Against Civil Aviation

CONVENTION

on the Suppression of Unlawful Acts Relating to International Civil Aviation

Done at Beijing on 10 September 2010

CONVENTION

sur la répression des actes illicites dirigés contre l'aviation civile internationale

Faite à Beijing le 10 septembre 2010

CONVENIO

para la represión de actos ilícitos relacionados con la aviación civil internacional

Hecho en Beijing el 10 de septiembre de 2010

КОНВЕНЦИЯ

Совершена в Пекине 10 сентября 2010 года

制止与国际民用航空有关的非法行为的公约

2010 年 9 月 10 日于北京

اتفاقية

BEIJING
10 SEPTEMBER 2010

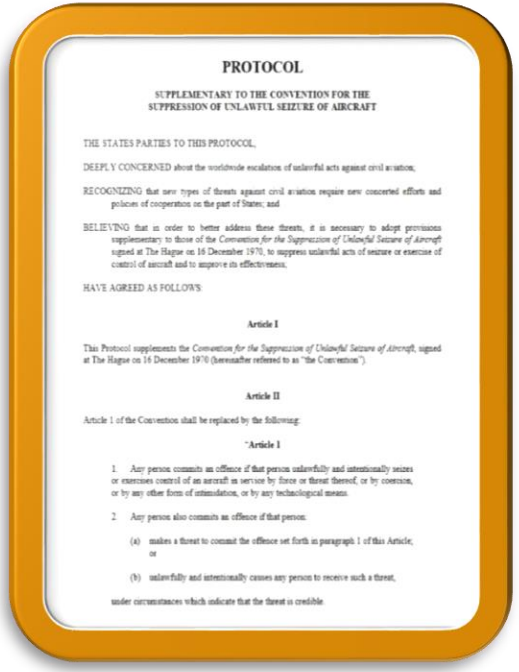
BEIJING
10 SEPTEMBRE 2010

BEIJING
10 DE SEPTIEMBRE DE 2010

BERLIN
10 СЕНТЯБРЯ 2010 ГОДА

北京
2010 年 9 月 10 日

بيجين
١٠ سبتمبر (أيلول) ٢٠١٠



PROTOCOL

SUPPLEMENTARY TO THE CONVENTION FOR THE SUPPRESSION OF UNLAWFUL SEIZURE OF AIRCRAFT

THE STATES PARTIES TO THIS PROTOCOL,

DEEPLY CONCERNED about the worldwide escalation of unlawful acts against civil aviation;

RECOGNIZING that new types of threats against civil aviation require new concerted efforts and policies of cooperation on the part of States; and

BELIEVING that in order to better address these threats, it is necessary to adopt provisions supplementary to those of the *Convention for the Suppression of Unlawful Seizure of Aircraft* signed at The Hague on 16 December 1970, to suppress unlawful acts of seizure or exercise of control of aircraft and to improve its effectiveness,

HAVE AGREED AS FOLLOWS:

Article I

This Protocol supplements the *Convention for the Suppression of Unlawful Seizure of Aircraft*, signed at The Hague on 16 December 1970 (hereinafter referred to as "the Convention").

Article II

Article 1 of the Convention shall be replaced by the following:

"**Article 1**

1. Any person commits an offence if that person unlawfully and intentionally seizes or exercises control of an aircraft in service by force or threat thereof, or by coercion, or by any other form of intimidation, or by any technological means.

2. Any person also commits an offence if that person:

(a) makes a threat to commit the offence set forth in paragraph 1 of this Article; or

(b) unlawfully and intentionally causes any person to receive such a threat,

under circumstances which indicate that the threat is credible.

ICAO's Work on Cybersecurity & Cyber Resilience

- **Legal Instruments:**
  - The Beijing Convention and The Beijing Protocol of 2010
- **Standards and Recommended Practices:**
  - Annex 17 – Aviation *Security*: Standard 4.9.1 and Recommended Practice 4.9.2

ICAO's Work on Cybersecurity & Cyber Resilience

Annex 17 to the Chicago Convention – Aviation *Security*

- **Standard 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.
- **Recommended Practice 4.9.2**
  - Recommendation— *Each Contracting State should ensure that the 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.*

ICAO's Work on Cybersecurity & Cyber Resilience

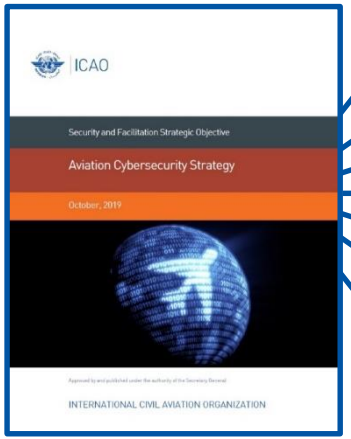
- **Legal Instruments:**
  - The Beijing Convention and The Beijing Protocol of 2010
- **Standards and Recommended Practices:**
  - Annex 17 – Aviation *Security*: Standard 4.9.1 and Recommended Practice 4.9.2
- **Assembly Resolutions:**
  - A39-19 and A40-10 Resolutions on Cybersecurity

ICAO's Work on Cybersecurity & Cyber Resilience

ICAO 40th Assembly Resolution A40 – 10: *Addressing Cybersecurity in Civil Aviation*

- Recognizes that cybersecurity risk can simultaneously affect a wide range of areas;
- Reaffirms the obligations States have under the Chicago Convention;
- Highlights the need for global universal adoption and implementation of the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing Convention) and Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing Protocol);
- Recognizes the need for aviation cybersecurity to be harmonized; and
- Calls upon States to implement the Cybersecurity Strategy.

The Aviation Cybersecurity Strategy



- International Cooperation
- Governance
- Effective Legislation & Regulations
- Cybersecurity Policy
- Information Sharing
- Incident Management & Emergency Planning
- Capacity Building, Training, & Cybersecurity Culture

https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx

The Cybersecurity Action Plan

- **First Edition** published in November 2020.
- **Second Edition** published in January 2022.
- **TLP Green** (asp@icao.int to request a copy) + **Published on ICAO-NET**.
- Provides **the Foundation** for ICAO, States and stakeholders to work together, and proposes a **Series of Principles, Measures, and Actions** to achieve the objectives of the Cybersecurity Strategy's seven pillars.
- **Develops the Seven Pillars** of the Aviation Cybersecurity Strategy into **32 Priority Actions**, which are further broken down into **51 Tasks** to be Implemented by ICAO, States, and Stakeholders.

The Cybersecurity Action Plan (Examples)

Action #	By	Traceability to the Aviation Cybersecurity Strategy	Traceability in Action Plan	Specific Measures/Tasks	Indicators	Priority	Start Date of Implementation
CyAP 2.3	ICAO, Member States, and Industry	2.2	6.3.2 See also para 8.1. of the Action Plan	Develop guidance material to support organizations in implementing coordinated cybersecurity management frameworks to support the establishment of a systematic approach to manage aviation cybersecurity risks and assess those frameworks' maturity and effectiveness.	Publication of guidelines.	High	2023
CyAP 4.4	ICAO, Member States, and Industry	4.3	8.1	Develop a policy for security by design as a basis for a secure life-cycle of civil aviation systems.	Policy for secure life-cycle of civil aviation systems formulated.	Medium	2022 - 2023
CyAP 4.8	ICAO, Member States, and Industry		8.2	ICAO to develop risk profiles for each operational domain. Member States and Industry to contribute by developing similar risk profiles at national and organizational levels.	Availability of risk profiles.	High	2023
CyAP 6.3	ICAO, Member States, and Industry	6.1	10.1	Develop guidance for civil aviation cyber-incident response and recovery capabilities, including contingency and emergency response plans.	Publish guidance for civil aviation cyber-incident response and recovery capabilities, including contingency and emergency response plans.	High	2022 - 2023

ICAO's Work on Cybersecurity & Cyber Resilience

- **Legal Instruments:**
  - The Beijing Convention and The Beijing Protocol of 2010
- **Standards and Recommended Practices:**
  - Annex 17 – Aviation *Security*: Standard 4.9.1 and Recommended Practice 4.9.2
- **Assembly Resolutions:**
  - A39-19 and A40-10 Resolutions on Cybersecurity
- **Guidance Material:**
  - Doc 8973 – *Aviation Security Manual*
  - Doc 9985 – *ATM Security Manual*
  - Aviation Cybersecurity Strategy
  - Cybersecurity Action Plan
  - Using Traffic Light Protocol
  - Cybersecurity Culture in Civil Aviation
  - Cybersecurity Policy Guidance

Cybersecurity Guidance Material

- ✓ Facilitates Cybersecurity information sharing using Traffic Light Protocol.
- ✓ Minimizes Human Error in sharing sensitive information.
- ✓ Supports cybersecurity & Cyber resilience objectives.

Cybersecurity Guidance Material

- ✓ Facilitates Cybersecurity information sharing using Traffic Light Protocol.
- ✓ Minimizes Human Error in sharing sensitive information.
- ✓ Supports cybersecurity & Cyber resilience objectives.

- ✓ Calls to focus resources and actions to achieve a systemic approach to cybersecurity in civil aviation.
- ✓ Supports the protection and resilience of international civil aviation's critical infrastructure against cyber threats.

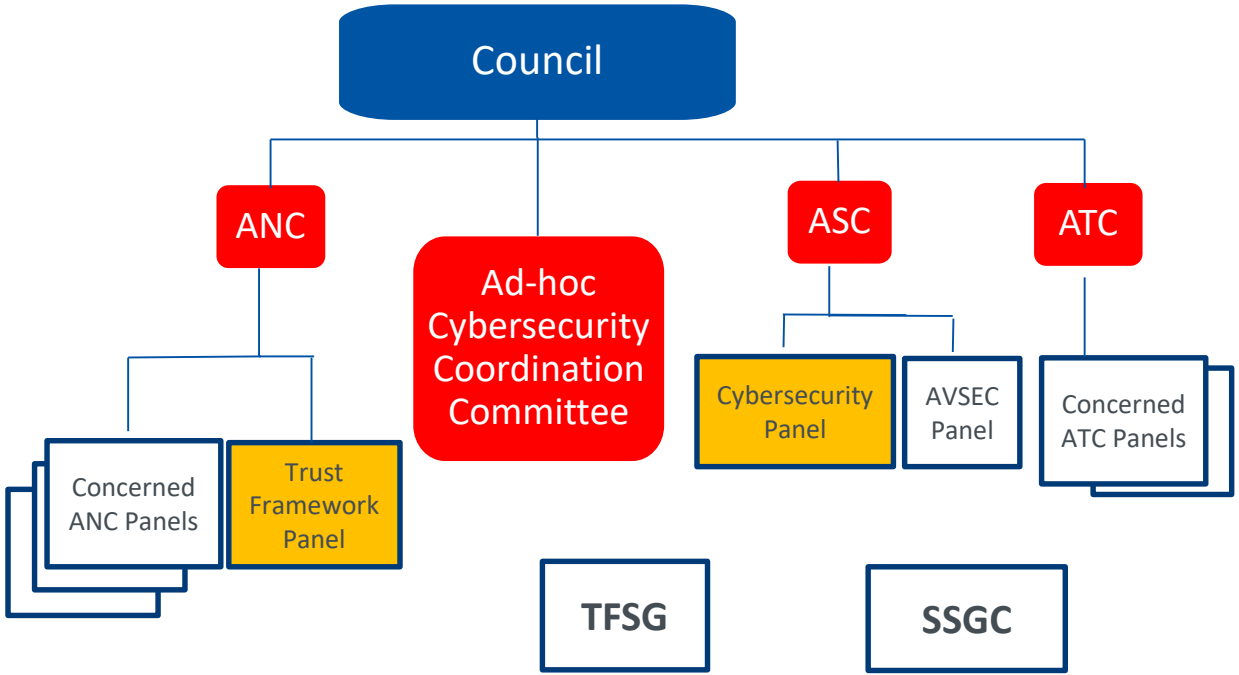
Cybersecurity Guidance Material

- ✓ Facilitates Cybersecurity information sharing using Traffic Light Protocol.
- ✓ Minimizes Human Error in sharing sensitive information.
- ✓ Supports cybersecurity & Cyber resilience objectives.

- ✓ Calls to focus resources and actions to achieve a systemic approach to cybersecurity in civil aviation.
- ✓ Supports the protection and resilience of international civil aviation's critical infrastructure against cyber threats.

- ✓ Supports the design and implementation of a robust cybersecurity culture in civil aviation.
- ✓ Builds on civil aviation's record in implementing successful aviation safety & aviation security cultures.

Enhanced Governance Structure for Cybersecurity & Cyber Resilience in ICAO



ICAO's Work on Cybersecurity & Cyber Resilience

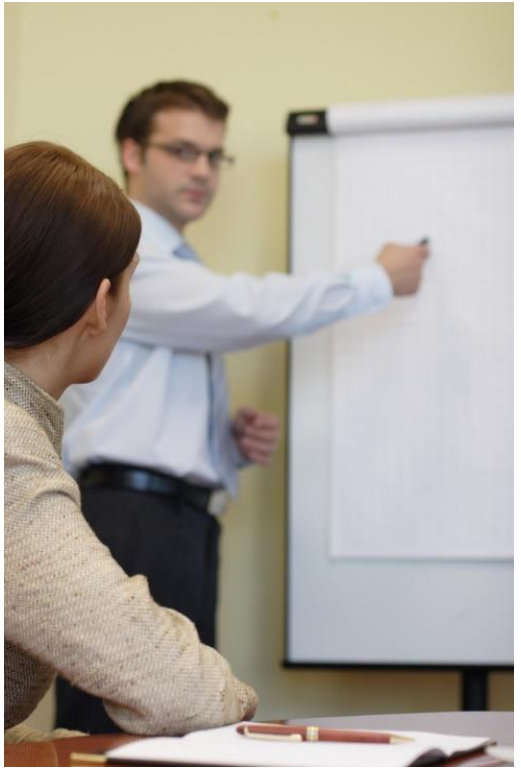
- **Legal Instruments:**
  - The Beijing Convention and The Beijing Protocol of 2010
- **Standards and Recommended Practices:**
  - Annex 17 – Aviation *Security*: Standard 4.9.1 and Recommended Practice 4.9.2
- **Assembly Resolutions:**
  - A39-19 and A40-10 Resolutions on Cybersecurity
- **Guidance Material:**
  - Doc 8973 – *Aviation Security Manual*
  - Doc 9985 – *ATM Security Manual*
  - Aviation Cybersecurity Strategy
  - Cybersecurity Action Plan
  - Using Traffic Light Protocol
  - Cybersecurity Culture in Civil Aviation
  - Cybersecurity Policy Guidance
- **Capacity Building**

Capacity Building

- **Foundations of Aviation Cybersecurity Leadership and Technical Management**
  - ✓ Partnership between ICAO and Embry-Riddle Aeronautical University (ERAU)
- **Conducted Sessions**
  - ✓ 4 – 15 October 2021 *(Virtual)*
  - ✓ 6 – 17 December 2021 *(Virtual)*
  - ✓ 14 – 29 March 2022 *(Virtual)*
- **Planned Session**
  - ✓ 23 – 27 May 2022 *(Physical – ERAU Frankfurt Campus)*

Link to Course *(Upcoming session in May 2022)*

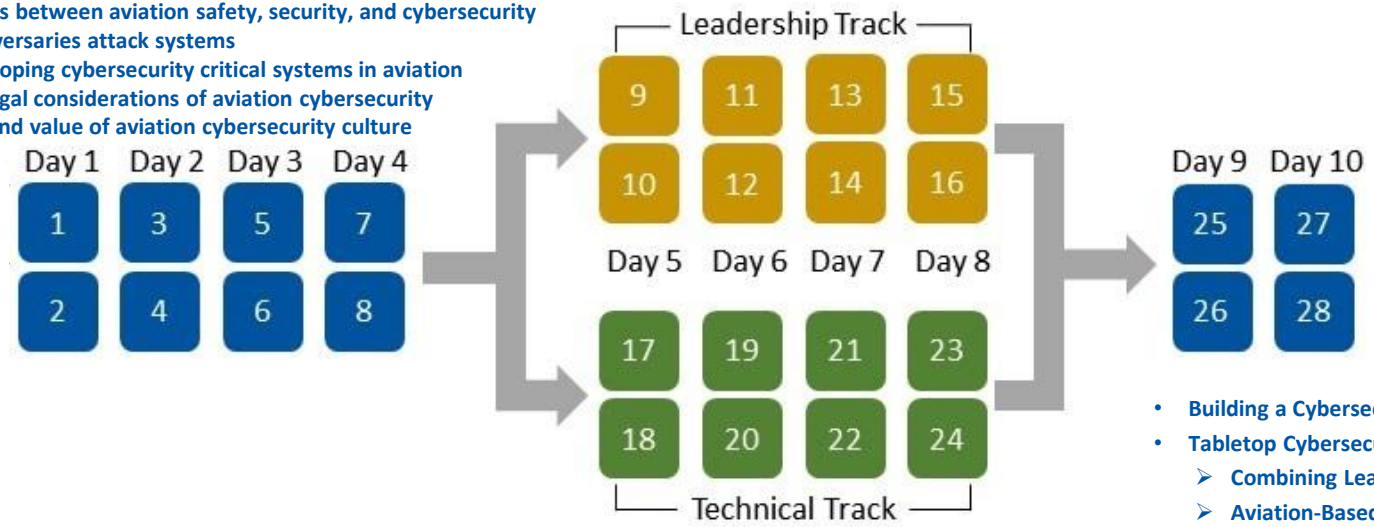
https://www.enrole.com/erau/jsp/course.jsp?categoryId=5586BD00&courseId=SGC-1102



Capacity Building

- How technology underpins all aviation systems
- Interdependencies between aviation safety, security, and cybersecurity
- Why and how adversaries attack systems
- Identifying and scoping cybersecurity critical systems in aviation
- Regulatory and legal considerations of aviation cybersecurity
- The importance and value of aviation cybersecurity culture

- Cybersecurity governance and oversight
- Cybersecurity risk management and assessment
- Managing supply chain risk
- Information sharing
- Staff awareness and training
- Organizational resilience and incident response



- Identity and access management
- Data Security
- System Security
- Resilient networks and systems

- Building a Cybersecurity Strategy
- Tabletop Cybersecurity Incident Exercise
  - Combining Leadership & Technical Aspects
  - Aviation-Based Scenario
  - Brings all Course Elements into Practice

Capacity Building

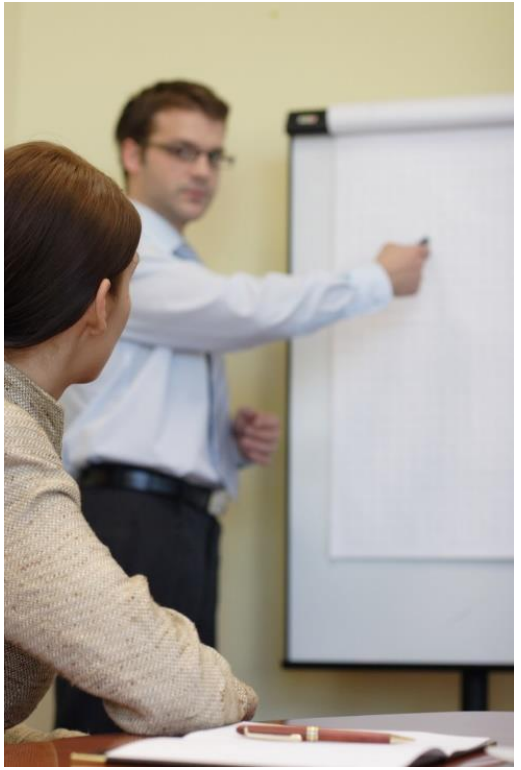
➢ Managing Security Risk in ATM *(Virtual)*

- Partnership between ICAO and EUROCONTROL.
- Combines physical security and cybersecurity in ATM.

Finalized & Planned for Delivery (7 to 11 November 2022)

Link to Course Description

https://learningzone.eurocontrol.int/ilp/pages/description.jsf#/users/@self/catalogues/4728296/coursetemplates/11291217/description



➢ Cybersecurity Oversight in Aviation

- Partnership between ICAO and UK CAAi
- Focuses on all aspects related to cybersecurity oversight

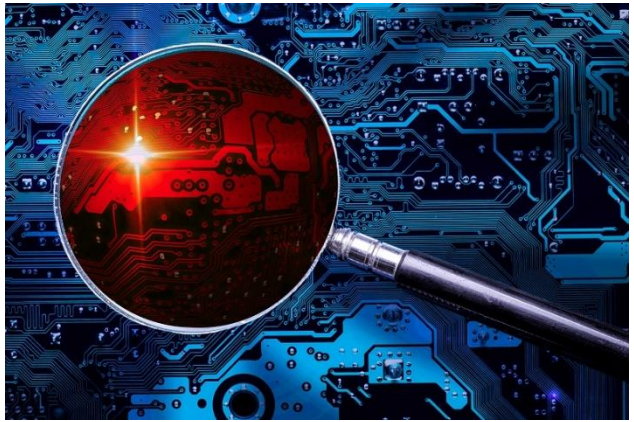
Under Development for Delivery in 2022

ICAO Universal Security Audit Programme (USAP)

- Evaluation of Aviation Security in Place in ICAO Contracting States.
- Audit States' Aviation Security Oversight Capabilities.
- Audit Security Measures at Selected Airports.

ICAO Universal Security Audit Programme (USAP)

Implementing Standard 4.9.1 in Annex 17 – *Aviation Security*

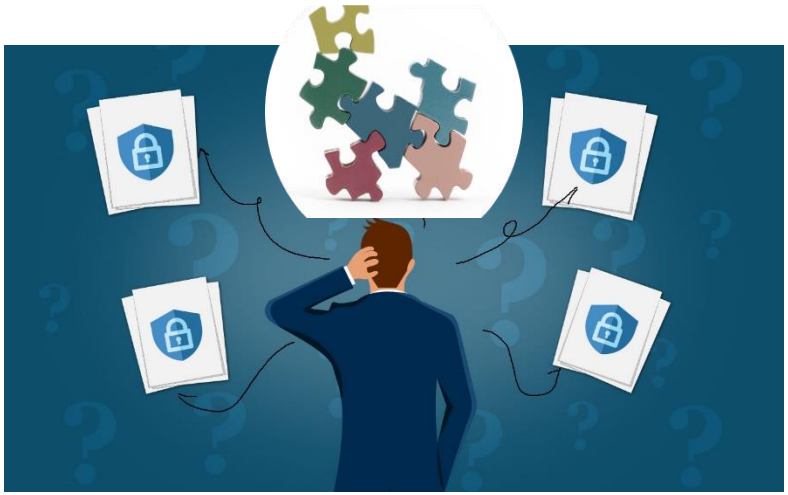


- 54 States Documentation-Based Cybersecurity Preparedness Audits:
  - 15% - No requirement for entities to identify their critical infrastructure and develop, in line with risk assessment, measures to protect this critical infrastructure.
  - 26% - No definition for entities' responsibilities in relation to aviation cybersecurity.
  - 41% - No criteria for the protection of critical infrastructure from unlawful interference.
- 35 States On-Site Audits:
  - 60% - No implementation of consistent and effective cybersecurity measures.

ICAO Universal Security Audit Programme (USAP)

Implementing Standard 4.9.1 in Annex 17 – *Aviation Security*

- Potential Reasons for Low-Level of Implementation of Aviation Cybersecurity Obligations (non-exhaustive):
  - Lack of Know-How.
  - Lack of Resources.
  - Developments are Undertaken by a separate national competent authority for cybersecurity but no effective coordination exists with the national civil aviation authority.



Thank You

ICAO