# Security at ESA

## Workshop of the European Interparliamentary Space Conference (EISC)

Stefano Zatti - Head of ESA Security Office

ESA Redu 14/05/2018

# Space: a basic element for the security of the European Citizens. The themes are:

For **Safety in Space**,

- Planetary Defence
- Space Weather
- Debris incl. mitigation, remediation, removal,…
- SST
- Space Traffic Management

For **Safety and Security Applications from Space**, (as part of sustainability, individual/community/society)

- Disasters (natural or man made) from Earthquake to Climate Change
- Migration and border control
- Transportation, logistics
- Secured communication
- Surveillance (land, sea, air, space)
- Energy
- Food and Water
- Critical Infrastructure (distribution of quantum key)

# But…can cyber incidents reach into space? 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



Mail Online

## 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.

# The challenge of inserting security in an open organization like ESA

ESA has one Corporate communications and information system that caters to all productivity and connectivity needs

Missions and Programmes develop their own cyber systems in support of their programmatic goals, like e.g., the Earth Observation Payload Data Ground Segment and the Galileo ground segment

Programme-specific data systems are normally located in specific De-Militarized zones subject to specific access policies and dedicated protection

Missions and Programmes must develop their own specific Data Policy, on the basis of which their systems will be configured

Each Programme must appoint a responsible security officer

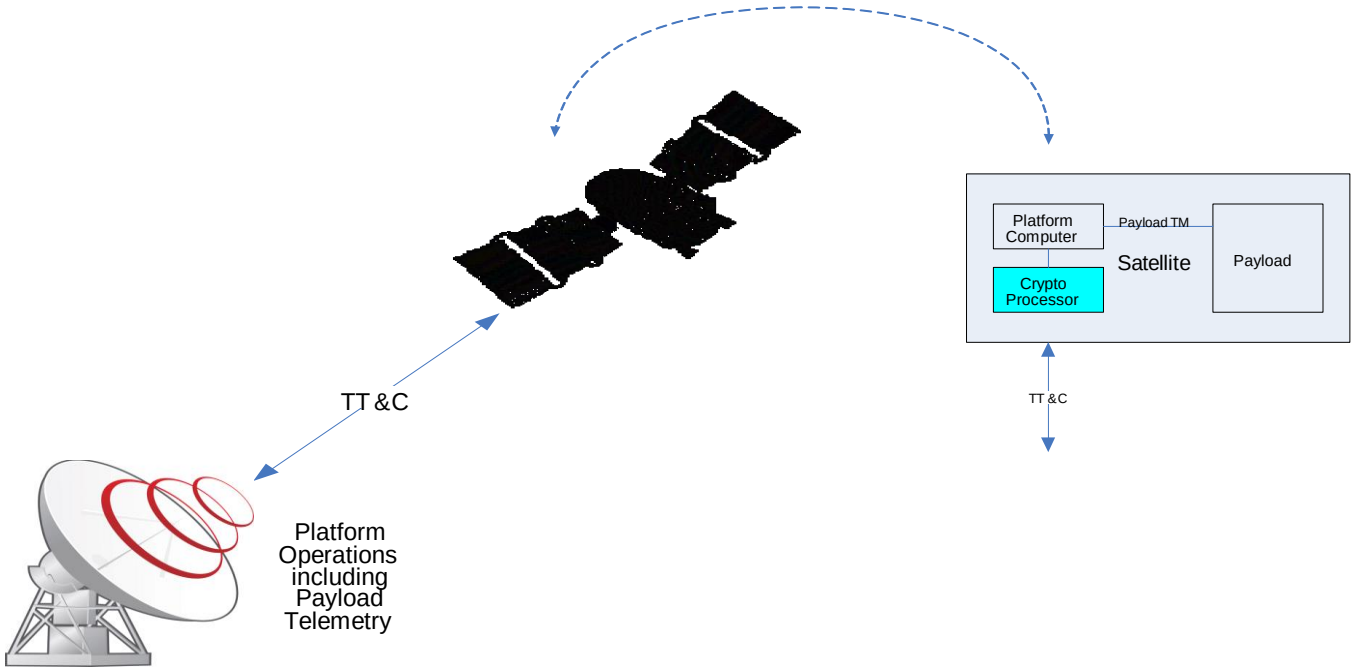
ESA security officers are linked in a network of expertise and operationally linked, coordinated by the ESA Security Office…

# The roman testudo: locked shields!

# 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, gain technological advantage
- **Terrorists:** Motivations of political-religious nature, aiming at critical infrastructures of different nature (e.g. health, energy, water, transportation, telecommunications, access to space)

# Enabler of all countermeasures: the crypto processor



# End-to-end cybersecurity at ESA: a holistic approach

- **Physical**: zoning, access control for data centers
- **Personnel:** vetting, clearances, trust, peer control
- **Information protection:** classified vs unclassified
- **Information assurance:** All systems are subject to ISO 27001 certification, to assure the properties of:

  - **Confidentiality -** encryption
  - **Integrity –** Media Access Code
  - **Availability -** redundancy
  - **Authenticity -** identity management**,** cross check, access control, signature of data
  - **Non-repudiation -** notarization, certificates

# 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 Copernicus and Galileo.
- 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.
- The globalization of manufacturing capabilities and the increased reliance upon commodity software and hardware for space and ground segments has expanded the opportunities for malicious modification in a manner that could compromise critical functionality -> inducing additional risks!