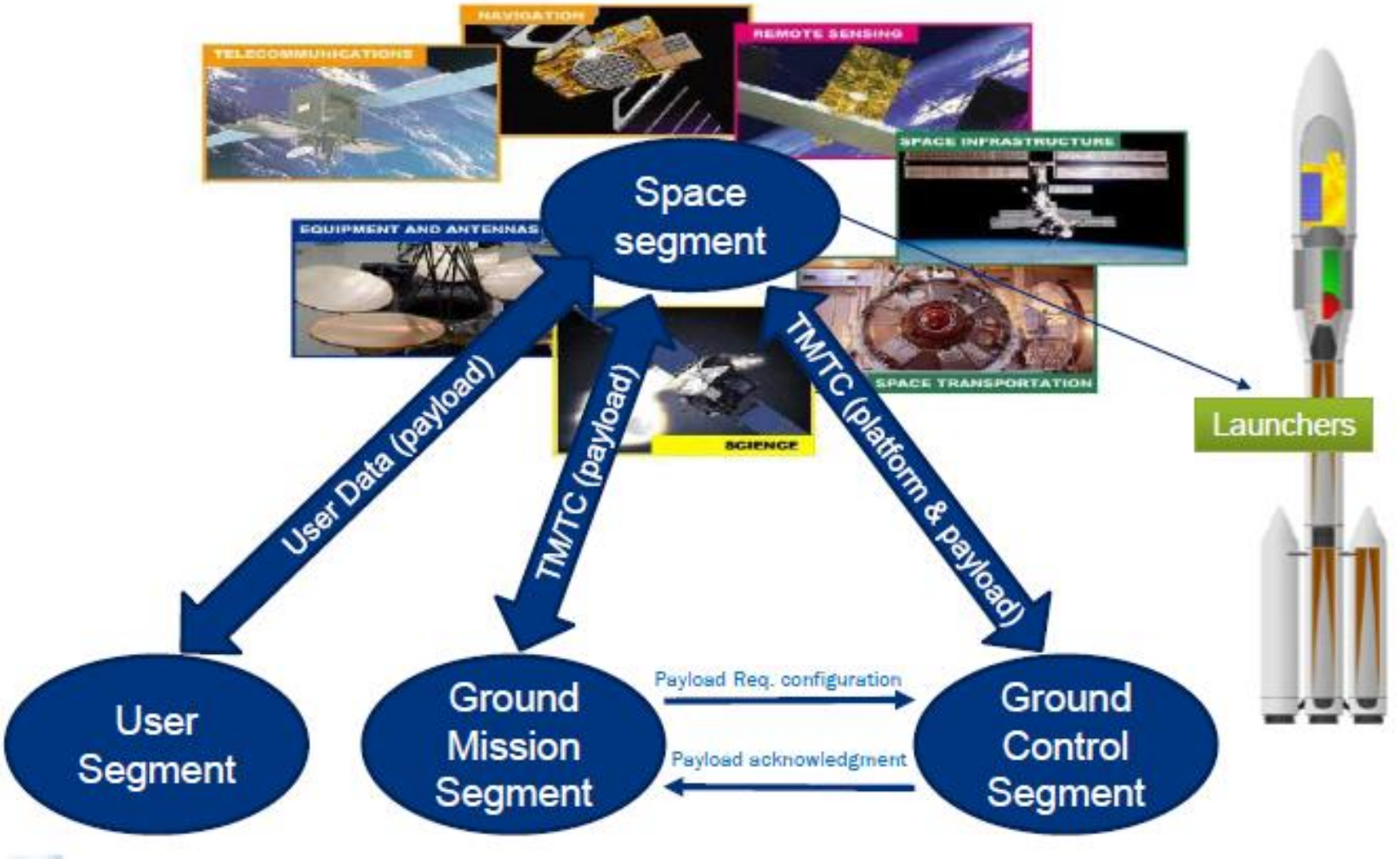
Cybersecurity of Space Missions

Jean Muylaert and
Luca Del Monte

Presentation at the Workshop of the European Interparliamentary Space Conference
14 May 2018

Space missions

Large variety of applications for Private, Public, Scientific and Defence sectors



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.**

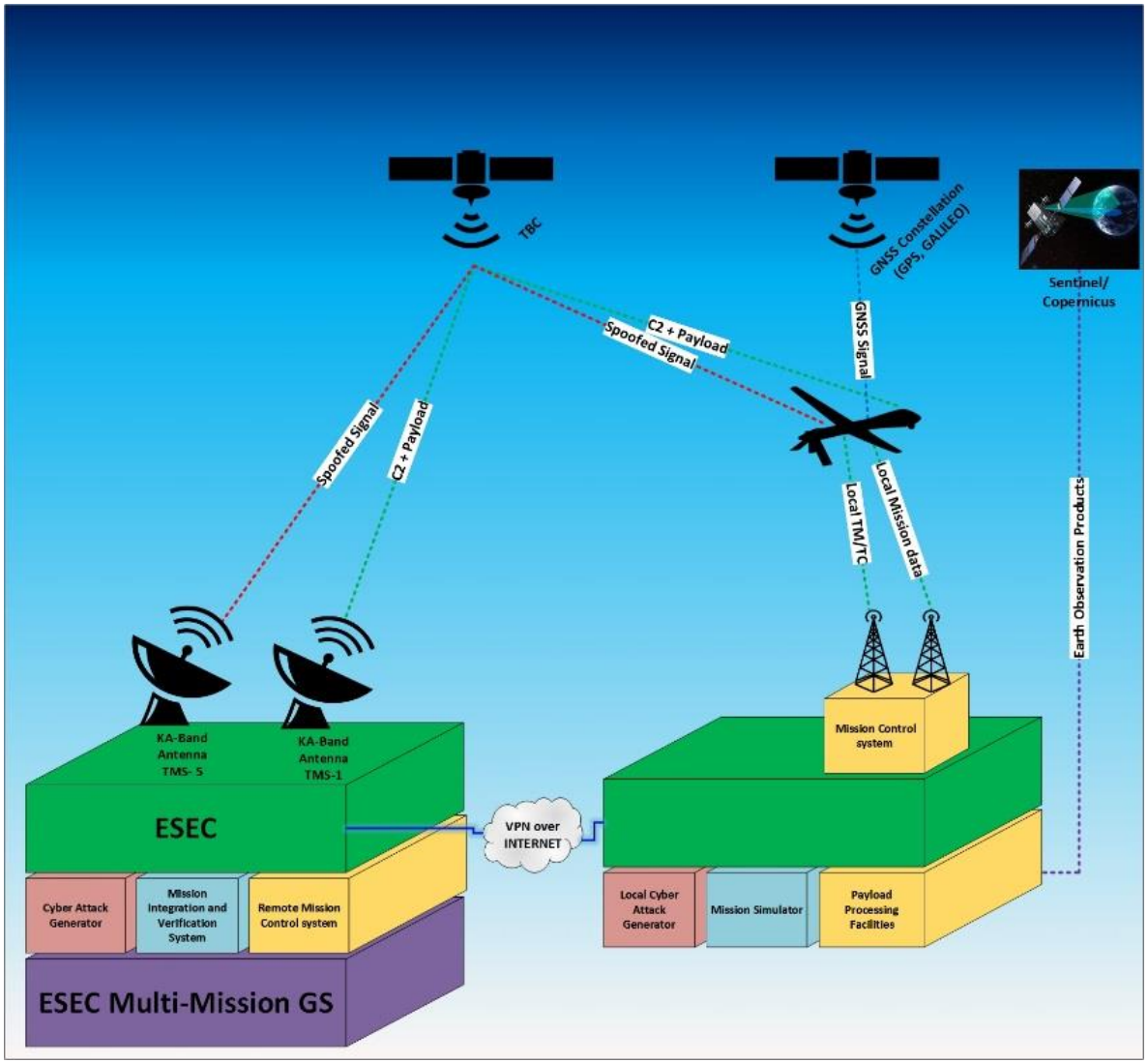
Typical risks

Jamming, spoofing and hacking attacks :

- **Communication net works**
  - **Attacks on satellites by taking control**
  - **Attacks on ground infrastructure, control and data centres**
- **Unmanned platforms : UAV's, Cars, UUV**
  - **Collision avoidance**
- **IRS (intelligence, reconnaissance, Surveillance) platforms**
  - **Anti jamming and spoofing protection**
- **Global system integration:**
  - **Cooperation between heterogeneous vehicles and within massive future micro Sat constellations**

More and more complexity with ever increasing entry points. Major risk of back door holes in encryption and other control systems with e.g. IoT

Example of future ESEC NewSpace cyber security capability development



Space Missions: security objectives

- Reminder of the 3 mains security Objectives
  - **Data Integrity** : Data must be reliable in order to be exploitable
  - **Data Availability** : Data must be available when needed
  - **Data Confidentiality** : Data must be accessible only to the authorized entity
- The main difference between civilian & defense mission is the management of Confidentiality

- **Defence missions constraints for confidentiality impact strongly security architecture**

ESA study on cybersecurity of space missions

- **ESA has the very specific need and obligation to protect the European tax-payer investments based in space (and sometimes in deep-space) from cyber menaces, both of operational nature, or hidden and latent in the on-board components of the spacecraft.**

- **Two parallel CLASSIFIED studies – with GMV (Spain) and THALES (with the support of ThalesAlenia Space France) – have been conducted by ESA. Results show that, alongside technology development, policy measures are needed to address the cyber threats to which ESA is exposed**

- **A third one with Thales on going**

Results Synthesis

Task 1
Feared Event analysis and modelling

- 3 Space Missions (i.e. Navigation, Telecommunication, Observation/Exploration) including launch phase – MODAF-based
- 10 Feared Events defined
- 94 Security Requirements

Task 2
Threat scenario and Vulnerabilities

- 18 basic threats retained (e.g. Jamming)
- 489 Threats Scenario selected (e.g. An external Jamming attack prevents to send/receive message)
- 203 Vulnerabilities identified (Uncovered TS)

Task 3
Risks Identification and evaluation

- 10 Attack Trees (1 per Feared Event)
- 228 Risks Identified

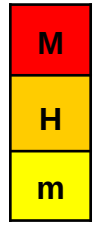
Task 4
Major Risks Recommend ations

- 76 Major Risks identified
- 80 sets of Security requirements

Feared Events

10 Feared Events per Space Mission (From Task#1)

		Gravity		
ID	**Feared Event**	**Nav.**	**Tel.**	**EO/E.**
FE-1	Loss availability of Ground infrastructures having an impact in the nominal system functioning	m	**H**	m
FE-2	Loss (Temporary or definitive) of one or more satellites of the constellation)	m	**H**	**H**
FE-3	Global system performances degradation under defined performance values	**H**	**H**	**H**
FE-4	Loss of Mission service availability for End User	**M**	**M**	**M**
FE-5	Incorrect Mission data received by end user	**M**	H	**M**
FE-6	Mission data Unauthorized access	**H**	**H**	m
FE-7	Loss of Know How for European institutions	**H**	**H**	**H**
FE-8	Regulatory issue about export control rules	**m**	**m**	**m**
FE-9	Public knowledge of security breaches not known by European institutions	**M**	**M**	**M**
FE-10	System Degradation without knowing whether it is an attack or a failure	**H**	**H**	**H**

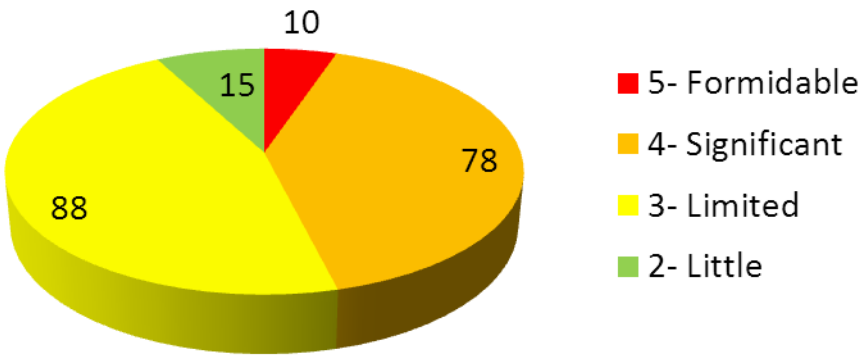


Risk Evaluation Results

228 Risks Identified:

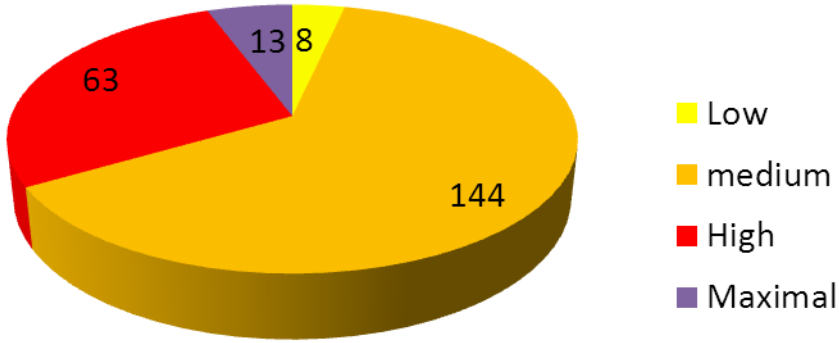
- FE01: **40** (Loss availability of Ground infrastructures having an impact in the nominal system functioning)
- FE02: **29** (Loss (Temporary or definitive) of one or more satellites of the constellation))
- FE03: **48** (Global system performances degradation under defined performance values)
- FE04: **16** (Loss of Mission service availability for End User)
- FE05: **26** (Incorrect Mission data received by end user)
- FE06: **20** (Mission data Unauthorized access)
- FE07: **1** (Loss of Know How for European institutions)
- FE08: **0** (Regulatory issue about export control rules)
- FE09: **0** (Public knowledge of security breaches not known by European institutions)
- FE10: **48** (System Degradation without knowing whether it is an attack or a failure)

Resources Required*



***Excluding only Accidental Risks**

Risk Value



Finding Summary

- **76 of the 228 identified Risks are assessed as "Major"** (Risk Level = High or Maximal).
- **80 Security Controls** are identified to mitigate the Major Risks. They are split in **13 thematic**:
  - Audit & tests
  - Command Protection
  - **Connection with Authority and Interest Group**
  - Message and Data Protection
  - **Personnel and Resources Management**
  - Security in Operations
  - **Security of Development and Design Life Cycle**
  - **Security of Partners and Externals**
  - Service continuity
  - Signal protection
  - Spacecraft Resiliency
  - System Access Control
  - System Monitoring
- Several of these mitigation measures are of **industrial policy** nature

Cybersecurity risks associated to the supply chain

- **Hardware and software can be maliciously modified undetected. The malicious capabilities could be triggered at a later time.**
- **Within the context of a space mission supply chain, some spacecraft on-board components available on the market may contain spyware or logic bombs.**
- **The globalization of manufacturing capabilities and the increased reliance upon commodity software and hardware for ground segments has expanded the opportunities for malicious modification in a manner that could compromise critical functionality.**
- **Another source of risks in the supply chain is the external personnel who are involved in the outsourced services**

Recommendations to address procurement security

- **The establishment of a verification team (full internal or with a trusted partner) to verify the security of the components/equipment provided by the manufacturers.**

- **The definition of a baseline Cyber security requirements list as a contractual document.**

- **Define all key terms about security in frame of Purchase and subcontracting activities, and share these terms with all the stakeholders**

- **Require contractually the manufacturers to be able to audit with respect to security aspects at each step of the realization and purchase required systems items only from original equipment manufacturers, or other trusted sources**

- **Incorporate "cyber security in acquisition" into required training curricula for all appropriate ESA and partners workforces**

ESA Cyber (training) Range at ESEC in Redu (B)

A training and simulation platform facility to provide training and testing and develop knowledge in Awareness, Detection, Investigation, Response and Forensics to counter cyber-attacks specific to space systems.

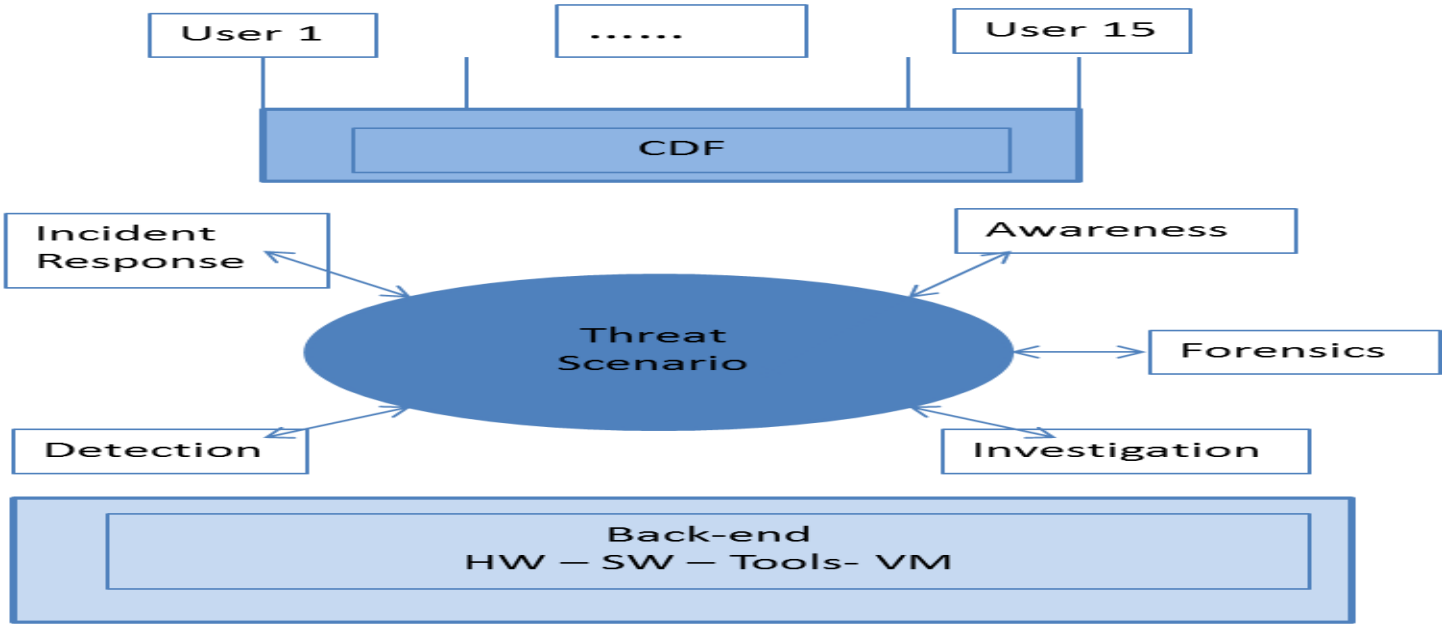


Figure 1: Cyber security training range set-up