



TECHNICAL CO-OPERATION BUREAU

Cyb-Air Security in Civil Aviation

Mona Al Achkar Jabbour

Lebanese University

Pan arab Observatory for Cyber Security

LITA

ICAO/UNOOSA Symposium, 28-31 August 2017

Security:

Safeguarding civil aviation against acts of unlawful interference.

Cyber security is about the preventative techniques used to protect the integrity of networks, programs and data from attack, damage, or unauthorized access. But, it is also about resiliency and survivability

This objective is achieved by a combination of:

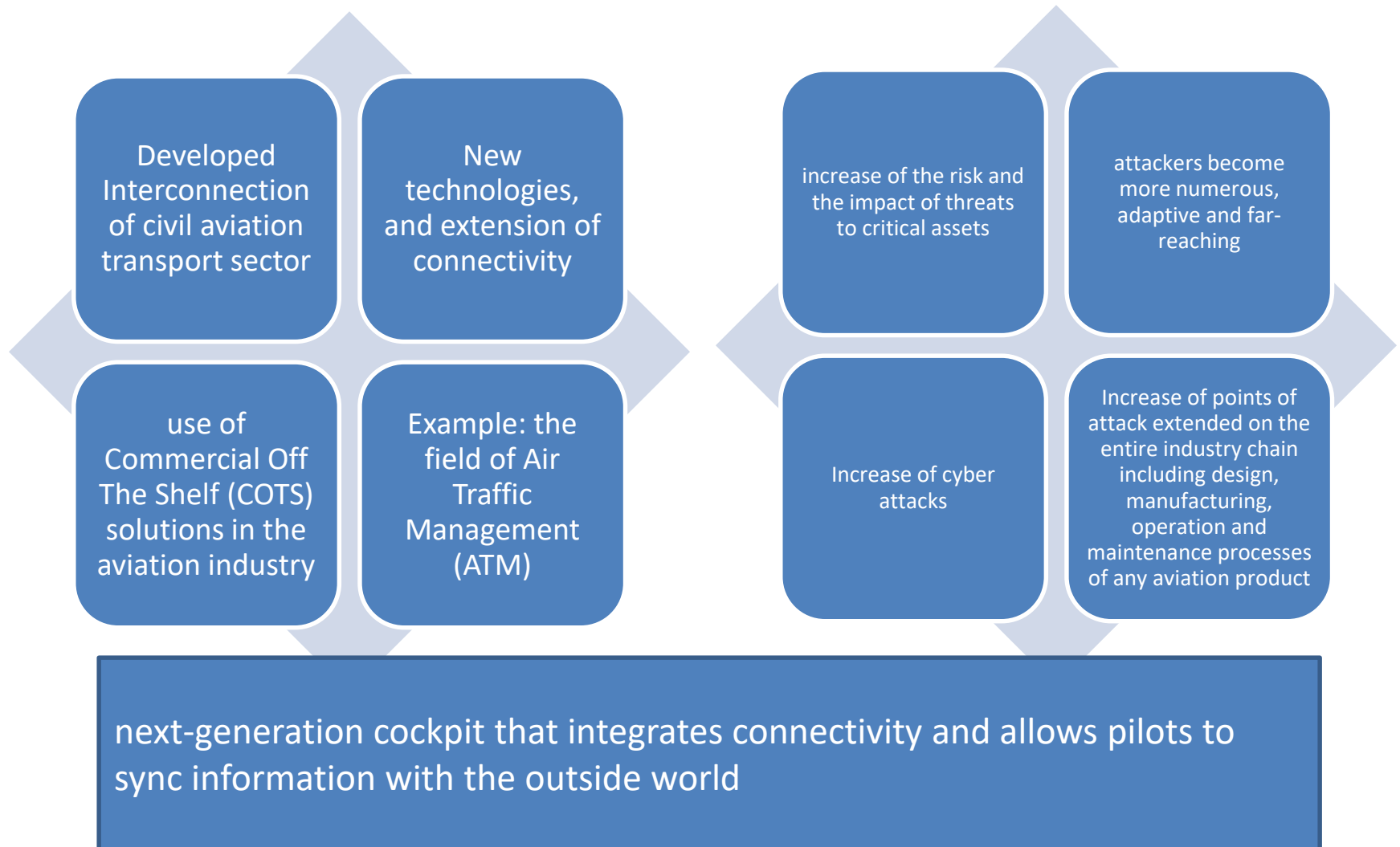
- measures
- human
- material resources



Deal with unlawful acts like :

- 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, bodily injury, or damage to property or the environment

Current landscape



Emerging challenges

Connectivity , digitization, Internet of things, cloud services, big data analytics, artificial intelligence, and cognitive systems bring:

- opportunity for growth
- efficiencies

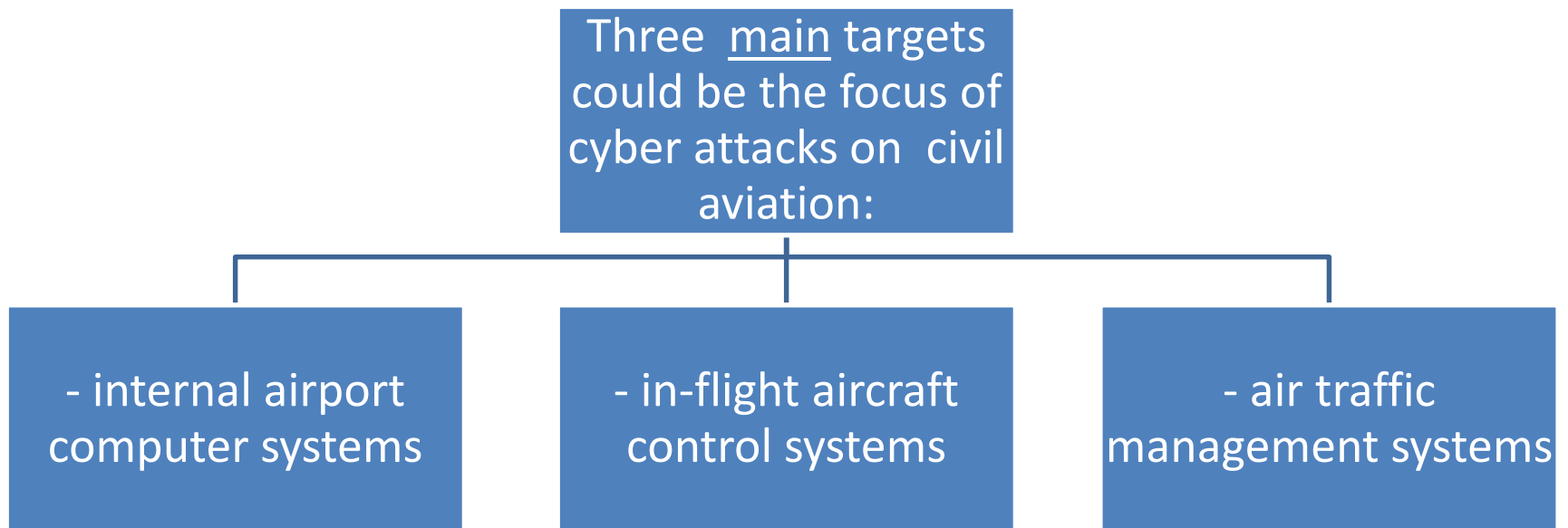
But?!

They also bring:

- new and novel threats
- vulnerabilities
- increasing systemic risk complexity

Cyber New threats Emerging Challenges

Aviation widely and deeply relies on computer:



Talking Cyber Security
concerns:

Operations

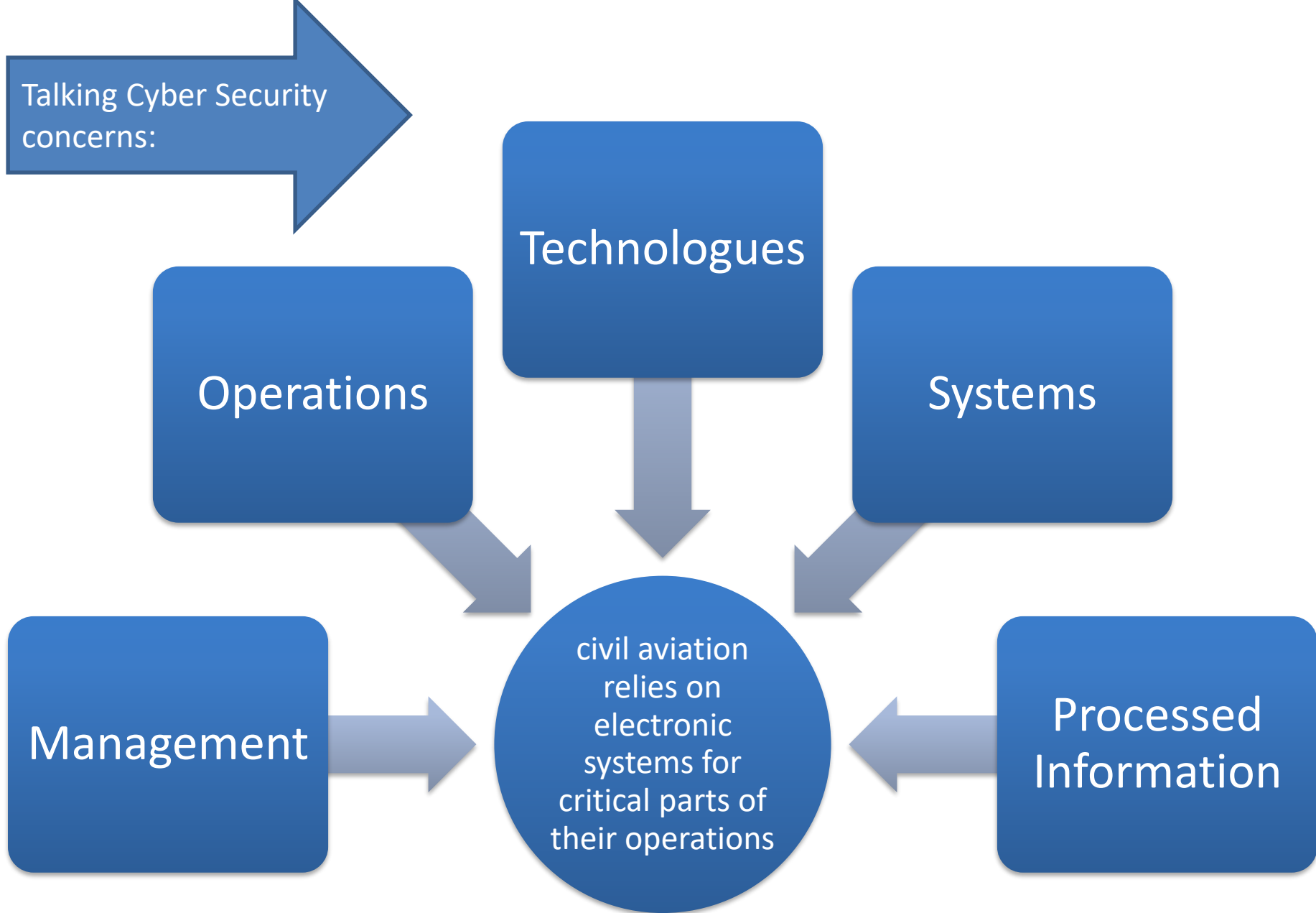
Technologies

Systems

Management

civil aviation
relies on
electronic
systems for
critical parts of
their operations

Processed
Information



Cyber New Threats

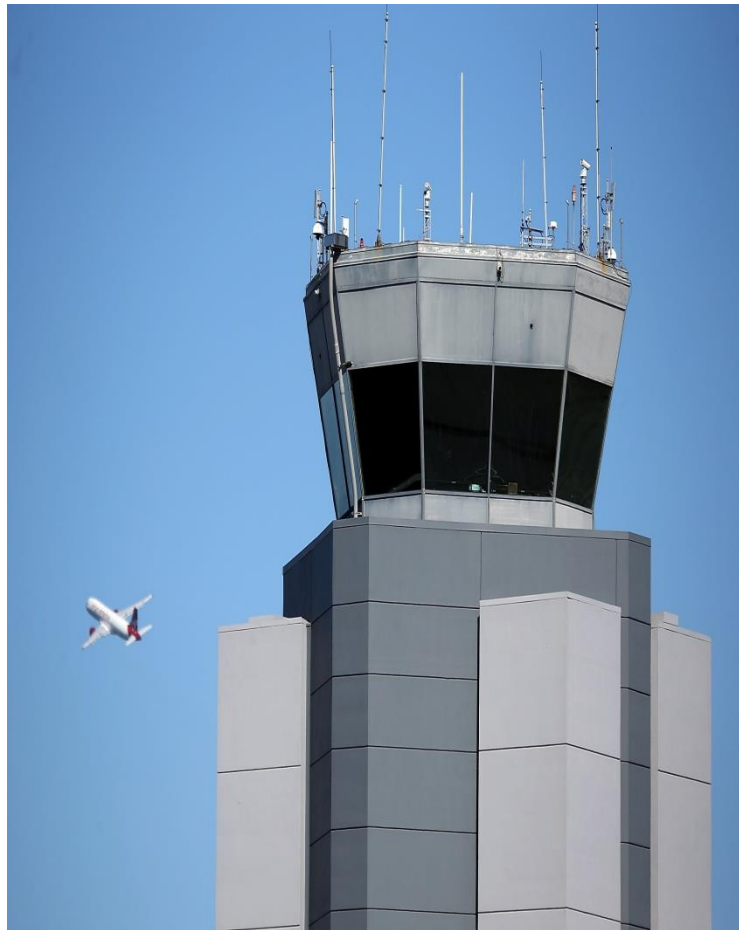
- cyber-attacks directly affect CA systems even in the physical domains
- numerous access points of attack
- Any physical connection that passes data, is a potential pathway for an attacker
- Examples: maintenance and logistic systems, radios, systems that connect operators and platforms (i.e. aircraft, pods).
- **Complexity:**
 - vulnerabilities are not static
 - new vulnerabilities may be introduced with Every software update, every new capability, and every new piece of equipment
 - many operations dependencies will lie outside CA influence

Cyber New Threats

- Disruption of flight schedules
- Blocking messages between cockpits and control systems
- Manipulation of flight data
- Data loss



Report: Hackers broke into FAA air traffic control systems



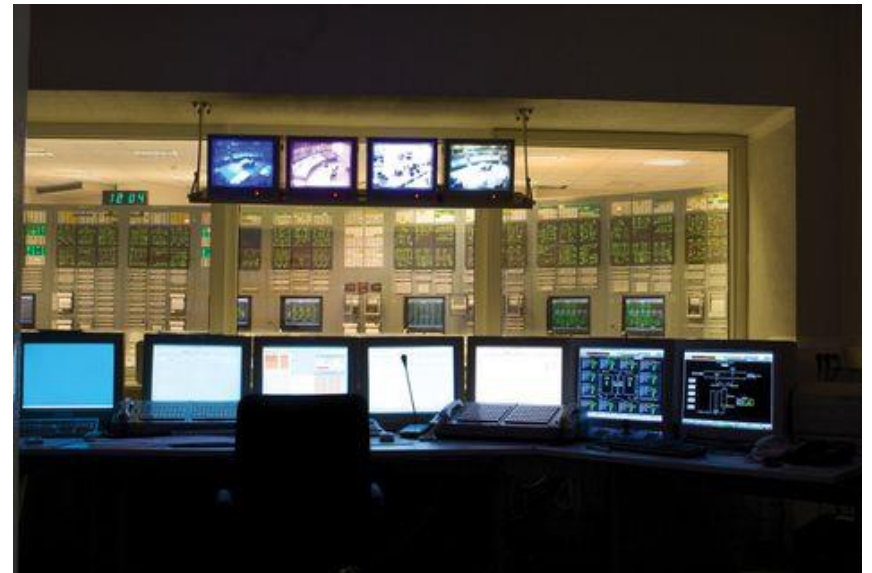
- Breaches exposed sensitive employee data, forced the shutdown of part of a network, and could have allowed hackers to disrupt the agency's mission-support network, a government report says.
- 2006 US Federal Aviation Administration (FAA) was forced to shut down some of its air traffic control (ATC) systems in Alaska
- 2009, An attack on an Federal Aviation Administration (FAA) computer
 - hackers obtained access to personal information on 48,000 past and present FAA employees

Carnage: The charred wreckage of the Spanair flight after the crash in Madrid in 2008 which killed 154



- August 2008 The crash of Spanair flight 5022, killing 154 people
 - Civil Aviation Accident and Incident Investigation Commission of Spain reported that the crash occurred because the central computer system used for monitoring technical problems on board the aircraft was infected with malware

- 2013, A cyber-attack led to the shutdown of the passport control systems at the departure terminals at Istanbul Atatürk and Sabiha Gökçen airports causing many flights to be delayed



Growing threats: IOT

Thanks to advanced technologies, Frequent Cyber-attacks can be carried out:

from virtually anywhere

by anyone with sufficient knowledge

low-budget methodologies

The goal of these attacks

(confidential, critical or sensitive information, to manipulate or erase information and/or to control or destroy systems or services

Results

- uncontrollability of aircraft
- local, limited , large scale
- taking down of system because of an indirect attack (victim of "collateral damage")

Growing threats: IOT

Every new connected device represents a new link on the network



- Risks are becoming physical
- Some new connected devices could cause serious real-world damage

SECURITY RISKS ARE INCREASING IN NUMBER, FREQUENCY AND IMPACT

Growing Danger

cyber-nihilism

weapons are no longer restricted to a small group of actors, including government agencies and coding virtuosos, who follow a set of ethics.

scary exploits are available (breaches at the NSA) , rogue nation states , criminals who purchase them on the dark net

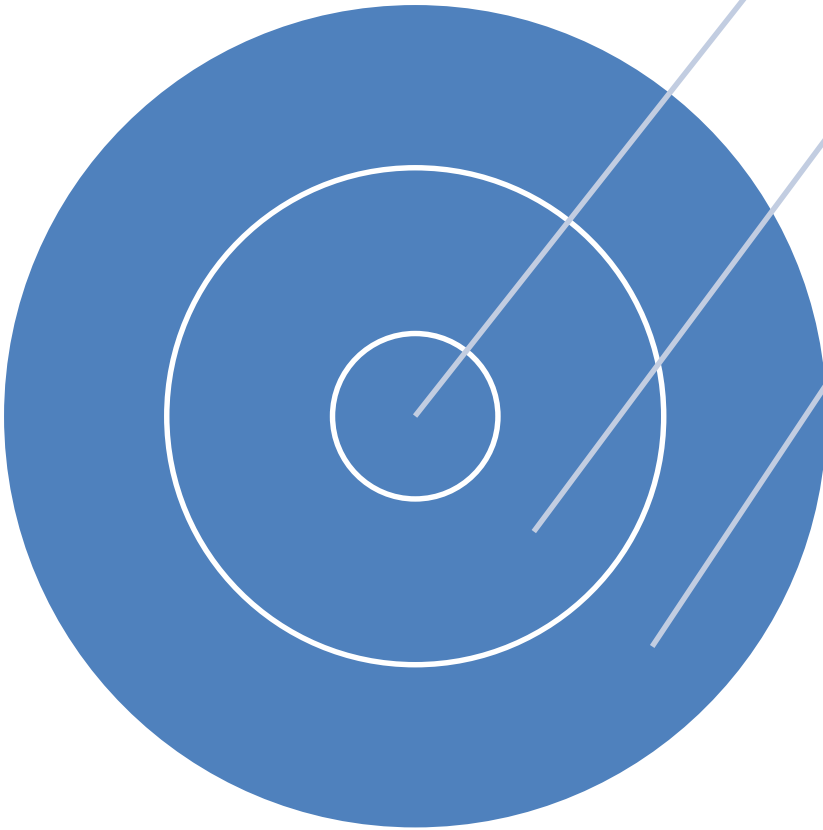
Warning

So far, The attacks have primarily disrupted some support functions

but they could get to the operational networks

- (time surveillance, communications and flight information)

Things can get worse, and damaging to the world peace, when we see that Nations attackers have been mentioned in many reports



National Security

Weaponized
malware

- stuxnet, Bear

Blurred lines
between cyber
security and
cyber attack

- States sponsored
attack

National security

Attacks

- Manufacturing plants seriously damaged
- Energy grids shut down
- Cars manipulated

Experts

- It's only a matter of time before such attacks become more common
- more physically dangerous to both people and property

National Cyber Security

- Cybersecurity involves protecting information and systems from major cyberthreats, such as cyber terrorism, cyber warfare, and cyber espionage.
- In their most disruptive form, cyberthreats take aim at secret, political, military, or **infrastructural assets** of a nation, or its people.
- Cybersecurity is therefore a critical part of any governments' security strategy.

International efforts

In the early 1970s, ICAO adopted the Annex 17 and published a Security Manual to assist its Member States to take measures for the prevention of unlawful interference, minimize its effects

Cyber security threat was left unaddressed

Chicago Convention on Civil Aviation still referred to cyber security as a “recommended practice” and not a “standard.”

International efforts

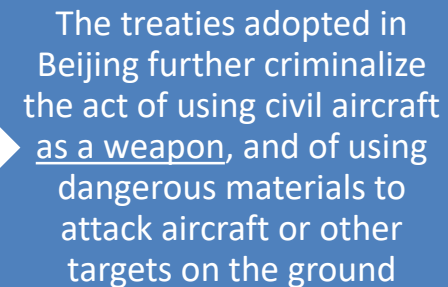
Chapter 4 of Annex 17 now deals with cyber threats:

- - Each Contracting State must develop measures in order to protect information and communication technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation
- The ICAO is working on new safety standards for 2018 on large unmanned aircraft that can fly across borders

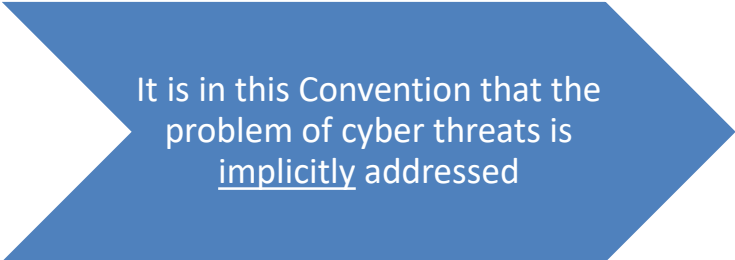
International efforts



Beijing Convention, 2010, hailed as the first step forward in securing the aviation industry



The treaties adopted in Beijing further criminalize the act of using civil aircraft as a weapon, and of using dangerous materials to attack aircraft or other targets on the ground



It is in this Convention that the problem of cyber threats is implicitly addressed

Beijing 2010

However, “in flight” may restrict the scope of this provision if such communication is made when the doors are open or when the aircraft is not actually in flight

An offence is also said to be committed where a person communicates information, which that person knows to be false, thereby endangering the safety of an aircraft in flight

This can be applied to situations where personas are engaged in interrupting air navigation services

DECLARATION ON CYBERSECURITY IN CIVIL AVIATION

DUBAI, UNITED ARAB EMIRATES April 2017

- 1. It is the responsibility of States to act in such a way as to mitigate the risk posed by cyber threats, to build their capability and capacity to address such threats in civil aviation, and to ensure their legislative framework is appropriately established to take action against actors of cyber-attacks;
- 2. Cyber capabilities applied to aviation should be used exclusively for peaceful purposes and only for the benefit of improving safety, efficiency and security;
- 3. Collaboration and exchange between States and other stakeholders is the sine qua non for the development of an effective and coordinated global framework to address the challenges of cybersecurity in civil aviation

DECLARATION ON CYBERSECURITY IN CIVIL AVIATION

DUBAI, UNITED ARAB EMIRATES April 2017

- 4. Cybersecurity matters must be fully considered and coordinated across all relevant disciplines within State aviation authorities;
- 5. Cyber-attacks against civil aviation must be considered an offense against the principles and arrangement for the safe and orderly development of the international civil aviation;

DECLARATION ON CYBERSECURITY IN CIVIL AVIATION

DUBAI, UNITED ARAB EMIRATES April 2017

- 6. The ratification and entry into force of the Beijing Instruments would ensure that a cyberattack on international civil aviation is considered an offence, would serve as an important deterrent against activities that compromise aviation safety by exploiting cyber vulnerabilities, and therefore it is imperative that all States and ICAO work to ensure the early entry into force and universal adoption of the Beijing Instruments, as called for in ICAO Assembly Resolution A39-10:
- Promotion of the Beijing Convention and Beijing Protocol of 2010; and Reiterate our commitment to the development of a robust, efficient and sustainable civil aviation system.

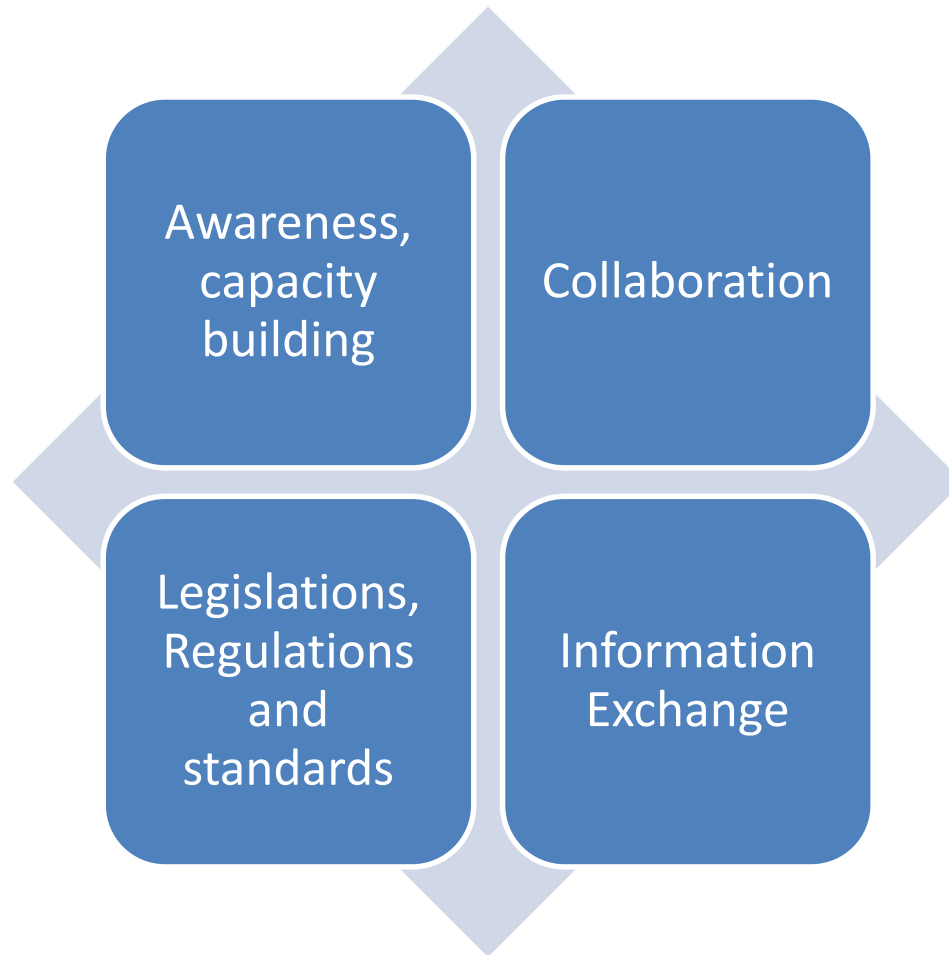
- Position civil aviation cyber security as a high priority on the international diplomatic agenda
- Adopt end-to-end holistic vision
 - create a robust cyber security risk response plan that may avoid gaps, overlaps, duplication of qualification/certification efforts or interoperability issues describes and monitors roles and responsibilities of all stakeholders to
- **States responsibilities**
 - guidelines to manage current and future cyber threats and vulnerabilities, and continuously update those through a comprehensive Air Transport Cyber security Management System;
 - establish Centre (National & international) for Cyber Security in Aviation
 - develop & increase capabilities in managing major cyber crisis in Aviation
 - Avoid unbalanced regulatory developments from different regions of the world

Mitigating cyber threats in civil aviation

Aeronautics, Space, Defence and Security Industries in Europe ASD's Civil Aviation task force

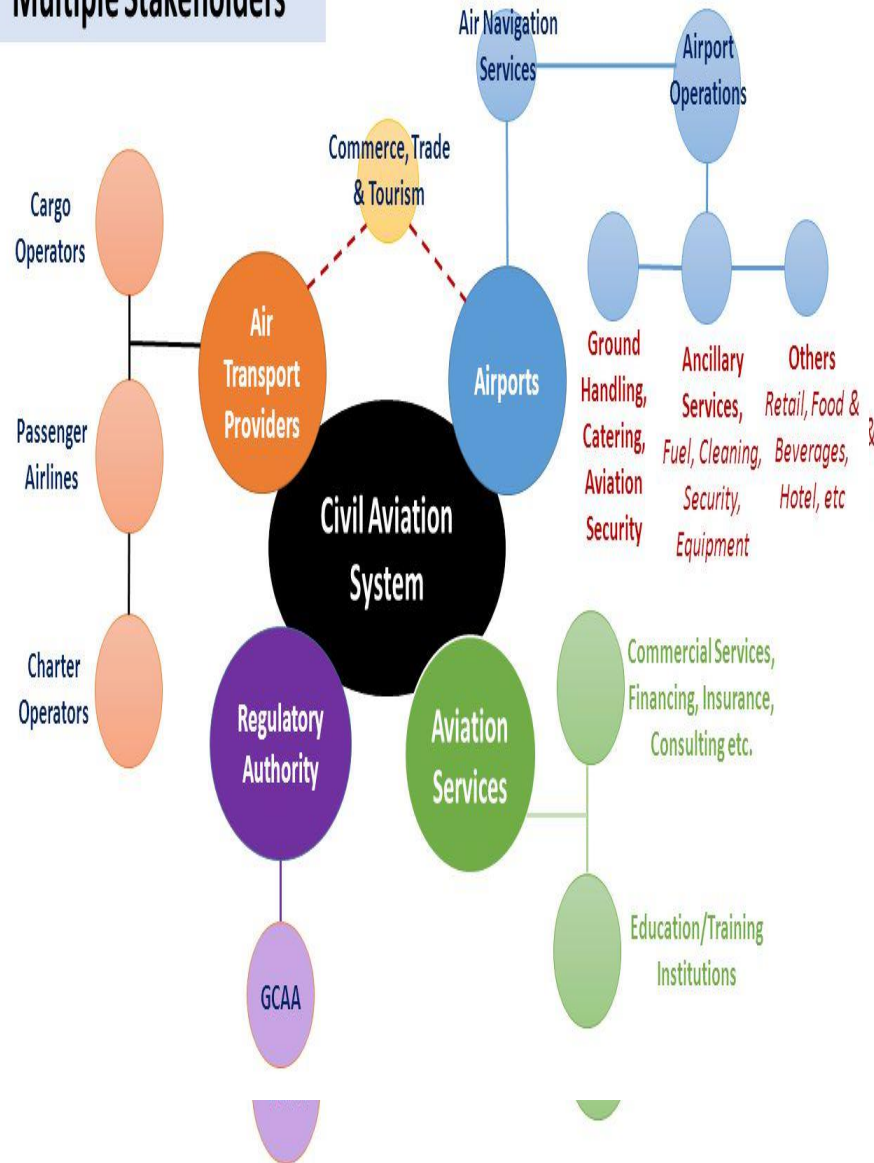


Plan of Action



Shared responsibility

Multiple Stakeholders



States' engagement

Giving the nature of the sector, and the cyber space, as well as the extended surface of implicated authors in the sector,

cyber protection is a shared responsibility among all stakeholders (governments, airlines, airports, and manufacturers)

Industry-Led Public Private Partnerships

The private sector should take the lead on developing the new regime

has expertise about their companies to know where their cyber security stands

what needs to be done to effectively increase their protection without misallocating company resources

Government participation adds important pieces to make this a reality

incentive

information

financial resources

ability to facilitate coordination among private companies

Specific & general approach

Specific Approach tailored to the civil aviation needs

a general approach must be considered

- transportation is part of the critical infrastructure
- technologies employed in civil aviation are also used in other sectors and are, therefore, subject to the same cyber threats
- **But:** A Framework designed to provide high-level guidance to all critical infrastructure sectors, that don't address the particularities of civil aviation's cybersecurity needs won't be effective

Proactive Law Approach

In civil Aviation industry engineering, management, operations, maintenance, etc... are conceptualized around ICTs' use

- Security and safety should follow

there is a need for the law to be conceptualize around the nature, the own challenges and the risks of technology, by adopting a proactive approach, that allows better adoption of the law to the new environment

The law has to discipline:

- the organization of internal controls
- the functioning
- roles and responsibilities related to the development and the management of Civil aviation ITC systems
- liabilities and obligations in all related activities, in administration, operations, services or other
- Nation States commitment

Existing blocks

- Air law conventions
- Cyber crime conventions
- Personal data protection
- Intellectual property
- illegal inception of transmission of computer data
- data interception and exchange interception
- NIS European Directive & other tools

Is it enough?

Proactive law helps:

applying sound legal practices:

- to create future facts
- - to plan a future course of conduct
- - to strengthen the awareness of the population for self-protection and a safe behavior in order to reduce risks and avoid legal trouble

– Predicting human behavior

– Adopting Interdisciplinary approach

– Using economic methods

– Avoiding Laws falling behind in context and time

Importance of this approach?

It aims at helping people avoid legal trouble, disputes, and litigation

It helps build a protective system or a defense mechanism that makes administration, its management and personnel, strong and resistant and keeps them in good legal situation and “immune” to the legal risks inherent in ICTs

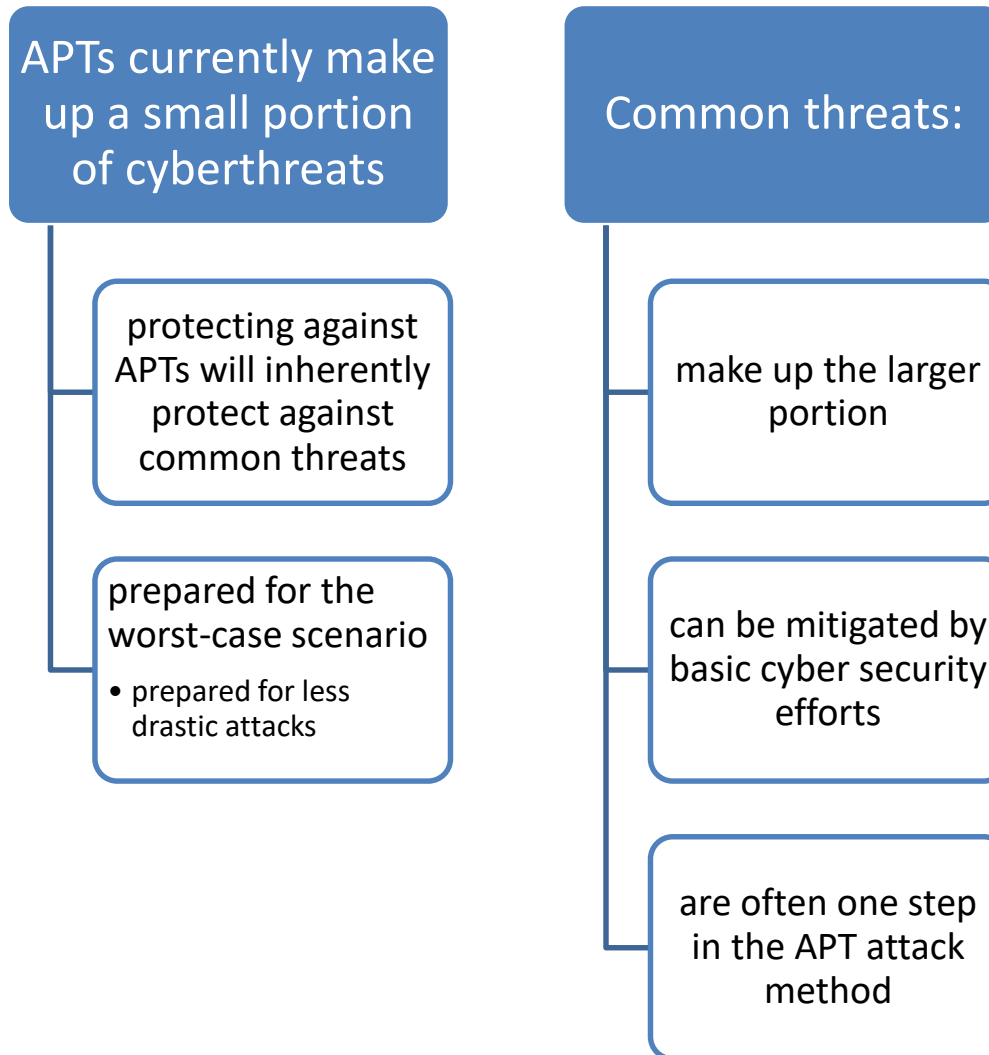
Technical Side

Rethink cybersecurity's approach "from walling off the system to detecting, monitoring and mitigating attacks on the system"

A combination of defense in depth, resiliency, and advanced defense measures

Making cyber defence testing part of the airworthiness certification process for ICAO and other organizations

Protecting against APTs protects to protect against common threats



Sector based risk Approach

develop regulations that are sector appropriate

The sector based risk assessments shall consider general framework of National Infrastructure Protection Plan

Legislation should:

- harmonize efforts between all multistakeholders to avoid neighborhood wars
- support collaboration between industry and government partners
- foster mutually agreed-upon solutions targeted at increasing collective security

Working toward Cyb Air Security

development of new national legislation that defines:

- how civil aviation sector assets are protected
- Organization of cooperation and collaboration between the public and private sectors

At the international level:

- Efforts to stop current and emerging information threats and attacks

Answer the challenges lying behind:

- understanding the needs and conditions that exist in both public and private sectors and of all stakeholders

- Reduce and eliminate lack of trust

– Build rules on international, regional or national agreements that consider all parties

Enhance collaboration between governments, industry, international bodies, private initiatives, academic sector, and all stakeholders

Working toward Cyb Air Security

Fostering a “digital Chicago’s provisions” for cyber security

Building strong partnerships

Developing a common regulatory culture for mutual recognition and understanding of emerging evolving cyber threats

Ensuring openness of air transport market and convergence of regulatory system in all domain in the civil aviation

The way ahead!

Adoption of security by design. integrated security systems by the industry

Working on performance metrics to “measure and report on the effectiveness of all of cyber risk mitigation activities or cybersecurity position”

Considering Mitigation of APTs as critical step to create stronger protection

Focusing on resilience and cyber survivability

The way ahead

Reinforcing cooperation between International Partners

Exchanging information and organization safety data

Enhancing interdependence to promote stability, security and sustainable development

Issuing c security certificates stating adoption of cyber standards and rules,

Thank you

Let's be Cyber Alerted

Make Cyber Security part of the sector DNA