ICAO SECURITY & FACILITATION

Implementation of Aviation Cybersecurity Requirements & Frameworks

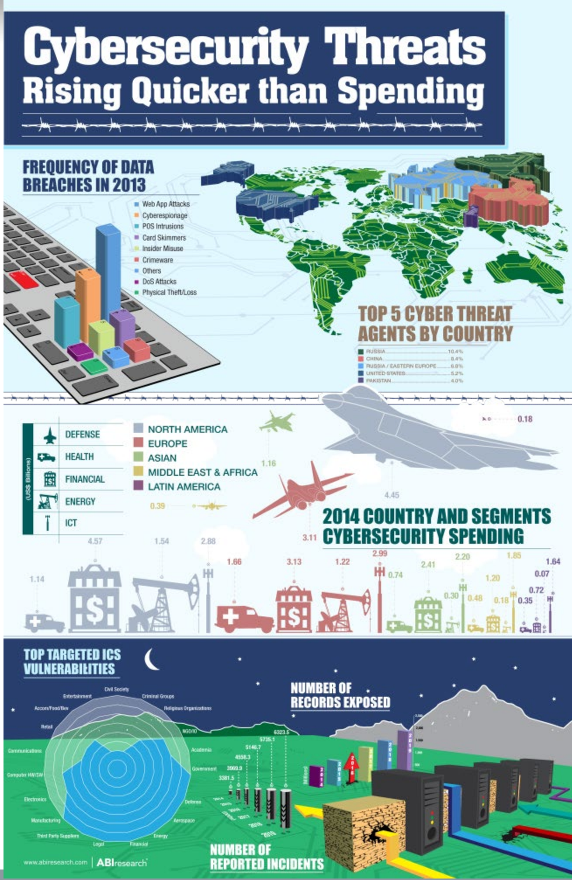
José María Peral Pecharromán

Regional Officer, Aviation Security and Facilitation
ICAO North American, Central American and Caribbean Regional Office

Santo Domingo, 5-9 May 2025

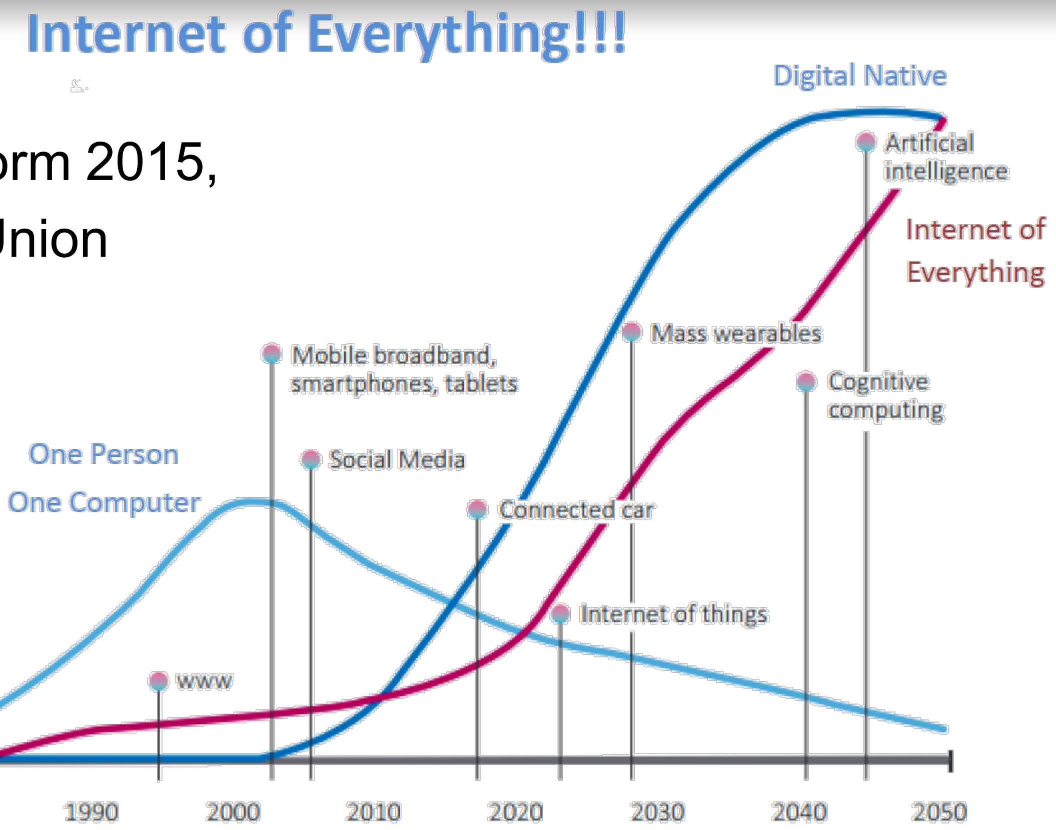
Global Cyber-trends

- 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



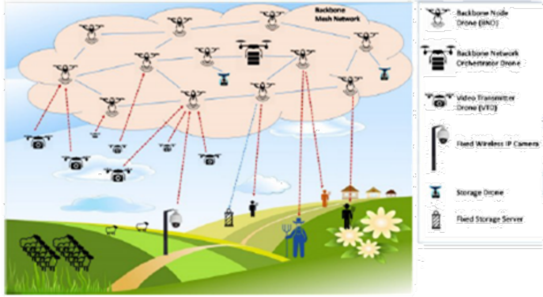
Global Cyber-trends

Trends in Telecommunication Reform 2015, International Telecommunication Union



Global Cyber-trends

Increasing Broadband access
Ubiquitous World


Backbone Mesh Network
Backbone Node Drone (BND)
Backbone Network Orchestrator Drone
Video Transmitter Drone (VTD)
Fixed Wireless IP Camera
Storage Drone
Fixed Storage Server

Drones is its applications

New applications in all areas
e-health / e-learning
e-government / e-commerce
e-banking / e-money
Entertainment / Media
Social networks
Communications in Disasters / GPS
Agriculture
Accessibility

Artificial Intelligence / Robots
Autonomous Cars
Smart Homes / Smart Cities
Etc.

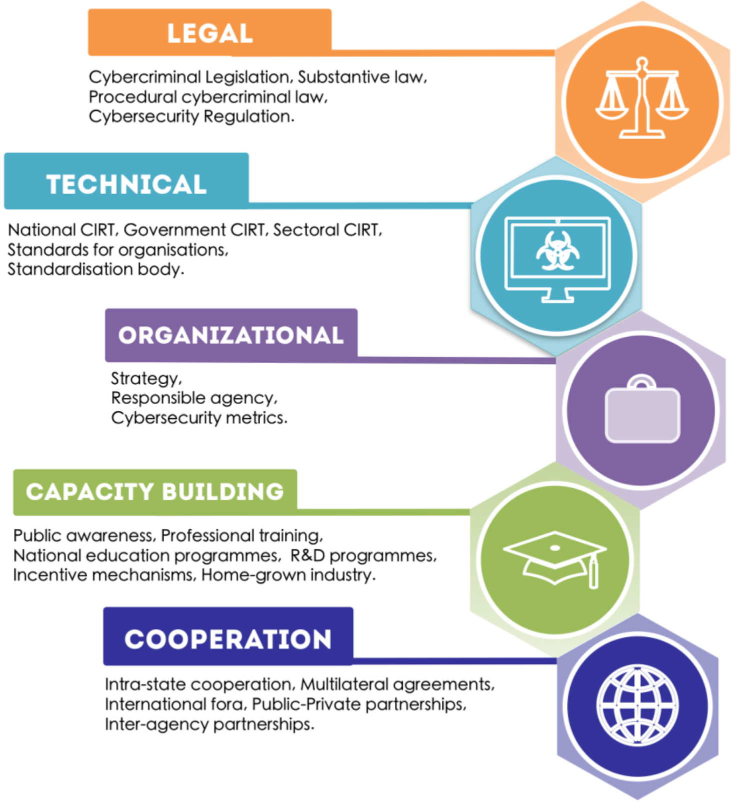
Increasing connections M2M
IoT – Internet of Everything
smarter sensors

5G networks / Smart Cities
Cloud Computing / Big Data

Everything is getting interconnected!!!

Hypercomplexity
+
Hyperconnectivity
+
Hyper volume of Data
=
Hypervulnerability

Global Cybersecurity Index



LEGAL

Cybercriminal Legislation, Substantive law,
Procedural cybercriminal law,
Cybersecurity Regulation.

TECHNICAL

National CIRT, Government CIRT, Sectoral CIRT,
Standards for organisations,
Standardisation body.

ORGANIZATIONAL

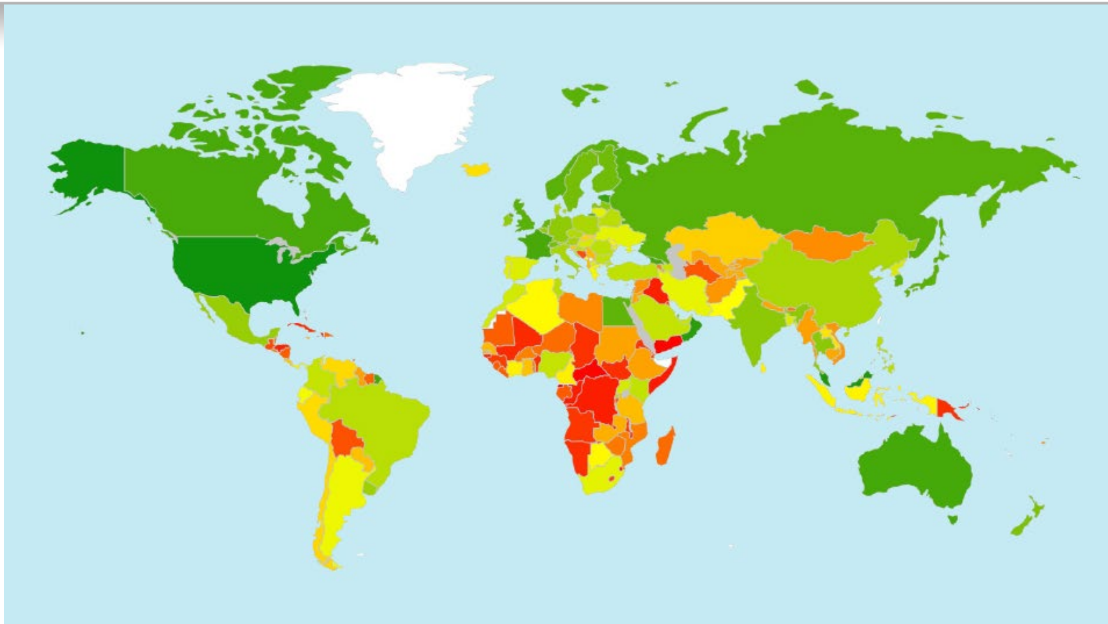
Strategy,
Responsible agency,
Cybersecurity metrics.

CAPACITY BUILDING

Public awareness, Professional training,
National education programmes, R&D programmes,
Incentive mechanisms, Home-grown industry.

COOPERATION

Intra-state cooperation, Multilateral agreements,
International fora, Public-Private partnerships,
Inter-agency partnerships.



ITU Global Cybersecurity Index

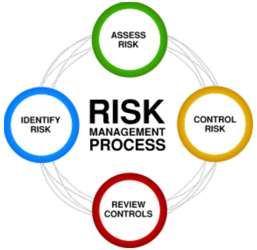
The **Global Cybersecurity Index (GCI)** measures the commitment of countries to cybersecurity.

Cybersecurity scope

Physical Security

Data Security

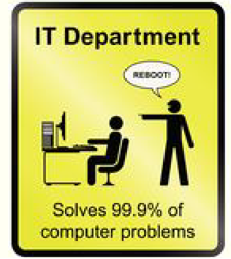
Security roles, responsibilities, and accountabilities



Risk Management

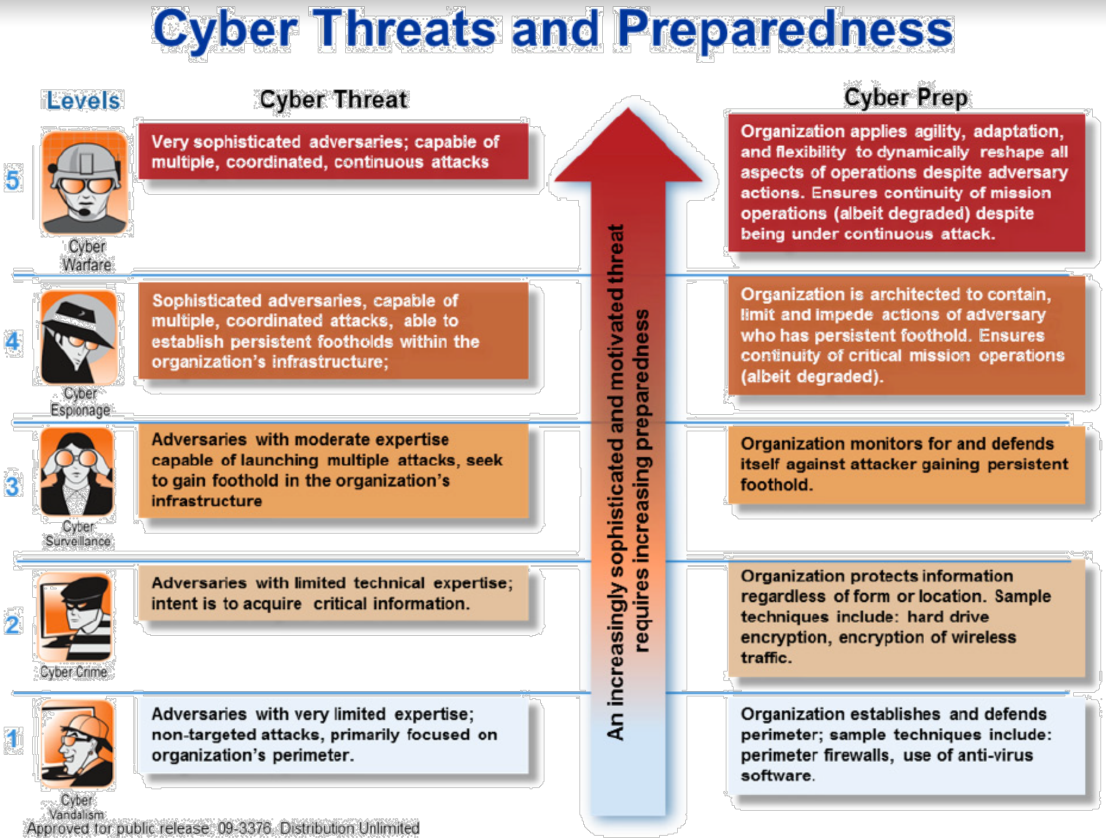
Education and training

Monitoring



Recovery

Cyber attacks and hacking



Cyber Threats and Preparedness

Levels	Cyber Threat	Cyber Prep
5 Cyber Warfare	Very sophisticated adversaries; capable of multiple, coordinated, continuous attacks	Organization applies agility, adaptation, and flexibility to dynamically reshape all aspects of operations despite adversary actions. Ensures continuity of mission operations (albeit degraded) despite being under continuous attack.
4 Cyber Espionage	Sophisticated adversaries, capable of multiple, coordinated attacks, able to establish persistent footholds within the organization's infrastructure;	Organization is architected to contain, limit and impede actions of adversary who has persistent foothold. Ensures continuity of critical mission operations (albeit degraded).
3 Cyber Surveillance	Adversaries with moderate expertise capable of launching multiple attacks, seek to gain foothold in the organization's infrastructure	Organization monitors for and defends itself against attacker gaining persistent foothold.
2 Cyber Crime	Adversaries with limited technical expertise; intent is to acquire critical information.	Organization protects information regardless of form or location. Sample techniques include: hard drive encryption, encryption of wireless traffic.
1 Cyber Vandalism	Adversaries with very limited expertise; non-targeted attacks, primarily focused on organization's perimeter.	Organization establishes and defends perimeter; sample techniques include: perimeter firewalls, use of anti-virus software.

An increasingly sophisticated and motivated threat requires increasing preparedness

Approved for public release 09-3376 Distribution Unlimited

IP Spoofing

Session hijacking

Man-in-the-Middle

Worms

Virus

Fishing

Spyware

Social Engineering

DoS, DDoS, rDoS

Ransomware

Exploits

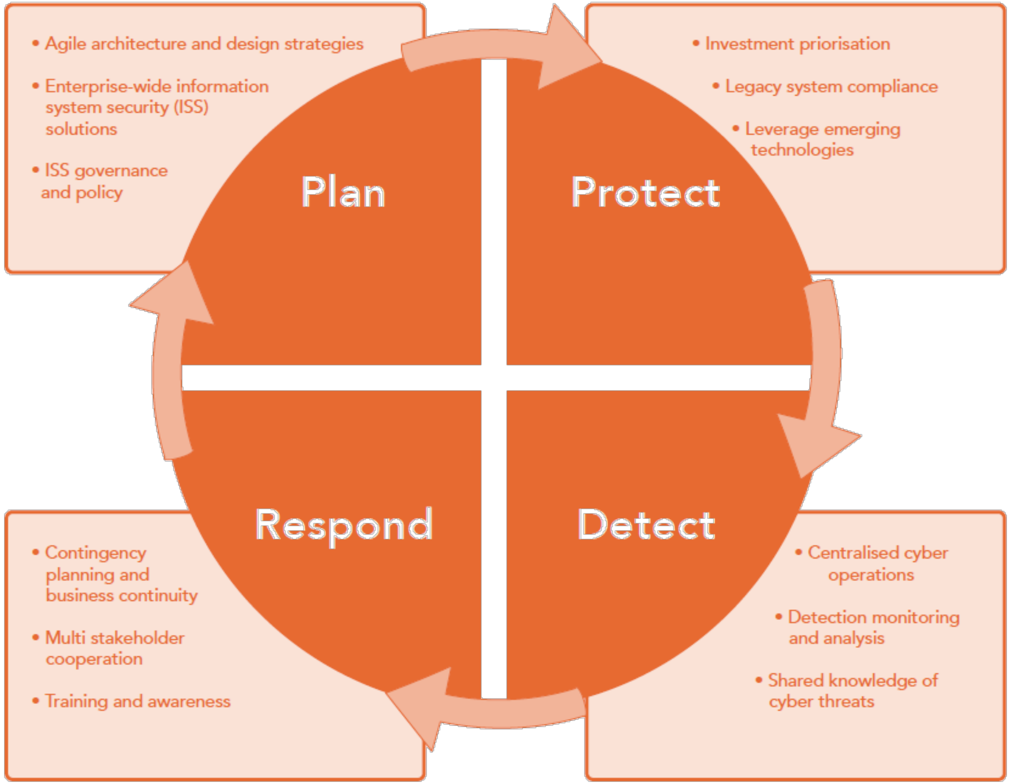
Credential Reuse

Spam

SQL Injection

Cybersecurity model

A model for effective cyber security



Plan

- Agile architecture and design strategies
- Enterprise-wide information system security (ISS) solutions
- ISS governance and policy

Protect

- Investment priorisation
- Legacy system compliance
- Leverage emerging technologies

Detect

- Centralised cyber operations
- Detection monitoring and analysis
- Shared knowledge of cyber threats

Respond

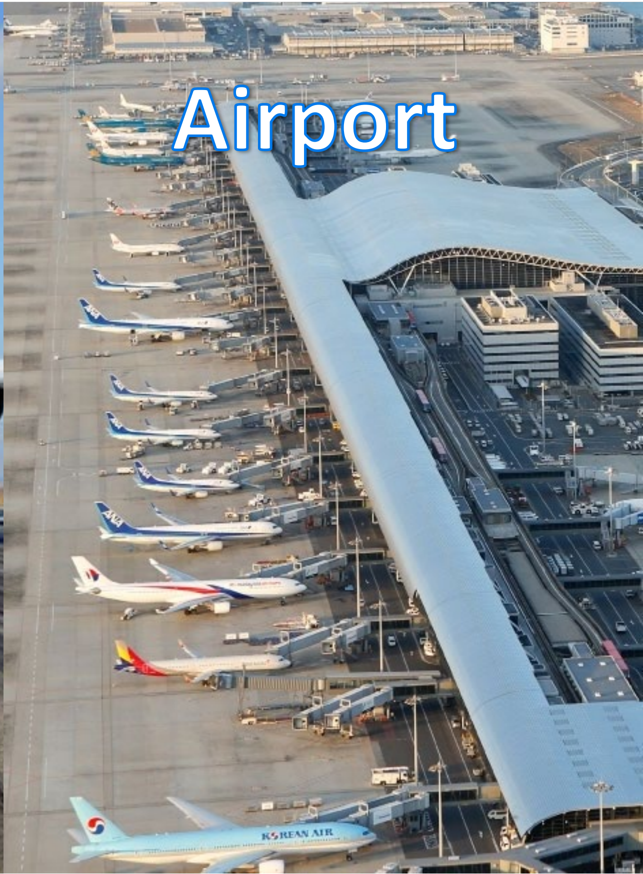
- Contingency planning and business continuity
- Multi stakeholder cooperation
- Training and awareness

To help organize efforts for responding to the cyber threat, most relevant international standards suggest applying an approach divided into four complementary steps: plan, protect, detect, and respond

Air transport ecosystem

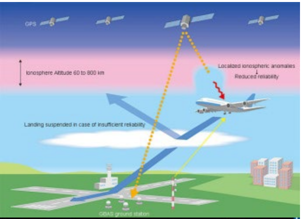
ATM

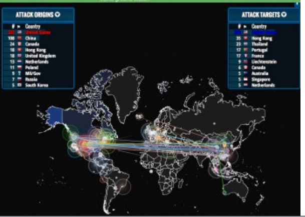
Aircraft



Airport

Concerning Scenarios


GPS
Ionosphere Altitude 60 to 800 km
Localized ionospheric anomalies
Reduced reliability
Landing suspended in case of insufficient reliability
GBAS ground station



ATTACK ORIGINS

#	Country
[illegible]	United States
108	China
24	Canada
18	Hong Kong
18	United Kingdom
13	Netherlands
11	Poland
9	Mil/Gov
7	Russia
5	South Korea

ATTACK TARGETS

#	Country
[illegible]	[illegible]
35	Hong Kong
23	Thailand
17	Portugal
17	France
9	Liechtenstein
6	Canada
5	Australia
5	Singapore
5	Netherlands

- 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

Recommended texts

Cyber-Security, a new challenge for the av
automotive industr

Hélène Duchamp, Ibrahim Bayram, Ranin

30/06/2016

Seminar in Information Systems: Applied Cybersecurity

Atlantic Council
BRENT SCOWCROFT CENTER ON INTERNATIONAL SECURITY

AVIATION CYBERSECURI

Finding Lift, Minimizing Drag

Pete Cooper

www.pwc.com/us/airlines

Aviation perspective

2016 special report series:
Cybersecurity and the airline indu

pwc

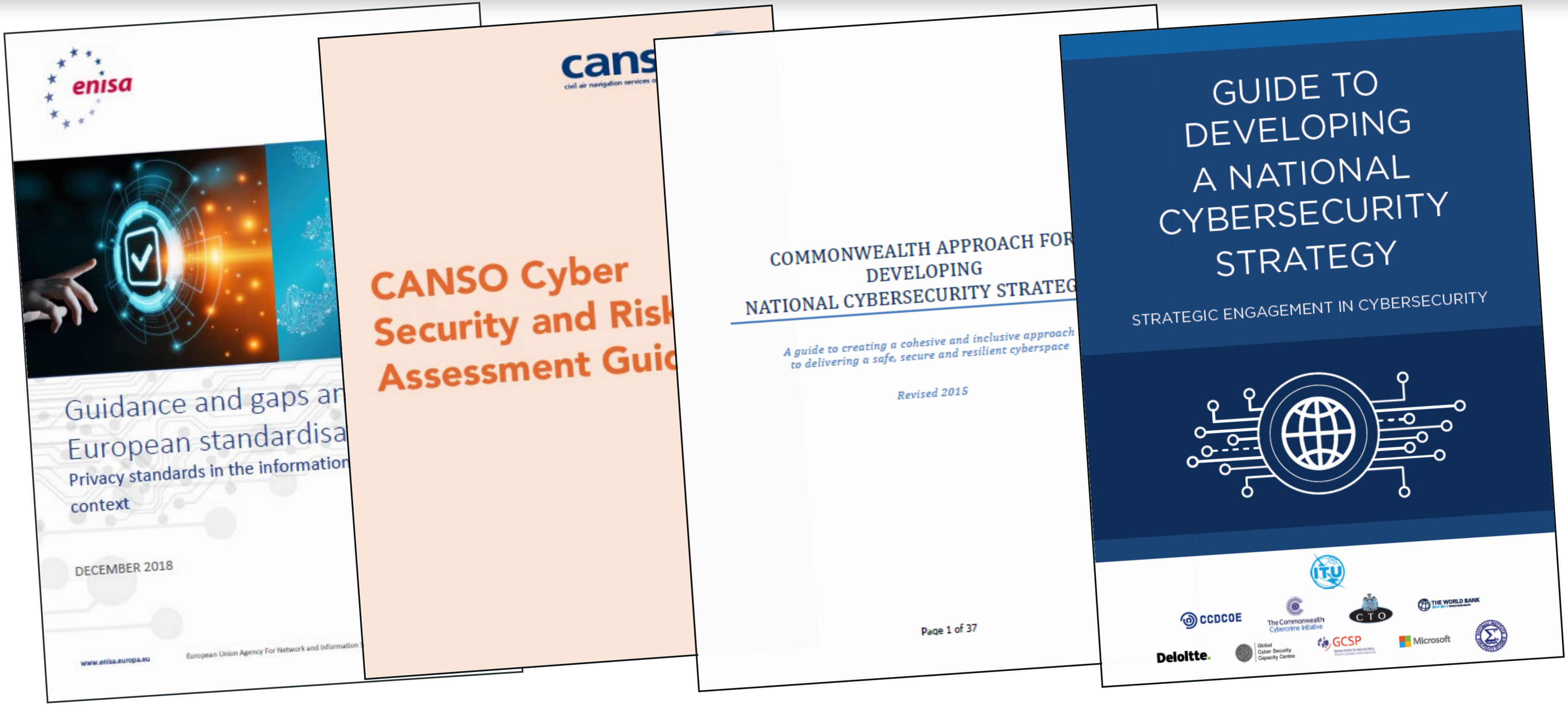
RAND EUROPE

Developing Cybersecurity Capacity

A proof-of-concept implementation guide

Jacopo Bellasio, Richard Flint, Nathan Ryan, Susanne Søndergaard, Cristina Gonzalez Monsalve, Arya Sofia Meranto, Anna Knack

Recommended texts



enisa

Guidance and gaps ar
European standardisa
Privacy standards in the information
context

DECEMBER 2018

www.enisa.europa.eu European Union Agency For Network and Information

cans
civil air navigation services o

CANSO Cyber
Security and Risk
Assessment Guid

COMMONWEALTH APPROACH FOR
DEVELOPING
NATIONAL CYBERSECURITY STRATEG

A guide to creating a cohesive and inclusive approach to delivering a safe, secure and resilient cyberspace

Revised 2015

Page 1 of 37

GUIDE TO
DEVELOPING
A NATIONAL
CYBERSECURITY
STRATEGY

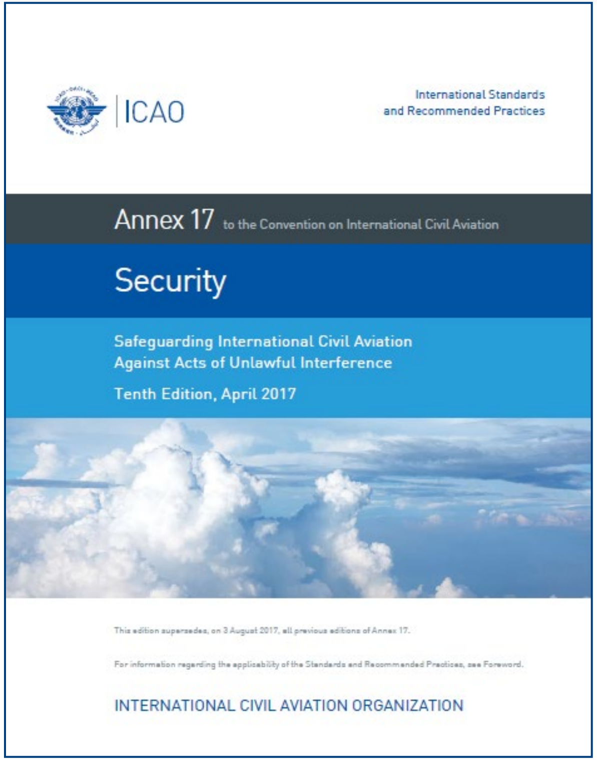
STRATEGIC ENGAGEMENT IN CYBERSECURITY

ITU
CCDCOE
The Commonwealth Cybercrime Initiative
CTO
THE WORLD BANK
Deloitte.
Global Cyber Security Capacity Centre
GCSP
Microsoft

Acts of unlawful interference

- These are acts or attempted acts such as to jeopardize the safety of civil aviation, including but not limited to:
  - 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.**

Annex 17 SARPs



International Standards and Recommended Practices

Annex 17 to the Convention on International Civil Aviation

Security

Safeguarding International Civil Aviation Against Acts of Unlawful Interference

Tenth Edition, April 2017

This edition supersedes, on 3 August 2017, all previous editions of Annex 17.

For information regarding the applicability of the Standards and Recommended Practices, see Foreword.

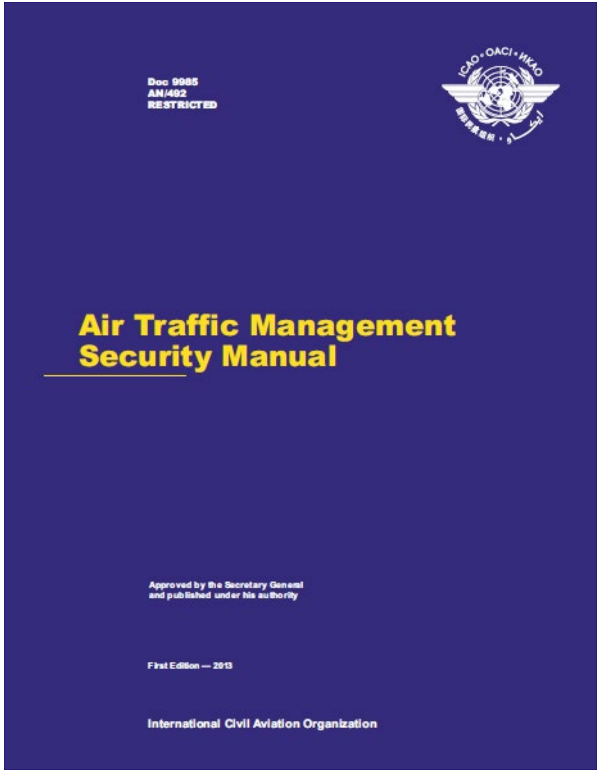
INTERNATIONAL CIVIL AVIATION ORGANIZATION

Measures relating to cyber threats

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 Manual



Doc 9985
AN/492
RESTRICTED

Air Traffic Management
Security Manual

Approved by the Secretary General
and published under his authority

First Edition — 2013

International Civil Aviation Organization

ATM security definition

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

- **ATM System Infrastructure Protection**
  - Physical security
  - Personnel security
  - ICT system security
  - Contingency planning for ATM security

- **ATM Security Operations**
  - ATM contribution to safeguarding against unlawful interference
  - ATM support for law enforcement
  - Disasters and public health emergencies
  - Airspace management for ATM security

ISO/IEC 27000 series

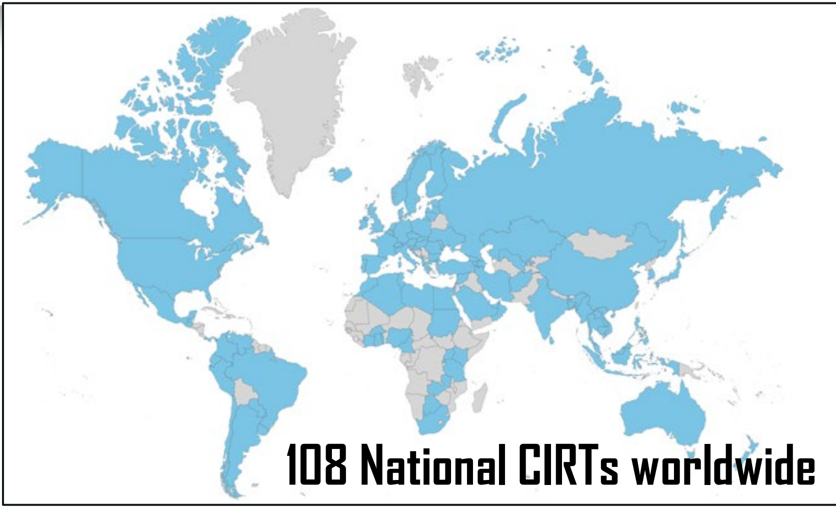
The **ISO/IEC 27000** series provides best practice recommendations on information security management and has a broad scope covering different issues: privacy, confidentiality, technical configurations, cybersecurity, etc.

Most of the standards are still under development!

Vocabulary	27000
Requirements	27001 27006 27009
Guidelines	27002 27003 27004 27005 27007 TR 27008 27013 27014 TR 27016
Sectorial Guidelines	27010 27011 27015 27017 27018 27019
Guidelines for monitoring	2703x 2704x

CERTs / CIRTs / CSIRTs

- National CIRTs are considered the first line of Cyber-Response
- Responsible for:
  - Coordinating incident response
  - Dissemination of early warnings and alerts
  - Facilitating communications and information sharing among stakeholders
  - Developing mitigation and response strategies
  - Publishing best practices in incident response as well as prevention advice;
  - Coordinating international cooperation on cyber incidents


108 National CIRTs worldwide

CSIRTs NETWORK

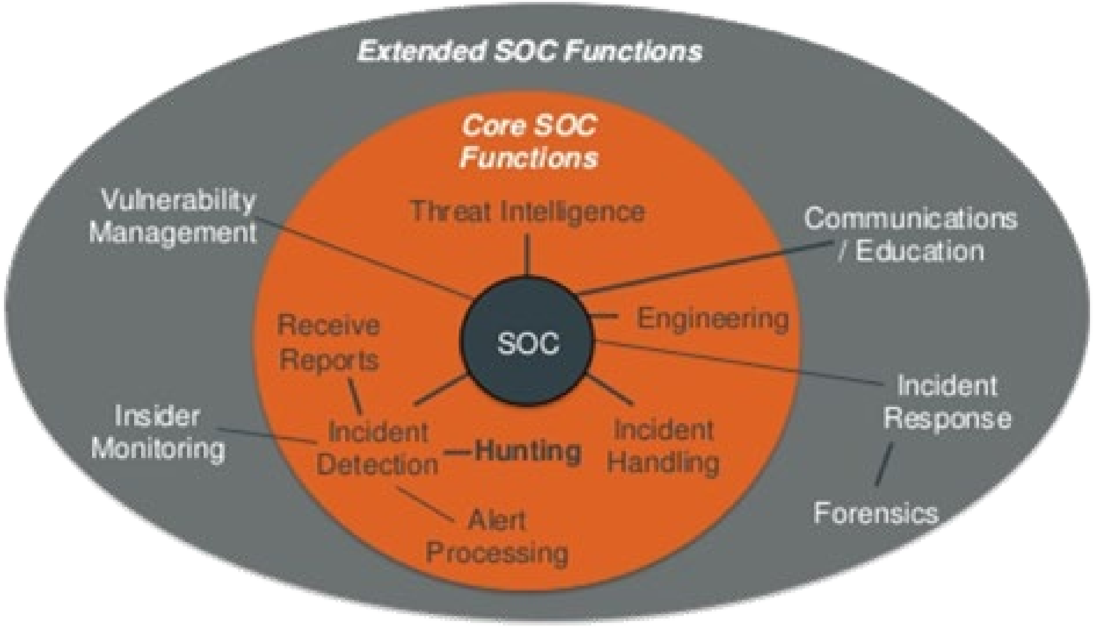
CSIRTamericas.org

APCERT Asia Pacific Computer Emergency Response Team

FIRST Improving Security Together

SOC / NOC

- SOC goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes



Our Experts

Chanell L. Hart
Director of Risk and Compliance, Civil Aviation Authority-Bahamas

Mariana Pérez Ulate
AVSEC/FAL/DG Specialist, Corporación Centroamericana de Servicios de Navegación Aérea COCESNA

Our Experts

Gustavo Lamas Sandoval
Coordinador Nacional de Seguridad de la Aviacion Civil, Dirección Nacional de Aeronáutica Civil, Paraguay

Janwillem Wiefkers
IT Director, Princess Juliana International Airport, Sint Maarten