ICAO Cybersecurity Approach and Regional Initiatives

José María Peral Pecharromán

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

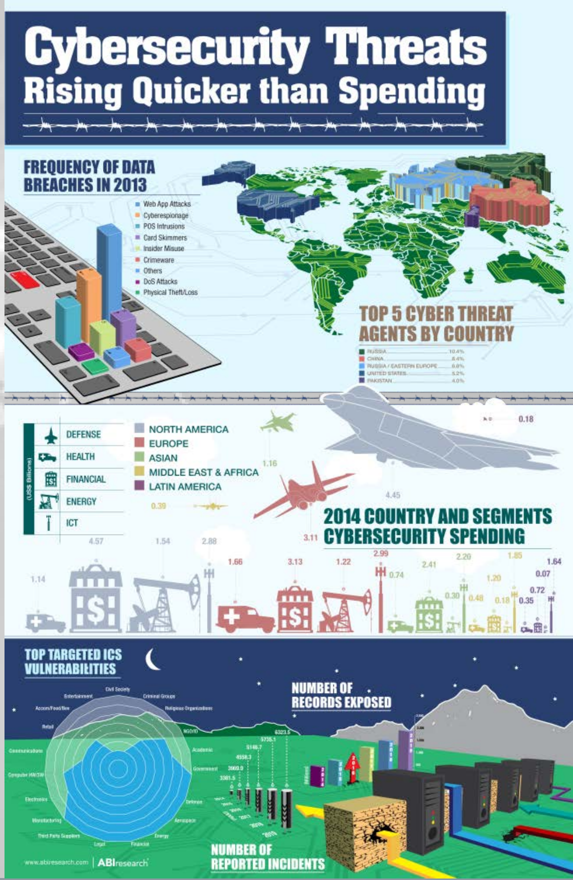
Mexico City, 4-6 December 2018

Overview

- Global Cyber-trends
- Cybersecurity scope
- Air transport ecosystem
- Concerning scenarios
- Acts of unlawful interference
- Annex 17 SARPs and guidance material
- ICAO developments on Cybersecurity
- Regional initiatives

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

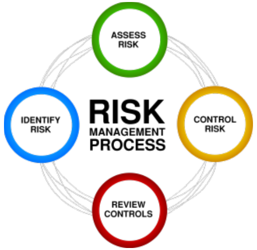


Cybersecurity scope

Physical Security

Data Security

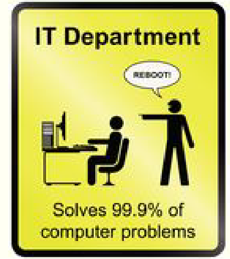
Security roles, responsibilities, and accountabilities



Risk Management

Education and training

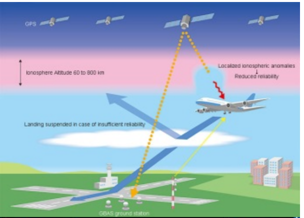
Monitoring

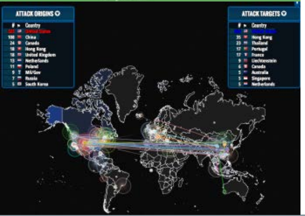


Recovery

Air transport ecosystem

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]	United States
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

Monografía 3

La Ciberamenaz
un riesgo del sig

Septiembre de 2017

Servicio de Soporte a la gestión de Crisis (SSgC)
Servicio de Gestión de Crisis y Resiliencia de las Organizaciones (SeCRO)

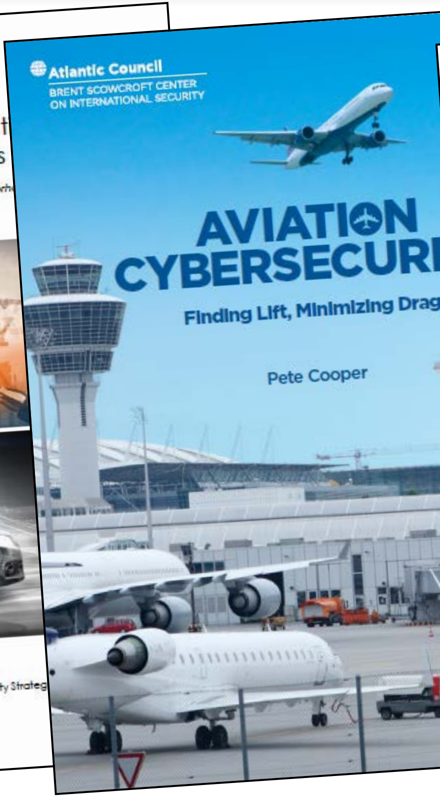
Institut Cerdà

Cyber-Security,
a new challenge for the aviat
automotive industries

Hélène Duchamp, Ibrahim Bayram, Ranim Korh

30/06/2016

Seminar in Information Systems: Applied Cybersecurity Strateg



Atlantic Council
BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

AVIATION
CYBERSECURI

Finding Lift, Minimizing Drag

Pete Cooper

www.pwc.com/us/airlines

Aviation perspectives

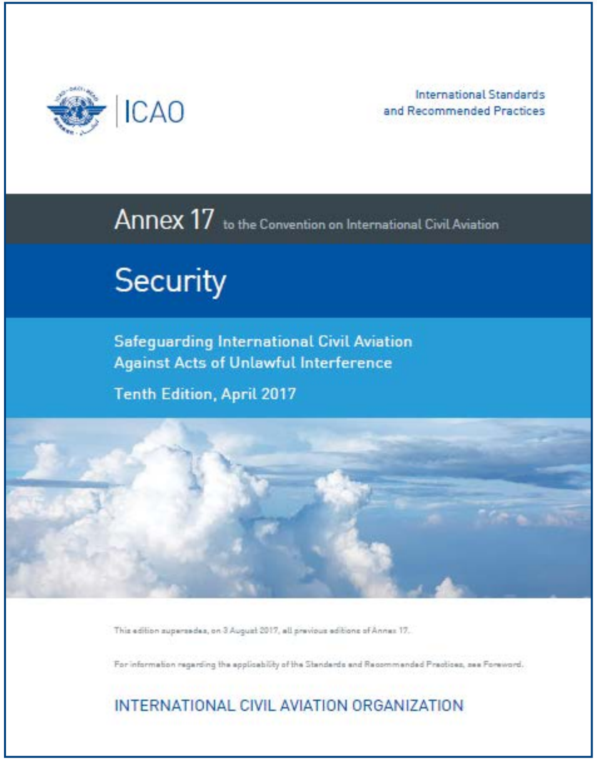
2016 special report series:
Cybersecurity and the airline industry

pwc

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



ICAO

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.

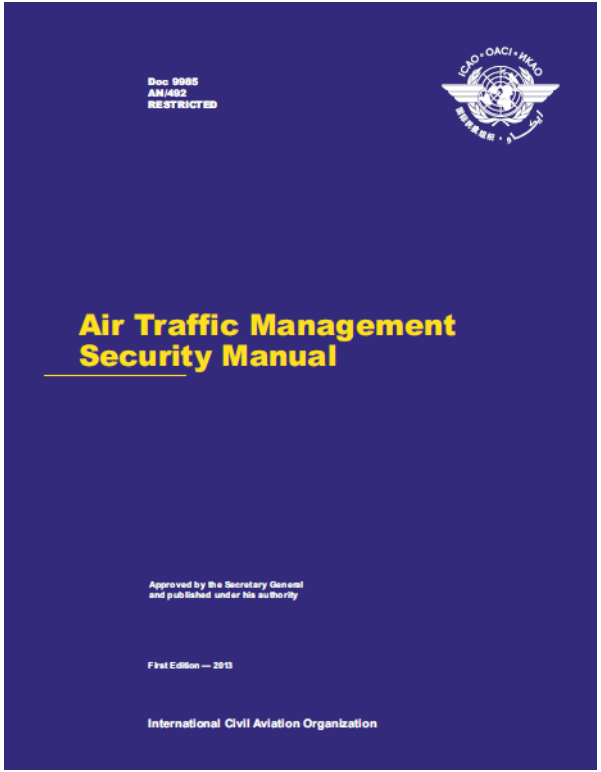
INTERNATIONAL CIVIL AVIATION ORGANIZATION

Measures relating to cyber threats

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

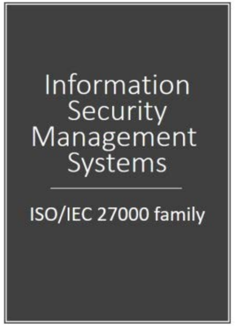
International Civil Aviation Organization

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



Information Security Management Systems

ISO/IEC 27000 family

ISO 27000

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			

ICAO Structure

ICAO Assembly
(192 States)

- Meets every 3 years and every member State has one vote
- Makes policy recommendations, reviews ICAO work
- **Elects the Council and determines the budget**

Council
(36 States)

- Permanent body and consist of 36 members elected in 3 groups
- **Adopts international standards and recommended practices**
- May act as arbiter between States

Secretary General and Secretariat

- 5 bureaus
- Give secretary services to Committees, Panels, meetings
- **Develop the work plan and assigned tasks**

39th ICAO Assembly

UN Security Council Resolutions (UNSCR)

UNSCR 2178 (2014)
Foreign terrorist fighters

UNSCR 2309 (2016)
Aviation security

UNSCR 2396 (2017)
Countering terrorism

A39-19 Addressing Cybersecurity in Civil Aviation

- The global aviation system comprises information and communications technology critical for the safety and security of civil aviation operations
- Calls States and Industry to… identify threats and risks, encourage understanding and coordination, promote standards and best practice, determine legal consequences, promote cybersecurity culture, …

Recommendation 5.4/1 – **Cyber resilience**

ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE
INTERNATIONAL CIVIL AVIATION ORGANIZATION
ICAO • OACI • ИКАО

- Provide ICAO support to establish a global trust framework;
- Cyber resilience requires coordination of all stakeholders and the need to respond to cyber events; and
- Work with ICAO to increase awareness and to share information related to cyber events.

- Establish a formal project to develop a globally harmonized aviation trust framework, and include aviation and non aviation expertise within the project group;
- Incorporate the trust framework into the GANP;
- Develop high-level policies and management frameworks for cyber resilience to help mitigate cyber threats; and
- Promote table top exercises.

5th SSGC (23 November 2018)

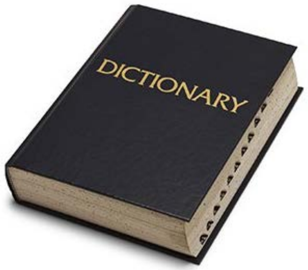
- The Secretariat Study Group on Cybersecurity (SSGC) comprises representatives of States and industry

- Milestones for ICAO Council 216th Session:
  - Present draft of the **ICAO Cybersecurity Strategy**; and
  - Present **feasibility study for Cybersecurity Panel**.

- Parallel Secretariat activities: participation at EASA Shared Trans-Organisation Risk Management (STORM); engagement with industry on data driven risk management for cybersecurity; Cybersecurity Repository; Cybersecurity Point of Contact Network

- Spin-off: **Cybersecurity Research Subgroup on Legal Aspects**

1st Cyber RSGLEG (22 November 2018)



- Categorization of cyber threats and vulnerabilities
- Establishment of common understanding and terminology;
- Analyze adequacy of current international legal framework;
- Analyze current States' legal provisions on cybersecurity and develop best practices;
- Analyze cyber security related international instruments;
- Identify matters that may require referral to the ICAO Legal Committee;
- Encourage ratification of Beijing Instruments

Regional initiatives

Civil Aviation Cybersecurity Workshop
(Montego Bay, Jamaica, 20-23 March, 2018)

2018 FAA Caribbean Initiative Cybersecurity Tabletop Exercise
(Washington D.C., United States, 17-19 July 2018)

NAM/CAR/SAM Cybersecurity Workshop (AVSEC and ANS)
(ICAO NACC Office – Mexico City, Mexico, 4-6 December 2018)

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