ICAO UNITING AVIATION

Informal Briefing to the ICAO Council

Update on Cybersecurity
The Trust Framework

Director, Air Navigation Bureau
Director, Air Transport Bureau

GREPECAS/18 Technical Workshop
11 April 2018

ICAO Cybersecurity Strategy

- Industry High Level Group (IHLG)
  - Agreed to handover cybersecurity-related tasks to the ICAO Secretariat Study Group on Cybersecurity (SSGC)
  - Civil Aviation Cybersecurity Action Plan (signed on 5 December 2014)
  - Preparatory work for ICAO Assembly **Resolution A39-19** *Addressing Cybersecurity in Civil Aviation*

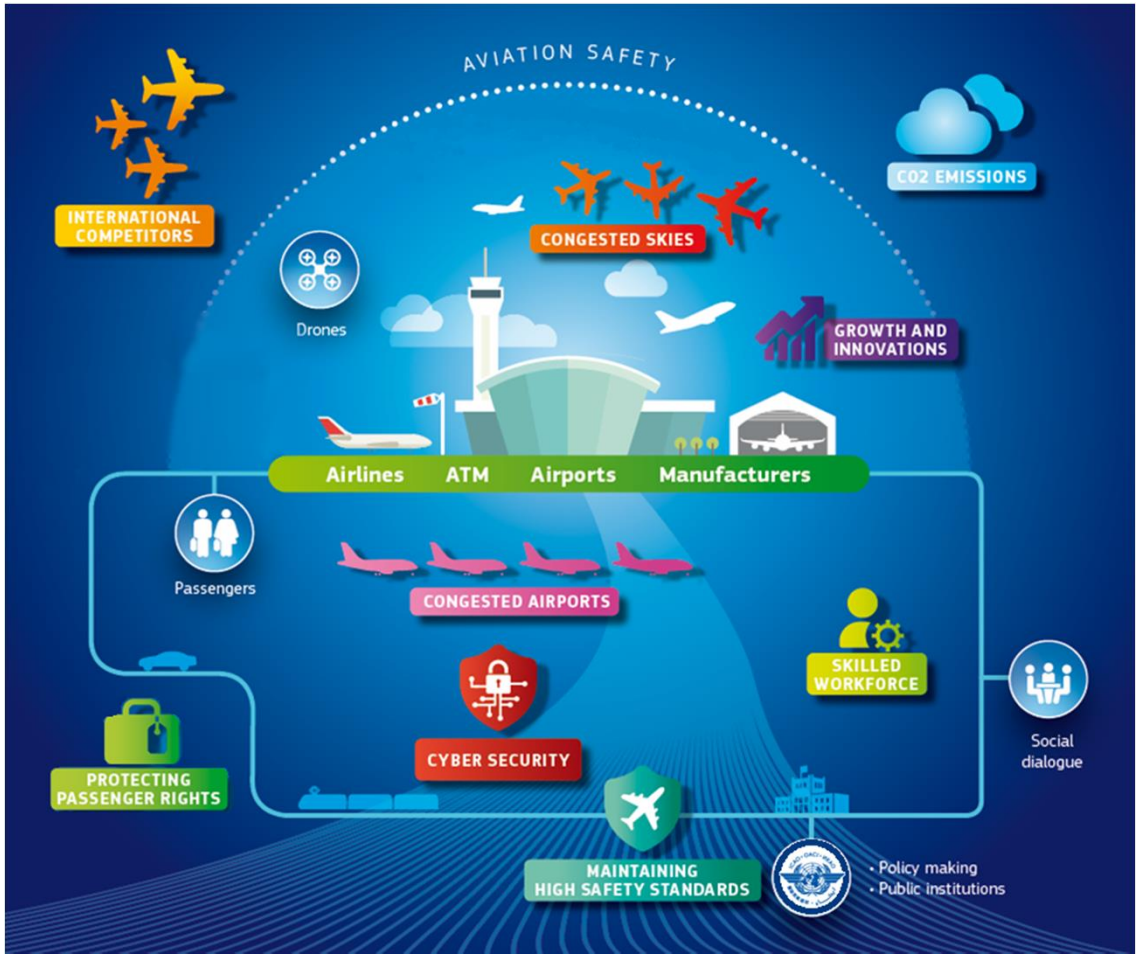
- A39-19 adopted by ICAO 39th Assembly (2016)
  - Aimed at addressing cybersecurity in civil aviation through a horizontal, cross cutting and functional approach

- Secretariat Study Group on Cybersecurity (SSGC)
  - Under the monitoring of the Secretariat Senior Management Group on Common Safety and Security Issues (CSSI)
  - Chaired by Deputy Director, Aviation Security and Facilitation and launched in August 2017
  - Established in response to ICAO Assembly Resolution A39 -19
  - To lead and seek to attain a comprehensive cybersecurity work plan and governance structure with all relevant stakeholders

SSGC Progress

- Two meetings:
  - First Meeting, 29 August 2017
  - Second Meeting, 10 January 2018
- Progress:
  - Approved Terms of Reference and Structure of Working Groups
  - Established a small task force to review and prepare a consolidation of existing SARPs related to cybersecurity. A report will be presented to the 3rd meeting of the SSGC to be held in May 2018
  - Endorsed roadmap to draft an ICAO cybersecurity strategy for the 40th Session of the ICAO Assembly (A40)

The aviation ecosystem



Capacity and efficiency - Congestion

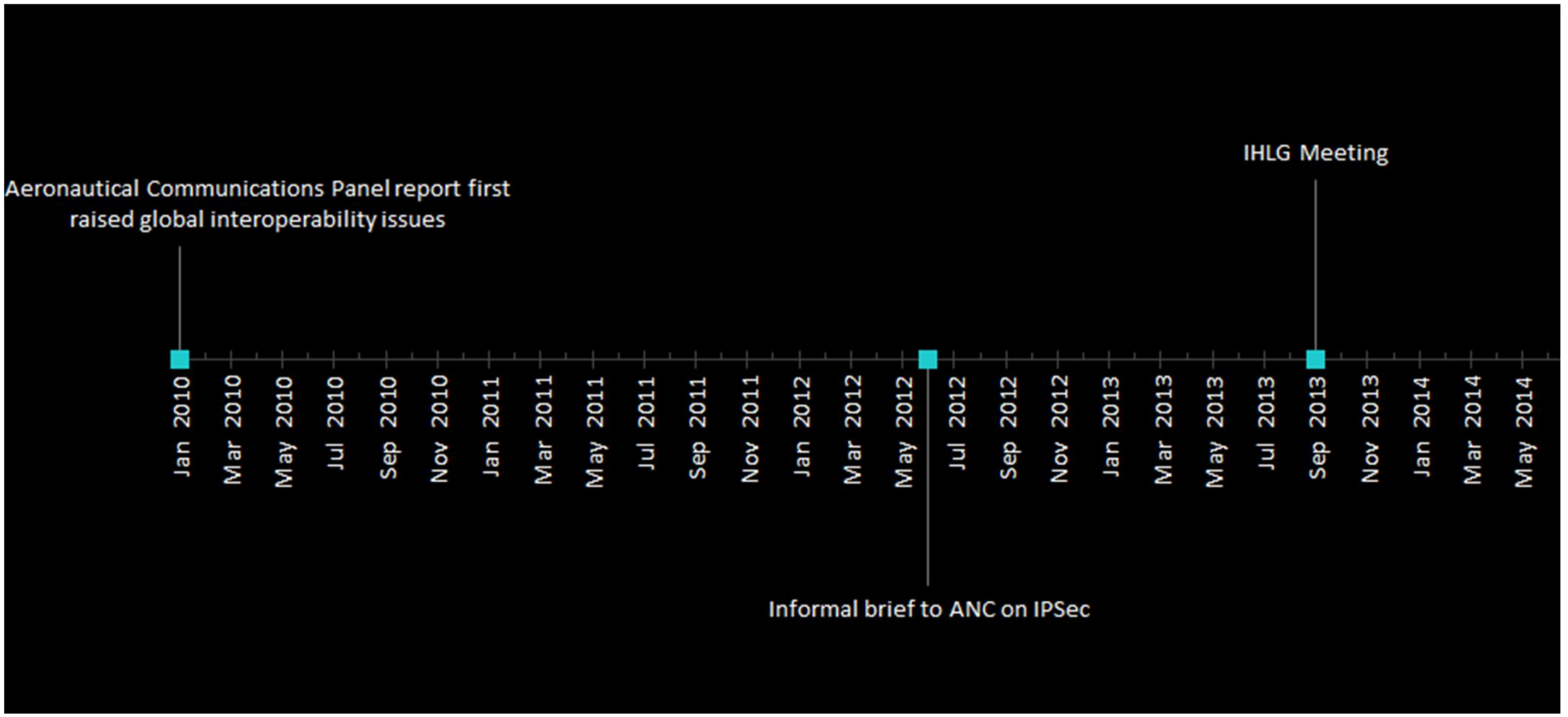
Information interoperability
- Between users
- Globally
- Securely with trust

New Entrants

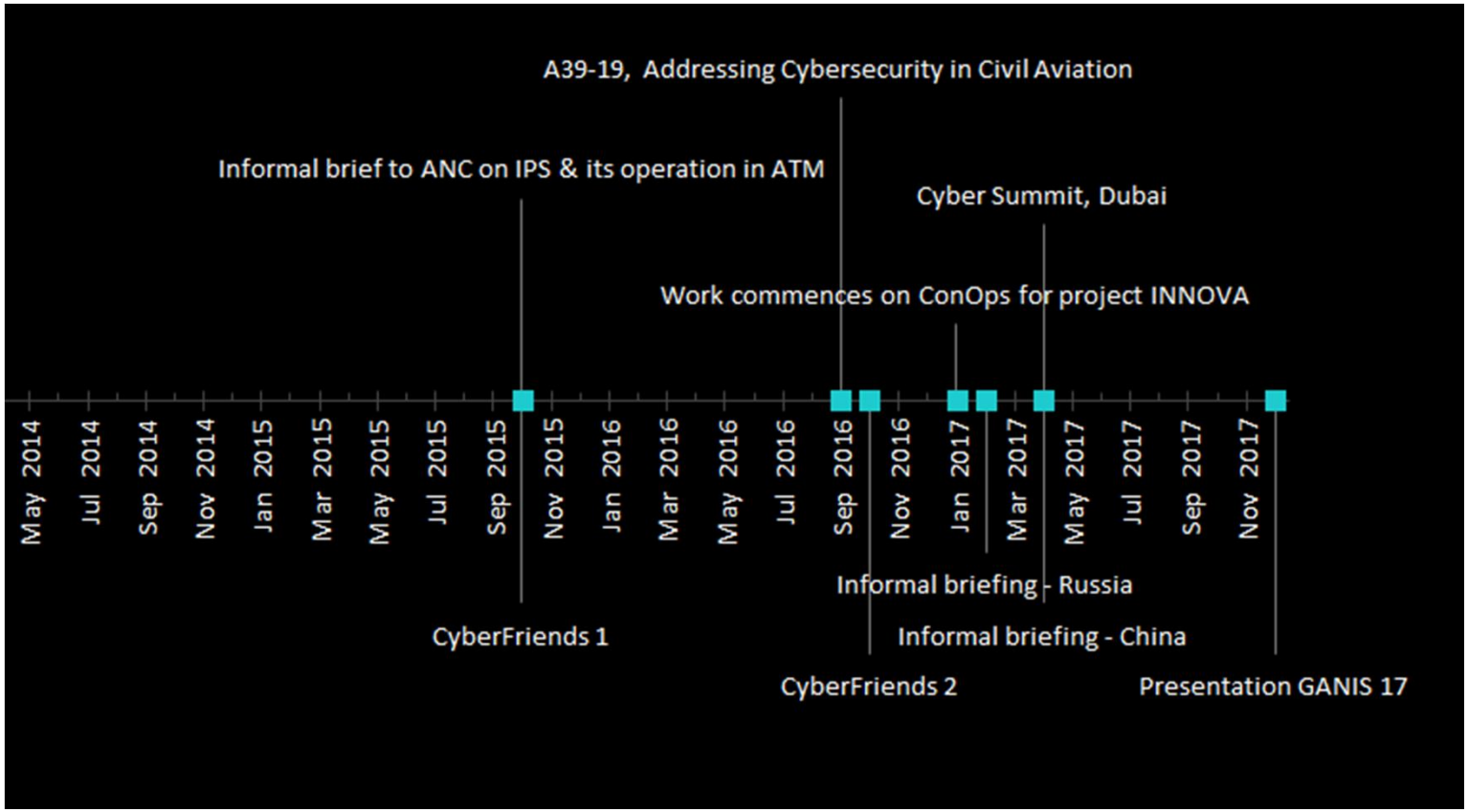
Cybersecurity for information systems critical to aviation safety (ANB)

- Airworthiness
  - EUROCAE WG72 (Aeronautical Information systems security) and RTCA SC-216
  - SSGC subgroup on airworthiness
- Future Air Navigation Systems
  - Various ICAO Groups have identified the need for a coordinated approach to information systems security for more than a decade. Expert groups papers are evidence of this
  - ICAO conferred with States, Industry, ANSPs, International Organizations, and communication providers
  - Information systems security assigned to Global Interoperable Systems Section of ANB
  - Our focus has been to identify the problem

Information systems security timeline in ANB



Information systems security timeline in ANB



Resilience

To maintain and recover ongoing operations during and following a disruption

- Governance
- Safety and security by design
- Coordination & information sharing
  - CERT activities
  - Aviation Information Sharing and Analysis Centre (A-ISAC)
- Cyber “hygiene”
  - Human factor (awareness, training, best practices)
  - Software patching
  - Maintenance

Security by design: *Trust framework*

- The problem is complex.
- Trust Framework is one cornerstone solution
  - The solution cuts across several sections in and out of the Bureau
  - Potentially stakeholders exist that aren't operational or yet active
  - The solution requires a coordinated approach with the aviation community
- Network interconnection, IT generalization and Internet of things have increased the attack surface exponentially
  - A Trust Framework will reduce the exposure
  - A structured governance will mitigate the risk, the impact of and the response to potential attacks

Identifying the problem

Future Issues

B2-SWIM
Enabling Airborne Participation in collaborative ATM through SWIM
Connection of the aircraft an information node in SWIM enabling participation in collaborative ATM processes with access to rich voluminous dynamic data including meteorology.

B3-RSEQ
Integrated AMAN/DMAN/SMAN
Fully synchronized network management between departure airports and arrival airports for all aircraft in the air traffic system at any given point in time.

Cannot be realized to its fullest

Current Issues

Data communication to the aircraft is unsecured

1. Discovery through ADS-B
2. Gather Info through ACARS (aircraft communications addressing and reporting system)
3. Exploit through ACARS

- ACARS frequencies are available on the Internet
- Kit available on line to change frequencies and spoof commands to the aircraft
- Hack has been confirmed by an intelligence agency

Has no identity management or integrity checking

State and Industry Consultation

To date consultation has been informal

The INNOVA concept of operations was identified as necessary so that States could understand the impact to them

A technical group of volunteers are developing a draft concept for consideration

An insight into the work of INNOVA:

- Proposes a network for the aviation community so that people and systems can exchange information globally in a trusted, secure and resilient environment
- A Trust Framework using common standards and procedures is required for the network. The Trust Framework can operate independently of INNOVA
- INNOVA is not a Cybersecurity solution, it is a network with security by design so that we reduce the threat surface and build safety and resilience
- INNOVA will impact most if not all sections of the ANB if it is realized

GANIS outcomes

GANIS was the opportunity to share ideas and to obtain industry feedback

Interoperable information systems cannot operate without trust

Again the objective is reducing the size of the threat surface

Community opinion was clear:

- ICAO needed to take a leadership role if a global Trust Framework was to be realized
- A decentralized system will collapse under its own weight

The aviation information exchange should be carried through a protected network not exposed to the public.

Trust Framework to 13th AN/Conf.

Global exchange of information for operational use cannot happen without TRUST

This is ICAO responding to States and industry

ICAO is the most appropriate organization to define and build TRUST

The aviation community requesting ICAO to take a leadership role

This was the genesis of the Secretariat ANCONF/13 WP on cyber

WP withdrawn from the 207 ANC Session, will be reformulated with additional supporting evidence for ANC consideration in next session

Funding

- Big Picture
  - A Trust Framework is not a revenue generating activity
  - This falls under ICAO's historic mandate
  - The new framework may present new funding sources
  - Such opportunities are enablers not the objectives
  - Such opportunities will be evaluated by the Council as part of their normal budgetary process

Funding cont'd

- Problem identified early by Secretariat
- Insufficient Regular Programme funding
- Problem becoming critical to safely accommodate growing traffic and emerging entrants
- ANB case to SG for Carry-over funds to validate problem
- Problem confirmed
- Request to ARGF for seed funding for trust framework
  - Conops
  - Top Level Domain Name
  - Governance Model
  - Operating System
  - Contract for Services

Summary

- ICAO work on Policy and Strategy in cybersecurity is on tracks
- ICAO work on a Trust Framework was very late getting underway and needs much support from all stakeholders: Council, ANC, States & Industry
- Cyber threats are a growing concern to civil aviation
- Mitigation of vulnerabilities to cyber threats is critical for the GANP
- A Trust Framework is a critical component of a resilient SWIM/FANS
- The Innova work is preliminary scoping by the Secretariat that will allow ICAO Council through the Commission to decide the definition of the Trust Framework

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