ICAO's Perspective & Work on Aviation Cybersecurity

Rashad Karaky
Aviation Cybersecurity Officer
ICAO – International Civil Aviation Organization

Agenda

- Cybersecurity in Civil Aviation
- ICAO's Work on Cybersecurity & Cyber Resilience
- The Aviation Cybersecurity Strategy and Action Plan
- Major ICAO Initiatives
- Cybersecurity Culture

Cybersecurity in Civil Aviation

Digitalization is **KEY** to Civil Aviation **INTEROPERABILITY** and Future Development Across **ALL Domains**

Impact of Technology

Cyber Threats are **BORDERLESS, COMPLEX, and AGILE**


Dozens of aircraft VANISH from air-traffic control radars sparking HACKING fears

DOZENS of aircraft VANISHED from Europe's skies in the past month, sparking fears of air-traffic control hacking attacks.

By GREG HEFFER

SHARE TWEET

Airlines under siege from hackers

The airline industry is under siege from cyberattackers, and lawmakers are struggling to help.

In recent months, hackers have infiltrated the U.S. air traffic control system, forced airlines to ground planes and potentially stolen detailed travel records on millions of people.

Yet the industry lacks strict requirements to report these incidents or even adhere to specific cybersecurity standards.

"There should be a requirement for immediate reporting to the federal government," Sen. Susan Collins (R-Maine), who chairs the Appropriations subcommittee that oversees the Federal Aviation Administration (FAA), told The Hill.

"We need to address that," agreed Sen. Bill Nelson (Fla.), the top Democrat on the Senate Commerce Committee.


Air France cyberattack: Who is the Moujahidin Team and why are they waging cyber-jihad?

By Vera Bell

April 2, 2015 18:18 BST

HACKED BY MOUJAHIDIN TEAM

Hackers break into Lufthansa customer database

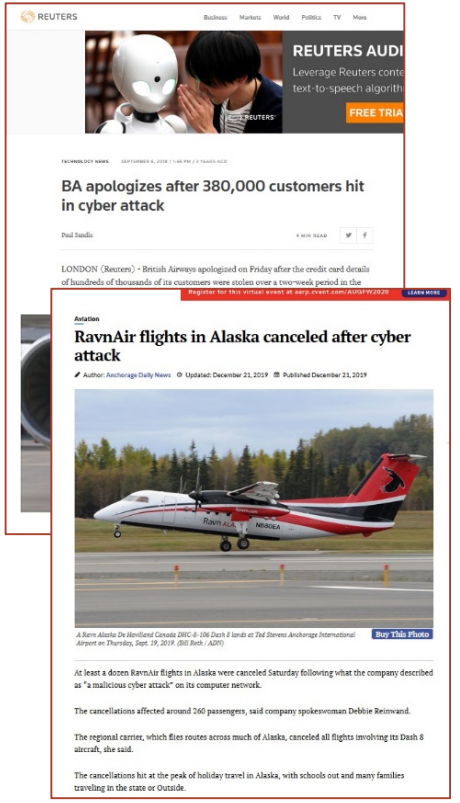
Cyber-attackers have obtained info on a number of passengers using the Lufthansa website. The hackers used frequent flyers miles to obtain vouchers and redeem rewards.

Miles & More Lufthansa

The attackers managed to gain access to individual passenger accounts on company's website LH.com,

The airline has taken prompt countermeasures, but it "had not been able to prevent illicit access to some customer files," according to company's representatives.

"We had to lock several hundred customer pages," a Lufthansa spokesman told DPA news agency after widely-read Germna magazine Der Spiegel broke the story.


REUTERS

REUTERS AUDI

Leverage Reuters conte text-to-speech algorith

FREE TRIA

BA apologizes after 380,000 customers hit in cyber attack

LONDON (Reuters) - British Airways apologised on Friday after the credit card details of hundreds of thousands of its customers were stolen over a two-week period in the

Aviation

RavnAir flights in Alaska canceled after cyber attack

Author: Anchorage Daily News Updated: December 21, 2019 Published December 21, 2019

A Ravn Alaska De Havilland Canada DHC-8-106 Dash 8 lands at Ted Stevens Anchorage International Airport on Thursday, Sept. 19, 2019. (Bill Roth / ADN)

Buy This Photo

At least a dozen RavnAir flights in Alaska were canceled Saturday following what the company described as "a malicious cyber attack" on its computer network.

The cancellations affected around 260 passengers, said company spokeswoman Debbie Reinwand.

The regional carrier, which flies routes across much of Alaska, canceled all flights involving its Dash 8 aircraft, she said.

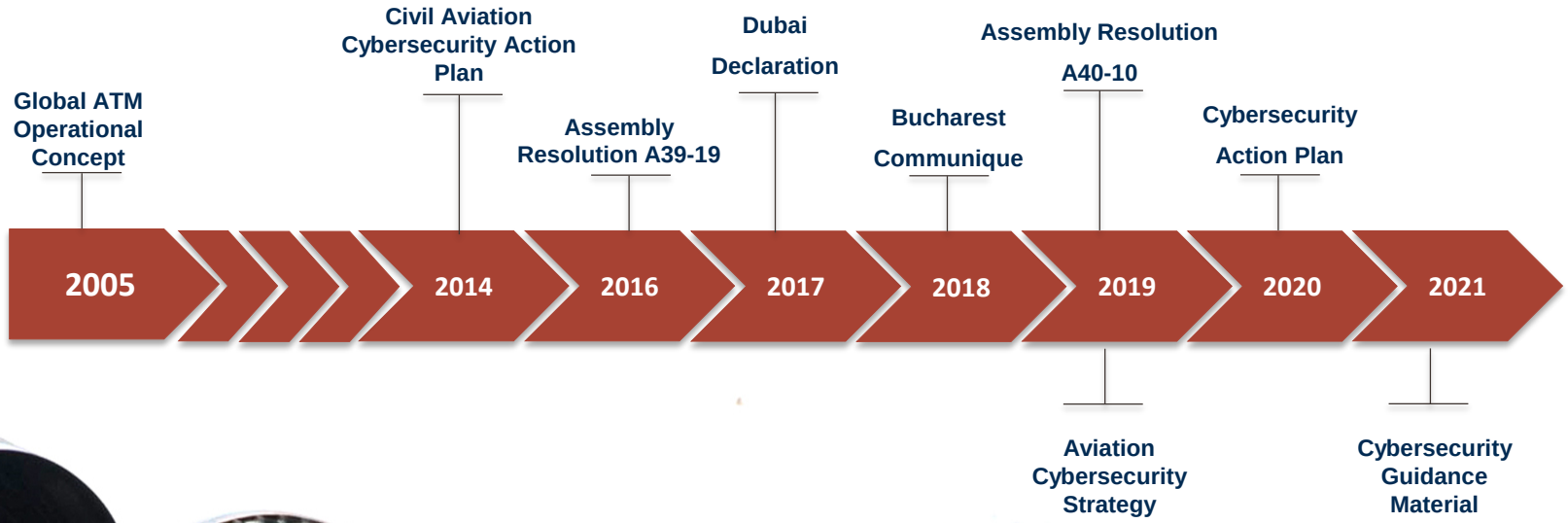
The cancellations hit at the peak of holiday travel in Alaska, with schools out and many families traveling in the state or outside.

Cybersecurity in Civil Aviation

Efforts to address cybersecurity should be:

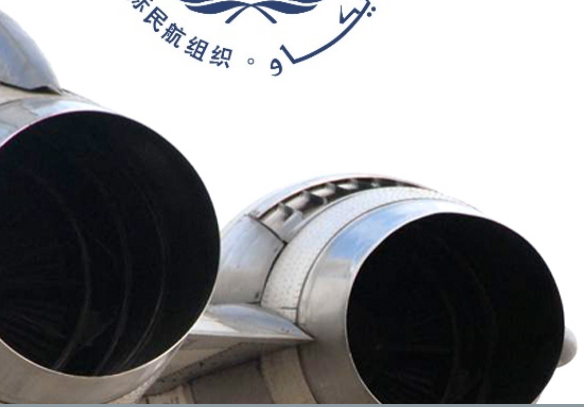
- Consistent
- Clear
- Harmonized
- Trusted
- Cross-cutting across aviation domains
- In line with global priorities
- Coordinated with IT Stakeholders outside the Aviation Sphere

ICAO's Work on Cybersecurity & Cyber Resilience



ICAO's Work on Cybersecurity & Cyber Resilience

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



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

о борьбе с незаконными актами в отношении международной гражданской авиации

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 日订于北京

اتفاقية

قمع الأعمال غير المشروعة المتعلقة بالطيران المدني الدولي

حررت في بيجين في ١٠ سبتمبر/أيلول ٢٠١٠

BEIJING
10 SEPTEMBER 2010

BEIJING
10 SEPTEMBRE 2010

BEIJING
10 DE SEPTIEMBRE DE 2010

ПЕКИН
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:

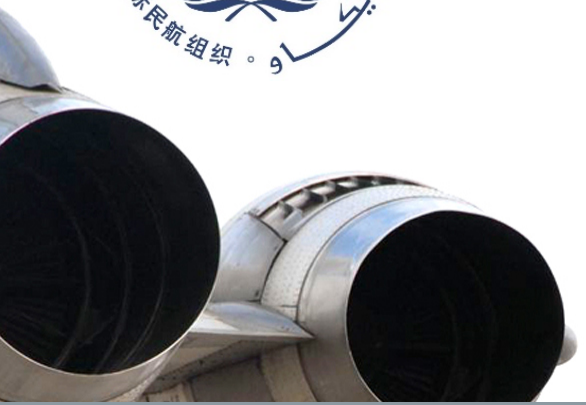
(a) makes a threat to commit the offence set forth in paragraph 1 of this Article; or

(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

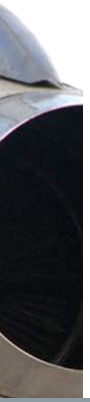
- **Legal Instruments:**
  - The Beijing Convention and The Beijing Protocol of 2010
- **Standards and Recommended Practices:**
  - Annex 17 – *Security*: Standard 4.9.1 and Recommended Practice 4.9.2



ICAO's Work on Cybersecurity & Cyber Resilience

Annex 17 to the Chicago Convention - *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

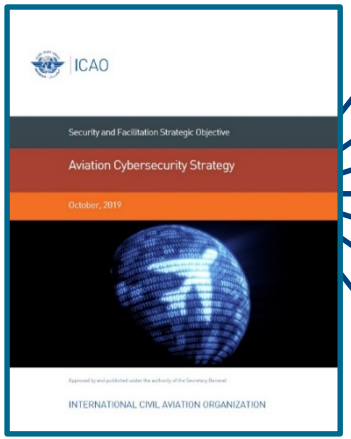
- **Legal Instruments:**
  - The Beijing Convention and The Beijing Protocol of 2010
- **Standards and Recommended Practices:**
  - Annex 17 – *Security*: Standard 4.9.1 and Recommended Practice 4.9.2
- **Assembly Resolutions:**
  - A39-19 and A40-10 Resolutions on Cybersecurity

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 Aviation 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

- The **First edition of the Cybersecurity Action Plan** was published in November 2020.
- **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 **29 Priority Actions**, which are further broken down into **54 Tasks** to be Implemented by ICAO, States, and Stakeholders.

The Cybersecurity Action Plan

Cybersecurity Action Plan (Example)

Priority Outcome	Pillar 3: DEVELOP EFFECTIVE LEGISLATION AND REGULATIONS
Priority Actions	• Ensure that appropriate regulation and legislation are in place for cybersecurity; • Develop appropriate guidelines for States and Industry in implementing cybersecurity related provisions; • Ensure that international legal instruments provide appropriate measure for the prevention, timely reaction to, and prosecution of cyber-incidents.

Actions

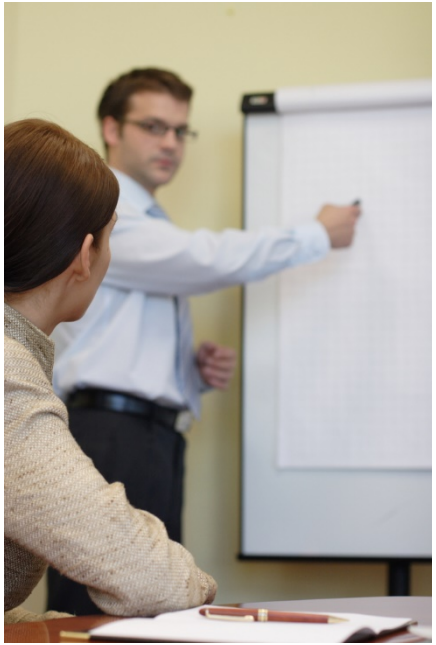
Action #	By	Traceability to the Cybersecurity Strategy	Traceability in Action Plan	Specific Measures/Tasks	Indicators	Maturity	Target
CyAP 3.1	Member States	3.3	8.4	Member States to ratify Beijing instruments.	Number of States having ratified Beijing instruments	Low	ongoing
CyAP 3.2	ICAO	3.3	8.3	Analysis of international air law instruments	Report and update plan	N/A	2020
CyAP 3.3	ICAO and Member States	3.3	8.2	Analysis of existing international and national legislation in the cybersecurity field and identify gaps, including criminal law.	Promote ratification of instruments to incriminate unlawful cyber acts.	Medium	2022 - 2023
CyAP 3.4	ICAO, Member States and Industry	3.3	8.1	Review existing ICAO standards to identify need for potential cybersecurity updates	Regulatory gap analysis	High	2021
CyAP 3.5	ICAO	3.2	5.4	Create, review and amend guidance material related to implementing cybersecurity requirements	Accepted and agreed cybersecurity guidance material	High	2021-2022

ICAO's Work on Cybersecurity & Cyber Resilience

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

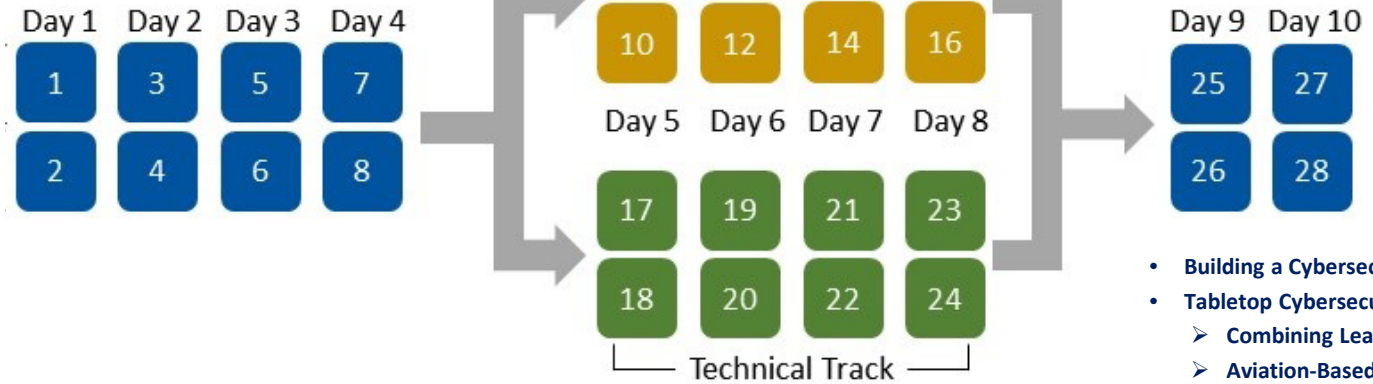
Major ICAO Initiatives

- **Foundations of Aviation Cybersecurity Leadership and Technical Management**
  - ✓ Partnership between ICAO and Embry-Riddle Aeronautical University
  - ✓ 10 Half-Days of virtual learning



Major ICAO Initiatives

- 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

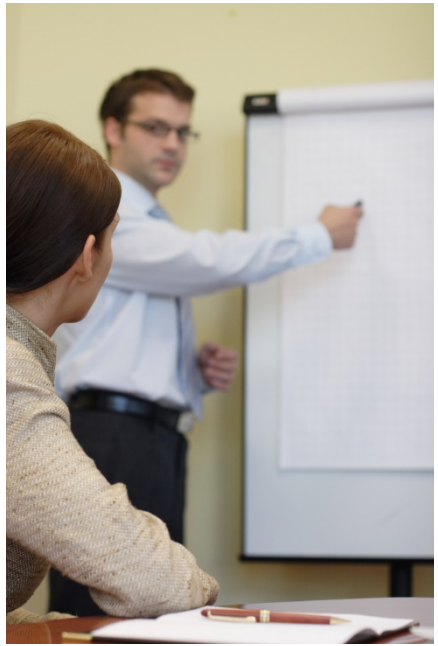
Major ICAO Initiatives

- **Planned Sessions**
  - ✓ First Session: 4 – 8 & 11 – 15 October 2021 (Central European Time) ***Conducted***
  - ✓ Second Session: 6 – 10 & 13 – 17 December 2021 (Eastern Time)

    In Class
- **Link to Course**
  - ✓ https://www.enrole.com/erau/jsp/course.jsp?categoryId=5586BD00&courseId=SGC-1101

Major ICAO Initiatives

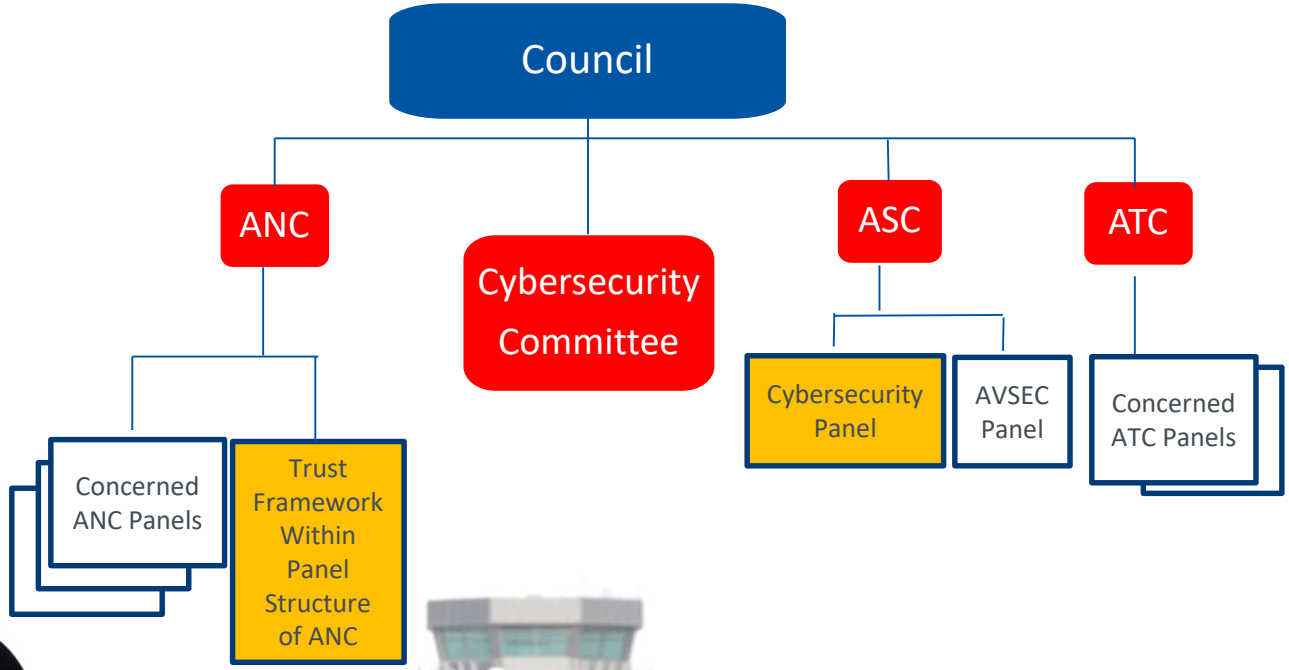
- **Foundations of Aviation Cybersecurity Leadership and Technical Management**
- **Managing Security Risk in ATM**
- **Cybersecurity Oversight** *(Under discussion)*



Major ICAO Initiatives

- **Secretariat Study Group on Cybersecurity – SSGC**
  - Research Sub-Group on Legal Aspects
  - Working Group on Airlines and Aerodromes
  - Working Group on Air Navigation Systems
  - Working Group on Cybersecurity for Flight Safety
  - Ad-hoc Working Group on Cyber-Attack Scenarios
  - Task Force on Cybersecurity Action Plan & Guidance Material
- **Trust Framework Study Group – TFSG**
  - Trust Reciprocity Operational Needs Working Group
  - Digital Identity Working Group
  - Global Resilient Aviation Interoperable Network Working Group
- **Several ICAO Panels**

Major ICAO Initiatives



Major ICAO Initiatives

ICAO Year of Security Culture (YOSC) - Objectives:

- To encourage the aviation industry to think and act in a **security-conscious manner**
- To **raise security awareness** in aviation operations - achieving a balance of security, safety, facilitation and the passenger experience
- To promote an effective and sustainable security culture, as a critical core value endorsed from top management: ***"security is everyone's responsibility"***

Major ICAO Initiatives

Cybersecurity Culture:

- Humans are the **weakest link** in the cyber chain, but also **the first line of defense** against cyber threats.
- **Cybersecurity Culture is a cornerstone** to protect civil aviation against cyber threats.

ICAO is incorporating Cybersecurity Culture in the Activities of the Year of Security Culture to promote and support the development and implementation of a Robust aviation Cybersecurity Culture that will support the efforts for a Cyber-Secure and Resilient Civil Aviation Sector

Digitalization is **ESSENTIAL** for the Growth of the Civil Aviation Sector

ICAO

North American Central American and Caribbean (NACC) Office
Mexico City

South American (SAM) Office
Lima

ICAO Headquarters
Montréal

Western and Central African (WACAF) Office
Dakar

European and North Atlantic (EUR/NAT) Office
Paris

Middle East (MID) Office
Cairo

Eastern and Southern African (ESAF) Office
Nairobi

Asia and Pacific (APAC) Sub-office
Beijing

Asia and Pacific (APAC) Office
Bangkok

THANK YOU