



ATM Cyber Security Awareness Workshop

Part I

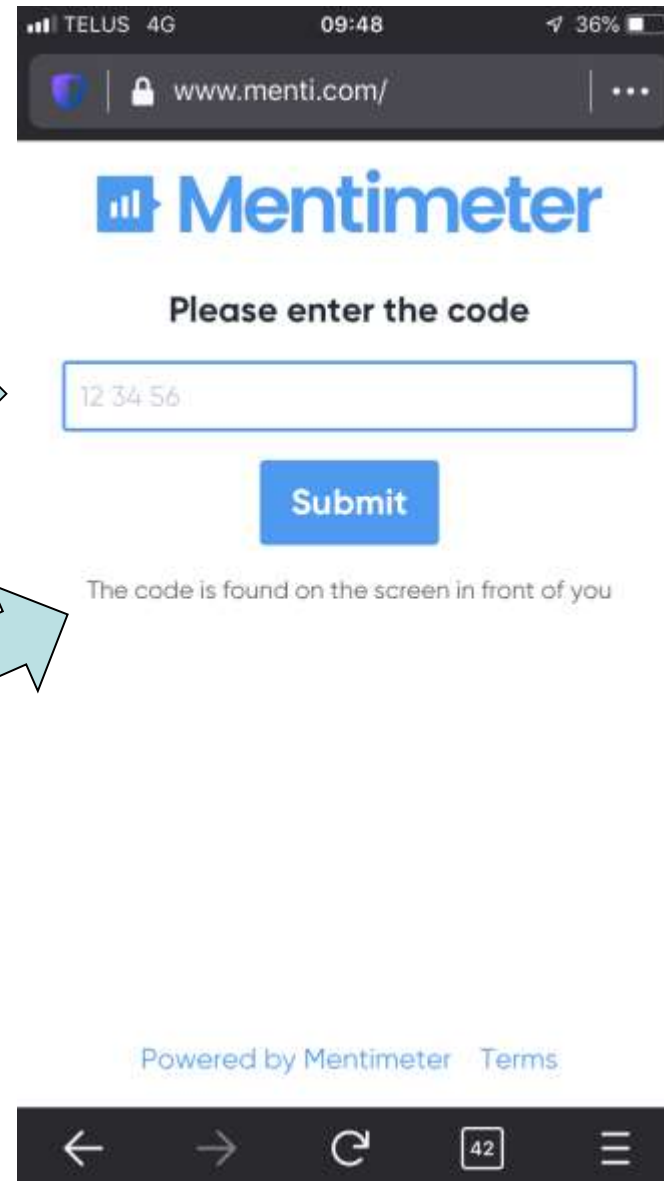
ICAO AVSEC 2019
Montreal, Canada

Dr John HIRD
Air Traffic Management Security Specialist, EUROCONTROL
20th September 2019

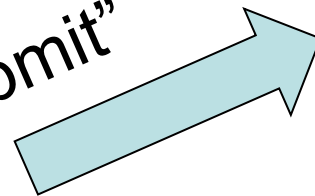
Go to www.menti.com on your Browser

Enter the code :

51 60 29



Press "Submit"



*If wi-fi is slow, and
if feasible, use 3G
or 4G*

*Quiz winners
receive prizes!*

MENTI SURVEY : WHO ARE WE



- **Organisation type**
- **Area of activity**
- **What does the word “Security” mean to you?**
- **ATM Security – level of knowledge**



ATM Cybersecurity Awareness Workshop



	Part I
1	Air Traffic Management (ATM) in Europe
2	Security Terminology
3	The Evolving ATM System
4	Security Incidents in ATM
5	Threats, Attackers, and Vulnerabilities
	Part II
1	Governance and Oversight
2	Regulations, Standards, and Guidance Material
3	Risk Management
4	Culture and Training
5	Trends in ATM Security

AIR TRAFFIC MANAGEMENT (ATM) IN EUROPE

EUROCONTROL Member States

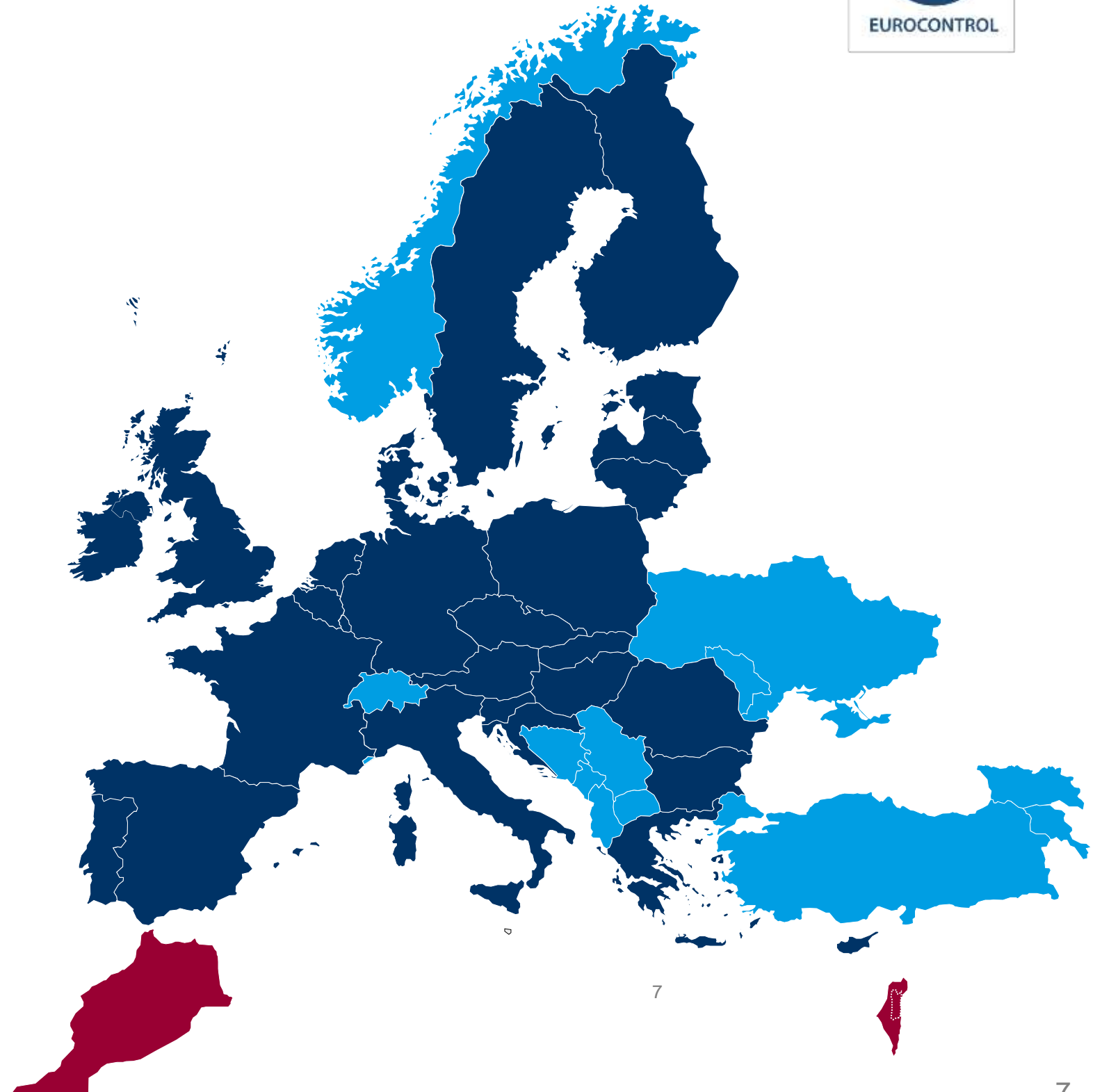


41 Member States & the European Union :

EUROCONTROL and EU

EUROCONTROL but not EU

**Two Comprehensive Agreement
States: Israel and Morocco**



EUROPEAN Air Traffic Management



11.5

Geographic area
(million km²)



37

Number of
civil ANSPs



17,794

Number of
air traffic controllers



55,130

Total staff



15.3

Flight hours
controlled (million)



68

Number of en-route
facilities



280

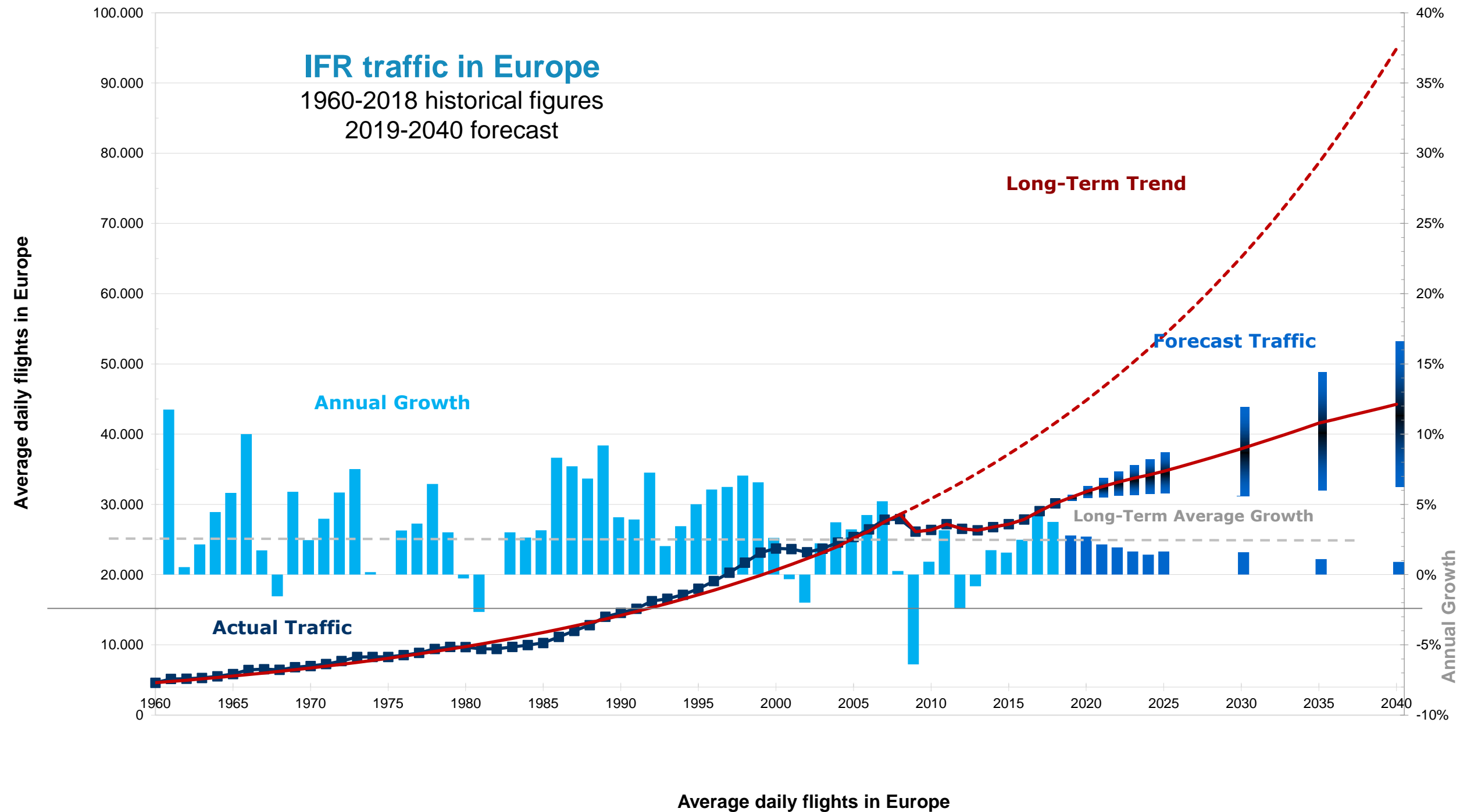
Number of terminal
facilities/approach control



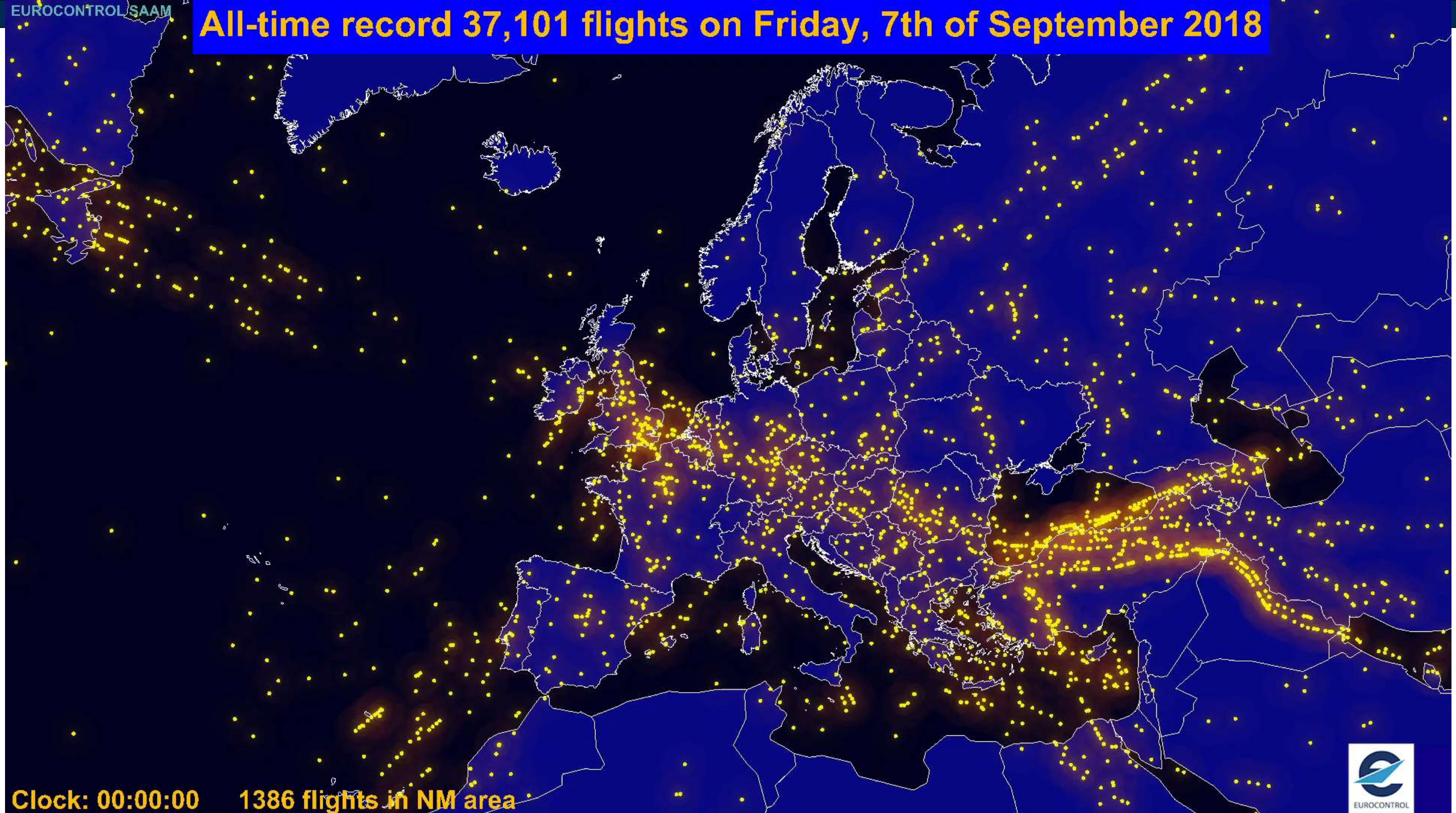
525

Airports with >10 flights a day

Traffic in Europe



All-time record 37,101 flights on Friday, 7th of September 2018



Clock: 00:00:00 1386 flights in NM area

- Safeguarding of the airport

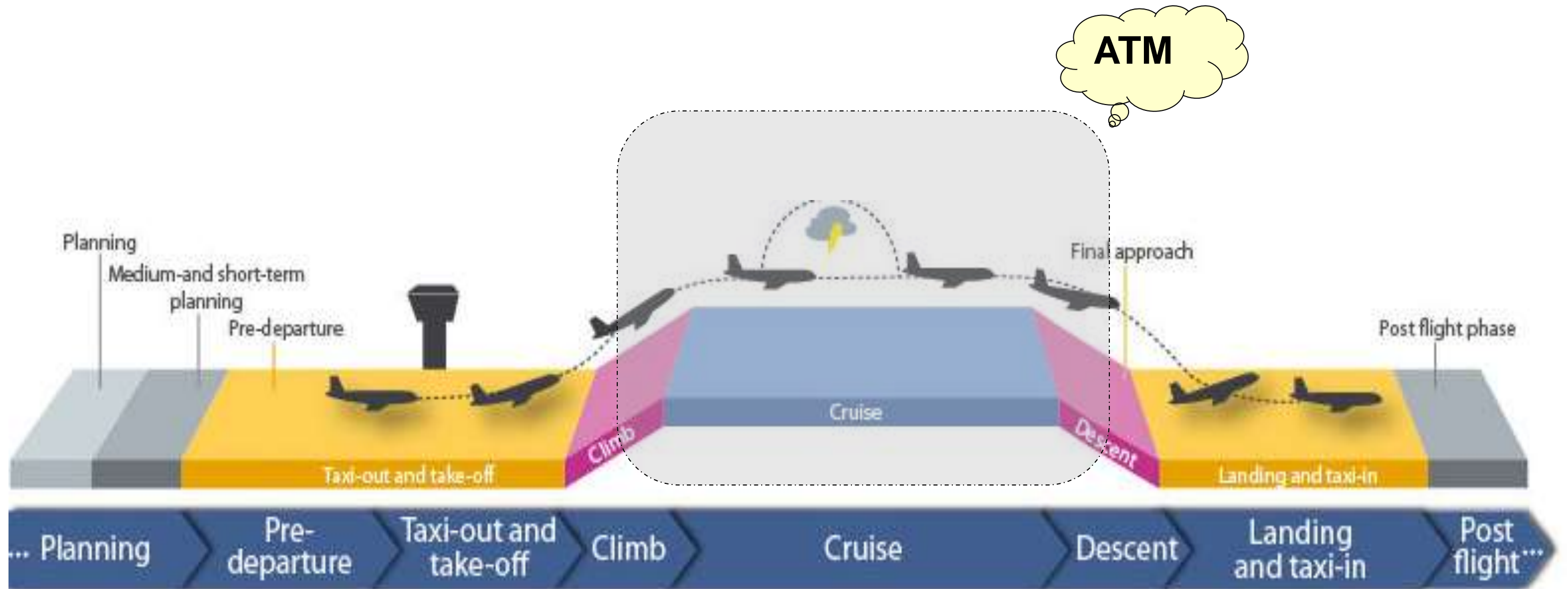
- Safeguarding of the aircraft

- Safeguarding of the airspace



- **Safeguarding of the ATM System**
- **Collaborative support to national / Pan European aviation security incident management**

Air Traffic Management (ATM) Security



Phases of Flight

SECURITY TERMINOLOGY

Security Terminology

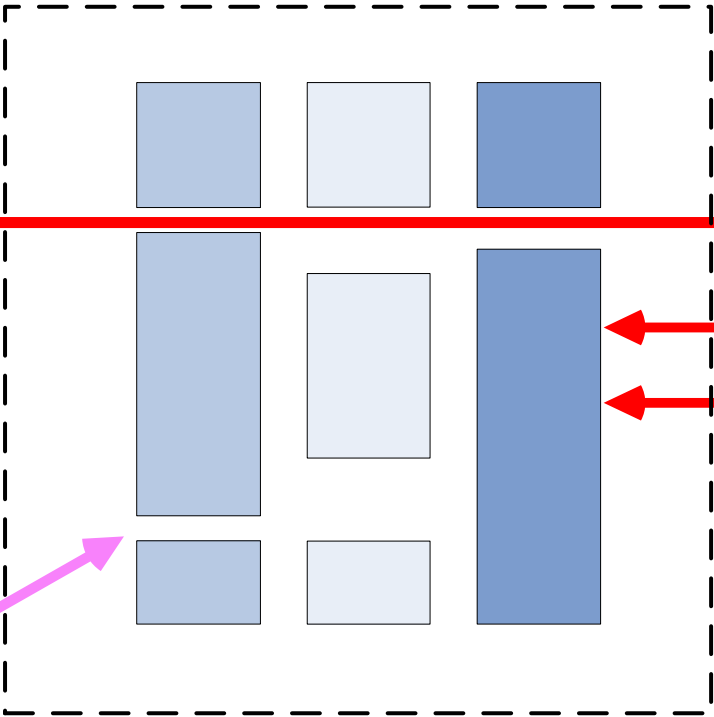


ASSETS

*Things you care about
and want to protect*



CONTROLS



*Potential causes of
unwanted incidents
which could result
in harm to assets*

Vulnerabilities

*Weaknesses in
a system*

*Security measures
to protect assets*

Confidentiality
Integrity
Availability

Confidentiality, Integrity & Availability (CIA)



Information Security - Preserving the *Confidentiality*, *Integrity* & *Availability* of information

- **Confidentiality**

information is not made available or disclosed to unauthorized individuals, entities, or processes
(e.g. information is not read or copied by unauthorized person)

- **Integrity**

safeguarding the accuracy and completeness of assets
(e.g. unauthorized changes are not made to information (corruption))

- **Availability**

being accessible and usable upon demand by an authorized entity
(e.g. information is neither erased nor becomes inaccessible; services must be accessible)

Aviation Assets to be Protected



Service Provision

Aircraft separation
Flow management



People

Staff
Passengers
3rd parties



Vehicles

Civil aircraft – passenger, cargo
Military aircraft
RPAS

Physical Infrastructure

Air traffic control centre
Airports



Infotainment Systems

Wi-fi
Telephone
Multi-media
Journey information

Communications Systems

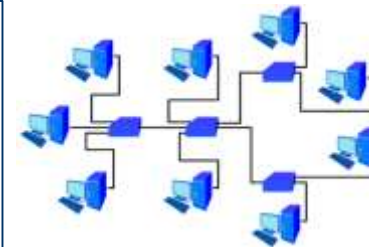
Controller-pilot communications (voice, data)
Airline operator communications
Aircraft sub-system communications

Information

Personal information (staff and passengers)
Aircraft technical information
Traffic management system technical information
Airport technical information
Airspace charts
Meteorological data
Aerodrome charts
Flight plans
CNS data

Information Systems

IT systems
OT systems
Networks



Organisational

Financial
Reputation

Surveillance Systems

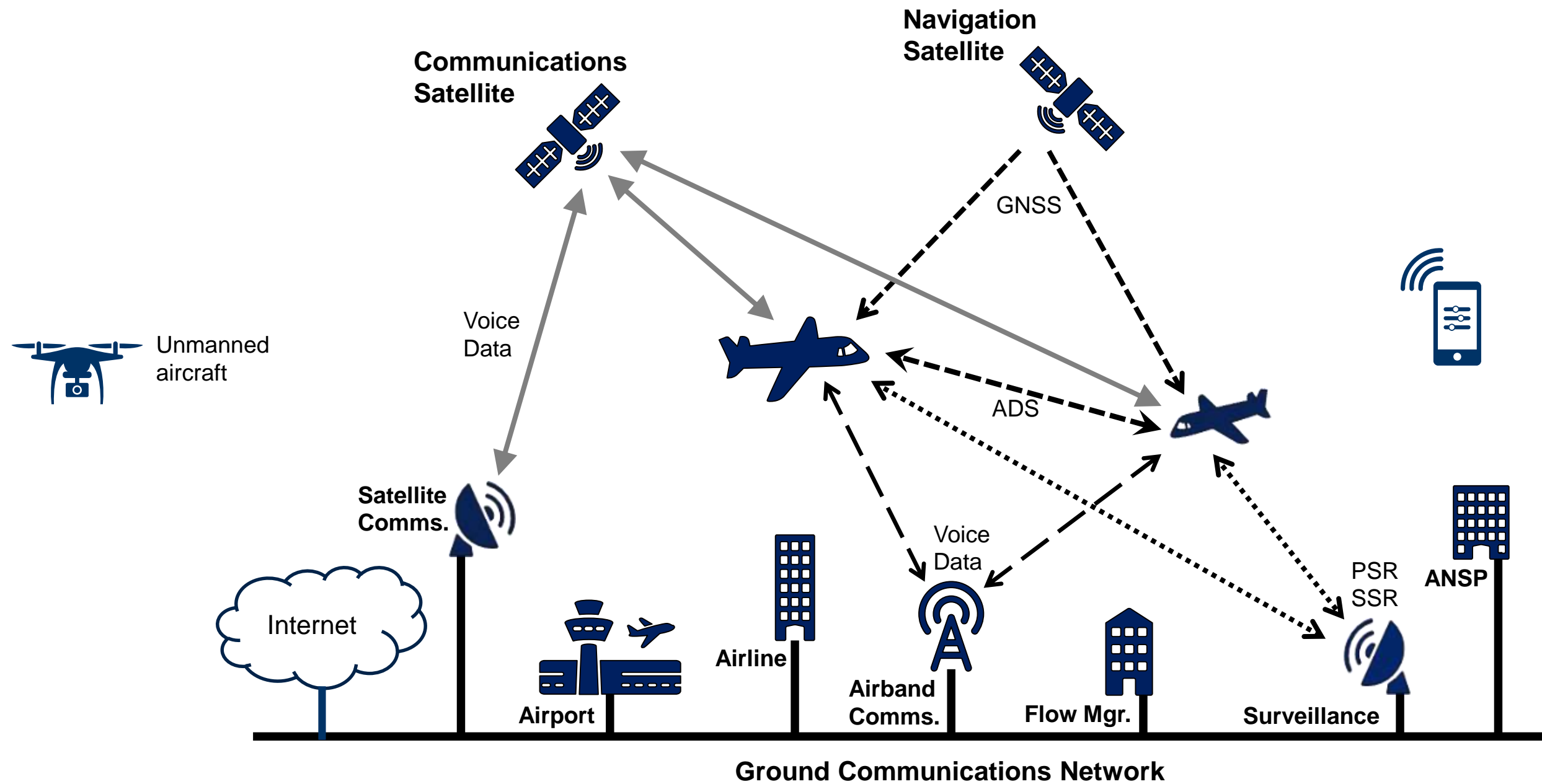
Radar – PSR, SSR
WAM
GNSS
ADS-B
ADS-C ...



Navigation Systems

GNSS
Integrated, hand-held
ILS, VOR, DME

Some System Components



False Instructions to Pilot During Approach to Istanbul Ataturk Airport (Menti : Quiz question 1)

.....There was someone on the frequency who told us to turn right heading 190 we are turning back now heading 170 is that correct?

.....There is another one on the frequency giving us instructions

Unfortunately we have disruption on the frequency 126425, there is another man who is not air traffic control giving some instructions ...

... so I am just warning you – **do not listen to any man**, we are two women working for approach control, **please only listen to women**

CIA?



MENTI QUIZ : CIA



- **Q1 : In the Istanbul approach example, which information attributes are impacted?**

Confidentiality

The attacker eavesdrops (listens in) on pilot – tower communications

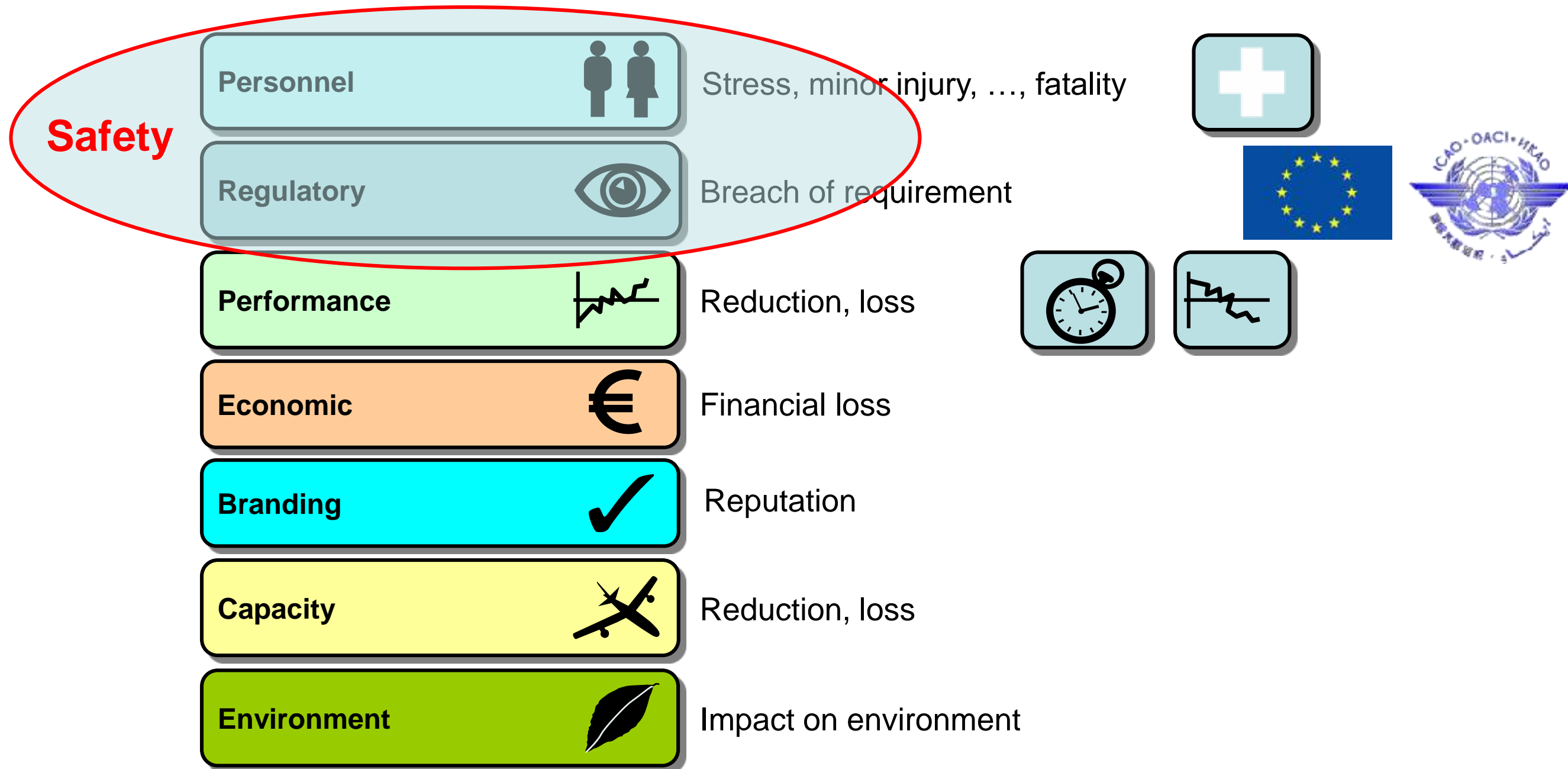
Integrity

The attacker provides false instructions to pilot

Availability

Approach control service availability continues – “don’t listen to any man”

Potential Consequences of an Attack – Impact Areas



Risk

- A risk is the combination of the
 - **impact** of an unwanted security event and its
 - **likelihood**



- Example Risk Matrix :

	Reviewed Impact				
Likelihood	1	2	3	4	5
5	Low	High	High	High	High
4	Low	Medium	High	High	High
3	Low	Low	Medium	High	High
2	Low	Low	Low	Medium	High
1	Low	Low	Low	Medium	Medium

- Risk appetite
 - The level of acceptable risk

Black Swan Event

A black swan event is one that

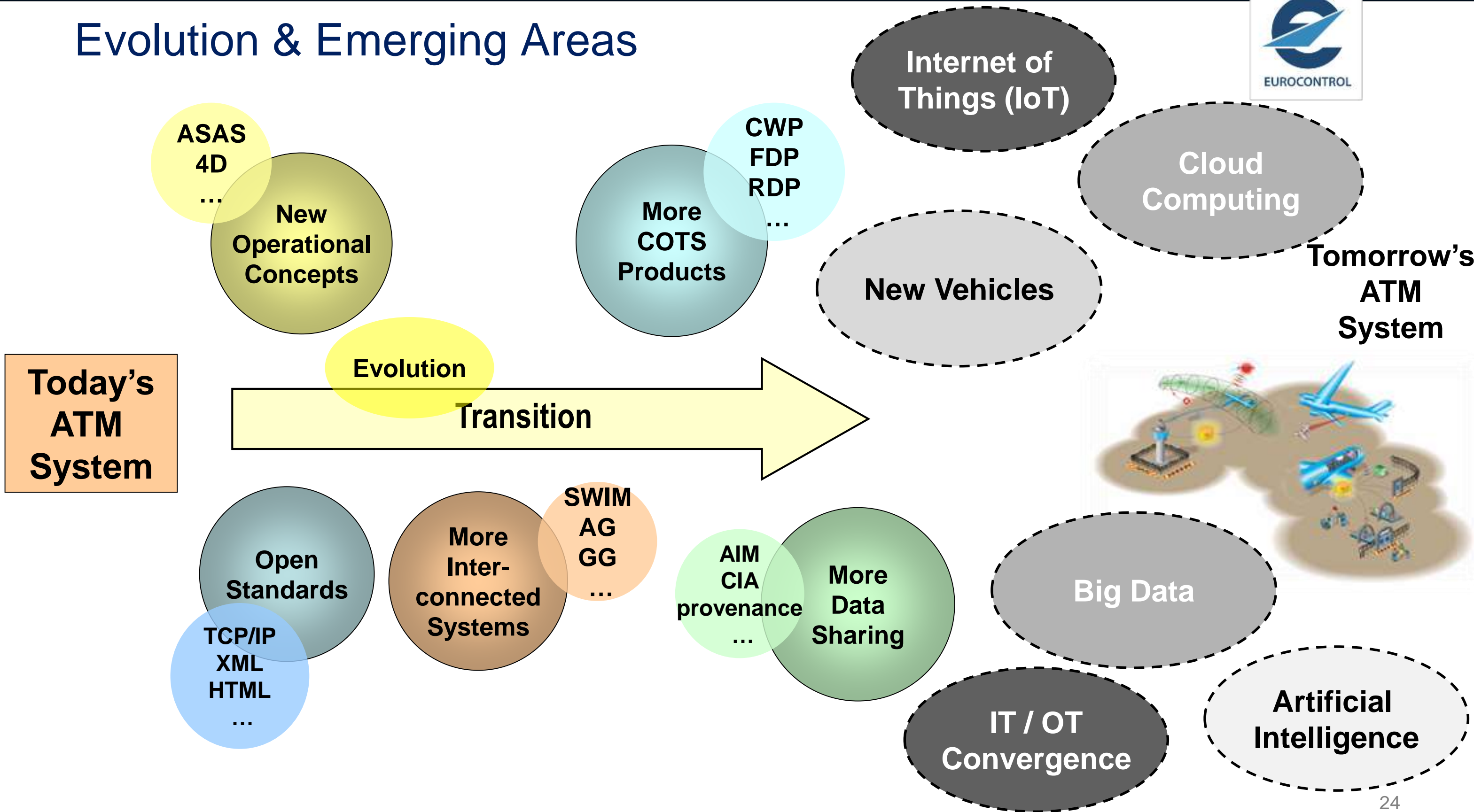
- comes as a surprise (Very low Likelihood),
- has a major effect (Very high Impact), and
- is often inappropriately rationalized after the fact with the benefit of hindsight

	Reviewed Impact				
Likelihood	1	2	3	4	5
5	Low	High	High	High	High
4	Low	Medium	High	High	High
3	Low	Low	Medium	High	High
2	Low	Low	Low	Medium	High
1	Low	Low	Low	Medium	Medium R

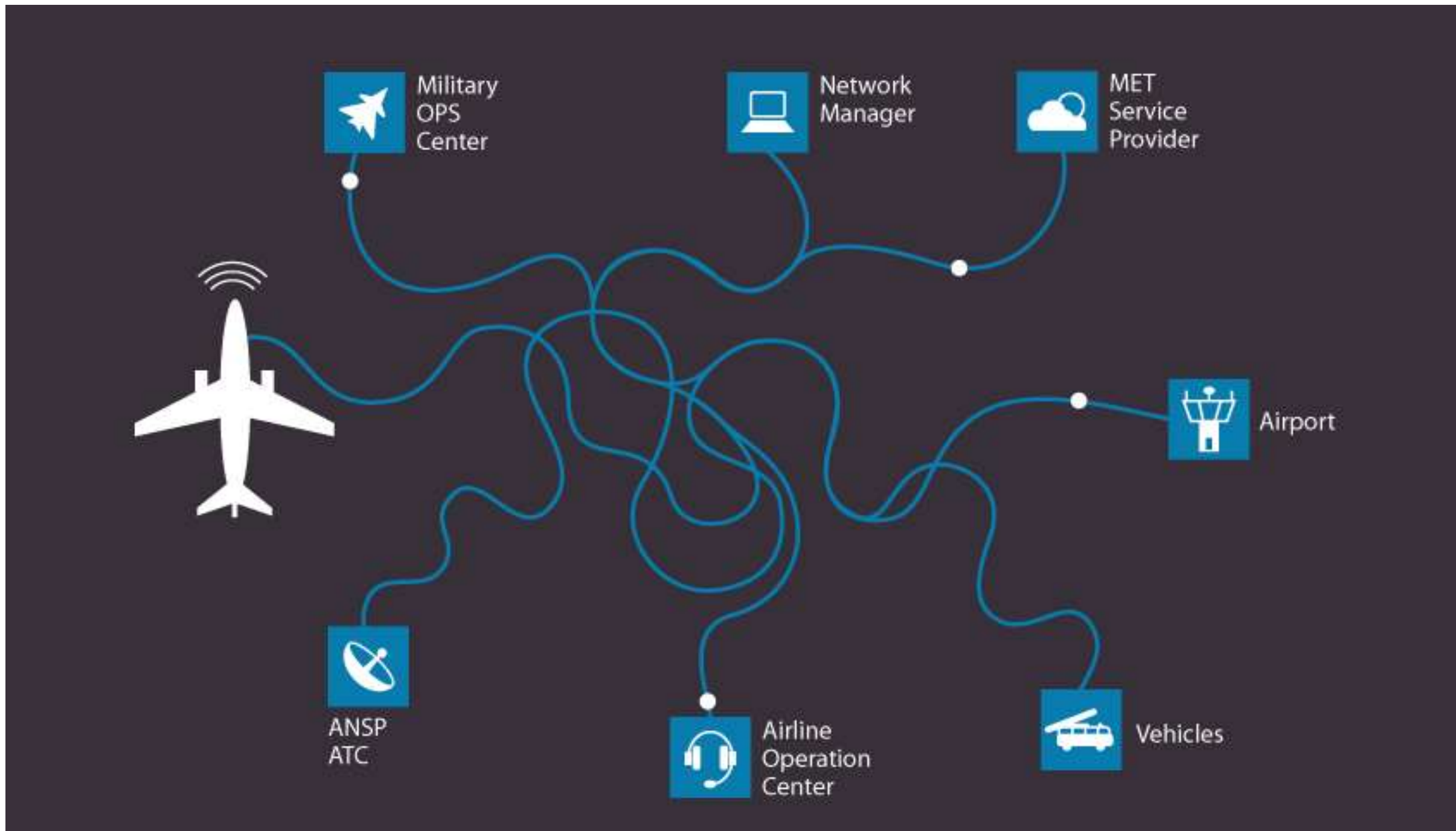


THE EVOLVING ATM SYSTEM

Evolution & Emerging Areas



Information Sharing Today – One-to-one Connections



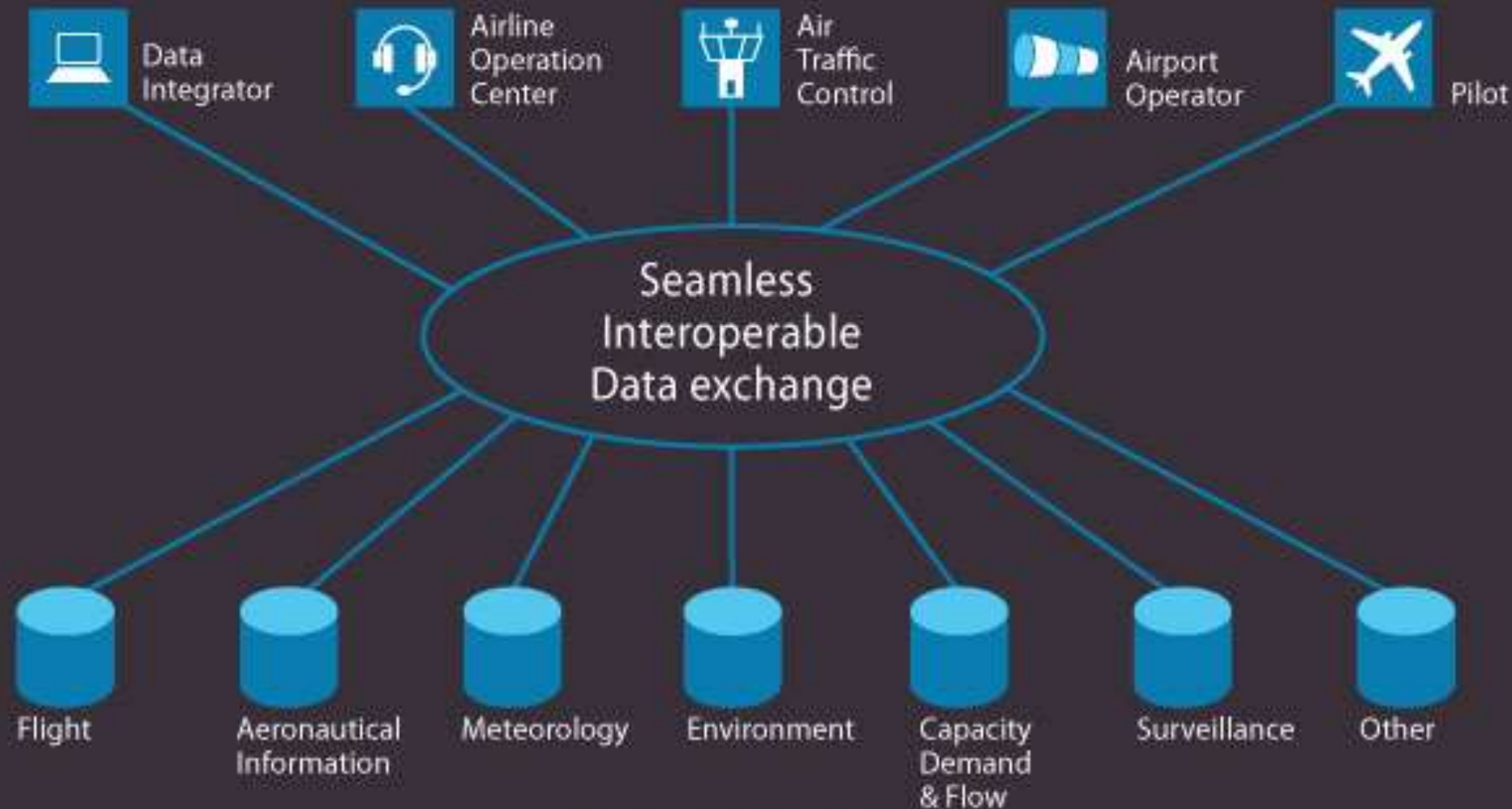
Information Sharing Tomorrow

Information Viewpoint

Data Usage

Open IM Standards

Networked Actor



Data Provision

New vehicles (drones)...

May be :

- Used as weapons (with or without a payload) on
 - ground-based or air-borne targets
- Used as platforms for RF spoofing, jamming, etc
- Deployed as swarms

May be vulnerable to :

- Spoofing (GNSS, communications)
- Jamming (GNSS, communications)
- Remote hi-jacking

Potential Impacts :

- Physical damage (aircraft, facilities), safety (injury, loss of life)
- Capacity, delays
- Financial



IT - OT Convergence

Information Technology (IT) - *the application of computers to the processing, transmission and storage of data, usually in business or enterprise environments.*

- Ecosystem of fast, inter-operable information processing technologies
- Continuous improvements in storage capacity and data processing speed
- Delivering new capabilities – e.g. cloud computing, data sciences

Operational Technology (OT) - *hardware and software systems that monitor and control physical equipment and processes. OT is found in critical infrastructures and control systems, such as ATM.*

- Long life-cycles - operational for 10, 20 years or more
- Designed for limited functionality, for reliability, integrity, stability
- Late adoption of new technology - systems may be generations behind enterprise systems
- Often designed to be isolated from the external world
- Connecting to external networks may create vulnerabilities

Traditionally, IT and OT have *not overlapped*, but *there are benefits to be gained* from doing so.

Potential Pros



Development / deployment



Time

Development / deployment



Delays



Capacity



Performance



Reputation

Potential Cons



**Threat Agents /
Attacker Population**



**Vulnerabilities /
Attack Surface**



Risks



**Threats /
Attack Vectors**



**Geographical
Area Impacted**

Risk Evolution in the Changing ATM Environment

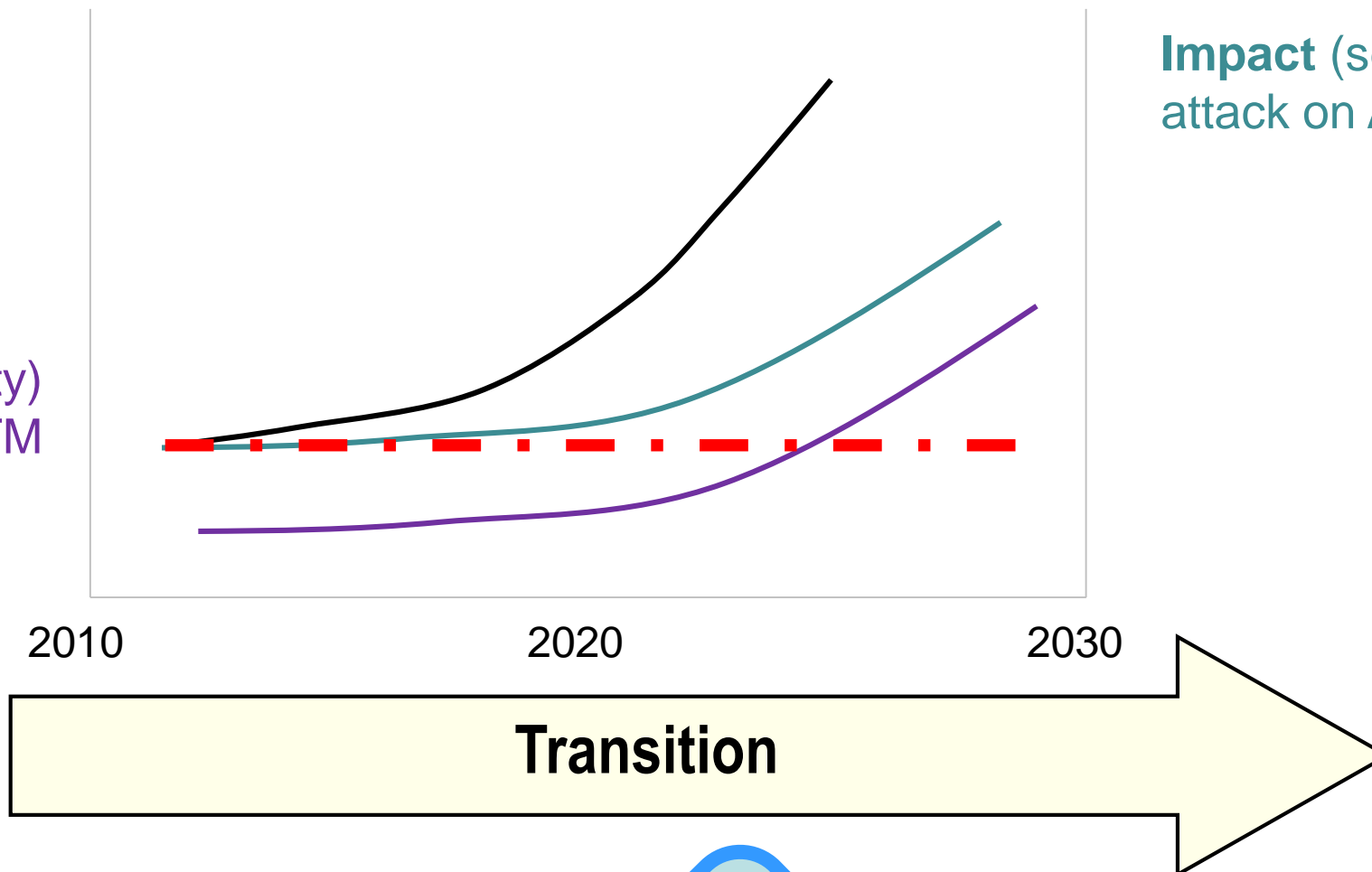
$$\text{Risk} = f(\text{Impact, Likelihood})$$

Drivers :
increased hacking;
criminality; State
sponsorship; ...

Likelihood (probability)
of attack on ATM

Impact (severity) of
attack on ATM

Drivers :
system
interdependency;
data sharing;
geographical area



LIKELIHOOD
How likely is
the event

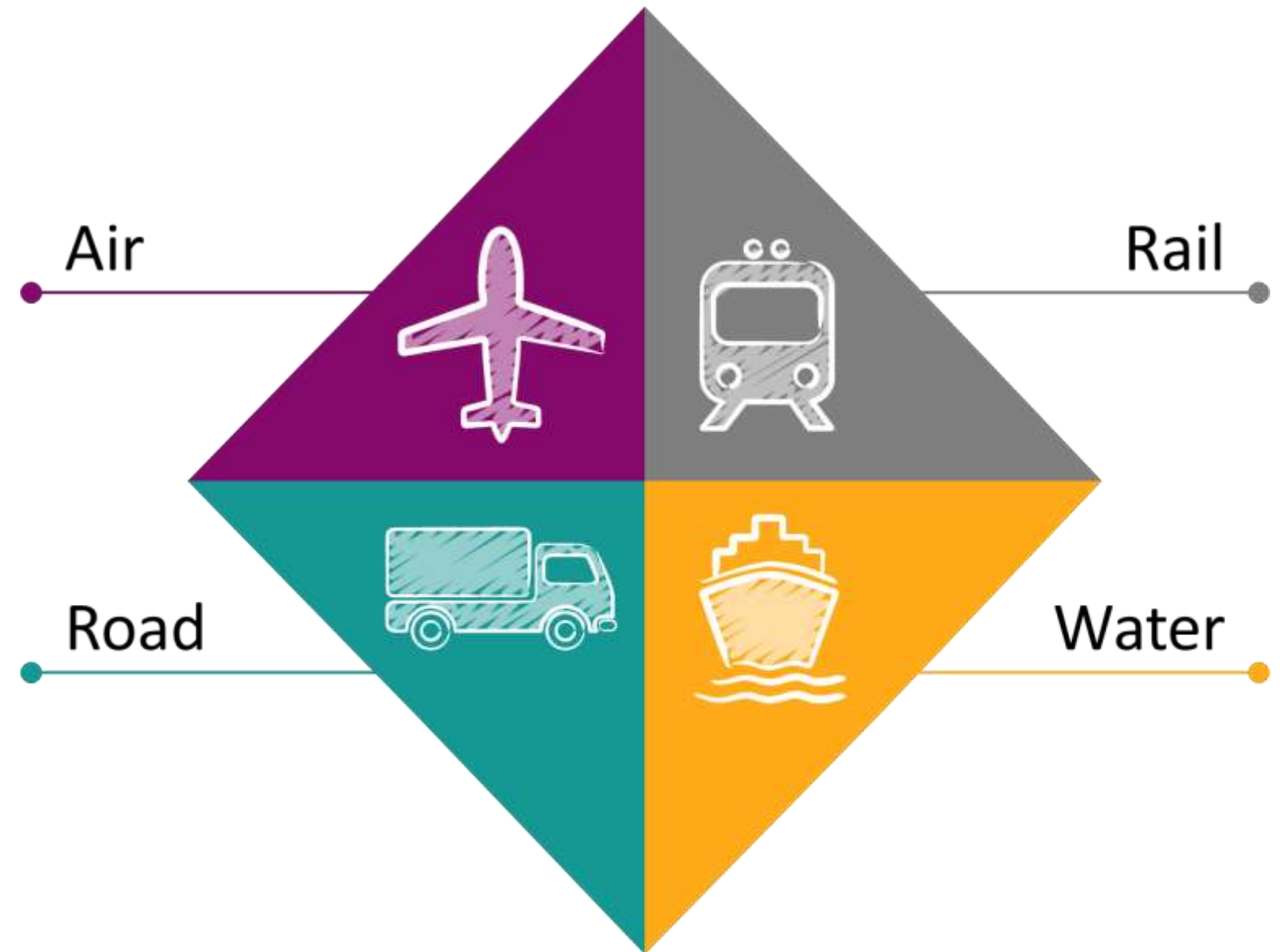
RISK
Combined
likelihood and
impact

IMPACT
How bad can
the event be?



Aviation is Not Alone!

- All transport modes impacted
 - Are following similar digitalisation paths
 - Use similar COTS products and services
 - Use some common technologies
 - Possess similar vulnerabilities
- Delivering Mobility as a Service (MaaS) requires
 - Closer cooperation of transport modes
 - More information sharing
 - More system interconnections
- Transport System Resilience
 - Cooperation
 - Trust



MENTI QUIZ : RISK EVOLUTION



- **Q2 : What is risk?**
- **Q3 : Which factor contributes to the evolution of the risk environment in ATM?**

SECURITY INCIDENTS IN ATM

ATM has never been attacked - ~~Imagine.....~~

- Theft of copper, batteries and other equipment ✓
- Injection of data, spoofing of systems ✓
- Unauthorised access to operational centers ✓
- Leaving 'suspect' packages to cause operational disruption ✓
- Electronic hacking into data systems ✓
- Deliberate use of substandard products in operational systems ✓
- IT systems containing unauthorised programmes (and viruses) ✓
- System overload (Denial of service attacks) ✓
- GPS jamming ✓

Luckily, so far :

- "Known" financial impact not substantial
- No businesses severely impacted
- No injuries or loss of life



Not a New Problem – FAA ATM Systems



2006 :

- Web-based viral attack infected ATC systems **I**
- Part of ATC system in Alaska had to be shut down **A**

2008 :

- Hackers briefly controlled FAA critical network servers **I**

2009 :

- Hackers breached public-facing website **I**
- Gained unauthorized access to personal information on 48,000 current and former employees **C**

Confidentiality
Integrity
Availability

Audit revealed : 3800+ vulnerabilities in 70 Web apps (760 high-risk)

"In our opinion, unless effective action is taken quickly, it is likely to be a matter of when, not if, ATC systems encounter attacks that do serious harm to ATC operations"

REVIEW OF WEB APPLICATIONS SECURITY AND INTRUSION DETECTION IN AIR TRAFFIC CONTROL SYSTEMS

Federal Aviation Administration

Report Number: FI-2009-049

Date Issued: May 4, 2009

Surveillance - Mode-S Flooding



MODE-S Flooding

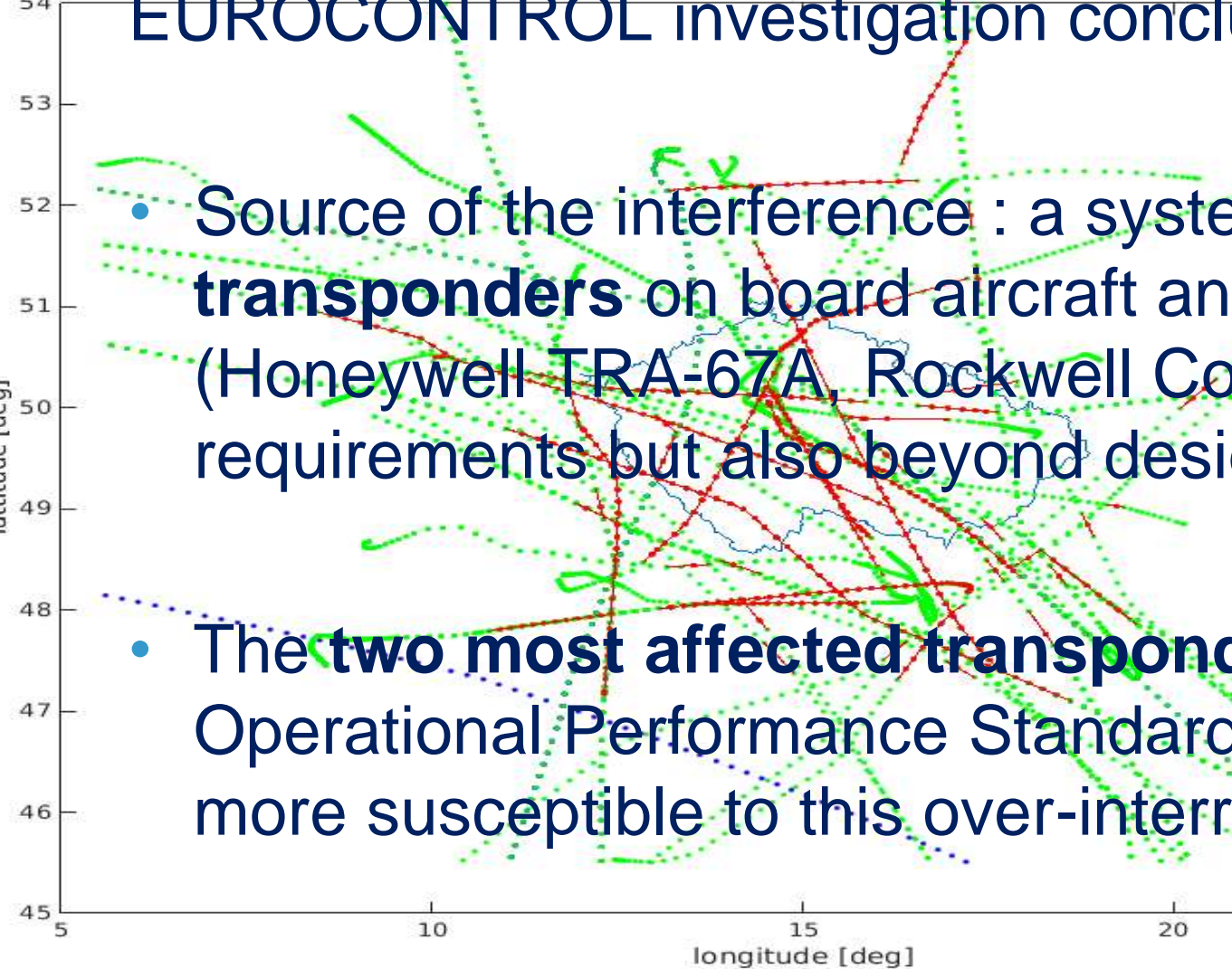
June 2014, Central Europe : Total and partial loss of surveillance tracks. Due to over-interrogating of transponders at 1030MHz.

<https://www.eurocontrol.int/sites/default/files/publication/files/netaalert-21.pdf>

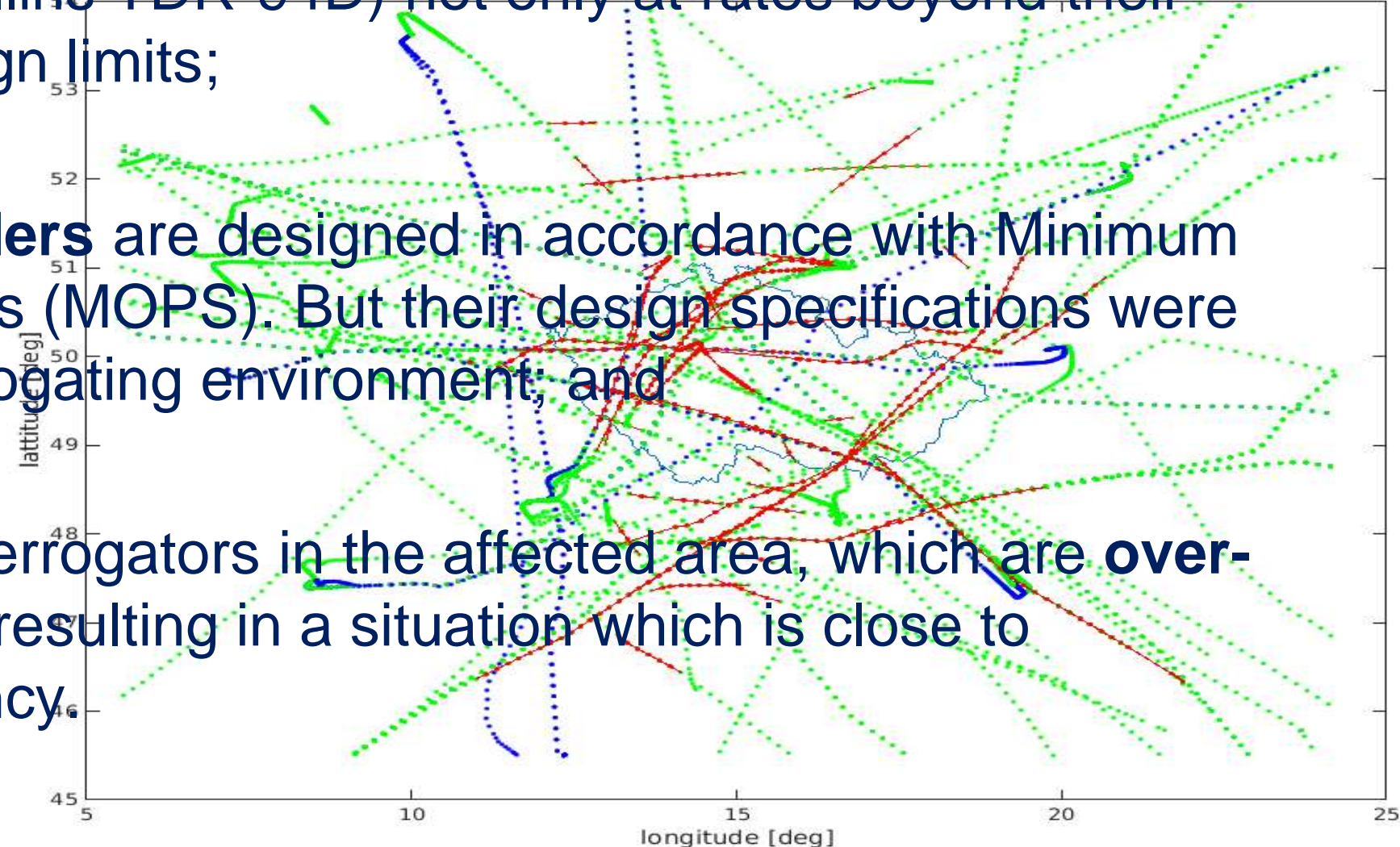
EUROCONTROL investigation conclusions :

- Source of the interference : a system or installation which **over-interrogated the transponders** on board aircraft and interrogated two specific transponders types (Honeywell TRA-67A, Rockwell Collins TDR-94D) not only at rates beyond their requirements but also beyond design limits;
- The **two most affected transponders** are designed in accordance with Minimum Operational Performance Standards (MOPS). But their design specifications were more susceptible to this over-interrogating environment; and
- A high number of ground based interrogators in the affected area, which are **over-soliciting airborne components**, resulting in a situation which is close to saturation of the 1030 MHz frequency.

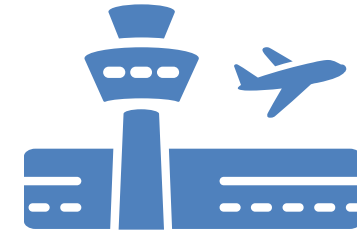
Radar Gap Plot (Gaps are in red) for 05.06.2014



Radar Gap Plot (Gaps are in red) for 10.06.2014



Airport Systems



May 2004 : Sasser Worm

British Airways (UK), Railcorp (Australia), and Delta Airlines (USA). Heathrow Terminal 4 check-in shutdown. British Airways call centres in Glasgow and Birmingham also went out of service. Departure delays.

2013 : Phishing Scam Targeted 75 US Airports

APTs present in at least 4 airports. Centre for Internet Security attributes attack to undisclosed nation-state seeking to breach aviation networks.

<https://www.informationweek.com/government/cybersecurity/phishing-scam-targeted-75-us-airports/d/d-id/1278762?>

July 2013 : Istanbul Passport Control Systems Attacked

Cyber-attack prevented passport checks in both Istanbul airports for several hours.

<http://www.hurriyetdailynews.com/virus-attack-strikes-at-both-istanbul-airports-51449>

July 2015 : Chopin Airport, Warsaw

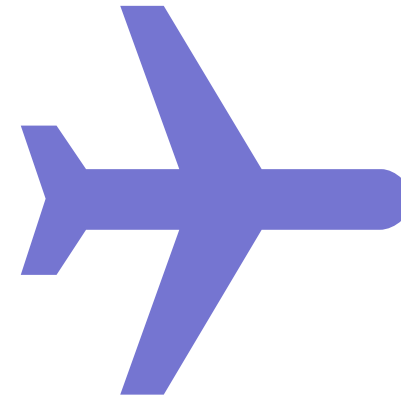
DDoS attack results in cancellations and delays affecting 1400 LOT passengers

<https://www.euractiv.com/section/justice-home-affairs/news/hackers-bombard-aviation-sector-with-more-than-1000-attacks-per-month/>

September 2018 : Bristol Airport

Passenger Information Display System taken offline due to cyber attack.

Aircraft Systems



The Kilted One...

@Sidragon1



Find myself on a 737/800, lets see Box-IFE-ICE-SATCOM, ?
Shall we start playing with EICAS messages? "PASS OXYGEN
ON" Anyone ? :)

9:08 PM - Apr 15, 2015

♡ 237 💬 253 people are talking about this



April 2015 : Aircraft systems (Chris Roberts)
Expressed intention to pirate the aircraft's Engine
Indicating and Crew Alerting System (EICAS).

November 2017 : Boeing 757 Testing Shows Airplanes Vulnerable to Hacking (DHS)

Aircraft remotely hacked in non-cooperative penetration (DHS Cybersecurity Division)

<http://www.aviationtoday.com/2017/11/08/boeing-757-testing-shows-airplanes-vulnerable-hacking-dhs-says/>

Navigation – GNSS

GNSS Jamming

2009-2010, Newark Airport : Sporadic outage of GBAS due to GPS jammer.
<http://laas.tc.faa.gov/documents/Misc/GBAS%20RFI%202011%20Public%20Version%20Final.pdf>



June 2013 : White Rose yacht -

- Hand-held GPS spoofing device, \$2000
- Course shifted 3 degrees to the north
- Yacht “underwater”

GNSS Mass Spoofing

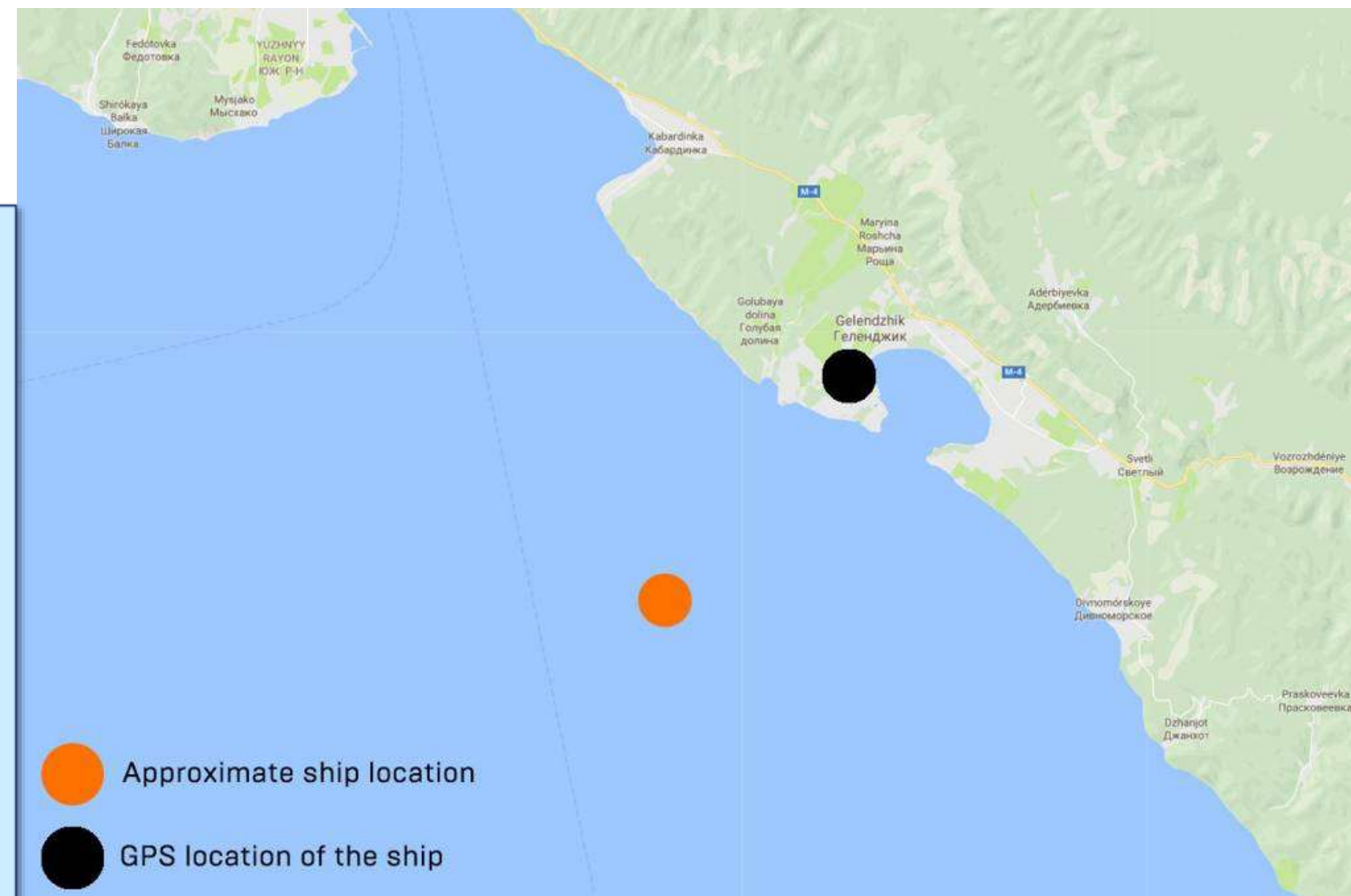
June 2017, Black Sea :

GPS sensors showed > 20 ships located near an airport several kms away from their actual position.

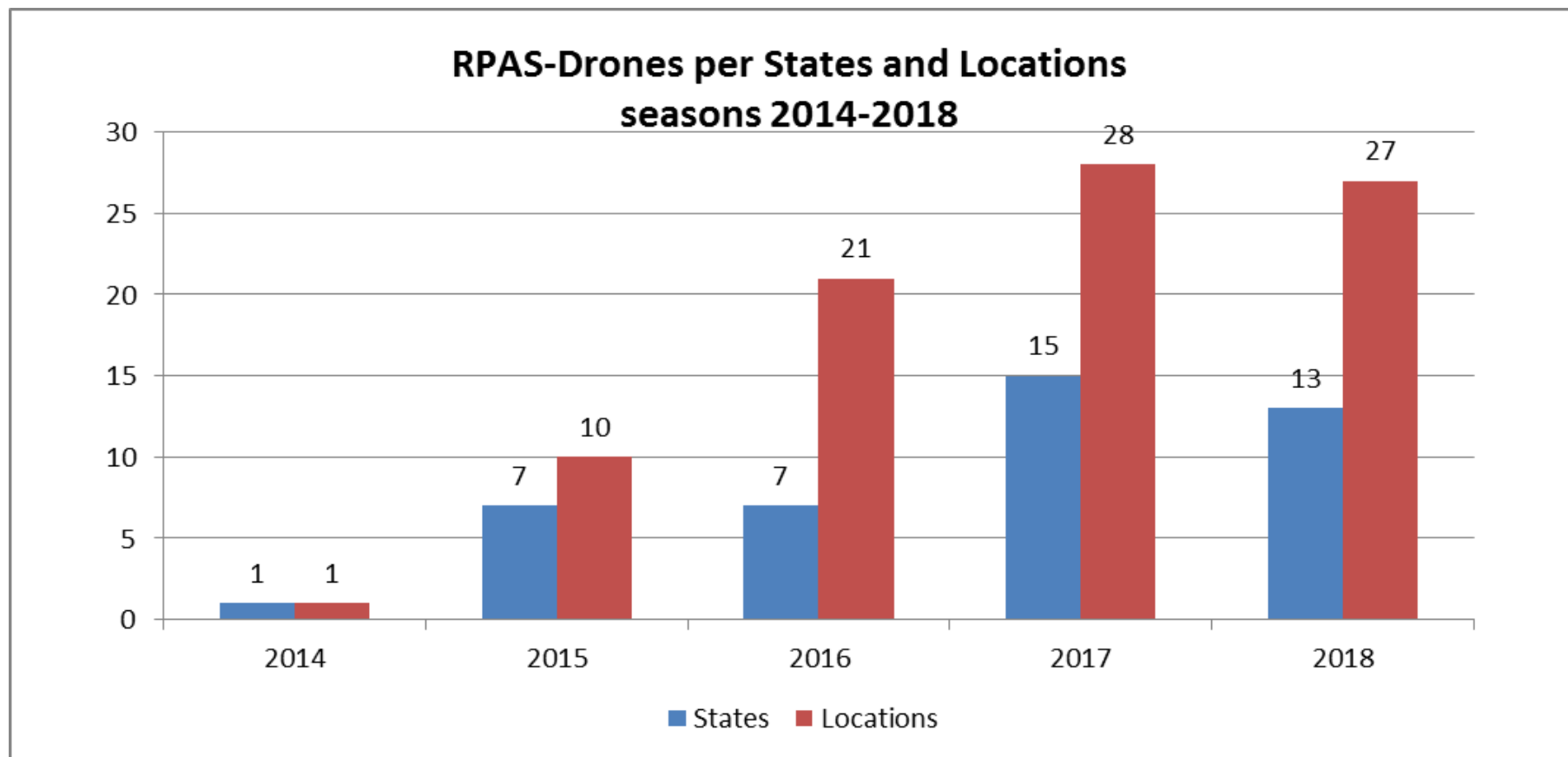
Spoofing from the coast?

Navigation warfare?

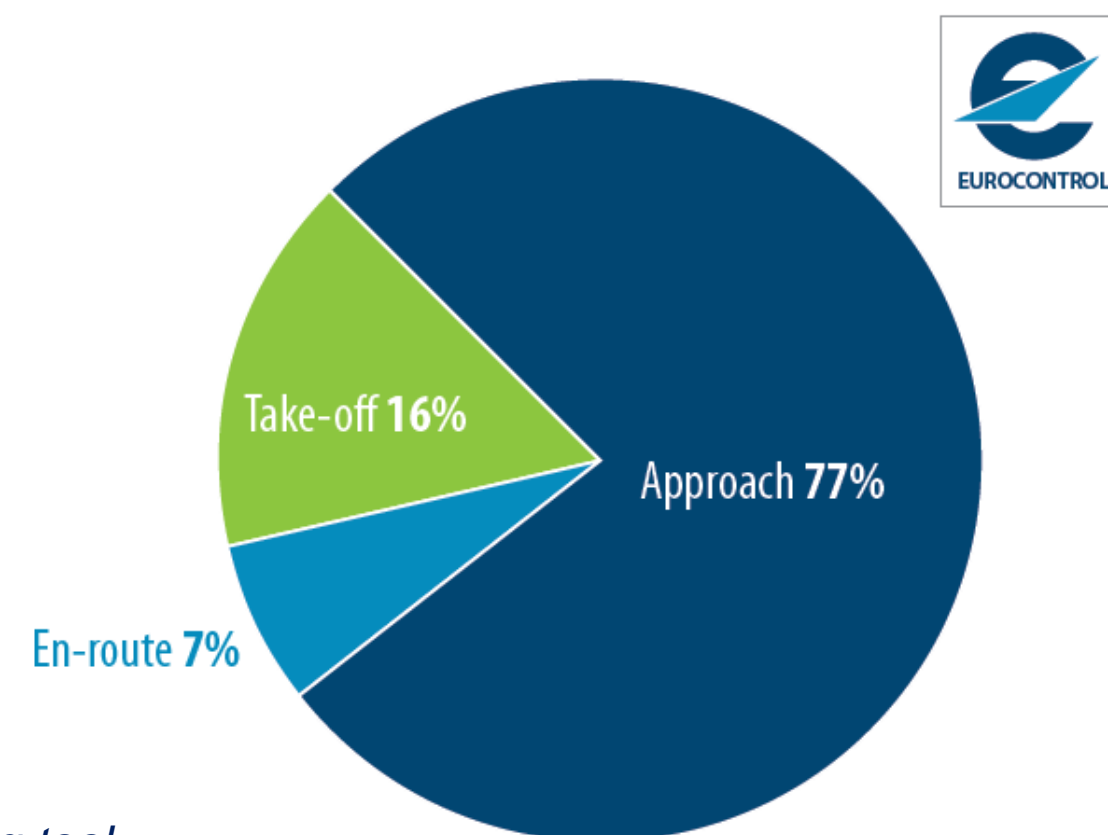
<http://gpsworld.com/spoofing-in-the-black-sea-what-really-happened/>



RPAS - Drones



For 16% of RPAS reports EVAIR got the altitude information. 87% of them occurred between 300ft – FL140 and 13% between FL145 and FL350

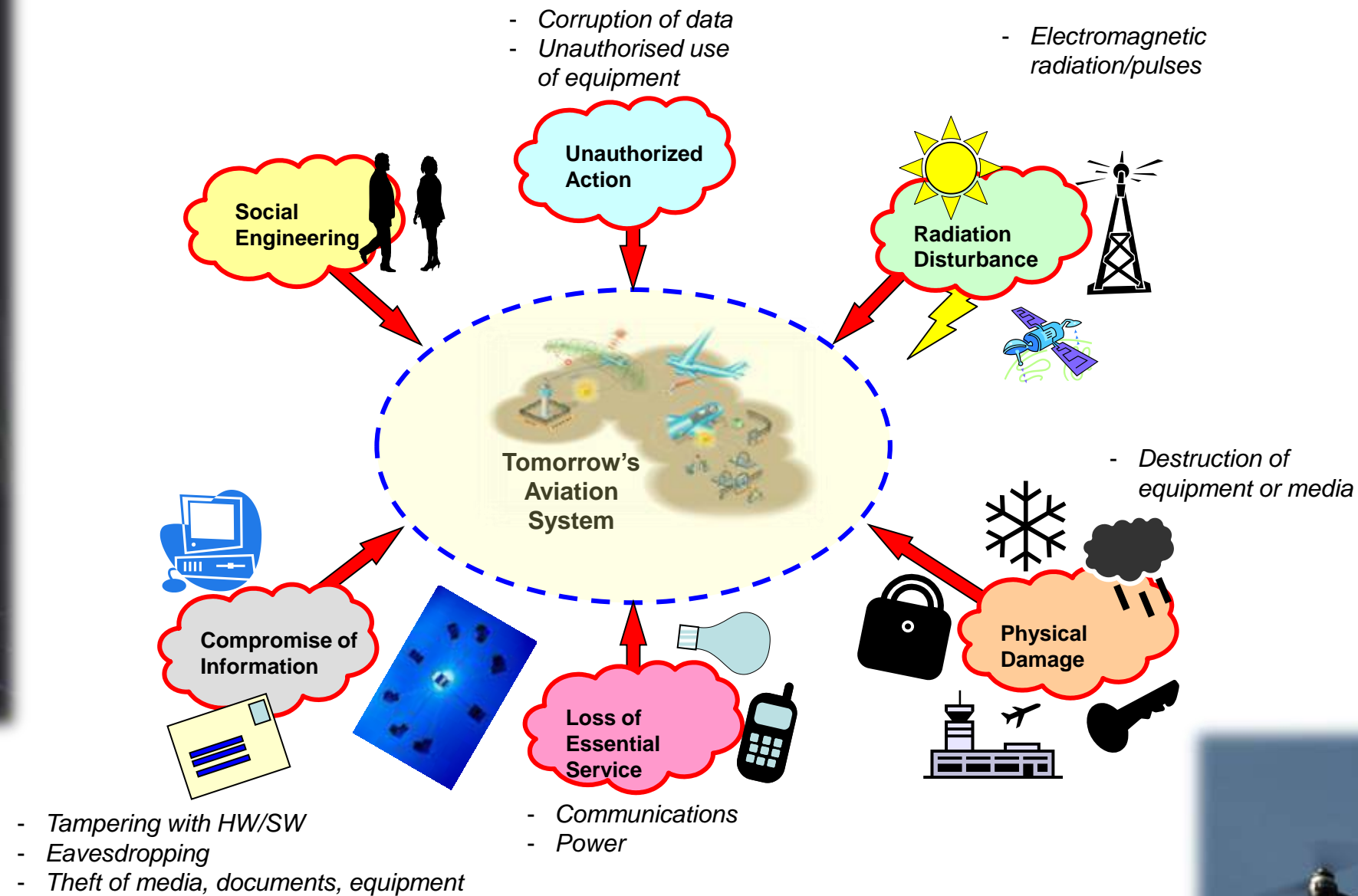


MENTI QUIZ : RISK EVOLUTION

- **Q4 : When did part of the Alaskan ATC system have to be shut down?**
- **Q5 : What percentage of drone reports in EVAIR relate to en-route traffic?**

THREATS

Potential Threats



Denial of Service (DoS)

Distributed Denial of Service (DDoS)

- Multiple compromised computer systems attack a target, such as a server, website or other network resource
- The flood of incoming messages, connection requests or malformed packets force it to slow down, crash, shut down
- Services to legitimate users or systems are denied

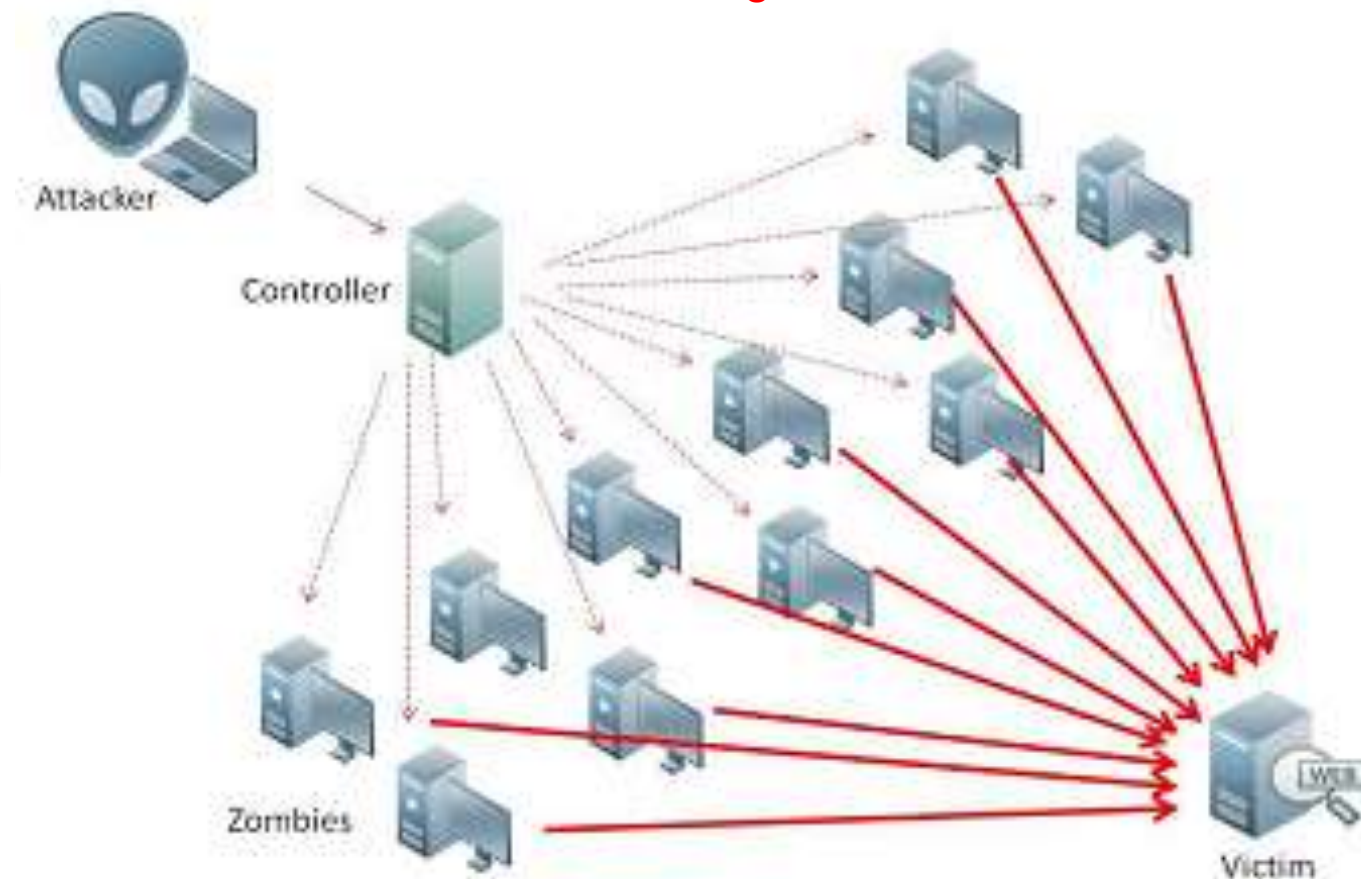
Telephone Denial of Service (TDoS)

- Possible due to rise of Voice over Internet Protocol (VoIP) systems

Internet of Things

- Vast Zombie population

<https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/>



Malware - Malicious Software

- Exists in a vast number of variant forms (e.g. Spyware, Virus, Worm, Trojan, Ransomware)
- May exploit vulnerabilities in operating systems or application software to acquire a presence on a system prior to executing its underlying code
- Is designed to access or damage devices, including
 - passenger and staff devices,
 - IT or OT computer systems,
 - IoT devices
 - Industrial Control Systems (ICS)
- Malware can result in a negative impact on infrastructure, and is often capable of propagating either autonomously, or by, for example, via 'phishing' emails sent to potential victims on other systems.



Malware – Wannacry

Ransomware cryptoworm

- Targeted MS Windows systems
- Encrypts data
- Demands bitcoin ransom for decryption key
- Attack began 12.05.2017 in Asia
- Attack stopped within a few days, due to:
 - Discovery of kill-switch domain
 - Release of emergency patches

Impact

- 200 countries
- Ransom paid in 150 countries
- Taiwan most affected



USA National Security Agency Connection

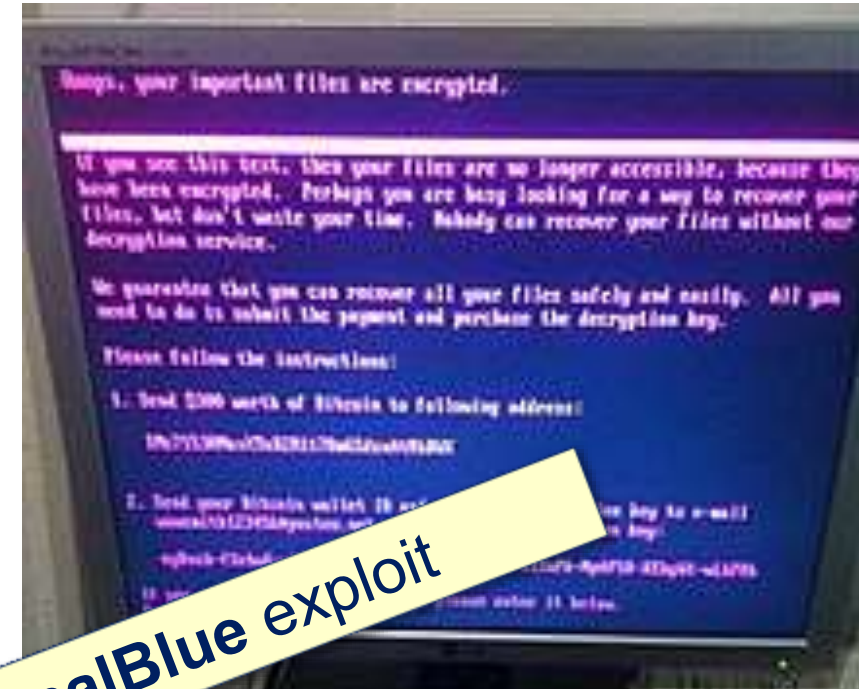
developed by the NSA for its own offensive work
(mysterious hacking group)



Malware - Petya / NotPetya

Ransomware

- Targets MS Windows systems
- Encrypts data
- Demands bitcoin ransom for decryption key
- 1st discovered in March 2016



New variant used for global cyberattack is

- Referred to as **NotPetya** since (unlike original 2016 version), it is unable to decrypt files
- Attack started 27.06.2017
 - Primary target - Ukraine
 - Believed to be a *politically motivated attack* (started on eve of Ukraine Constitution Day)
 - Targeted energy companies, power grid, bus stations, metro systems, fuel stations, airport, banks



Industrial Control Systems (ICS); Supervisory Control and Data Acquisition (SCADA) Systems

Nuclear Facility - STUXNET

2010, Iran : **Stuxnet malware** shut down uranium enrichment at Natanz for a week from Nov. 16 to 22, causing substantial damage. Targeted Siemens Programmable Logic Controllers (PLCs). Worm believed to be USA/Israel cyberweapon.

<https://en.wikipedia.org/wiki/Stuxnet>

Metals Industry

2014, Germany : **Social engineering** attack to gain access to the company control system network. Furnace could not be shut down, substantial damage.

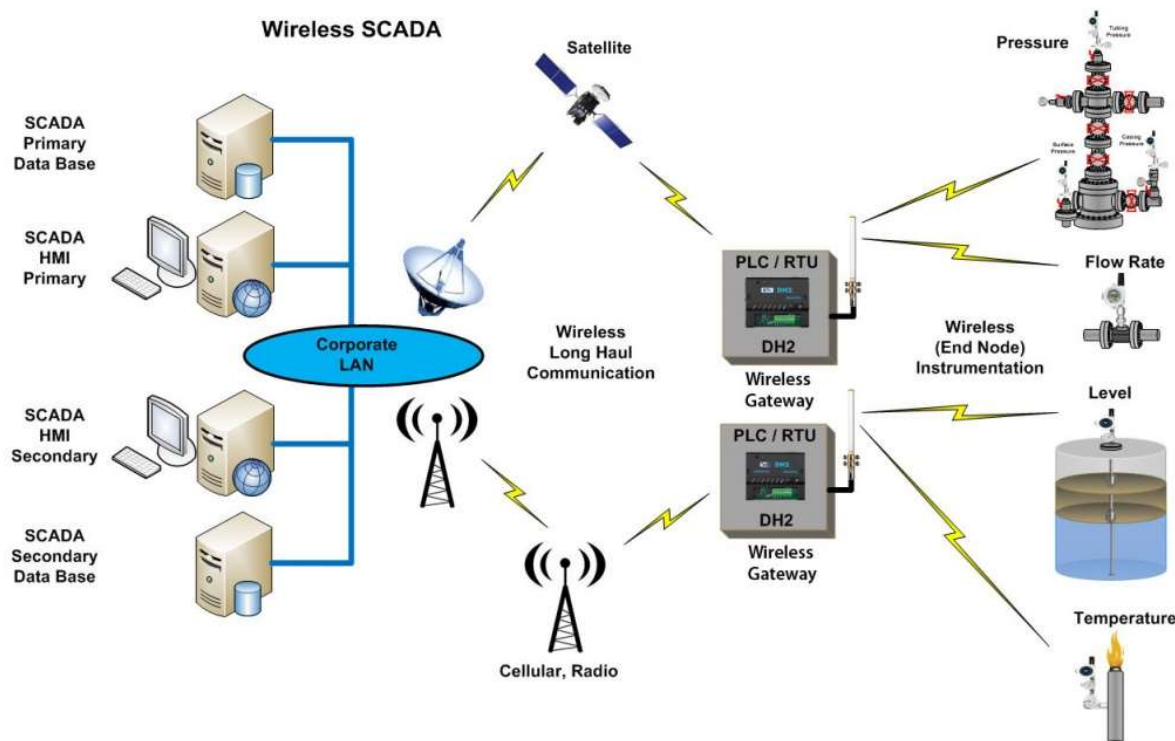
Power Utilities

23.12.2015, Ukraine : 57 electricity sub-stations taken off-line due to **cyber-attack on Industrial Control Systems**. First power-outage proven to have been caused by a cyber-attack.

<https://blog.fortinet.com/2016/04/05/scada-security-report-2016>

<https://www.enisa.europa.eu/publications/can-we-learn-from-scada-security-incidents>

http://www.risidata.com/Database/event_date/desc

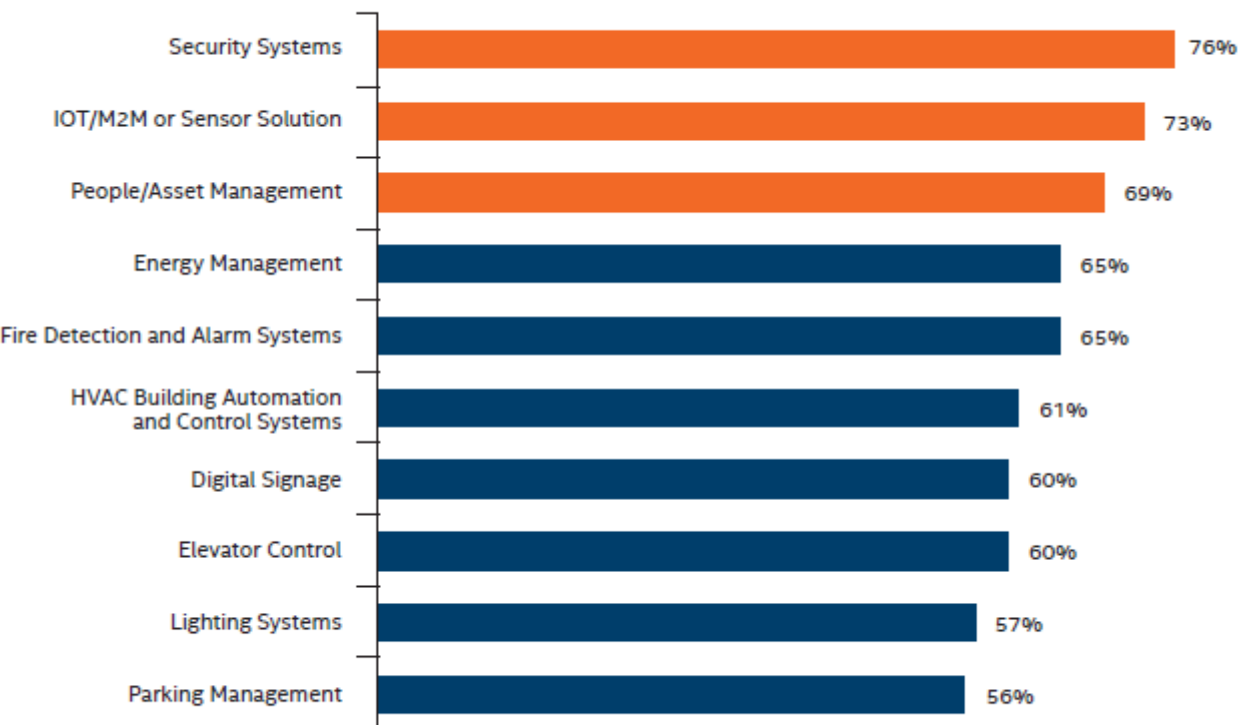


Building Management Systems

- Standard in new builds and major renovations
- *ANSP, Airport, ATFM, ...?*

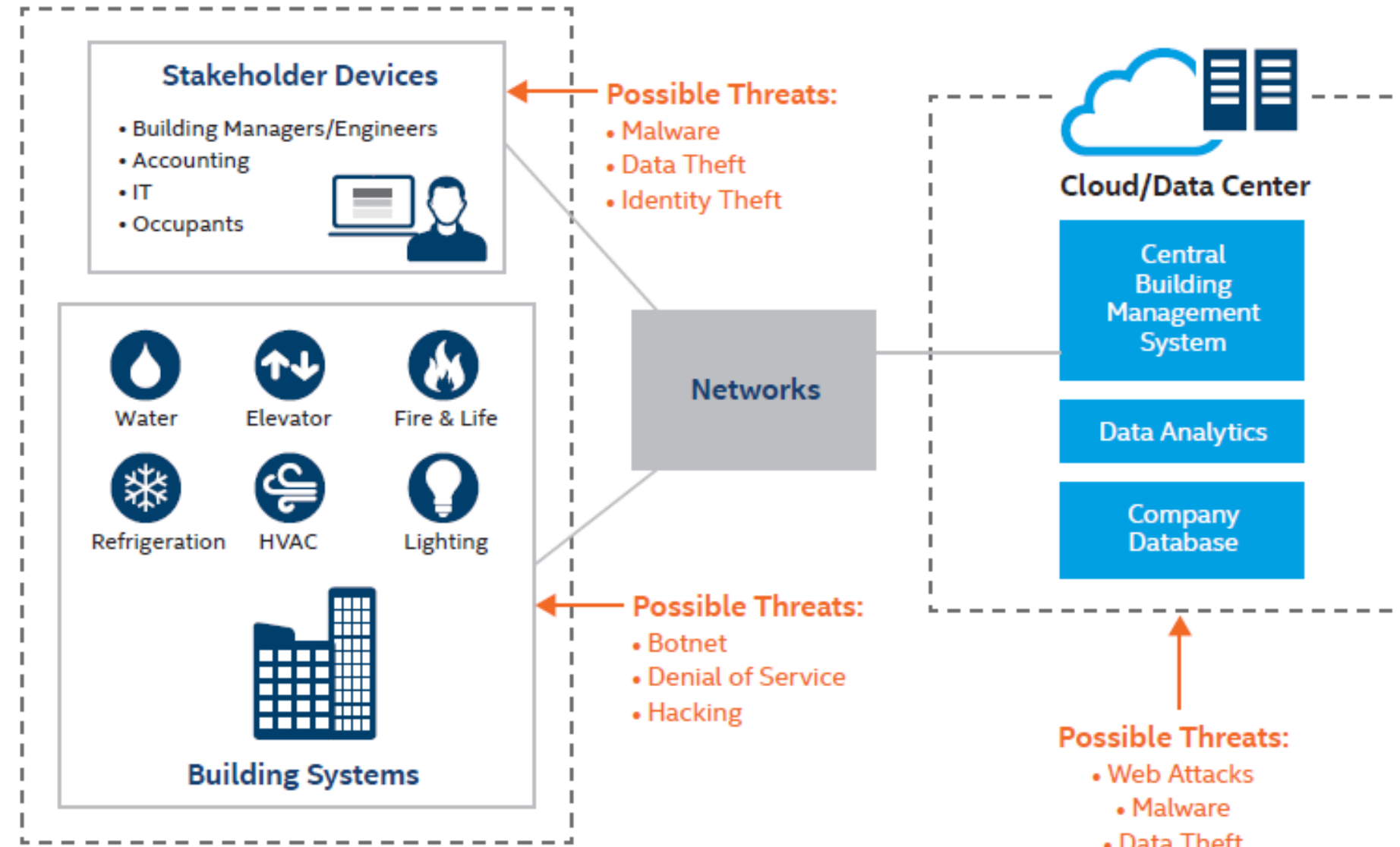
High Cybersecurity Risk

Sample Size = 502, percentage of those scoring 4 (somewhat high) and 5 (extremely high)



On a scale of 1 to 5 (with 1 being low and 5 being extremely high), which of the following products/solutions do you believe are high cybersecurity risks?

Perceived Risk [1]



Possible Security Threats for Smart Building Solutions (Intel [1])

[1] <https://www.intel.com/content/www/us/en/smart-buildings/security-practices-smart-buildings-brief.html>

Social Engineering

Phishing

Email sent under false pretences to trick users into supplying attackers with login information



Spear Phishing

Targeted phishing email (source of 91% of advanced attacks)

Vishing

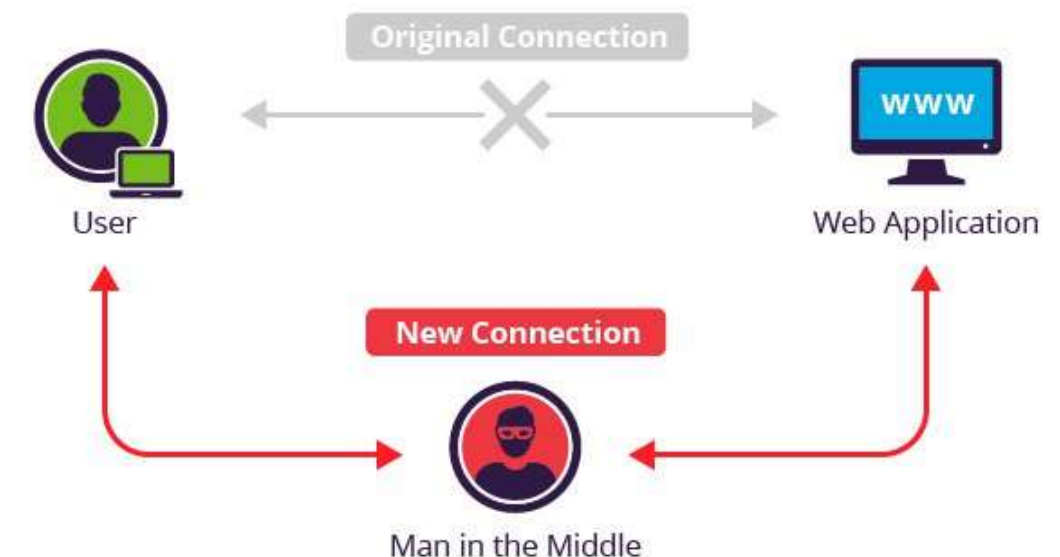
Voice communication with a target, pretending to be a person of authority (e.g. IT helpdesk) to obtain sensitive information. Cost to UK banks : GBP 21 million in 2014.

Man in the Middle Attack

Attacker hi-jacks an SSL connection between a browser and legitimate web server by exploiting a server-side vulnerability

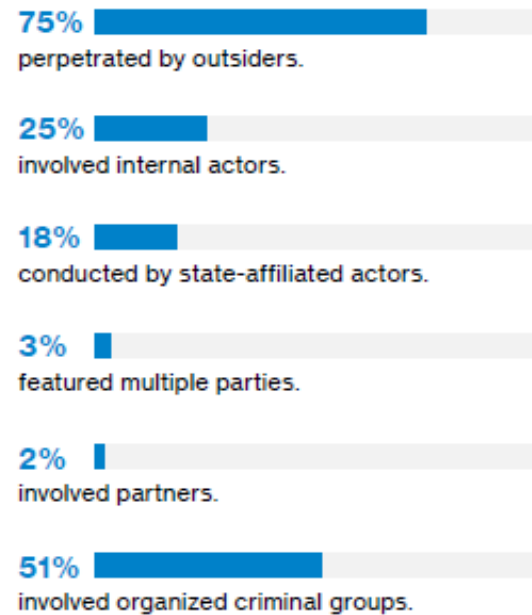
Mining Social Media

Learning more about targets using social media to build more effective phishing lures

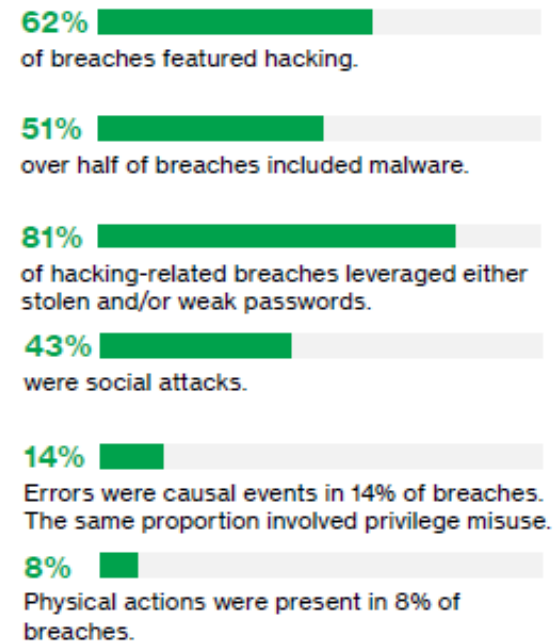


Learning from Other Sectors

Who's behind the breaches?



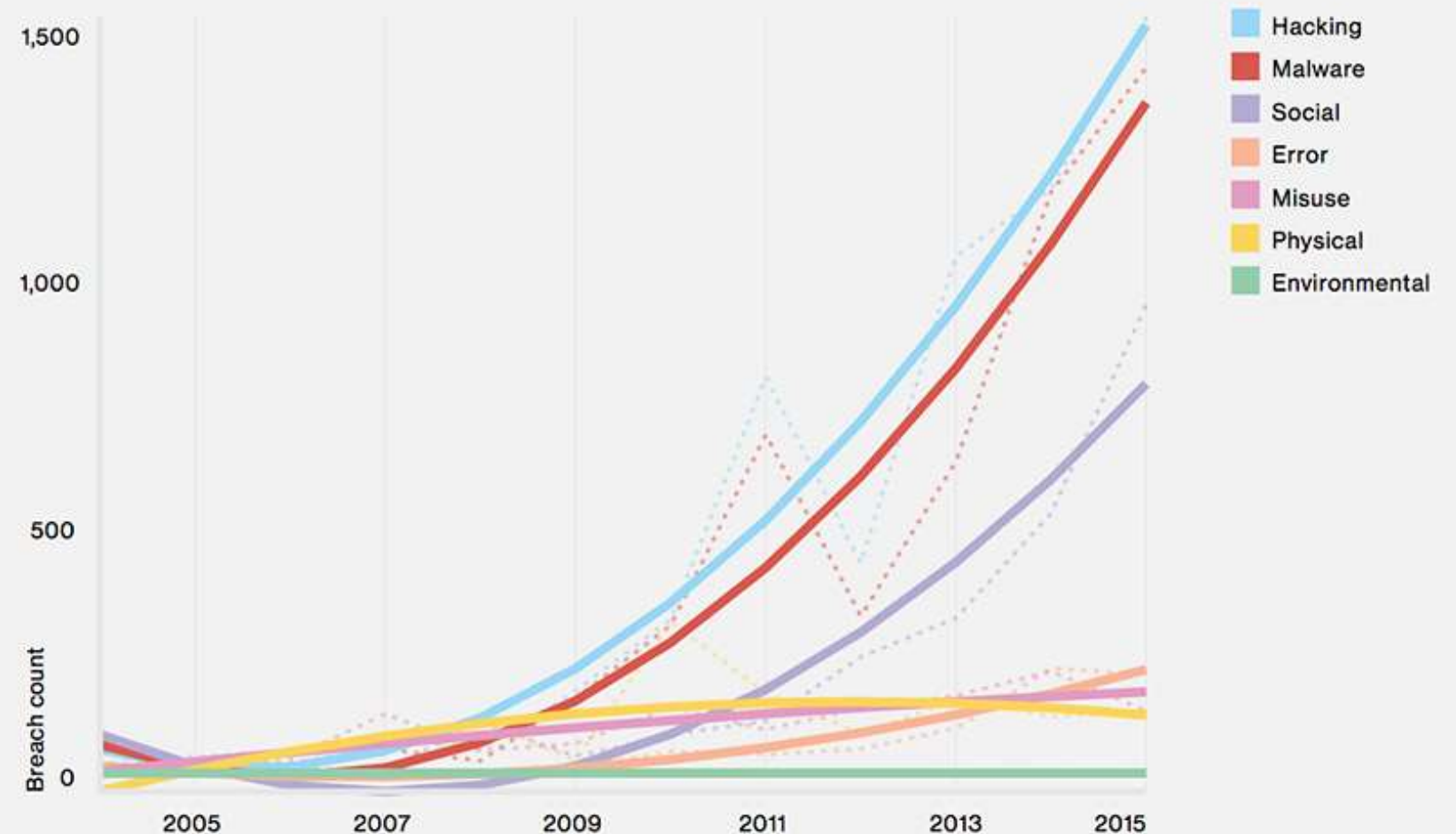
What tactics do they use?



Who are the victims?

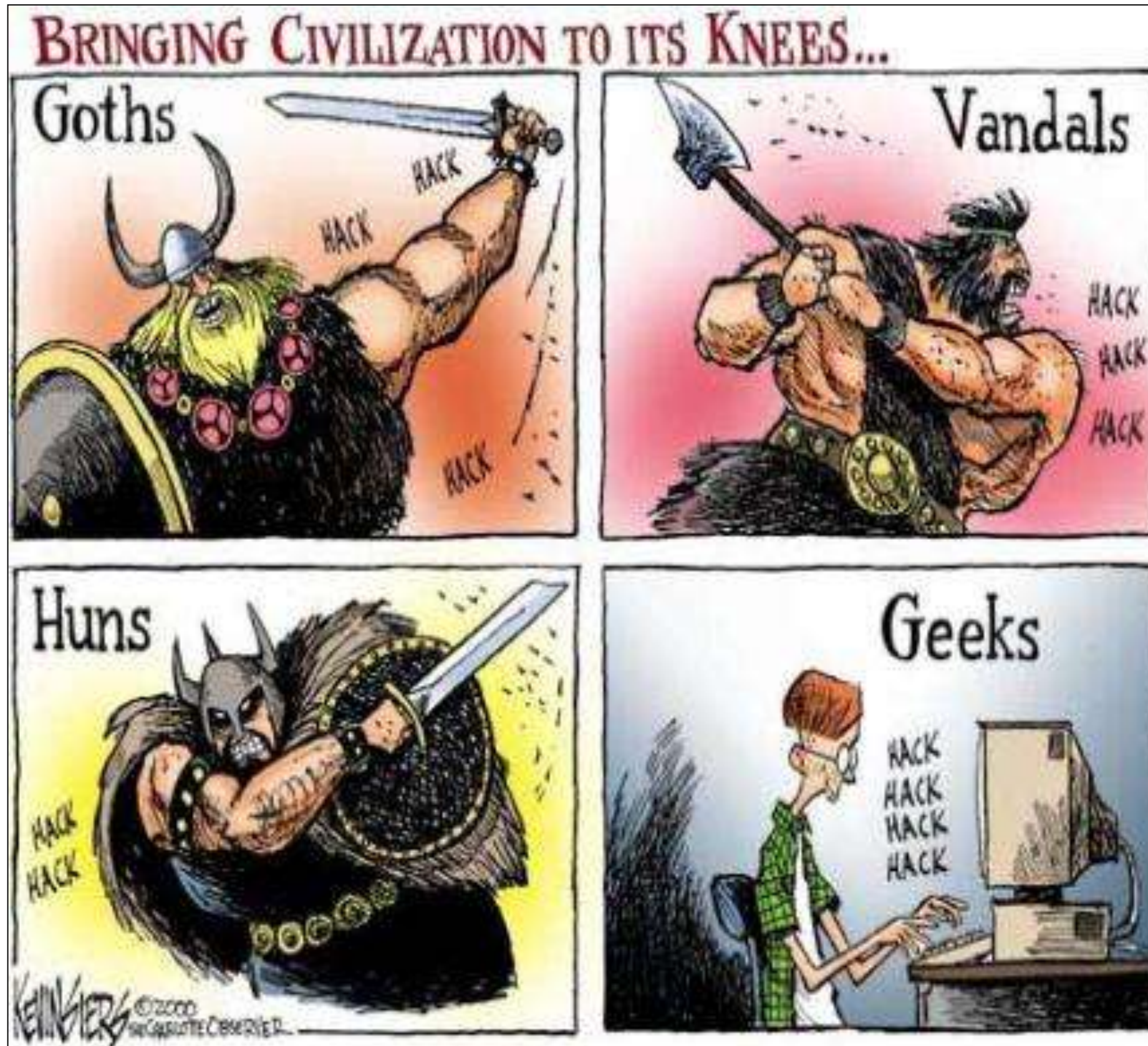


What else is common?



Data from : Verizon 2017 Data Breach Investigations Report

POTENTIAL ATTACKERS



Bad guys ...

past and
present

Attacker (*Threat Agent*) Examples

Insiders - those with legitimate access to security critical assets include :

- Administrators
- Users with legitimate roles
- Employees of companies that interface with the system



Credible external attackers include :

- Other States
- Terrorist or criminal attackers
- Hackers
- Competitors
- Natural disasters; weather events
- Journalists
- Equipment failures

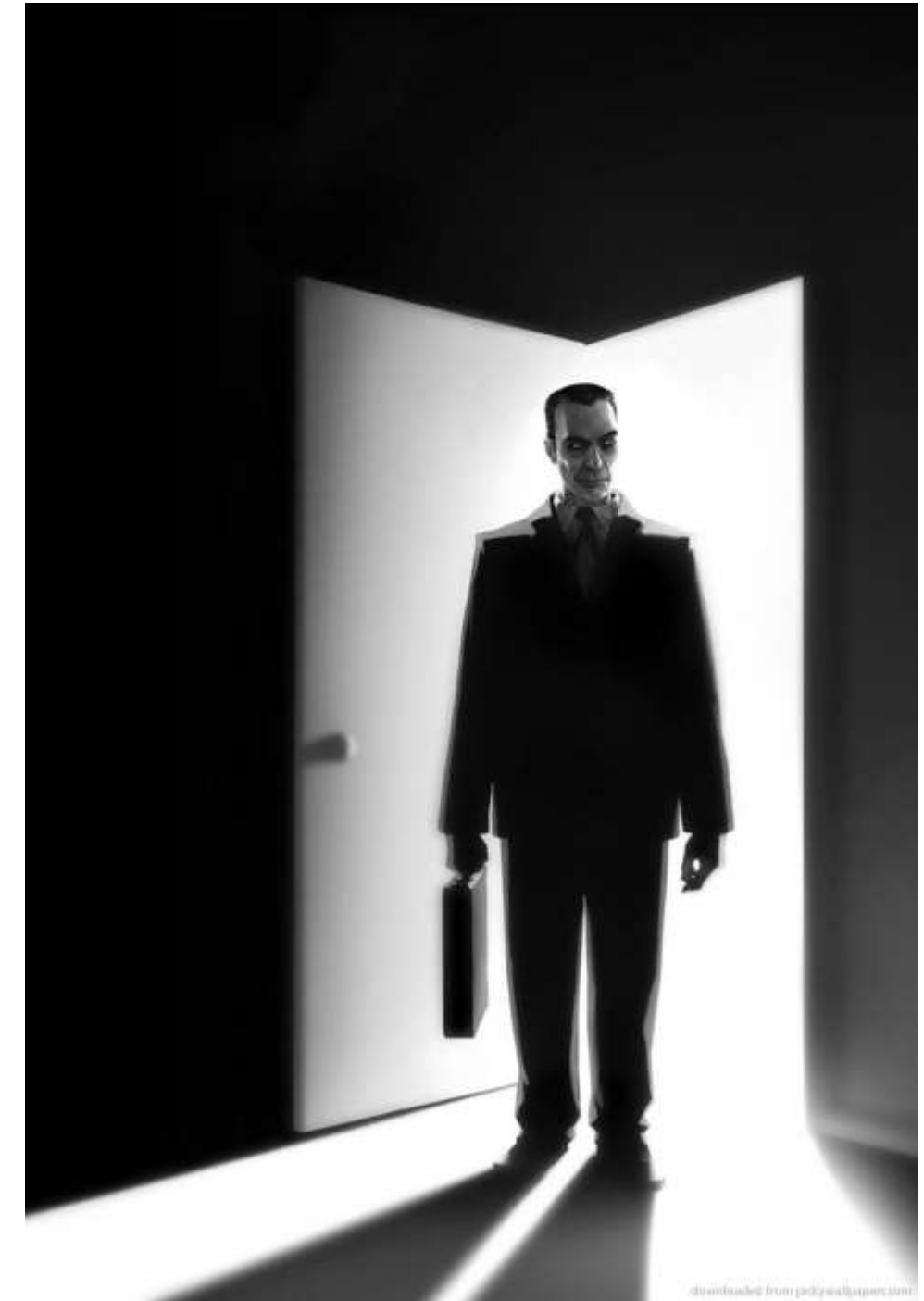
An attacker may use a third party to initiate an attack.

- Employee unintentionally injecting a virus via a USB key
- Suicide bomber
- Compromised employee stealing confidential information
- A sleeper stealing confidential information

VULNERABILITIES

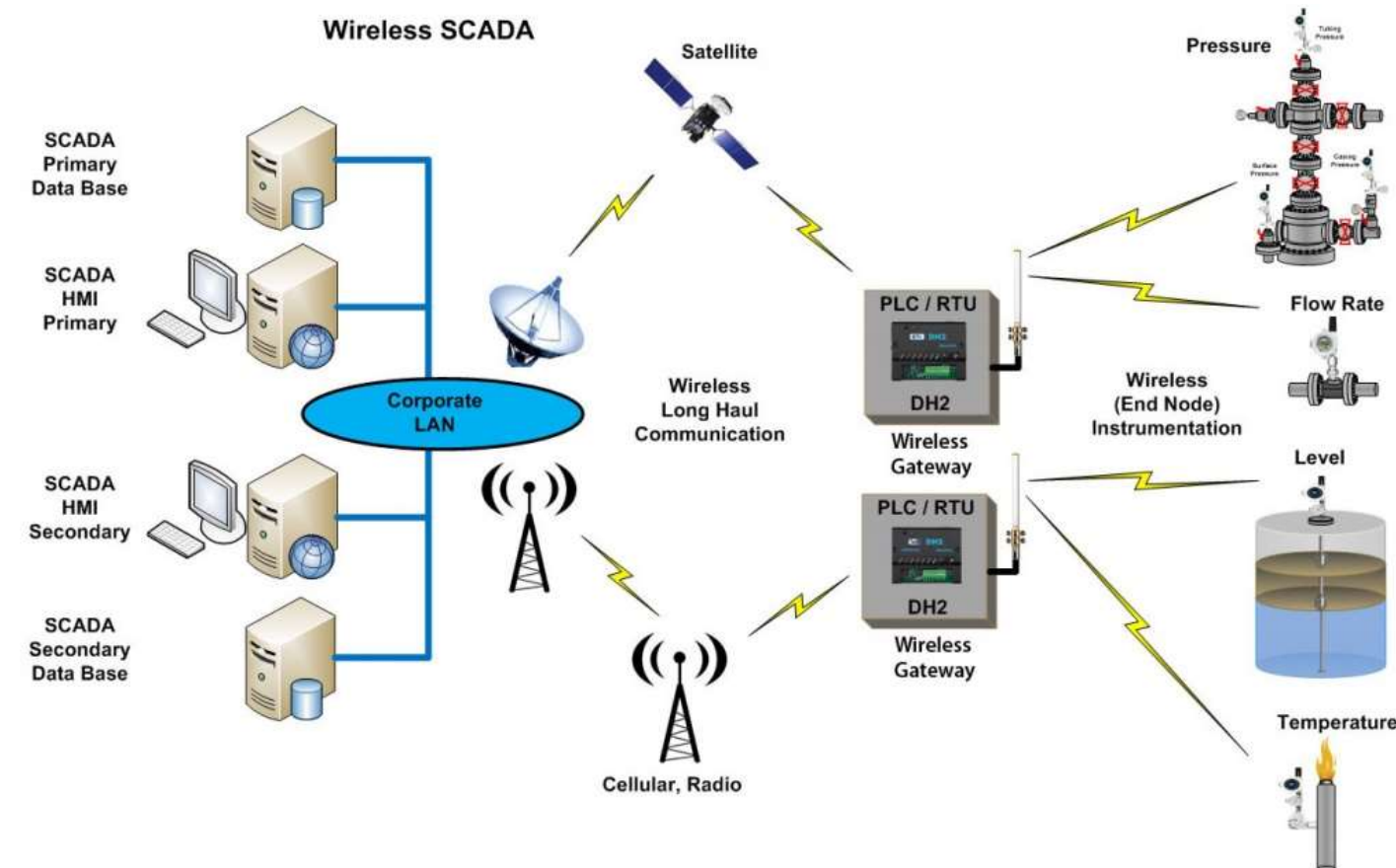
Vulnerabilities

- ***Intrinsic properties*** of something resulting in susceptibility to a risk source that can lead to an event with a consequence (ISO Guide 73:2009).
- A ***weakness*** in a system, physical controls, security procedures, internal controls or implementation that could be exploited or triggered by a threat agent.
- An ***Attacker*** will attempt to ***exploit a vulnerability*** in an ***Asset*** to achieve their goal.

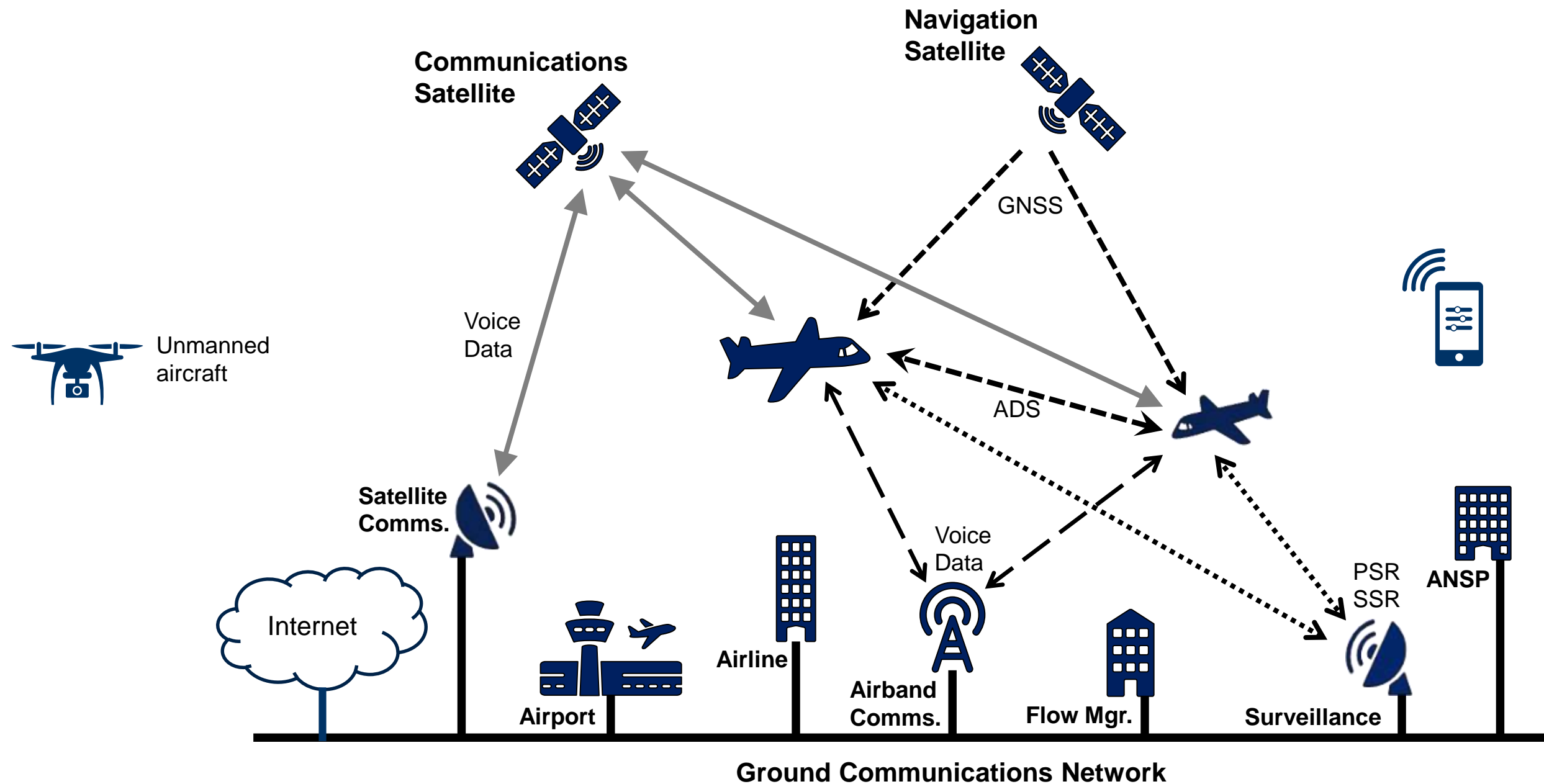


IT / OT Vulnerabilities

- OT systems
 - May have originally been designed to be isolated from other systems
 - System software may not be regularly updated with security patches - or may no longer be supported
 - Business reasons may drive connection to enterprise systems
 - Remote monitoring and maintenance
 - Performance assessment
 - Process analysis and optimisation
 - Wired or wireless connection may create vulnerabilities
- Ensure IT/OT issues are included in all security risk assessment activities



Some Aviation System Components



Inherent Wireless Vulnerabilities

CNS Protocols (e.g. CPDLC, GNSS, ADS-B, SSR, ACARS, ...)

- In some cases :
 - Security is often *not designed-in*
 - May be susceptible to *eavesdropping* (potential pre-cursor to other exploits)
 - May be susceptible to *message injection / deletion / modification*
 - *Authentication* may be weak or absent
 - *Integrity checks* may be weak or absent
 - They may be susceptible to *jamming* and *flooding*

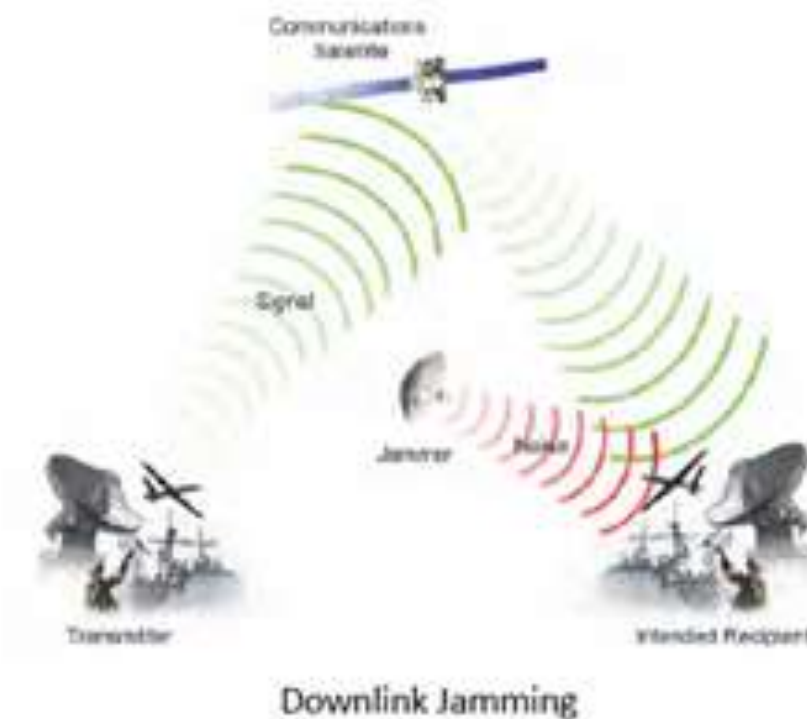
CPDLC – Controller-Pilot Data-Link Communications

GNSS – Global Navigation Satellite System

ADS-B – Automated Dependent Surveillance-Broadcast

SSR – Secondary Surveillance Radar

ACARS - Aircraft Communications Addressing and Reporting System

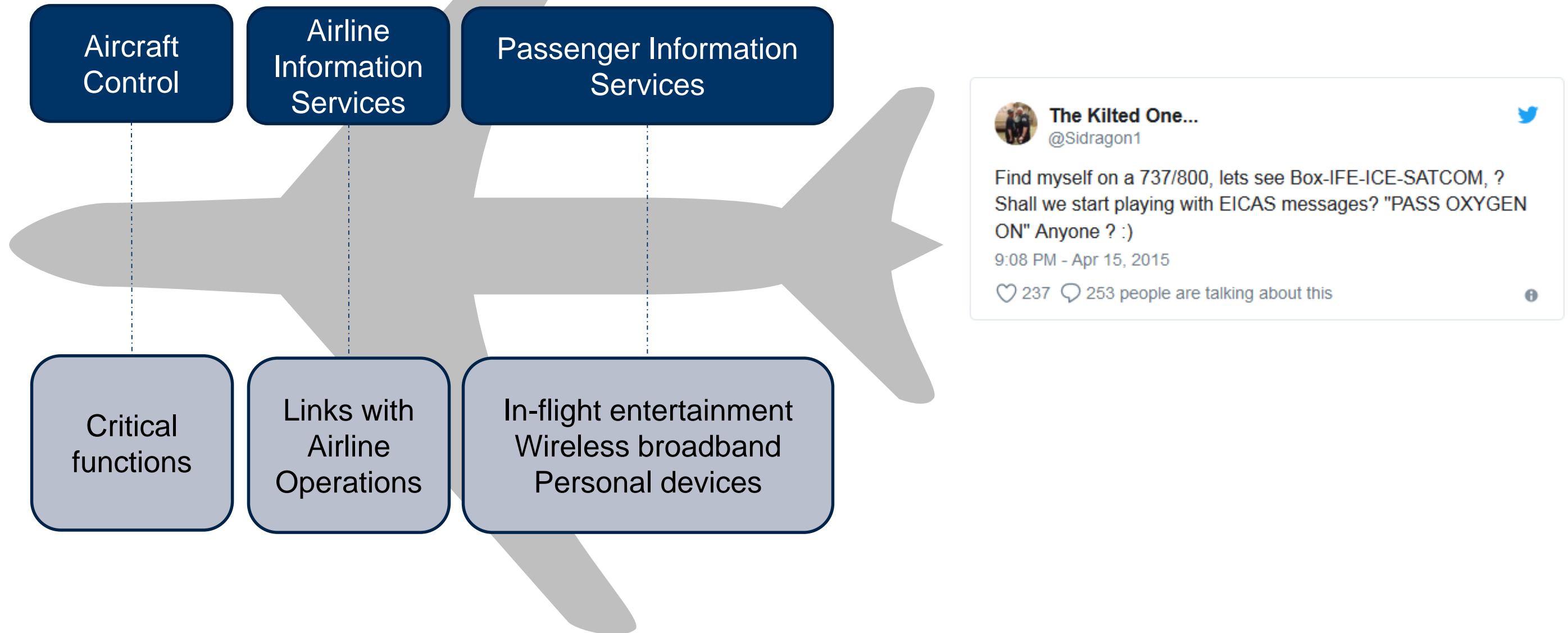


Example : ADS-B Vulnerabilities

Vulnerability	Description	Potential Impact (C/I/A)
Eavesdropping	The act of listening to the unsecured broadcast transmissions. Several service providers (e.g. FlightAware, FlightRadar24) use this information to provide visualisation of flights and additional information over the internet.	<ul style="list-style-type: none">• Loss of confidentiality of ADS-B message contents. (C)
Jamming	Denial of service. Broadcasting with sufficiently high power at the frequencies used by ADS-B (1090MHz if using Mode-S), preventing the transmission or reception of messages by one or more ADS-B participants.	<ul style="list-style-type: none">• Ground station flooding (Denial of service). (A)• Aircraft flooding. (A)
Message Injection	The injection of correctly modulated and formatted, but false ADS-B messages into the communications system. No authentication measures are implemented in ADS-B.	<ul style="list-style-type: none">• Ground station target ghost injection/flooding. (I/A)• Aircraft target ghost injection/flooding (IA)
Message Deletion	Legitimate messages can be 'deleted' from the wireless medium by using constructive or destructive interference.	<ul style="list-style-type: none">• Aircraft disappearance (I)
Message Modification	Injection of arbitrary data into the messages	<ul style="list-style-type: none">• Virtual aircraft hijacking. (I) Virtual trajectory modification (I)

Note : Information such as that in the table above is in the public domain.

Connected Aircraft – Potential Vulnerabilities



November 2017 : Boeing 757 Testing Shows Airplanes Vulnerable to Hacking (DHS)

Aircraft remotely hacked in non-cooperative penetration (DHS Cybersecurity Division)

<http://www.aviationtoday.com/2017/11/08/boeing-757-testing-shows-airplanes-vulnerable-hacking-dhs-says/>

Research on Potential Vulnerabilities



ACARS - Aircraft Communications
Addressing and Reporting System

April 2013 : Manipulation of ACARS information (Hugo Teso)

Laboratory study on modification of ACARS messages and exploitation of Flight Management System (FMS) bugs. Claimed to use smartphone to manipulate ACARS data.

Presentation : <https://conference.hitb.org/hitbsecconf2013ams/materials/D1T1%20-%20Hugo%20Teso%20-%20Aircraft%20Hacking%20-%20Practical%20Aero%20Series.pdf>

August 2014 : Aircraft Satellite Communications via Wi-Fi (Ruben Santamarta)

In theory, a hacker could use on-board WiFi or inflight entertainment system to hack into avionics equipment, potentially interfering with navigation and safety systems.

"The current status of the products [we] analyzed makes it almost impossible to guarantee the integrity of thousands of SATCOM devices". Ruben Santamarta

Paper : <https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf>

MENTI QUIZ : RISK EVOLUTION



- **Q6 : Which category of malware is Wannacry?**





- Rewards and Recognition in Security

Coffee Break