



| ICAO

INTERNATIONAL CIVIL AVIATION ORGANIZATION

A UN SPECIALIZED AGENCY



Setting the scene

From the ICAO resolutions to the ICAO strategy and action plan

Sonia HIFDI

Aviation Security Policy Section, Chief
ICAO



ICAO

AVIATION SECURITY AND FACILITATION

Overview of milestones achieved and future developments

2005
Global Operational ATM concept

2014
IHLG - Civil Aviation Cybersecurity Action Plan
1st SARP in Annex 17

2016
A39-19

2017
SSGC

2019
Aviation Cybersecurity Strategy – A 40-10
TFSG

2020
Cybersecurity Action Plan –
1st Edition

2022
Cybersecurity Action Plan -2nd Edition
A 41-19: Establishment of:

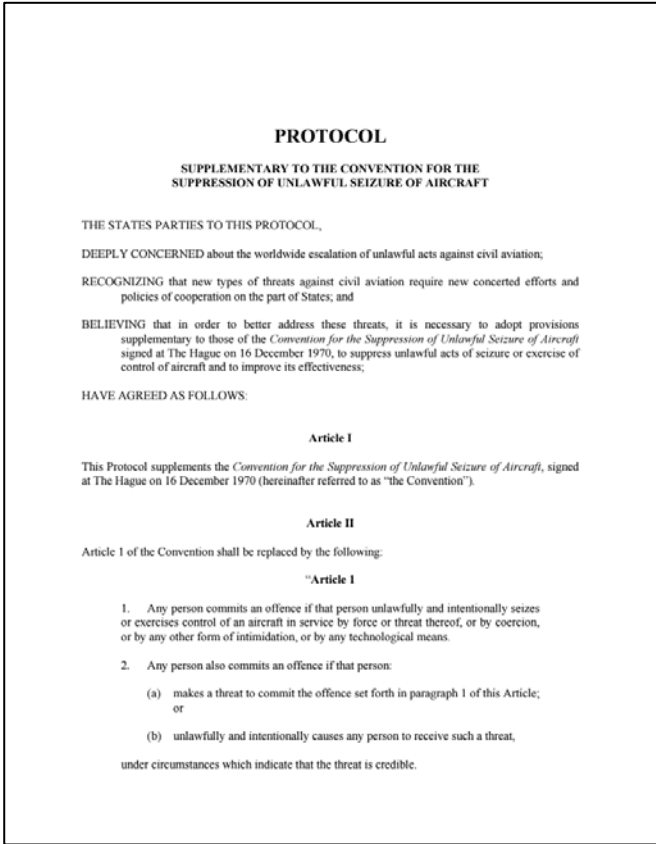
- the Ad Hoc Cybersecurity Coordination Committee (AHCCC)
- Cybersecurity Panel (CYSECP)
- Trust Framework Panel (TFP)

2023
First two meetings of the CYSECP
First meeting of the TFP
First meeting of the AHCCC

ICAO's Work on Aviation Cybersecurity – International Legal Instruments



The Beijing Convention (2010)

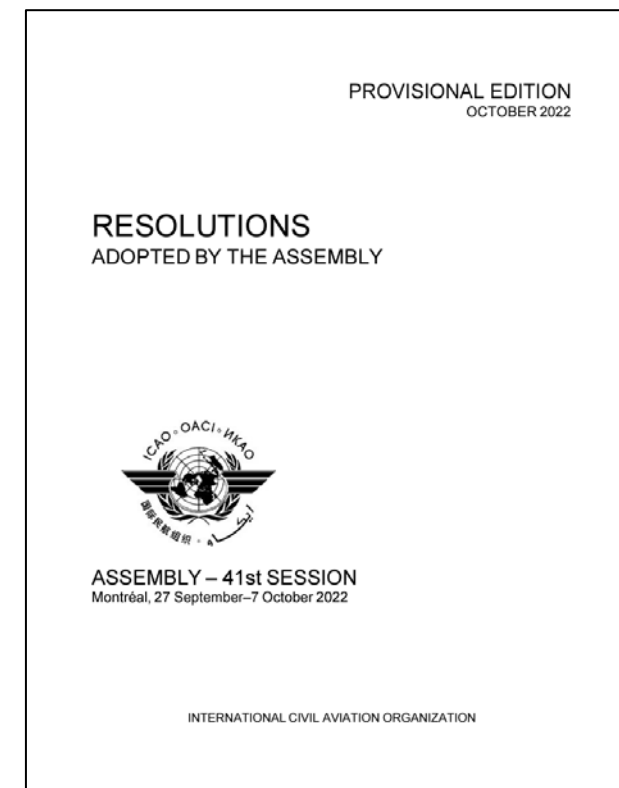


The Beijing Protocol (2010)

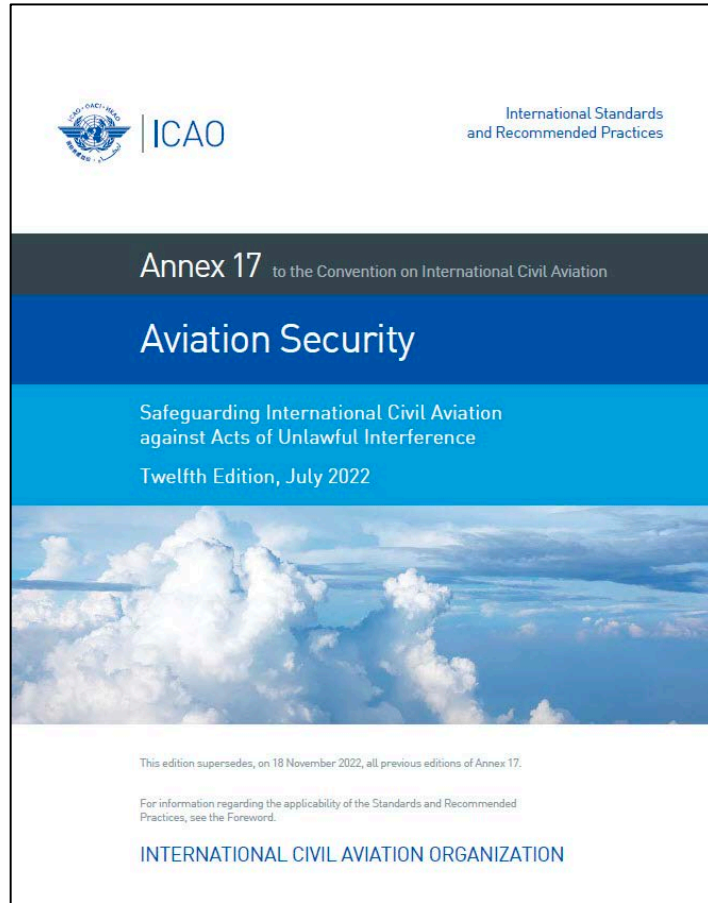
Governments' Adoption of the Beijing Instruments is an Important
DETERRENT of Cyber-Attacks Against Civil Aviation

ICAO's Work on Aviation Cybersecurity – Assembly Resolutions

A41–19: Addressing Cybersecurity in Civil Aviation



Annex 17



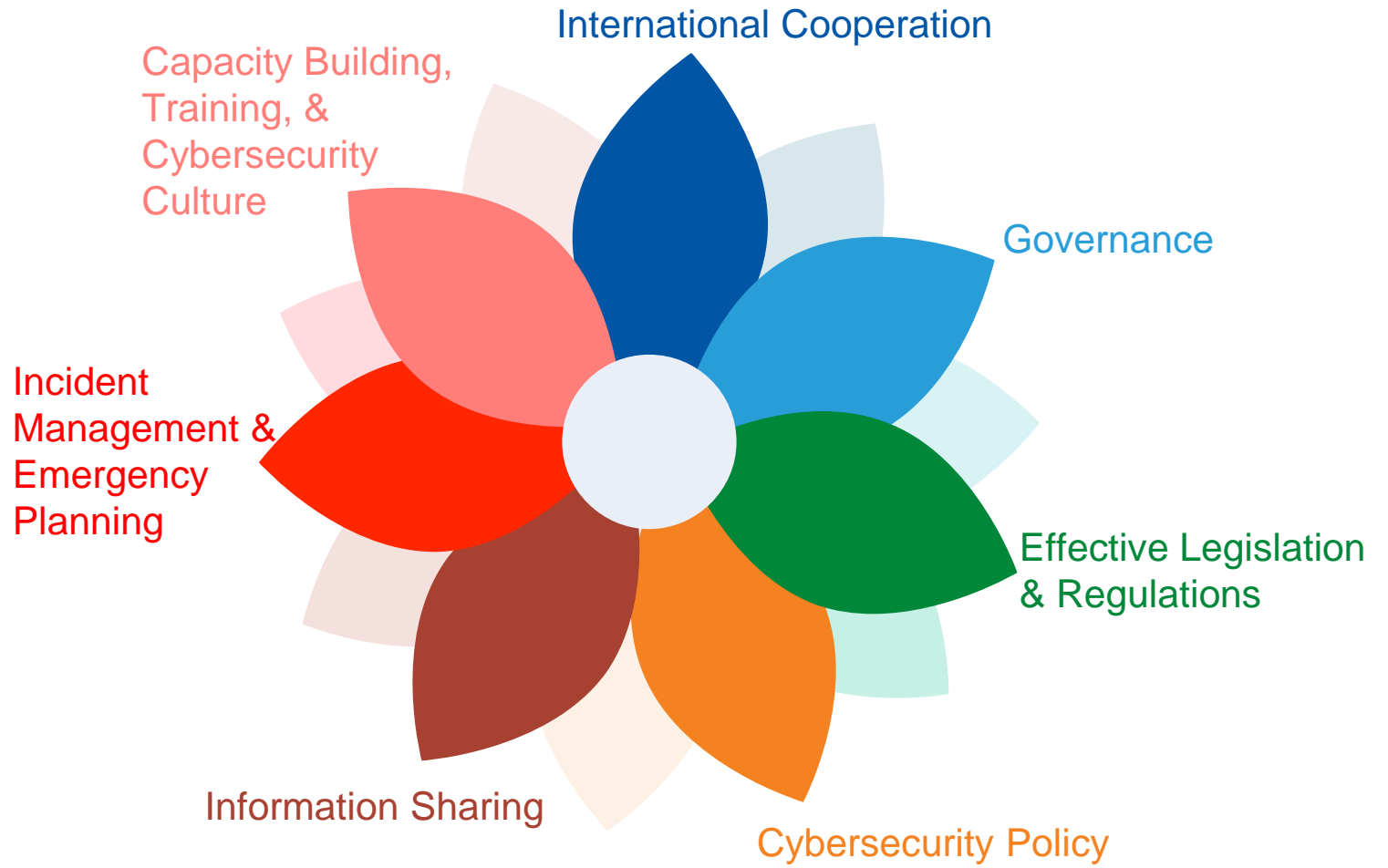
Standard 4.9.1

- 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

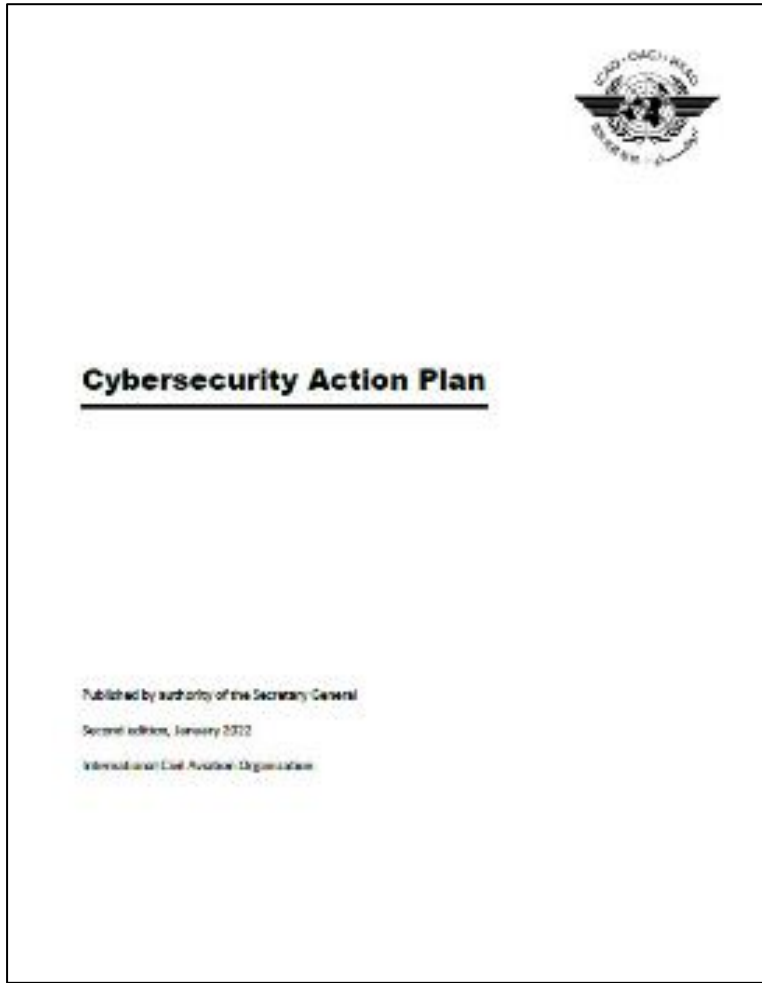
Recommended Practice 4.9.2

- 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

The Aviation Cybersecurity Strategy



The Cybersecurity Action Plan



First Edition published in November 2020



Second Edition published in January 2022



Available on ICAO Public Website

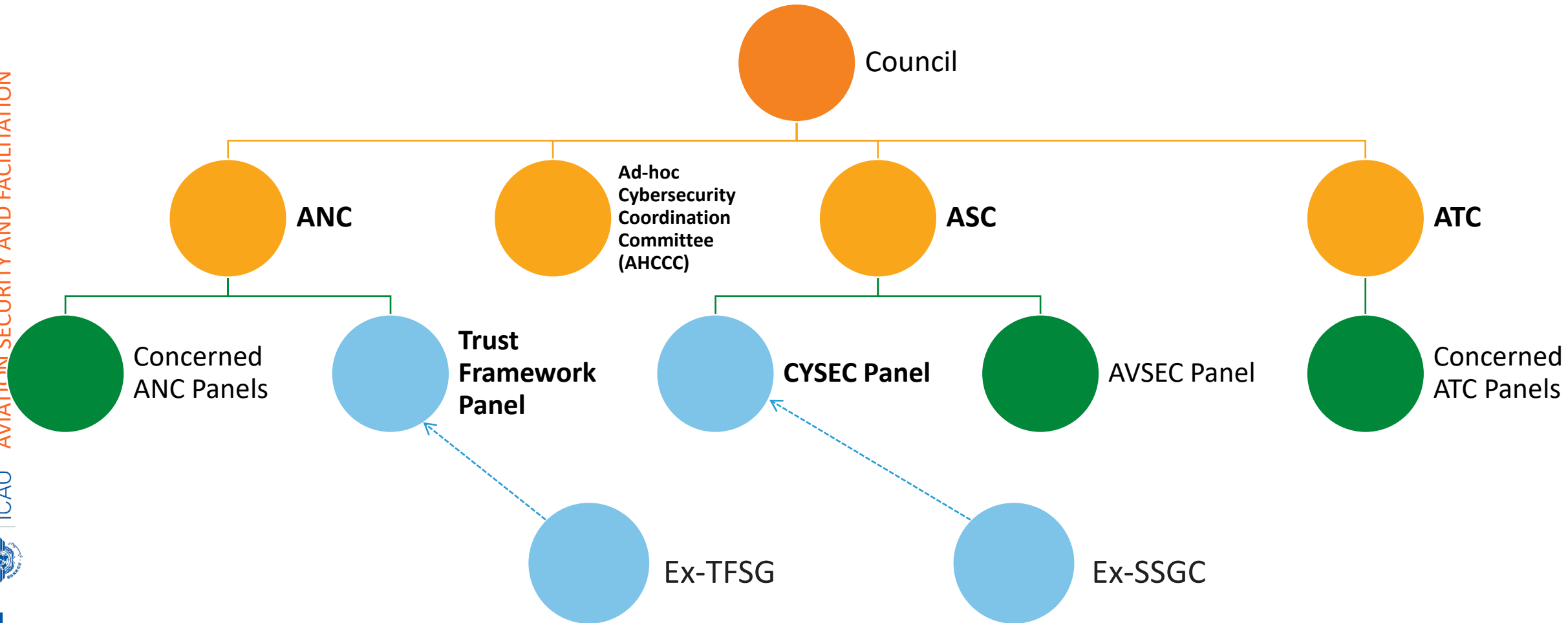


Provides the Foundation for ICAO, States and stakeholders to work together



Develops the **7 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

Cybersecurity Governance Structure



ICAO Aviation Security Resources – Capacity Building

Foundations of Aviation
Cybersecurity Leadership and
Technical Management

Cybersecurity has become an essential component
of a safe, secure and resilient aviation system

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

Advisory Services | Aviation Training | Exams & Licensing | Sectors | About Us | Media | Contact | Q

Aviation Cybersecurity Oversight

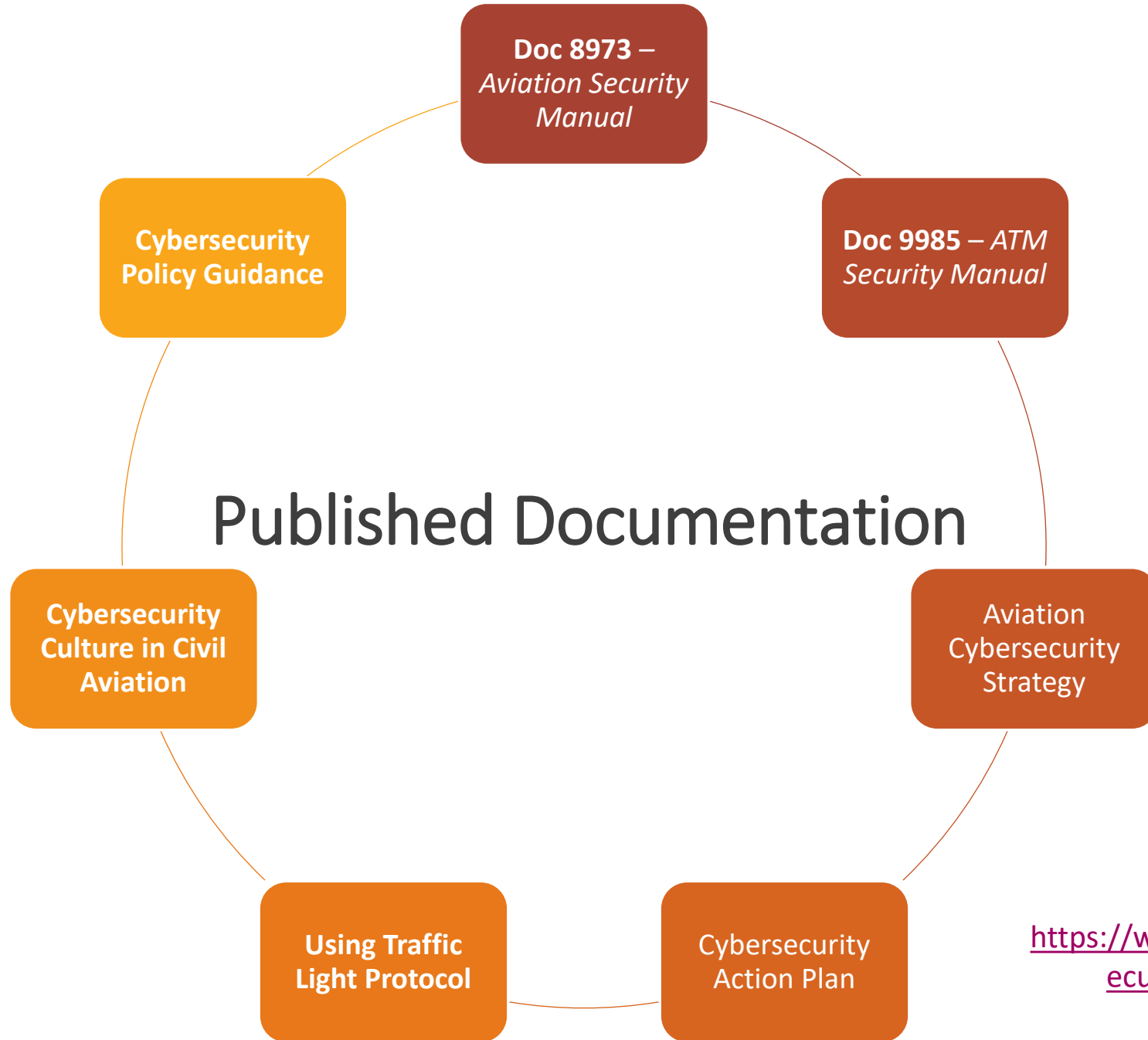
In cooperation with

3-day course | Classroom & In-company training, or
4-day course | Virtual training (5-hour daily sessions)

- ✓ ICAO TRAINAIR PLUS COURSE
- ✓ Interpret the 6 steps of the UK CAA's Cybersecurity Oversight Process for Aviation
- ✓ Learn how to conduct a critical systems scoping exercise
- ✓ Explore the synergies between SMS and SeMS

feefo Service Rating 457 reviews

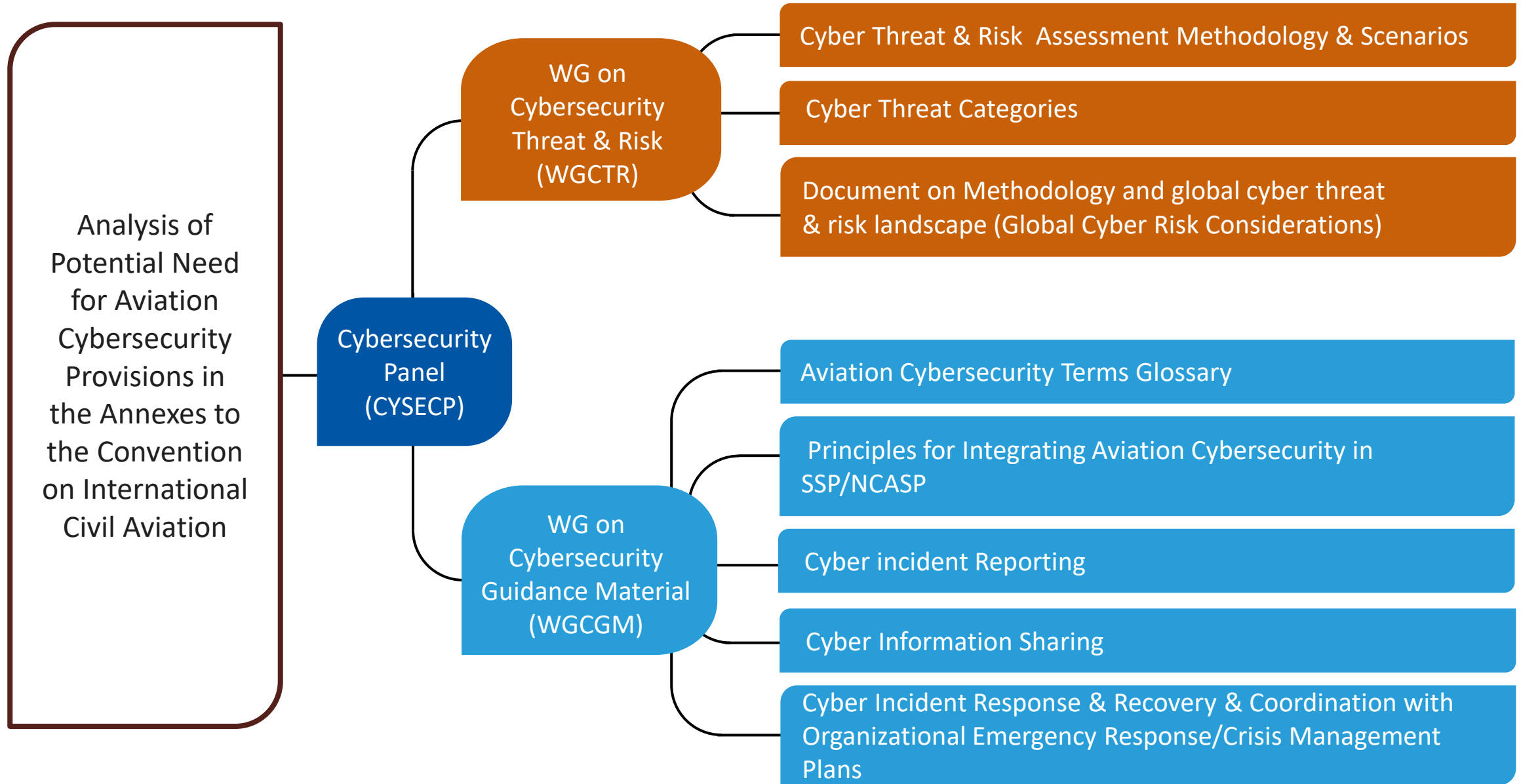
<https://caainternational.com/course/icao-aviation-cybersecurity-oversight/>



<https://www.icao.int/aviationcybersecurity/Pages/Guidance-material.aspx>



Cybersecurity Panel's ongoing Work Programme



Setting the scene

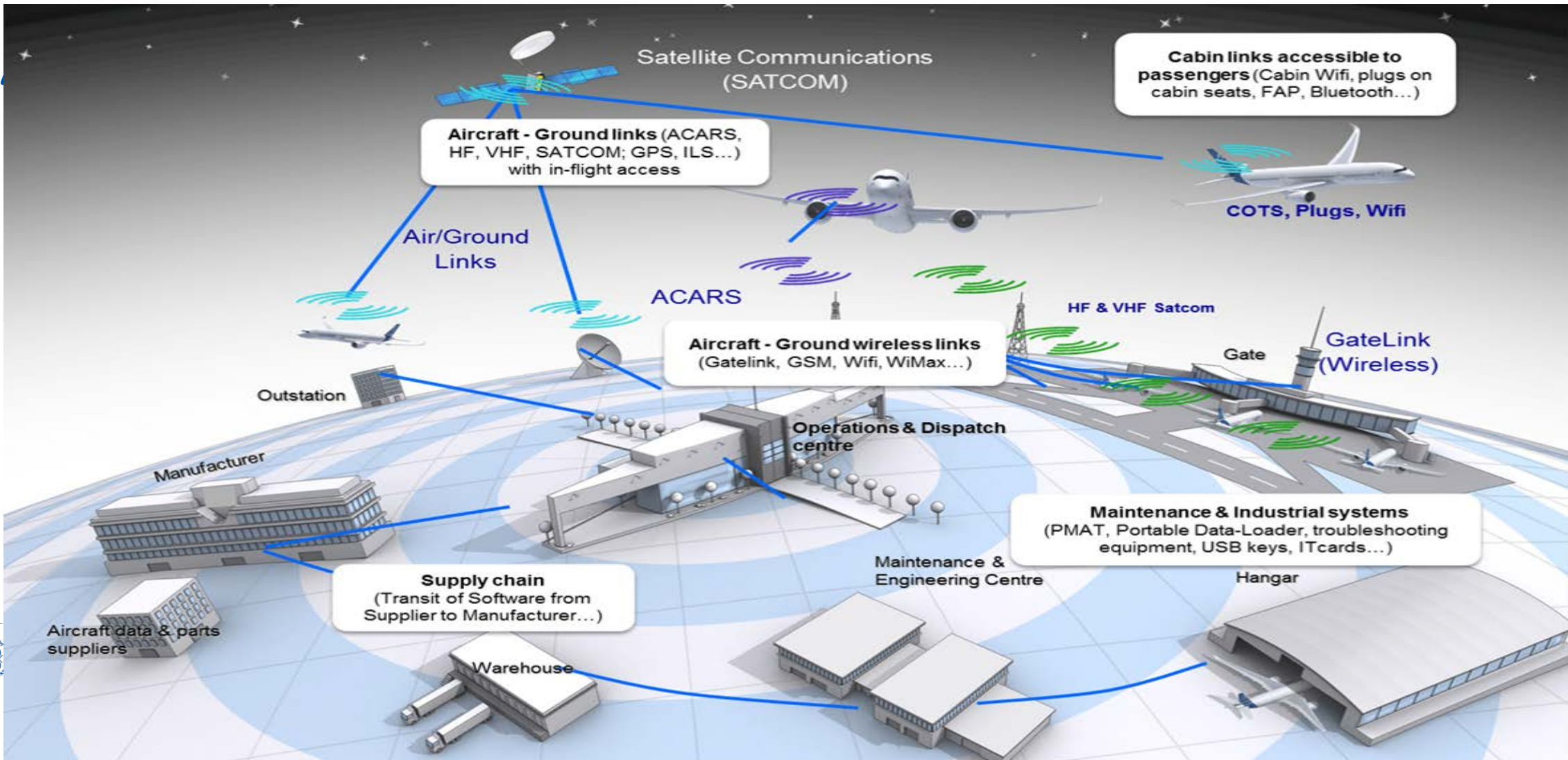
Air Navigation & Safety Considerations

—
Mike GOODFELLOW

Technical Officer, Globally Interoperable Systems
Air Navigation Bureau

Cyber in Air Navigation and Safety

- Critical enabler of ANS and other systems
- Important considerations for legacy systems
 - Bandwidth limitations
 - Lack of authentication/encryption
 - Upgrade cycle and costs
- Purpose-focused



Areas of cyber work



- Navigation Systems
 - GNSS Interference
 - SBAS Authentication
- Communications
 - ATN Security
 - Air/ground links
- RPAS
 - C2 Links
 - UTM
- SWIM
- Meteorology
- ATM
 - FF-ICE
 - Connected Aircraft
- Licensing
 - Personnel
 - Operations
- Digital Trust
 - Identity Management
 - Information Assurance



Thank You