The Protection of Space Missions: Threats and Cyber Threats

Stefano Zatti – European Space Agency
Former Head of ESA Security Office

Universitá di Roma La Sapienza, 18/03/2019

Summary

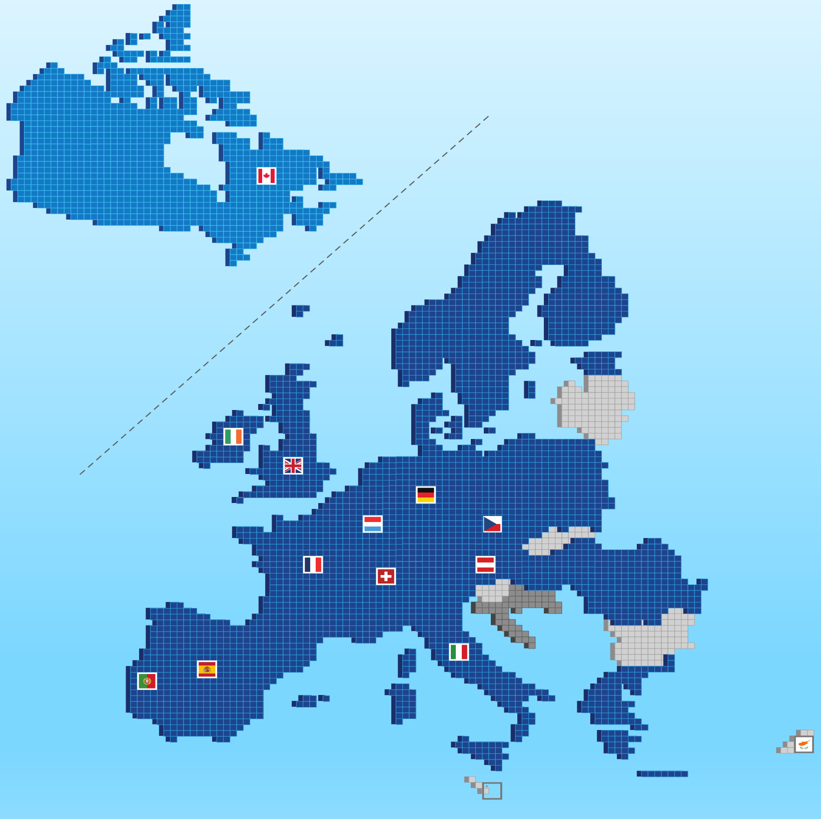
- Introduction to the European Space Agency
- Space missions with security flavour
- Space as an element for the security of European citizens
- Impact of cyber-threats on space missions
- Threats and countermeasures
- Conclusions

The European Space Agency and its member states

ESA has 22 Member States: 20 states of the EU (AT, BE, CZ, DE, DK, EE, ES, FI, FR, IT, GR, HU, IE, LU, NL, PT, PL, RO, SE, UK) plus Norway and Switzerland. UK will remain in ESA after Brexit

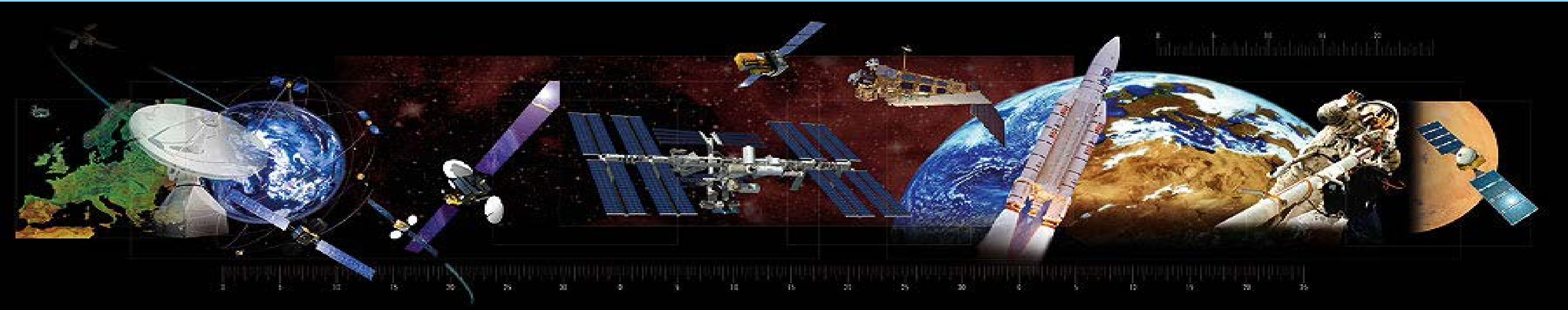
Seven other EU states have Cooperation Agreements with ESA: Bulgaria, Cyprus, Latvia, Lithuania, Malta, Slovakia and Slovenia. Discussions are ongoing with Croatia.

Canada takes part in some programmes under a long-standing Cooperation Agreement, that is currently being renewed.



ESA is one of the few space agencies in the world to combine responsibility in nearly all areas/categories of space activity.

- Space science
- Human spaceflight
- Exploration
- Earth observation
- Launchers
- Navigation
- Telecommunications
- Technology
- Operations

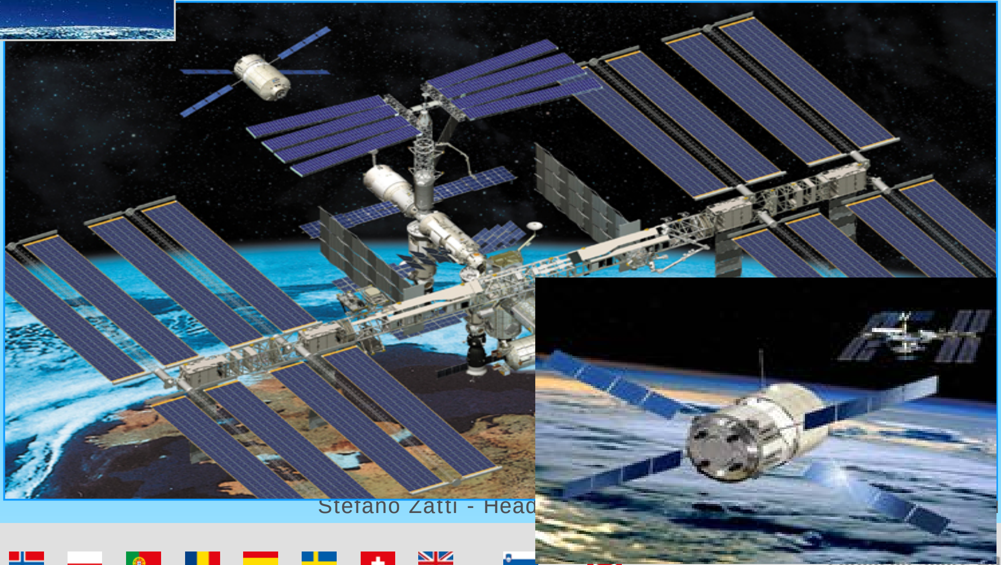


Some of the current ESA missions

Venus Express

Rosetta

Mars Express

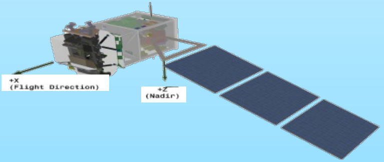


Space Station (ISS) :
ATV & Columbus

Copernicus (used to be: GMES)

An Earth observation programme for global monitoring for environment and security.

Led by the **European Commission** in partnership with ESA and responding to Europe’s need for geo-spatial information services, it provides autonomous and independent access to information for policy-makers, particularly for environment and security issues. ESA is implementing the space component: developing the **Sentinel** satellite series, its ground segment and coordinating data access.



Sentinel 1 – SAR imaging – Launch 3 April 2014
All-weather day/night applications, interferometry

Sentinel 2 – Multispectral imaging – Launch 23 June 2015 and 7 March 2017
Applications on territory: urbanization, forestry, agriculture

Sentinel 3 – Monitoring of oceans and dry land – Launch 16 February 2016 and 25 April 2018.
Ocean colour, salinity, vegetation, sea/land temperatures, altimetry

Sentinel 5P – Atmospheric Monitoring – Launch 13 October 2017.
Trace gases that affect air quality such as carbon monoxide, nitrogen, dioxide and ozone.

Galileo: Satellite Navigation "Made in Europe"

A complete navigation system under full European Control, developed by ESA on EU behalf.

- 30 satellites on three circular orbits, at
- inclination of 56° at Equator, at an altitude of 23 222 km
- Since 2010, **EGNOS** has been improving accuracy and augmenting GPS, offering safety-critical applications for aviation users.
- **Galileo** is expected to spawn a wide range of applications, based on positioning and timing for transport by road, rail, air and sea, infrastructure and public works management, agricultural and livestock management and tracking, e-banking and e-commerce. Key asset for public services, such as rescue operations and crisis management.
- Launch with Ariane 5 of 4 satellites on 25/07/2018

Space: a basic element for the security of the European Citizens

Elements of security and space from the ESA Council:

Security on Earth

- Critical Infrastructures Protection
- Maritime surveillance
- Land surveillance
- Humanitarian crisis support and rescue tasks
- Public Safety (incl. Civil Protection)
- Other emerging security threats (e.g., climate change)

Security in Space

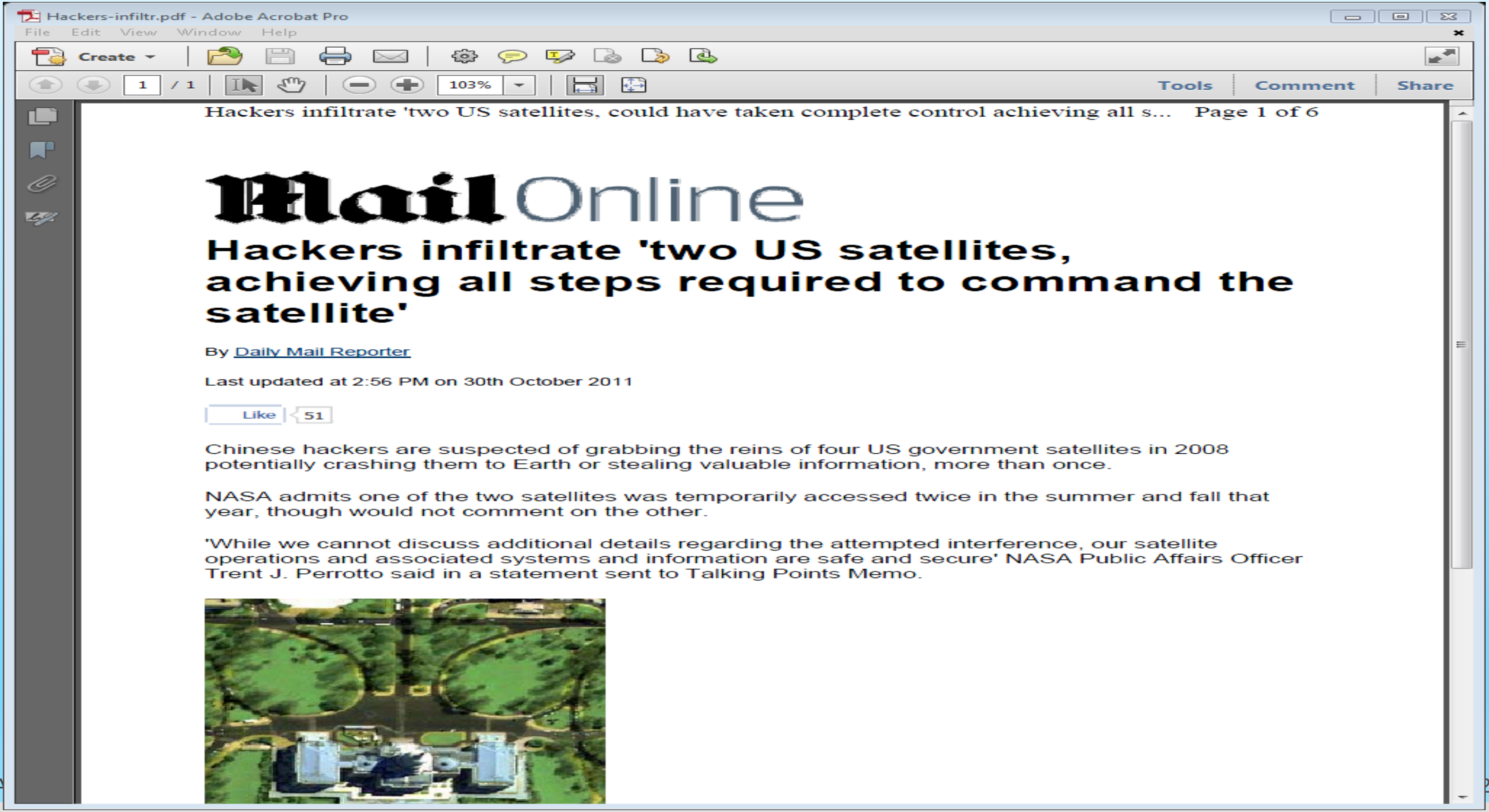
- Space situational awareness:
    - Near-Earth Objects
    - Space weather
    - Satellite tracking

Examples of hacking, spoofing, spying in space

Some unclassified examples from open literature include:

- In 1998, German-US ROSAT space telescope inexplicably turned towards the sun, irreversibly damaging a critical optical sensor following a cyber-intrusion at the Goddard Space Flight Center.
- On October 20, 2007, Landsat 7 experienced 12 or more minutes of interference. Again, on July 23, 2008, it experienced other 12 minutes of interference. The responsible party did not achieve all steps required to command the satellite, but the service was disturbed.
- In 2008, NASA EOS AM–1 satellite experienced two events of disrupted control: in both cases, the attacker achieved all steps required to command the satellite, but did not issue commands.

…and it gets known!


Hackers-infiltr.pdf - Adobe Acrobat Pro
File Edit View Window Help
Create
1 / 1
103%
Tools
Comment
Share

Hackers infiltrate 'two US satellites, could have taken complete control achieving all s... Page 1 of 6

MailOnline

Hackers infiltrate 'two US satellites, achieving all steps required to command the satellite'

By Daily Mail Reporter

Last updated at 2:56 PM on 30th October 2011

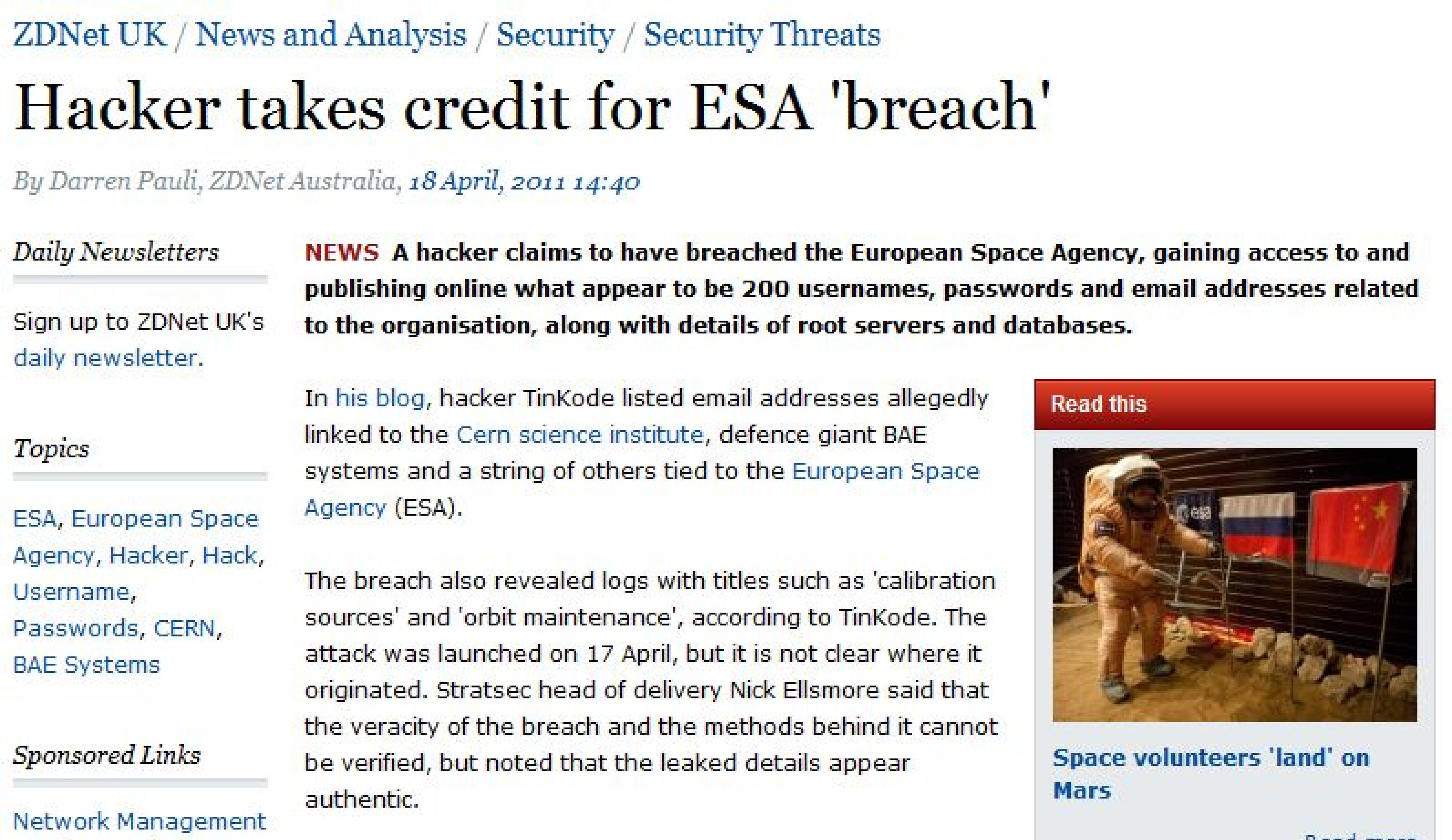
Like 51

Chinese hackers are suspected of grabbing the reins of four US government satellites in 2008 potentially crashing them to Earth or stealing valuable information, more than once.

NASA admits one of the two satellites was temporarily accessed twice in the summer and fall that year, though would not comment on the other.

'While we cannot discuss additional details regarding the attempted interference, our satellite operations and associated systems and information are safe and secure' NASA Public Affairs Officer Trent J. Perrotto said in a statement sent to Talking Points Memo.

..and in ESA?



ZDNet UK / News and Analysis / Security / Security Threats

Hacker takes credit for ESA 'breach'

By Darren Pauli, ZDNet Australia, 18 April, 2011 14:40

Daily Newsletters

Sign up to ZDNet UK's daily newsletter.

Topics

ESA, European Space Agency, Hacker, Hack, Username, Passwords, CERN, BAE Systems

Sponsored Links

Network Management

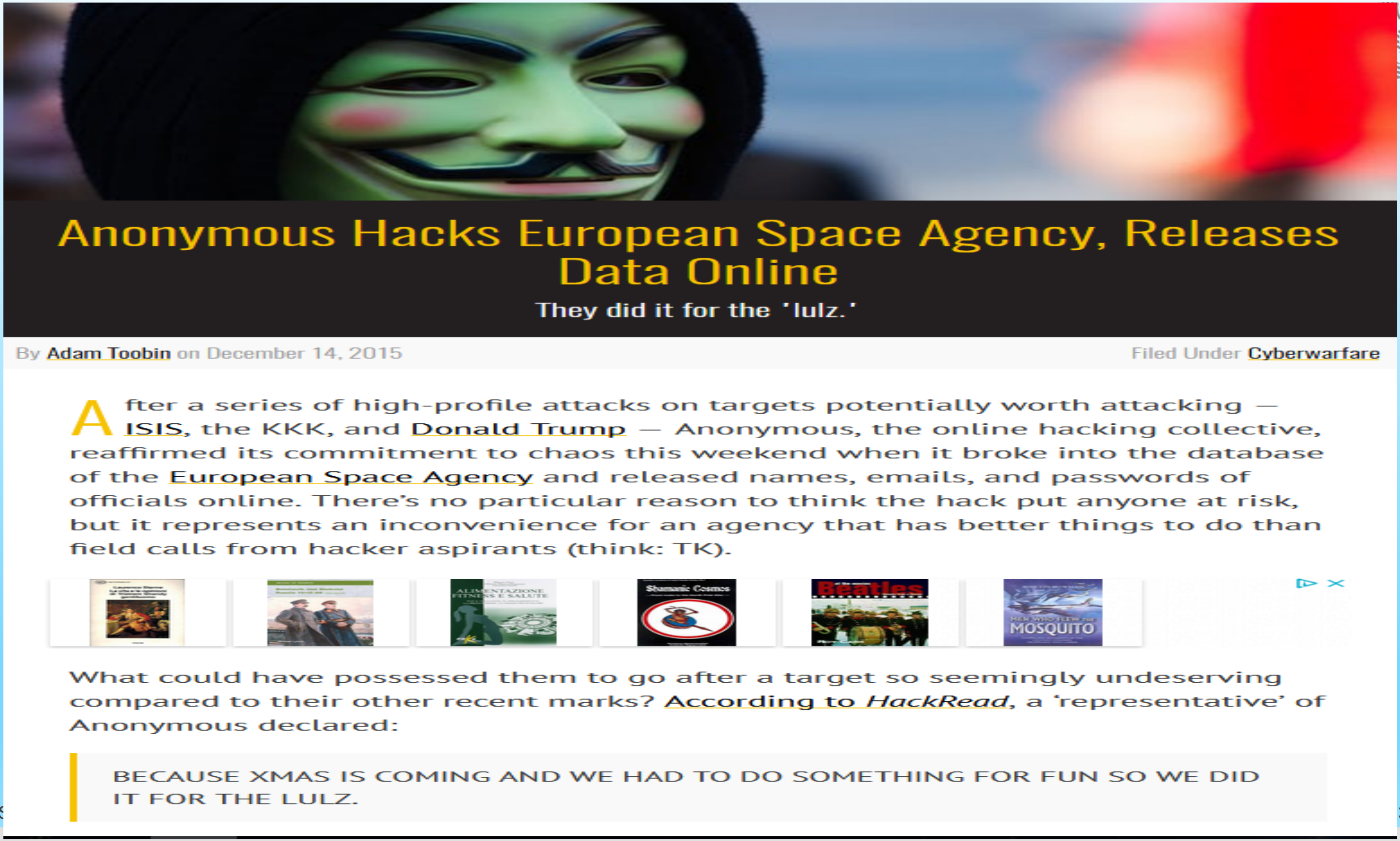
NEWS A hacker claims to have breached the European Space Agency, gaining access to and publishing online what appear to be 200 usernames, passwords and email addresses related to the organisation, along with details of root servers and databases.

In his blog, hacker TinKode listed email addresses allegedly linked to the Cern science institute, defence giant BAE systems and a string of others tied to the European Space Agency (ESA).

The breach also revealed logs with titles such as 'calibration sources' and 'orbit maintenance', according to TinKode. The attack was launched on 17 April, but it is not clear where it originated. Stratsec head of delivery Nick Ellsmore said that the veracity of the breach and the methods behind it cannot be verified, but noted that the leaked details appear authentic.

Read this

Space volunteers 'land' on Mars



Anonymous Hacks European Space Agency, Releases Data Online

They did it for the 'lulz.'

By Adam Toobin on December 14, 2015 Filed Under Cyberwarfare

After a series of high-profile attacks on targets potentially worth attacking — ISIS, the KKK, and Donald Trump — Anonymous, the online hacking collective, reaffirmed its commitment to chaos this weekend when it broke into the database of the European Space Agency and released names, emails, and passwords of officials online. There's no particular reason to think the hack put anyone at risk, but it represents an inconvenience for an agency that has better things to do than field calls from hacker aspirants (think: TK).

What could have possessed them to go after a target so seemingly undeserving compared to their other recent marks? According to *HackRead*, a 'representative' of Anonymous declared:

> BECAUSE XMAS IS COMING AND WE HAD TO DO SOMETHING FOR FUN SO WE DID IT FOR THE LULZ.

Real impacts

Navigation

- **Denial of service :** On January 2010, a software update of the GPS Ground Segment caused a denial of service. Impact observed on 8,000 to 10,000 military receivers during several days
- **Spoofing:** In 2009, a group of students at the University of Texas at Austin successfully tested a GPS spoofing device to remotely redirect an $80 million yacht

Observation Exploration

- **Deliberate interference and control loss:** On October 20, 2007 and On July 23, 2008, , Landsat-7, experienced 12 or more minutes of interference. All steps required to command the satellite not achieved
- **Targeted interference and control take-over:** On October 22, 2008, Terra EOS AM–1 experienced nine or more minutes of interference. Achieved all steps required to command the satellite but no commands.
- **Viral attack** : The Windows XP-based laptops on the ISS were infected with a virus called W32.Gammima.AG in 2008, after a cosmonaut brought a compromised laptop aboard which spread the malware to the networked computers.

Telecom

- **Deliberate Jamming :** ARABSAT “Deliberate jamming incidents have dramatically increased in 2012 which indeed put a threat on services over Satellites”
- **Unauthorized access :** The conjunction of open standard and cheap DVB cards for computer made possible the rise of Open Source Software dealing with the automated capture of image flow or data flow, for Private Person As a consequence, a “radio ham” captured the pictures/video of the NATO surveillance flights, during the Balkan War, as they were using an insecure satellite link.

Global Cyber Threats – Who is target?

Major industries susceptible to Cyber threats

Industry	Motivation	Target
Aerospace		
Government	European governments are targeted by both state and non-state-sponsored actors. State-sponsored actors seek information for purposes that align with the state's interests, including intelligence on foreign affairs and diplomatic and defense networks.	• Foreign and defense ministries • **International operations** • Military alliances
Telecommunications	State sponsored actors from China, Russia and the West targeting EMEA firms. Motivation include obtaining information on the European Union and collecting signals intelligence to benefit domestic military forces.	• **Cellular and mobile carriers** • **IT business services** • **Telecommunications devices** • **Satellite operators**

Global Cyber Threats – Bad boys, sneaky tactics

Who is behind?

75% perpetrated by outsiders

25% involved internal actors

51% involved organised criminal groups

18% conducted by state-affiliated actors

5% multiple parties and involved partners combined to 5% of actors

What are the tactics?

62% of breaches featured hacking

81% of hacking related breaches leveraged either stolen and/or weak passwords

51% over half of breaches included malware

43% were social attacks

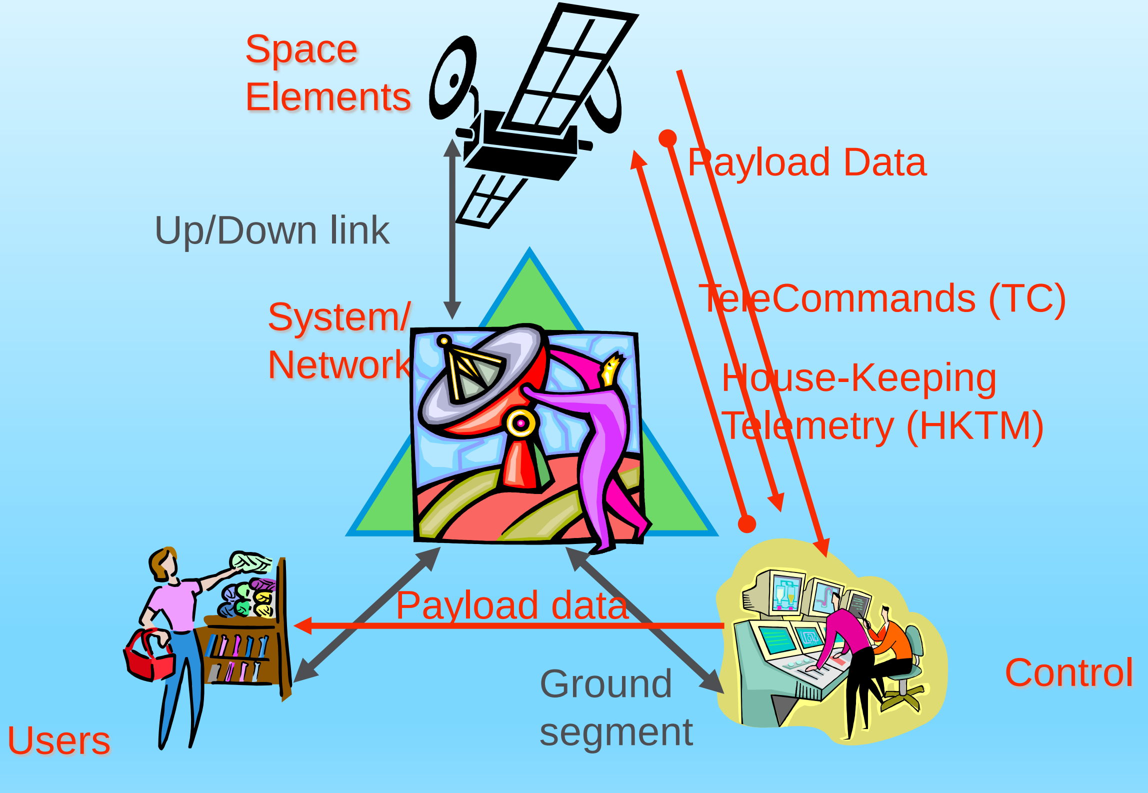
14% errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

Cyber Attack Trends – The Behaviour

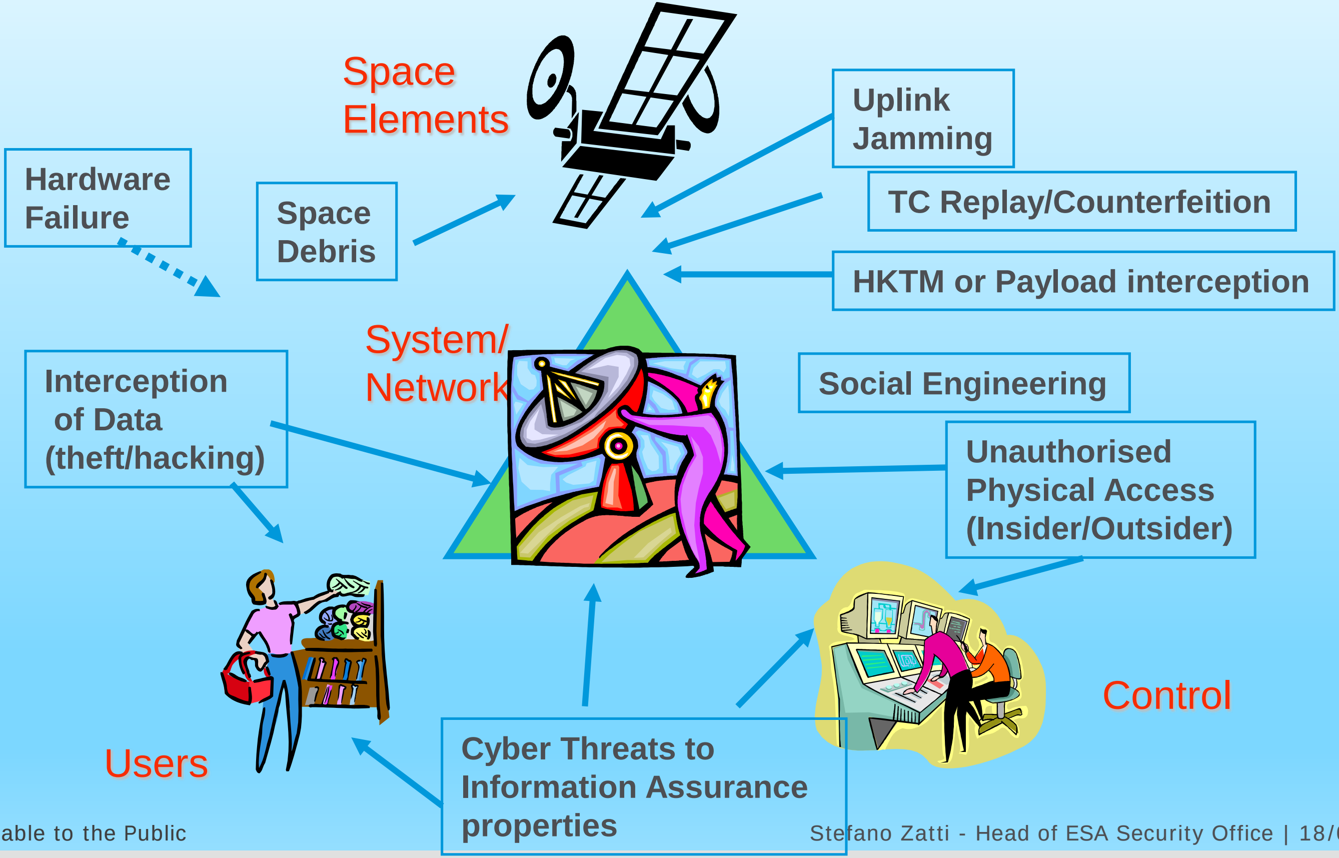
"When it comes to attack trends, we are seeing a much higher degree of sophistication than ever before."

- Today, the line between the level of sophistication of certain (e.g. financial) attackers and advanced state-sponsored attackers is not just blurred – it no longer exists
- Sophisticated attackers tailor their phishing mails to a specific client, location or employee
- They call victims on the telephone to help them enable macros in a phishing document, or to obtain a personal email address where the phishing document could be sent to avoid controls protecting corporate email

A typical Space Mission



Threats to a typical Space Mission



Space Elements

Hardware Failure

Space Debris

Uplink Jamming

TC Replay/Counterfeition

HKTM or Payload interception

System/ Network

Interception of Data (theft/hacking)

Social Engineering

Unauthorised Physical Access (Insider/Outsider)

Users

Control

Cyber Threats to Information Assurance properties

What are the sources of the threats and their motivations?

- **Competitors**, possibly by means of third parties: they are after information and knowledge
- **Cyber-criminals:** financial gain (of some sort)
- **Employees:** ranging from negligence to open hostility
- **Hacktivists:** politically and socially motivated to hamper space advance
- **Nations/States:** information, strategic advances, testing new types of attacks /cyber warfare
- **Terrorists:** Motivations of political-religious nature, aiming at critical infrastructures of different nature (e.g. health, energy, water, transportation, telecommunications)

What is the damage that can be made to a space mission?

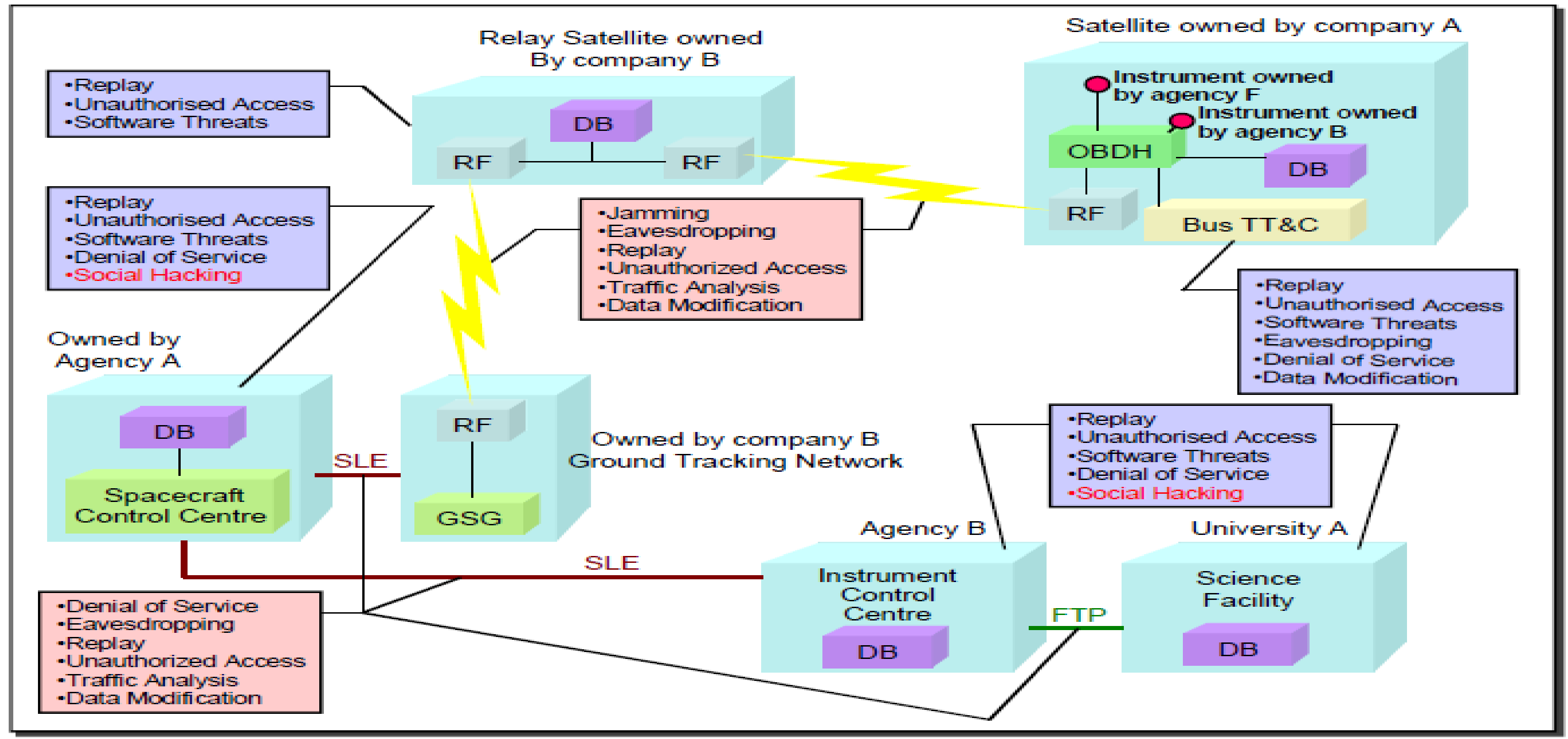
Tangible:

- Change trajectory and focus
- Hijack spacecraft, mission
- Deorbit, loss of device
- Add to space debris

Intangible:

- **Reputation, image**
- Data stealth, impact depending on data policy

The CCSDS Communication architecture and specific threats


Relay Satellite owned By company B
DB
RF
RF
Satellite owned by company A
Instrument owned by agency F
Instrument owned by agency B
OBDH
DB
RF
Bus TT&C
Owned by Agency A
DB
Spacecraft Control Centre
SLE
RF
GSG
Owned by company B Ground Tracking Network
SLE
Agency B
Instrument Control Centre
DB
FTP
University A
Science Facility
DB

- Replay
- Unauthorised Access
- Software Threats

- Replay
- Unauthorised Access
- Software Threats
- Denial of Service
- Social Hacking

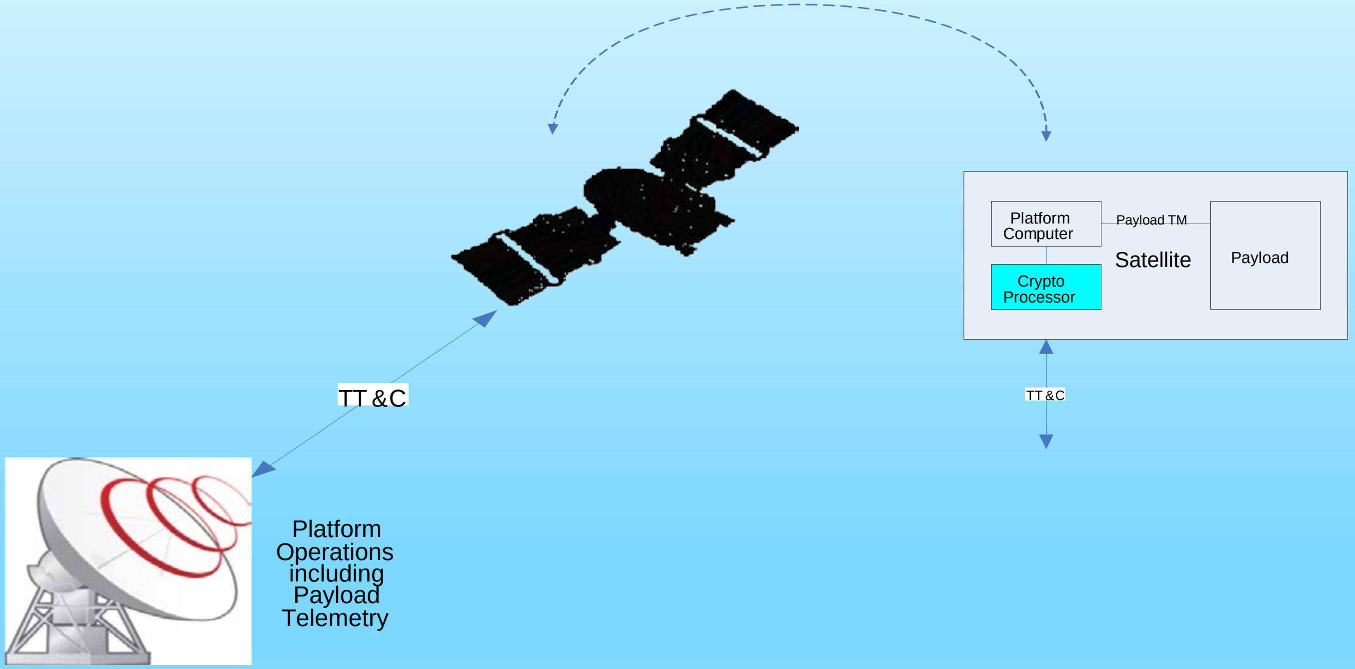
- Jamming
- Eavesdropping
- Replay
- Unauthorized Access
- Traffic Analysis
- Data Modification

- Replay
- Unauthorised Access
- Software Threats
- Eavesdropping
- Denial of Service
- Data Modification

- Replay
- Unauthorised Access
- Software Threats
- Denial of Service
- Social Hacking

- Denial of Service
- Eavesdropping
- Replay
- Unauthorized Access
- Traffic Analysis
- Data Modification

Enabler of all countermeasures: the crypto processor on board



TT &C

Platform Operations including Payload Telemetry

Platform Computer

Payload TM

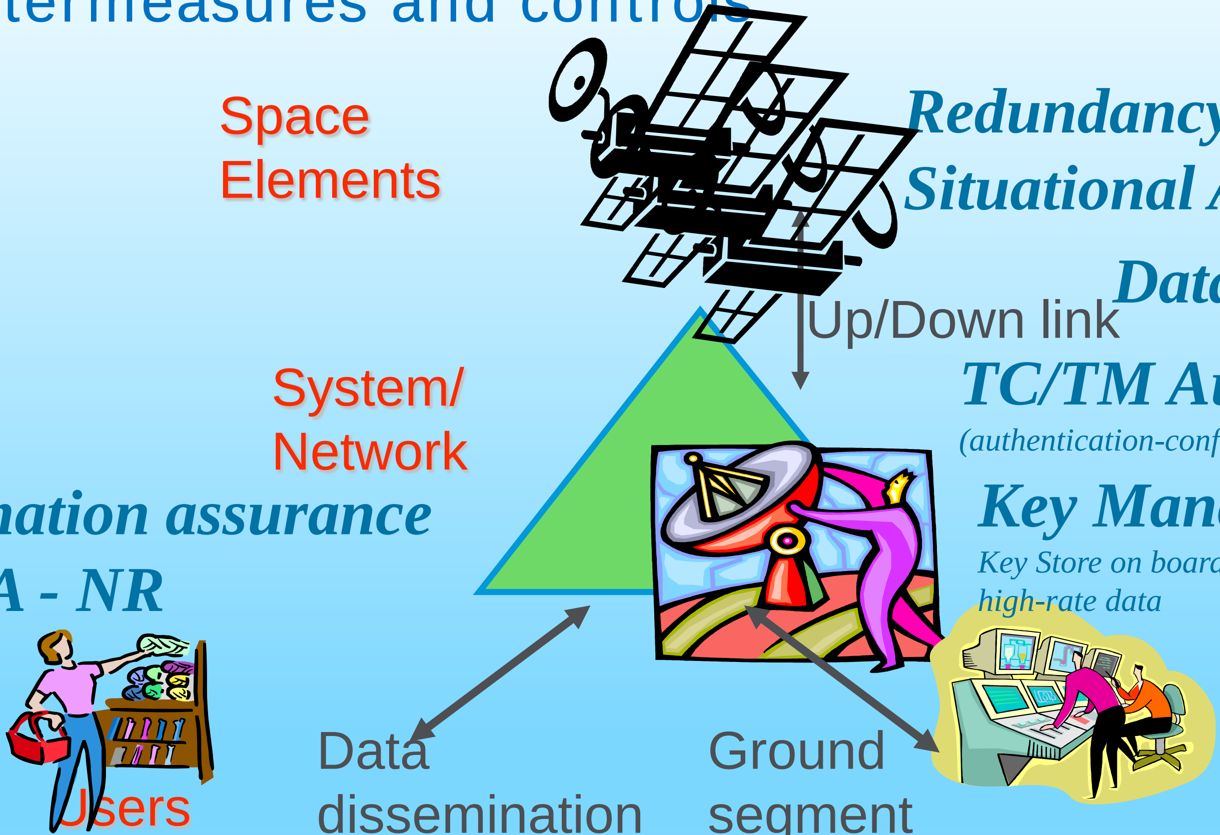
Satellite

Payload

Crypto Processor

TT &C

Countermeasures and controls



Space Elements

System/ Network

Up/Down link

Users

Data dissemination

Ground segment

Control

Redundancy – Situational Awareness

Data Encryption

TC/TM Authentication

(authentication-confidentiality-integrity)

Key Management

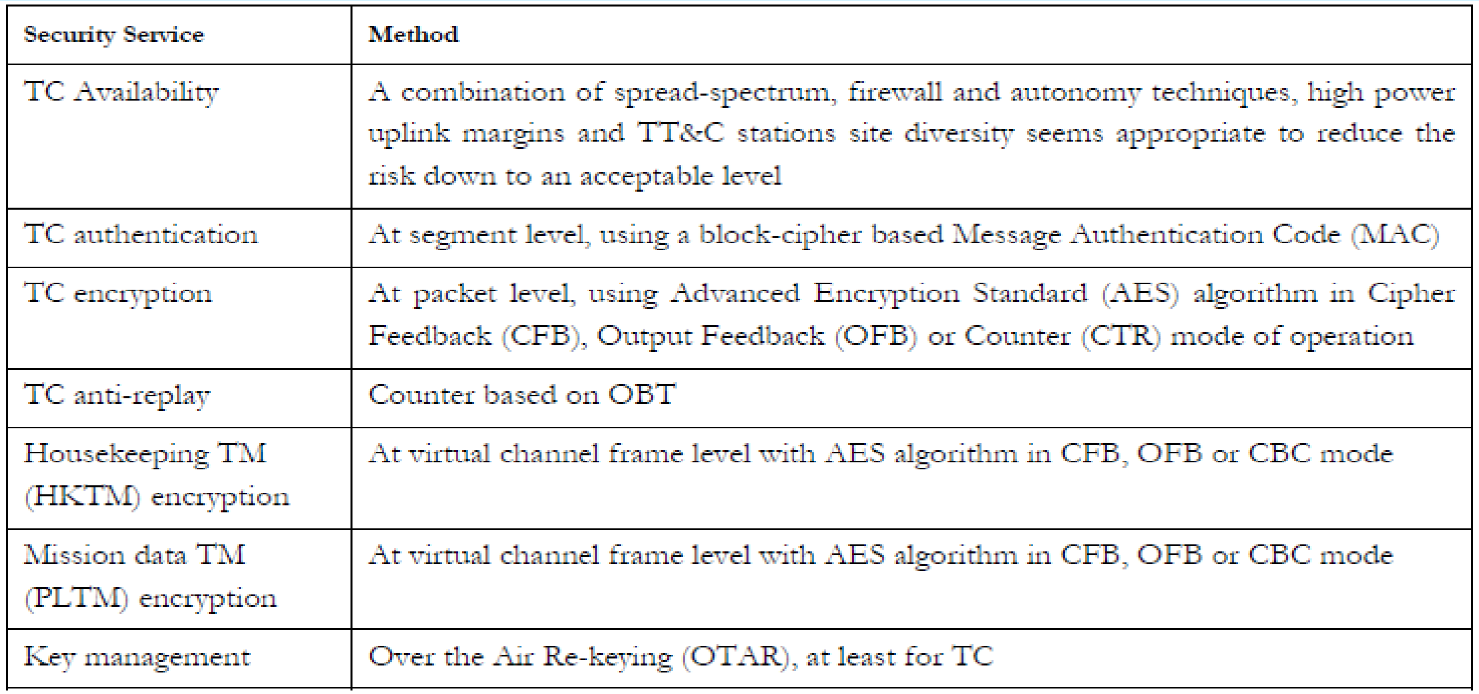
Key Store on board – Key management for high-rate data

Information assurance

CIA - A - NR

End-to-end cyber security: physical, personnel, classification

Selection of countermeasures – general framework

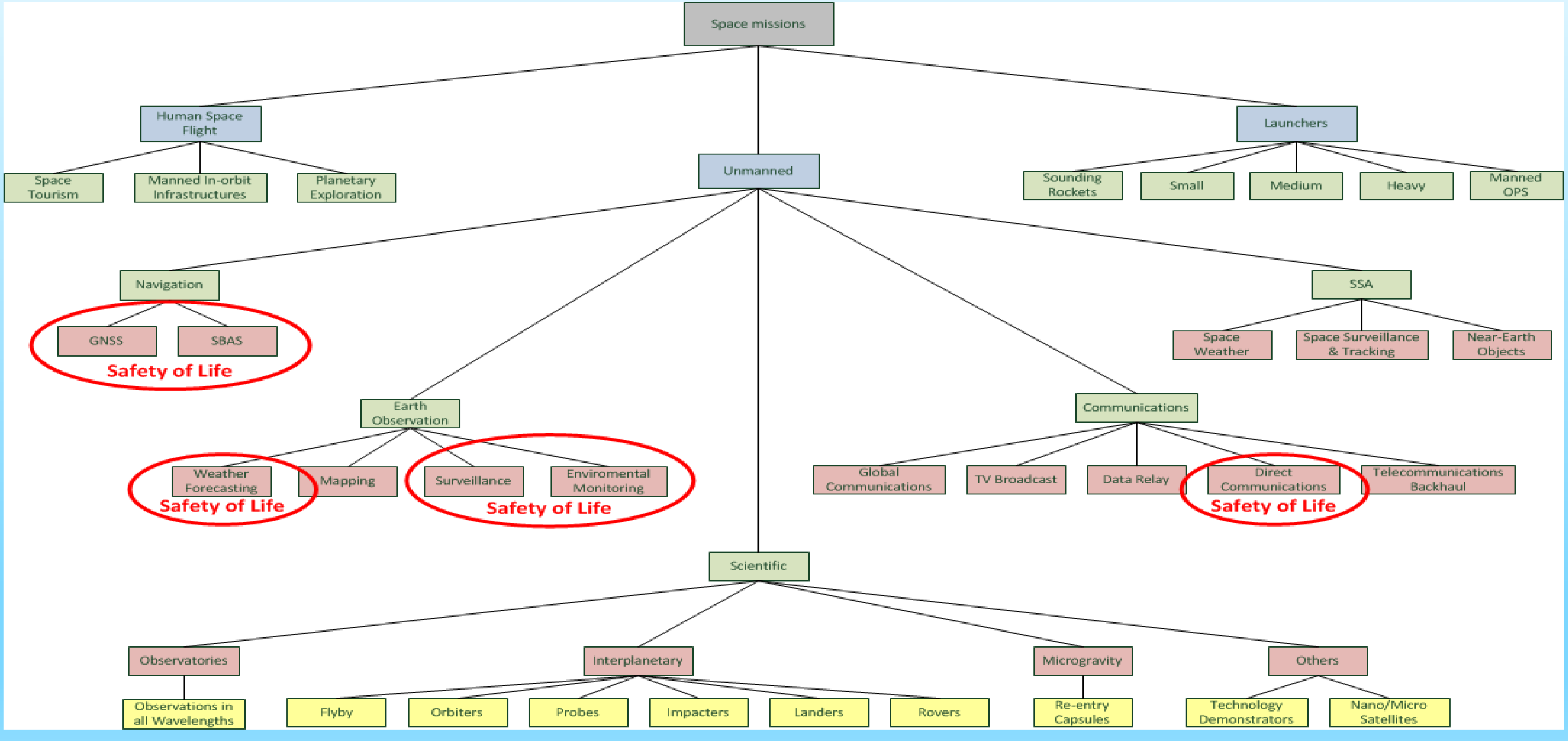


Security Service	Method
TC Availability	A combination of spread-spectrum, firewall and autonomy techniques, high power uplink margins and TT&C stations site diversity seems appropriate to reduce the risk down to an acceptable level
TC authentication	At segment level, using a block-cipher based Message Authentication Code (MAC)
TC encryption	At packet level, using Advanced Encryption Standard (AES) algorithm in Cipher Feedback (CFB), Output Feedback (OFB) or Counter (CTR) mode of operation
TC anti-replay	Counter based on OBT
Housekeeping TM (HKTM) encryption	At virtual channel frame level with AES algorithm in CFB, OFB or CBC mode
Mission data TM (PLTM) encryption	At virtual channel frame level with AES algorithm in CFB, OFB or CBC mode
Key management	Over the Air Re-keying (OTAR), at least for TC

End-to-end cybersecurity

- **Physical**: zoning, access control for data centers
- **Personnel:** vetting, clearances, trust, peer control
- **Information protection:** classified vs unclassified
- **Information assurance:**
    - **Confidentialty -** encryption
    - **Integrity -** MAC
    - **Availability -** redundancy
    - **Authenticity -** identity management**,** cross check, access control, signature of data
    - **Non-repudiation -** notarization, certificates

Characterization of mission categories



- Space missions
  - Human Space Flight
    - Space Tourism
    - Manned In-orbit Infrastructures
    - Planetary Exploration
  - Unmanned
    - Navigation
      - GNSS
      - SBAS
      - Safety of Life
    - Earth Observation
      - Weather Forecasting
        - Safety of Life
      - Mapping
      - Surveillance
      - Enviromental Monitoring
        - Safety of Life
    - Scientific
      - Observatories
        - Observations in all Wavelengths
      - Interplanetary
        - Flyby
        - Orbiters
        - Probes
        - Impacters
        - Landers
        - Rovers
      - Microgravity
        - Re-entry Capsules
      - Others
        - Technology Demonstrators
        - Nano/Micro Satellites
    - Communications
      - Global Communications
      - TV Broadcast
      - Data Relay
      - Direct Communications
        - Safety of Life
      - Telecommunications Backhaul
    - SSA
      - Space Weather
      - Space Surveillance & Tracking
      - Near-Earth Objects
  - Launchers
    - Sounding Rockets
    - Small
    - Medium
    - Heavy
    - Manned OPS

Mission Protection Profiles

Different mission categories have different security requirements

Missions are categorized by different types of risks:

- Scientific
- Earth Observation
- Navigation
- Meteo
- Manned spaceflight and exploration

Five different **protection profiles** of Tele-commands and Telemetry, that can be applied to different mission categories (0 to 4)

TC/TM Security Solutions : 0

Profile 0: no specific security

- No TC authentication and encryption
- No House-Keeping Telemetry or science data encryption
- Standard terrestrial links security (firewalls, IDP, SIEM etc…)
- Implemented in ERS/ENVISAT and Earth Explorers

TC/TM Security Solutions: 1/2

Profile 1: static Tele Command protection

- TC authentication and anti-replay
- Authentication key pre-loaded on board
- TC authentication can be enabled/disabled automatically or by ground
- Currently implemented on MetOp and ATV

Profile 2: dynamic TC protection

- TC authentication and anti-replay
- Authentication keys are loaded by ground using preinstalled Master Keys for the encryption of the related TCs
- TC authentication can be enabled/disabled automatically or by ground
- Implemented in the Sentinels

TC/TM Security Solutions 3/4

Profile 3: dynamic TC + payload data protection

- Payload data is encrypted
- 4 types of keys: Master key, TC authentication key, payload data encryption key, TC encryption key
- Payload data encryption can be enabled/disabled automatically or by ground

Profile 4: dynamic TC + payload + HKTM data protection

- HKTM data is also encrypted
- 5 types of keys: Master key, TC authentication key, data encryption key, HKTM data encryption key, TC encryption key
- HKTM data encryption can be enabled/disabled automatically or by ground

Example: Sentinel Security Baseline

Selection of Profile 2 - Dynamic TC protection as baseline, with additions

- TC authentication + anti-replay
- TC ‘encryption’ limited to security related TCs (new keys)
- ‘Encryption’ affects ONLY TC ‘data field’
- No HKTM and payload data encryption
- Preinstalled fixed Master keys: used as key encryption keys
- Session keys: used for authentication - uploaded by ground using master keys
- Keys are referenced by meta-information avoiding the need to encrypt HKTM
- TC authentication can be by-passed automatically upon critical mission failure
- TC authentication by-pass can be enabled/disabled by ground via authenticated TC or by a *watchdog* based on timeout

NewSpace = new cyber threats

- The cybersecurity of space missions is a matter of competiveness for the European space industry, and, at the same time, is a vital subject for the EU as owner of the Copernicus and Galileo Programmes.

- The need to guarantee high production rates (e.g. 4 satellites per day in the case of the most dense constellations) requires the system integrators to stretch globally the existing supply chain, and to include new components providers in the chain of trust.

- The globalization of manufacturing capabilities and the increased reliance upon commodity software and hardware for space and ground segments (as opposed to bespoke as in the past) has expanded the opportunities for malicious modification in a manner that could compromise critical functionality -> additional risks!