

Cybersecurity in CNS/ATM – Current & future challenges

Engage

Patrick MANA

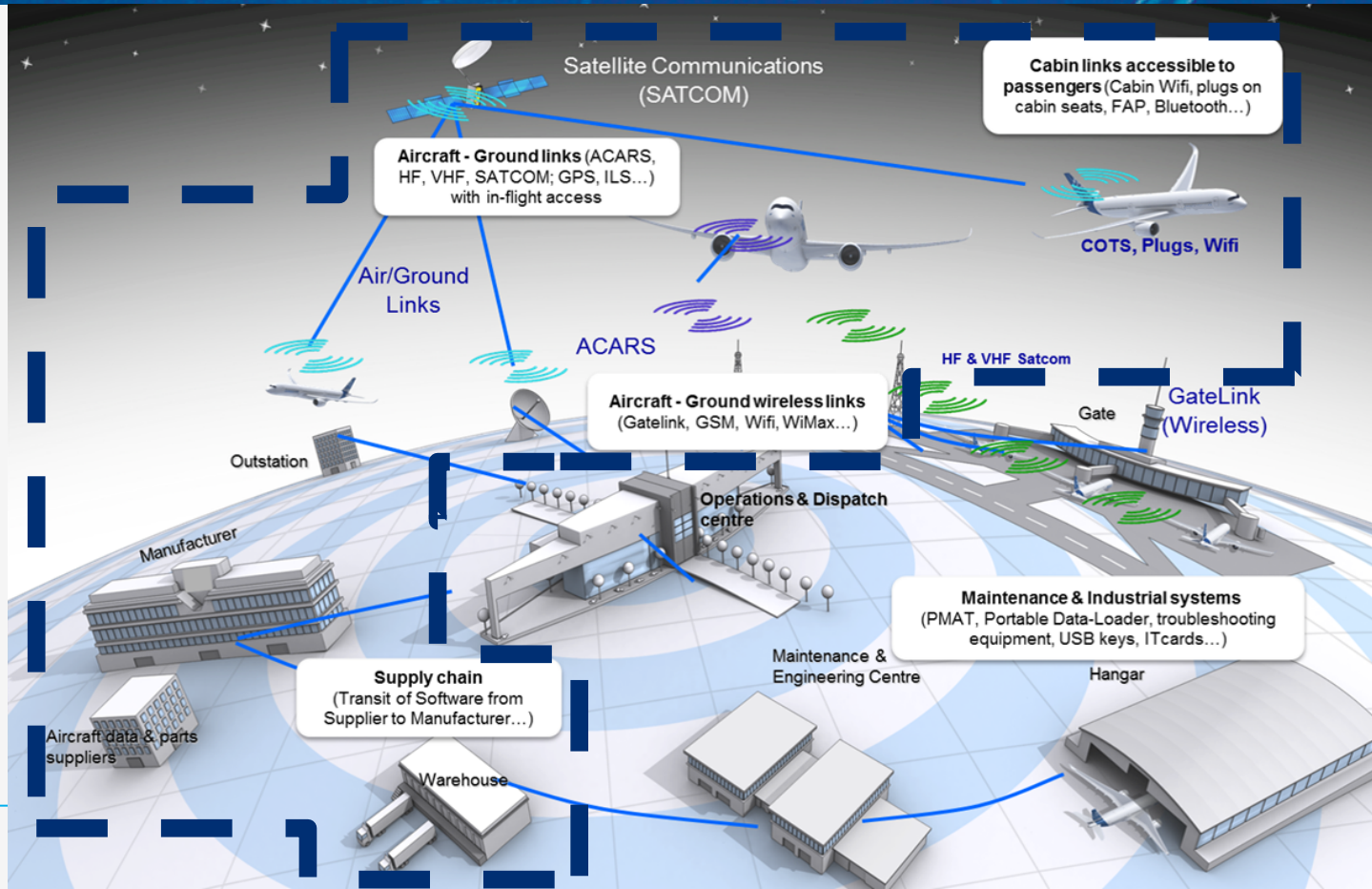
Cyber-Security Cell & EATM-CERT Manager

26/03/2019

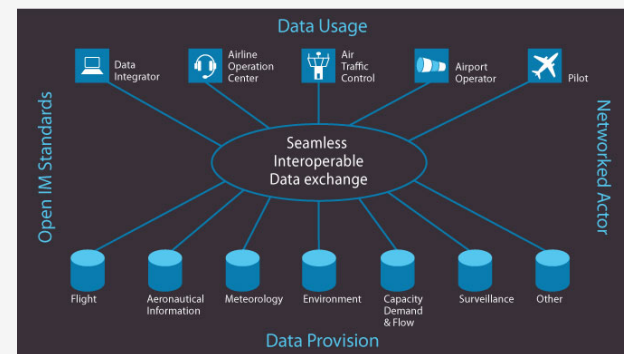
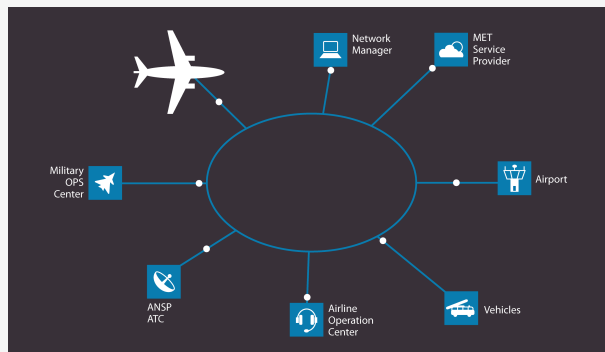
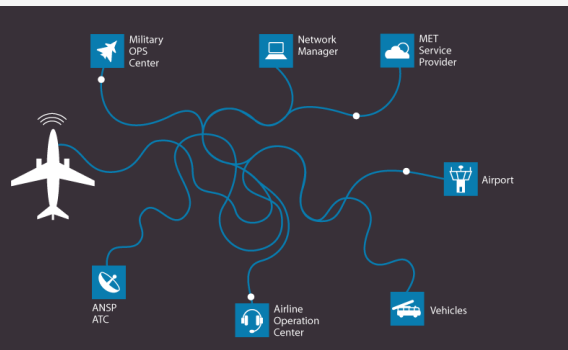


EUROCONTROL

Complexity of Securing the Aviation Ecosystem



Evolution ...




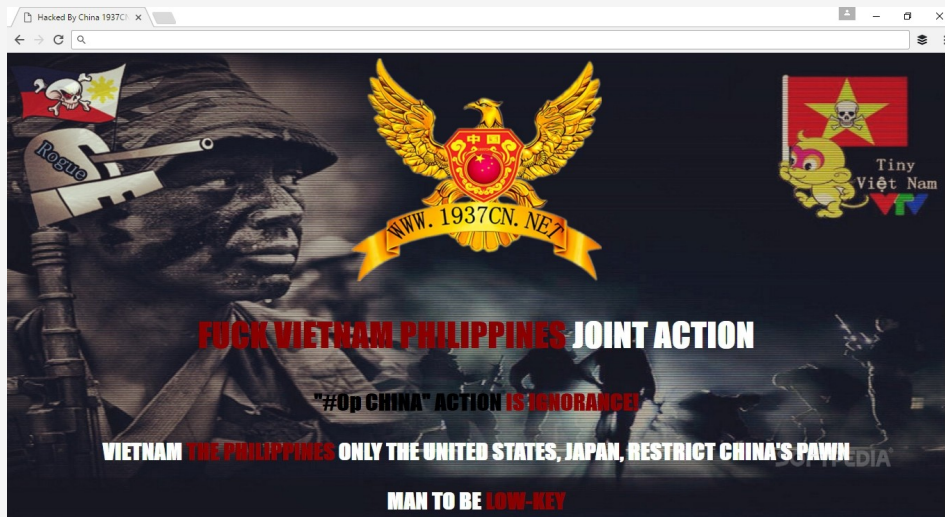


Diagram of an AND gate. It has two inputs, X and Y, and one output, Z. The output Z is labeled as $Z = X \cdot Y$.

Geo-political



Motivation and Cost to Compromise Cybercrime

Malware Products

Account Stealer	\$ 32 - \$ 324
Bank Trojan	\$ 1,273 - \$ 3,956
Basic Malware Kit	\$ 323 \$ 97 /month \$ 258 /year
Advanced Malware Kit	\$ 450 /week \$ 1,800 /month
Custom Kit	\$ 323 - \$ 8,075
Malware vs AV checks	\$ 20
Zero-day money back guarantee	+10%

Command & Control Rental

Bulletproof VPN	\$ 25 /month
Bulletproof hosting	\$ 50 /month
Bulletproof domains/fast flux	\$ 50 /month
Custom C&C	\$ 1000 -

DDOS Services

DDOS kit rental	1 month	\$ 81
	6 months	\$ 161
	1 year	\$ 258
DDOS service / day	1 GB	\$ 16
	10 GB	\$ 161
	DNS server	\$ 323

Compromised Hosts

Asia	1000	\$ 20
NA/EU	1000	\$ 200 - \$ 270
Mix	1000	\$ 35
Handpicked		\$...

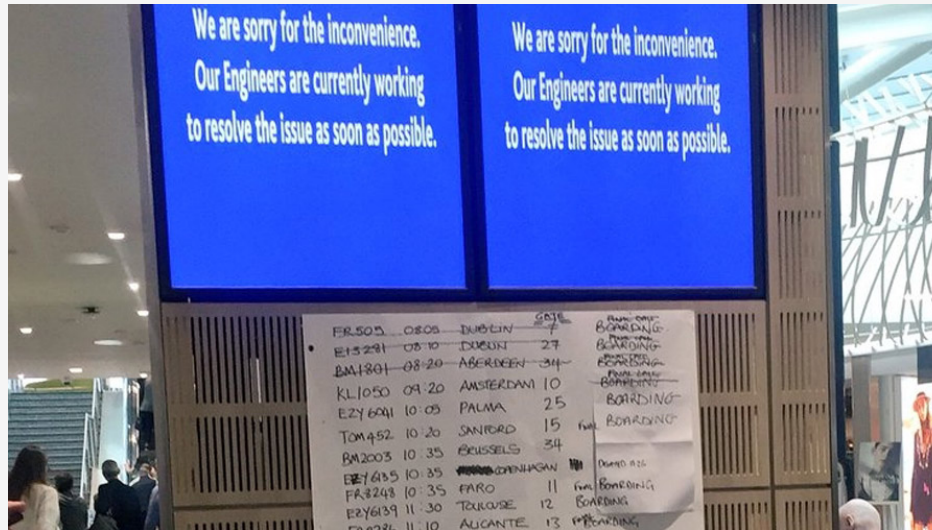
Stolen Data Products

Credit Card US	\$ 4 - 8
Credit Card EU / Asia	\$ 12 - 18
Credit Card + stripe data	\$ 19- 28
US Fullz (ID, SSN, address, ...)	\$ 25
EU Fullz (ID, SSN, address, ...)	\$ 30 - 40
Bank Account + credentials (\$70k+)	\$ 20 - 300

Professional Services

Doxing / Targeting	1 person	\$ 25 - 1000
Fake bank site		\$ 81 - 1000
File Cracking	zip, xls, ..	\$ 45
Hacking	Personal email	\$ 47
	Corporate email	\$ 81 - ...
	Website	\$ 100 - \$ 300
Coordinator / remote support		\$ 50 / hour
Zero Day exploit		\$ 500 - 250,000

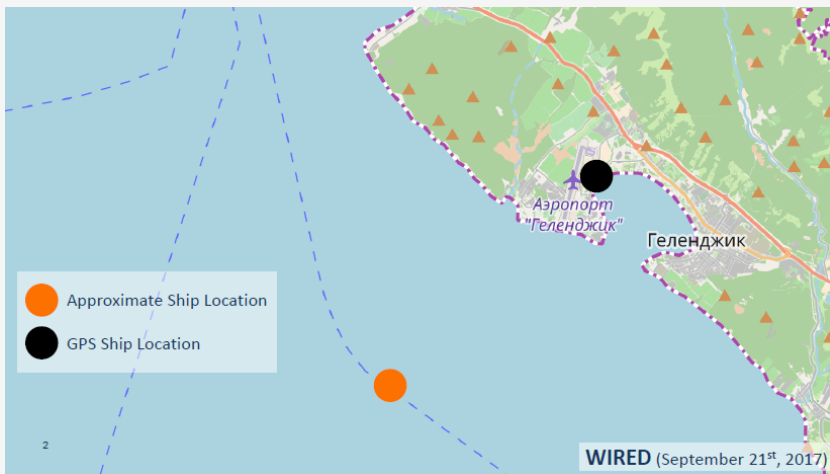
Cyber-crime e.g. ransomware



Hacktivism ... more and more

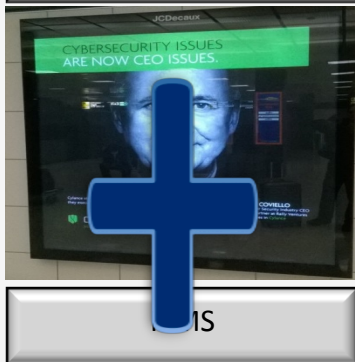


Via technical means



Challenges

Change of culture/
mindset



New
regulatory
framework

GDPR
NIS Directive
EC373/2017

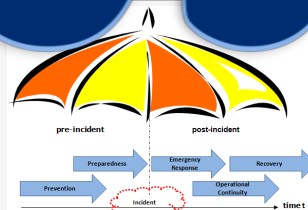
Need for:
AMC
Guidance
Standards
Training

Safety
Security

ty
- Never change
a running system
- Open
- Stop
Versus
Security
- Patch
- Locked access
- Encryption
- Observe attack

Not “if”
But “when”

Risk-based approach
Likelihood subject to
external events
=> Cyber resilience



National
approach

Networks are
national only
Aviation network
Need for
coordination:
Pan-European
Sectorial
Civil/MIL

	National CERT Status A	National CERT Status A	National CERT Status A	National CERT Status A	National CERT Status A	National CERT Status A
Energy						
Aviation						
Health care						
Finance						
...						

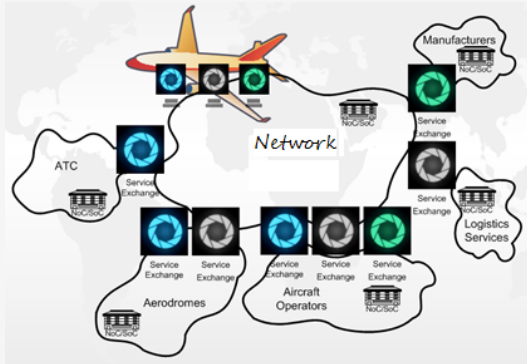


People

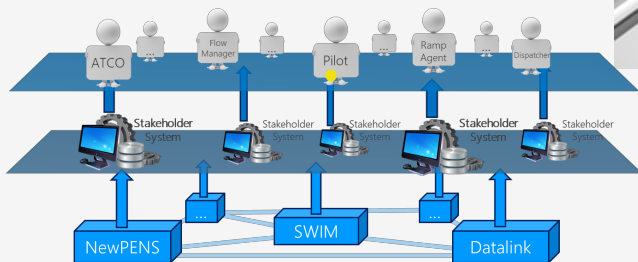
Procedure

Equipment

No State/Stakeholder left behind



ICAO/INNOVA-ACORNS



Cybersecurity services are effective
if all stakeholders adopt them, not only some.
Common Trust Framework with multiple levels

We are as strong as the weakest link !

Principles to get prepared

- **Collaborate for security:** A framework must be in place for system-wide security governance addressing policy, regulation and oversight, and the application of appropriate security management systems.
- **Engage personnel and society:** The means to develop a security culture must be established and implemented across the aviation industry.
- **Security Intelligence:** to provide the information necessary to effectively identify current threats and vulnerabilities, and predict and prepare for those emerging in the future.
- **Operational Security:** Capabilities in Incident Management must be developed to deliver the means of detecting security incidents in real-time, and responding and recovering rapidly
- **Design, Manufacture and Certify for Security:** to ensure that security is addressed in all phases of the life-cycle, including design, manufacture, deployment, operations and decommissioning, supported by the provision of appropriate methods, tools, guidance material, and standards.

Areas for R&D

- Developing capabilities in secure information acquisition, storage and dissemination;
- Developing system architectures which support the development of secure, resilient systems, capable of rapid adaptation to novel attack vectors;
- Developing modelling and simulation tools capable of demonstrating the compliance of a system with security requirements;
- Applying Intelligent Systems to a variety of areas of aviation security. The application of AI to user-behaviour analytics, network surveillance, incident forensics, for example, could provide a system with the capability to react autonomously to breaches, adaptively delaying or neutralising ongoing or developing attacks;
- Research into the safety assessment and certification of safety-critical systems which comprises technology based on Artificial Intelligence.

AIR TRAFFIC MANAGEMENT CYBER SECURITY SERVICES



Are you hacked?

- incident response support & coordination
- artifact analysis (forensics)



Are you vulnerable?

- penetration testing
- red team/blue team scenarios
- security best practices review



Are you prepared?

- cyber threat intelligence
- log collection & intrusion detection
- alerts & warnings
- advisories & announcements
- security awareness building
- cyber security training

KEEP CALM & CALL EATM-CERT

eatm-cert@eurocontrol.int or +32 2 729 46 55

THANK YOU



eatm-cert@eurocontrol.int
patrick.mana@eurocontrol.int



+32.2.729.46.55