CYBERSECURITY IN THE SPACE SECTOR

Carlo Sarto
Head of Security Eng., Qascom S.r.l.

17 Feb. 2025
University of Padua

LESSON CONTENT

- Cybersecurity in the space sector
  - The space sector, market segments and applications
  - The security needs of the space industry
  - Security threats of space missions
  - Security standards and practices

1.

The space sector, market segments and applications

- Space Sector definition
  - All the economic activities directly and indirectly related to outer space, including engineering and manufacturing of spacecrafts, satellites, space-based services and user equipment.
- Key players
  - Military agencies
  - Private companies
  - Research institutions
  - Governmental agencies: EUSPA (EU Agency for Space Programs), ESA (European Space Agency), NASA (US), Roscosmos (RU), Jaxa (JP), ISRA (IN), CNSA (CN), ASI (IT), CNES (FR), DLR (DE), …

VALUE CHAIN AND MARKET SEGMENTS

- The value chain of the space economy refers to the various activities and processes that are involved in creating and delivering products and services related to space.

UPSTREAM

- Provision of space technologies
  - Engineering
  - Manufacturing
  - Launch
  - Science
  - R&D

DOWNSTREAM

- Use and commercialization of the products and services that result from space technologies
- Space infrastructure operations and “down-to-earth” products and services that directly rely on satellite data and signals to operate and function

DERIVED / INDUCED

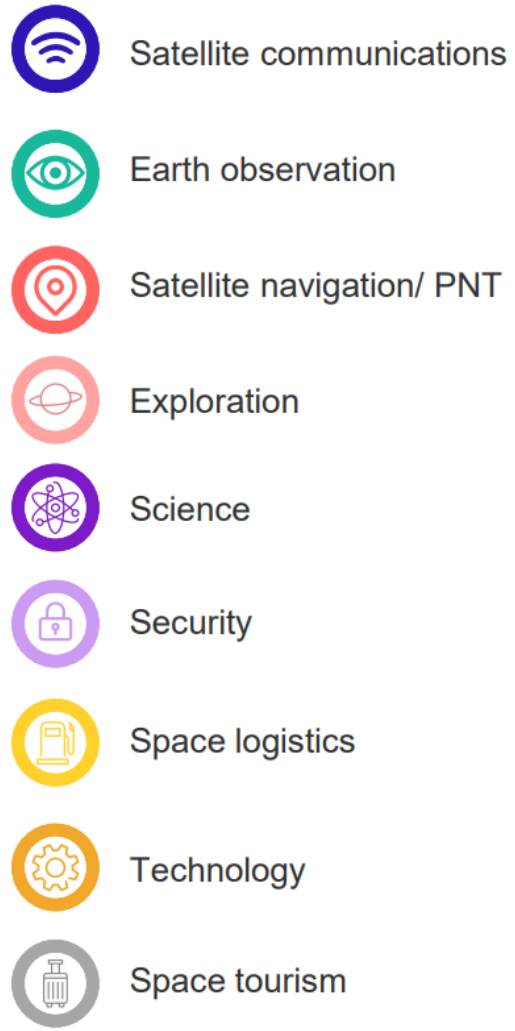
- Activities that are derived from space activities but are not dependent
- Technology transfer

ESA Report on “The Space Economy” 2024

- Type of customers: Commercial, Civil government, Defense

SPACE MISSIONS

- Missions
  - Satellite Communication
    - Telecommunications, television broadcasts, internet access, and more
    - COMSATCOM, GOVSATCOM, MILSATCOM
  - Earth observation (EO)
    - Weather, Environmental monitoring, Geospatial mapping
  - Satellite navigation
    - Galileo/GPS/GLONASS/BEIDOU (GNSS), EGNOS/IRNSS/QZSS(SBAS)
  - Exploration and scientific
    - Lunar, interplanetary, deep space, astrobiology
  - Security
  - Human Spaceflight
  - Commercial missions
  - Planetary defence

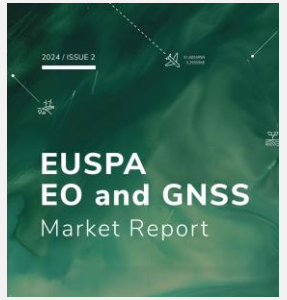


Source: EUROCONSULT SPACE ECONOMY REPORT 2024

MARKET APPLICATIONS

- Agriculture
- Critical infrastructures
- Aviation and drones
- Maritime
- Telecommunications
- Environmental monitoring
- Security and defense
- Scientific research
- Transportation
- Insurance and Finance

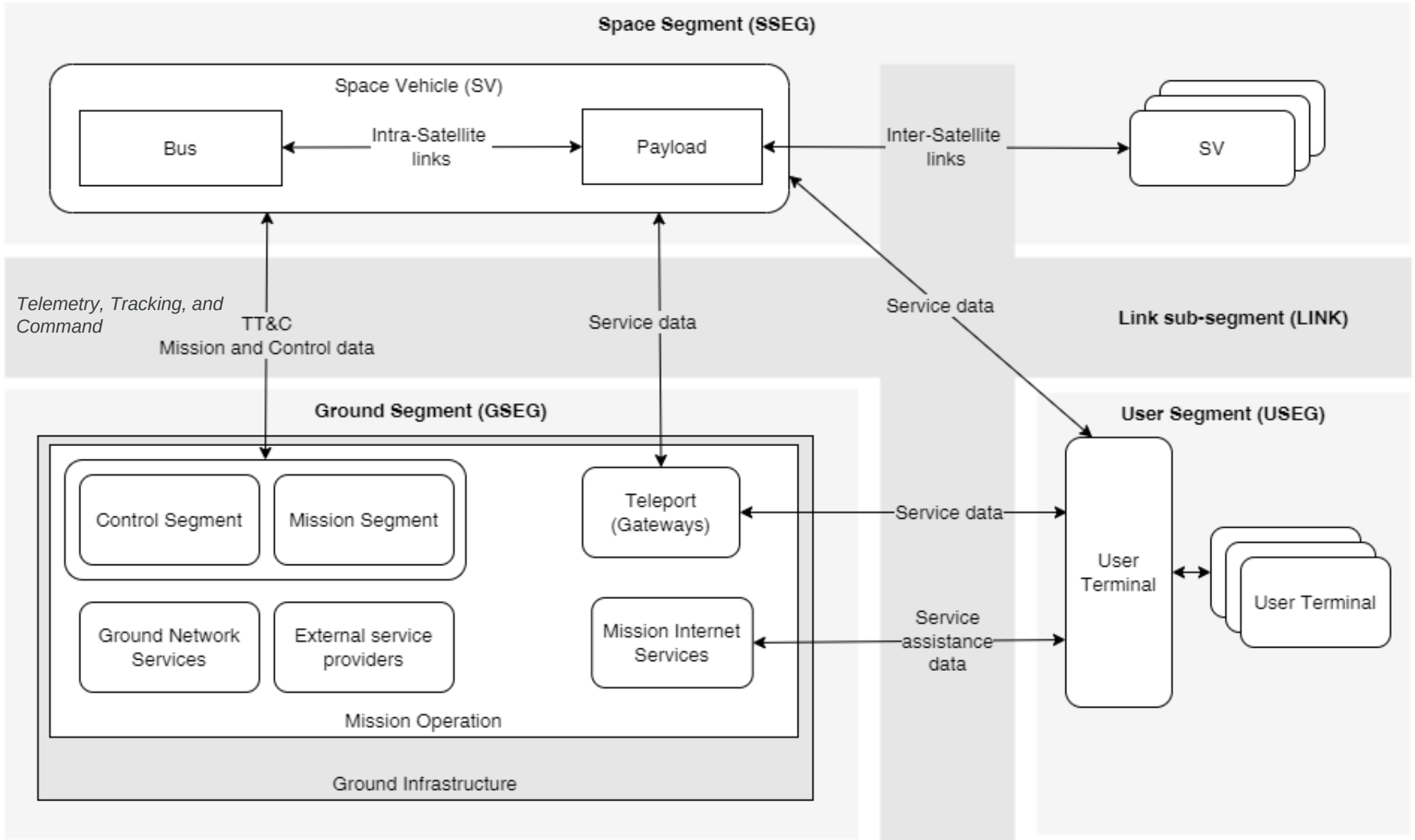
- **Galileo**
  - European Global Navigation Satellite System
    - 30 in-orbit spacecraft (24 in full service and 6 spares)
    - Orbital altitude: 23,222 km
  - Services
    - Open Service (OS)
    - High Accuracy Service (HAS)
    - Public Regulated Service (PRS)
    - Search and Rescue Service (SAR)
    - Galileo Emergency Warning Satellite Service (EWSS)
    - Open Service Navigation Message Authentication (OSNMA)
    - Signal Authentication Service (SAS)
    - Timing Service (TS)
  - Market applications
    - EUSPA Market Report (link)



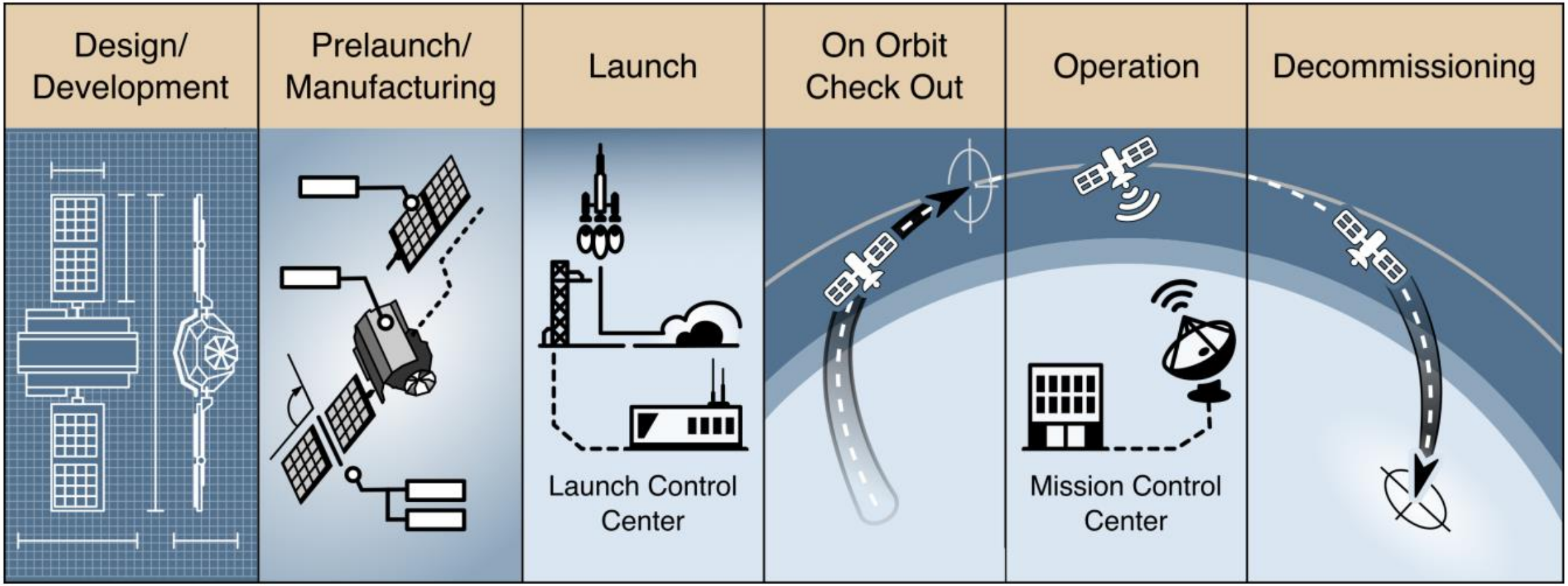
2.

The security needs of the space industry

GENERIC SATCOM ARCHITECTURE



MISSION PHASES

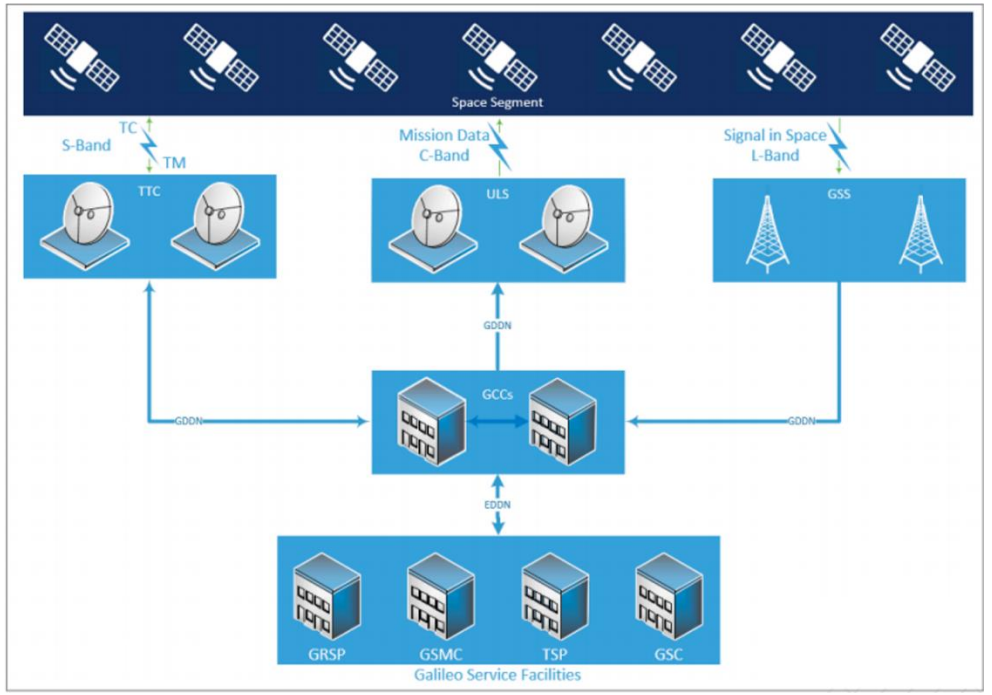


Picture Source: Introduction to Cybersecurity for Commercial Satellite Operations, NISTIR 8270

GALILEO ARCHITECTURE

- Example of a satellite system architecture (Galileo)

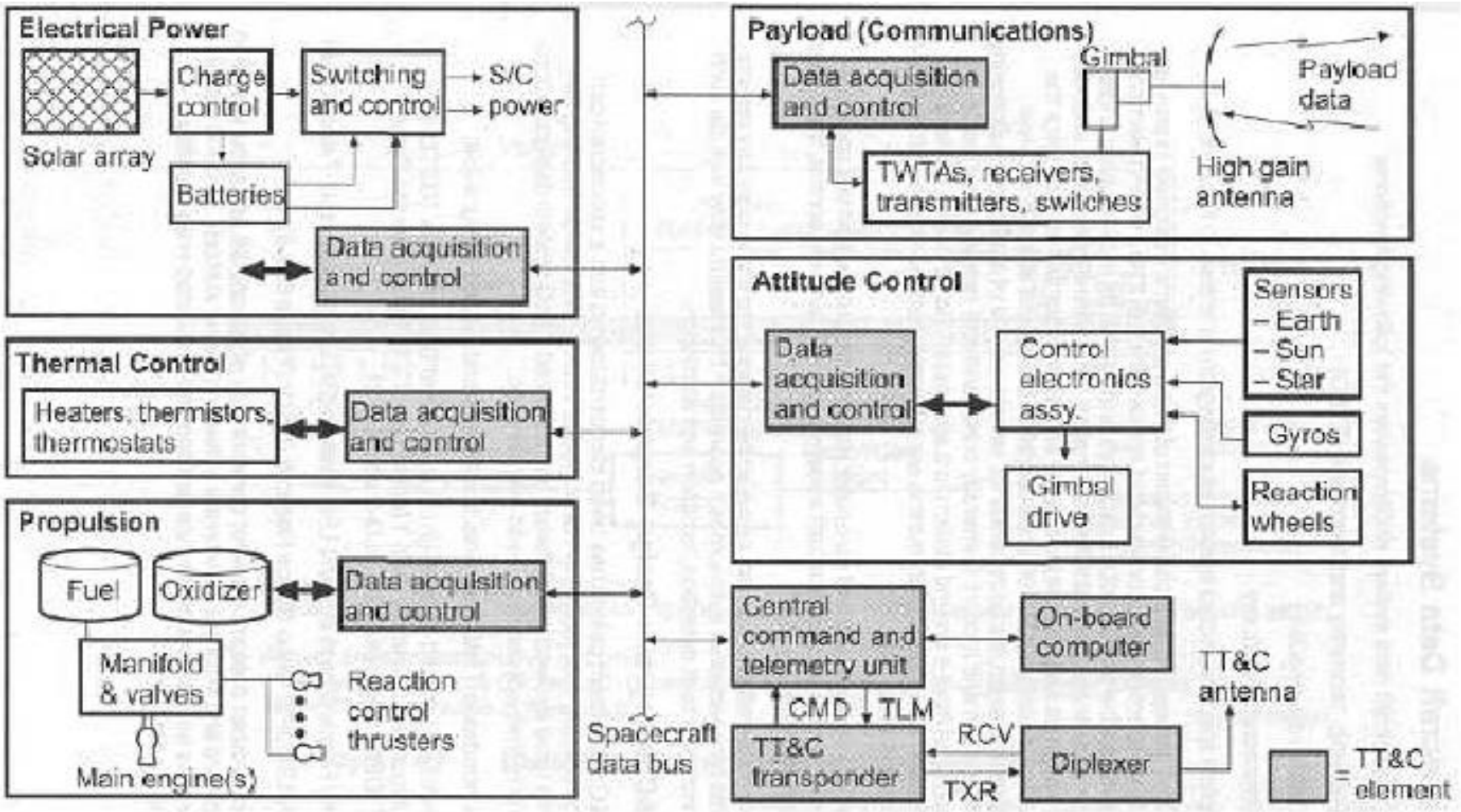
- **GROUND SEGMENT**
  - Galileo Control Segment (GCS)
    - 2x Galileo Control Centres (GCC IT/DE) and the six globally distributed Telemetry Tracking and Control (TT&C) stations
    - A hybrid Communication Network interconnects the remote stations (ULS, GSS, and TT&C stations) with the GCC by different means of standard and special radio, wired data and voice communication links, assuring the communication between all the sites.
  - Galileo Mission Segment (GMS)
    - Facilities deployed in the two Galileo Control Centres (GCCs) plus a series of Mission Up-Link Stations (5x ULS) and Galileo Sensor Stations (GSS) deployed at remote sites located around the world



[Galileo Ground Segment - Navipedia]

GENERIC SATELLITE ARCHITECTURE

- Generic Space Vehicle architecture (block diagram)



Souza, P. N.: CITS Lecture Notes. Slides - INPE - (2002)

SECURITY NEEDS

- CIA (Confidentiality, Integrity, Availability) vs AIC
- Context est., security objectives, SRA (ISO 27005, EBIOS)
- Security goals/objectives and business goals need to align
  - Evaluation of a loss of CIA in terms of
    - Safety
    - Financial
    - Legal / Compliance
    - Business / Strategy
    - Reputation
- Space missions have unique security needs due to the harsh environment, long distances, and critical nature (or impact) of their operations and applications.
- Security domains

- Cybersecurity
  - Protecting against cyberattacks
  - Securing communication links
  - Ensuring data security
- Physical Security
  - Securing ground infra. and stations
  - Protecting launch facilities
  - Securing supply chains
- Operational Security
  - Contingency planning and incident management
  - Secops
  - Personnel security

SECURITY NEEDS (EXAMPLE)

- Global Navigation Satellite System
  - Who are the users of the service?
  - How is the service used?
  - What is the impact of a CIA loss?
    - Safety
    - Financial
    - Legal / Compliance
    - Business / Strategy
    - Reputation
- How can we avoid a CIA loss?
- Why is it important to have a European GNSS system?

3.

Security threats of space missions

THREAT SOURCES

Adversarial Sources:

- ☐ terrorists and criminals;
- ☐ foreign intelligence services;
- ☐ subversives or political activists;
- ☐ computer hackers;
- ☐ commercial competitors;

Insider Sources:

- ☐ dishonest maintenance personnel;
- ☐ dishonest systems personnel;
- ☐ disgruntled staff members;
- ☐ trusted business partners;
- ☐ inadvertent actions of staff members;
- ☐ rogue astronauts;

Environmental Sources:

- ☐ natural or man-made disasters;
- ☐ pandemics;
- ☐ space weather (e.g., solar flares);
- ☐ space debris;
- ☐ infrastructure failures/power outages;

Structural Sources:

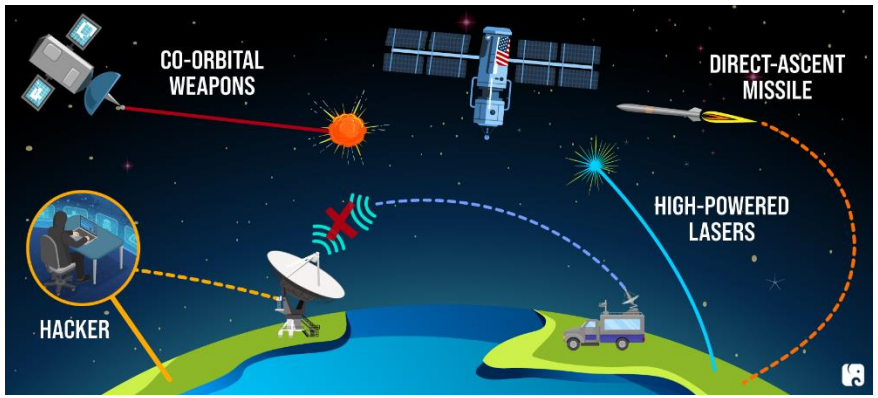
- ☐ software failures;
- ☐ hardware failures.

[Threats to the U.S. in Space]

SECURITY THREATS

- Threat intelligence and public knowledge bases
  - MITRE ATT&CK ®: A knowledge base of adversary tactics and techniques based on real-world observations. Used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
  - The ESA SPACE-SHIELD: An ATT&CK® like knowledge-base framework for Space Systems. It is composed by threats that are relevant for Space systems, leveraging the available and related literature.
  - SPARTA: Another instance of MITRE ATT&CK (tailored for space) that is well maintained/updated by the Aerospace Corp. (nonprofit org. founded in the ’60).

Reconnaissance 6 techniques	Resource Development 4 techniques	Initial Access 5 techniques	Execution 3 techniques	Persistence 4 techniques	Privilege Escalation 2 techniques	Defense Evasion 4 techniques	Credential Access 4 techniques	Discovery 4 techniques	Lateral Movement 4 techniques	Collection 2 techniques	Command and Control 3 techniques	Exfiltration 5 techniques	Impact 12 techniques
Active Scanning (RF/Optical) (4)	Acquire or Build Infrastructure (4)	Direct Attack to Space Communication Links (2)	Modification of On Board Control Procedures modification	Backdoor Installation (5)	Become Avionics Bus Master	Impair Defenses (1)	Adversary in the Middle (1)	Key Management Policy Discovery	Compromise a Payload after compromising the main satellite platform	Adversary in the Middle (2)	Protocol Tunnelling	Exfiltration Over Payload Channel	Data Manipulation (3)
Gather Victim Mission Information (3)	Compromise Account (1)	Ground Segment Compromise (2)	Native API	Key Management Infrastructure Manipulation (2)	Escape to Host (1)	Indicator Removal on Host (1)	Brute Force (1)	Spacecraft's Components Discovery	Compromise of another partition in Time and Space Partitioning OS or other types of satellite hypervisors	Data from link eavesdropping (3)	Telecommand a Spacecraft (3)	Exfiltration Over TM Channel	Ground Segment Jamming (1)
Gather Victim Org Information (3)	Compromise Infrastructure (2)	Supply Chain Compromise (3)	Payload Exploitation to Execute Commands	Pre-OS Boot (1)		Masquerading	Communication Link Sniffing (1)	System Service Discovery	Compromise the satellite platform starting from a compromised payload		TT&C over ISL	Optical link modification	Loss of spacecraft telecommanding (1)
In orbit proximity intelligence (6)	Develop/Obtain Capabilities (9)	Trusted Relationship (3)		Valid Credentials (3)		Pre-Os Boot (1)	Retrieve TT&C master/session keys (3)	Trust Relationships Discovery	Lateral Movement via common Avionics Bus			RF modification	Permanent loss to telecommand satellite (1)
Passive Interception (RF/Optical) (4)		Valid Credentials (3)										Side-channel exfiltration	Resource damage (7)
Phishing for Information (2)													Resource Hijacking
													Saturation of Inter Satellite Links (1)
													Saturation/Exhaustion of Spacecraft Resources (5)
													Service Stop (2)
													Spacecraft Jamming (3)
													Temporary loss to telecommand satellite (1)
													Transmitted Data Manipulation

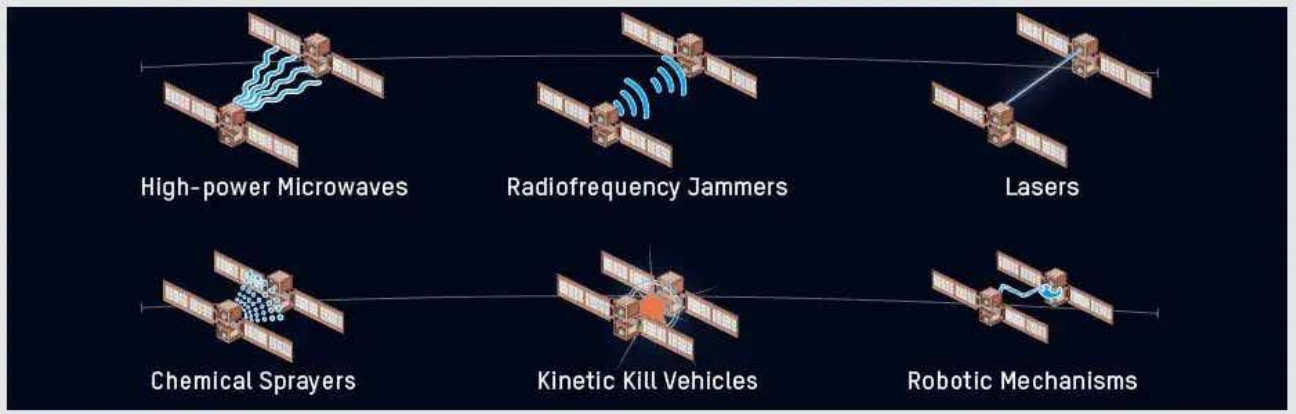


Threats to the U.S. in Space

SECURITY THREATS

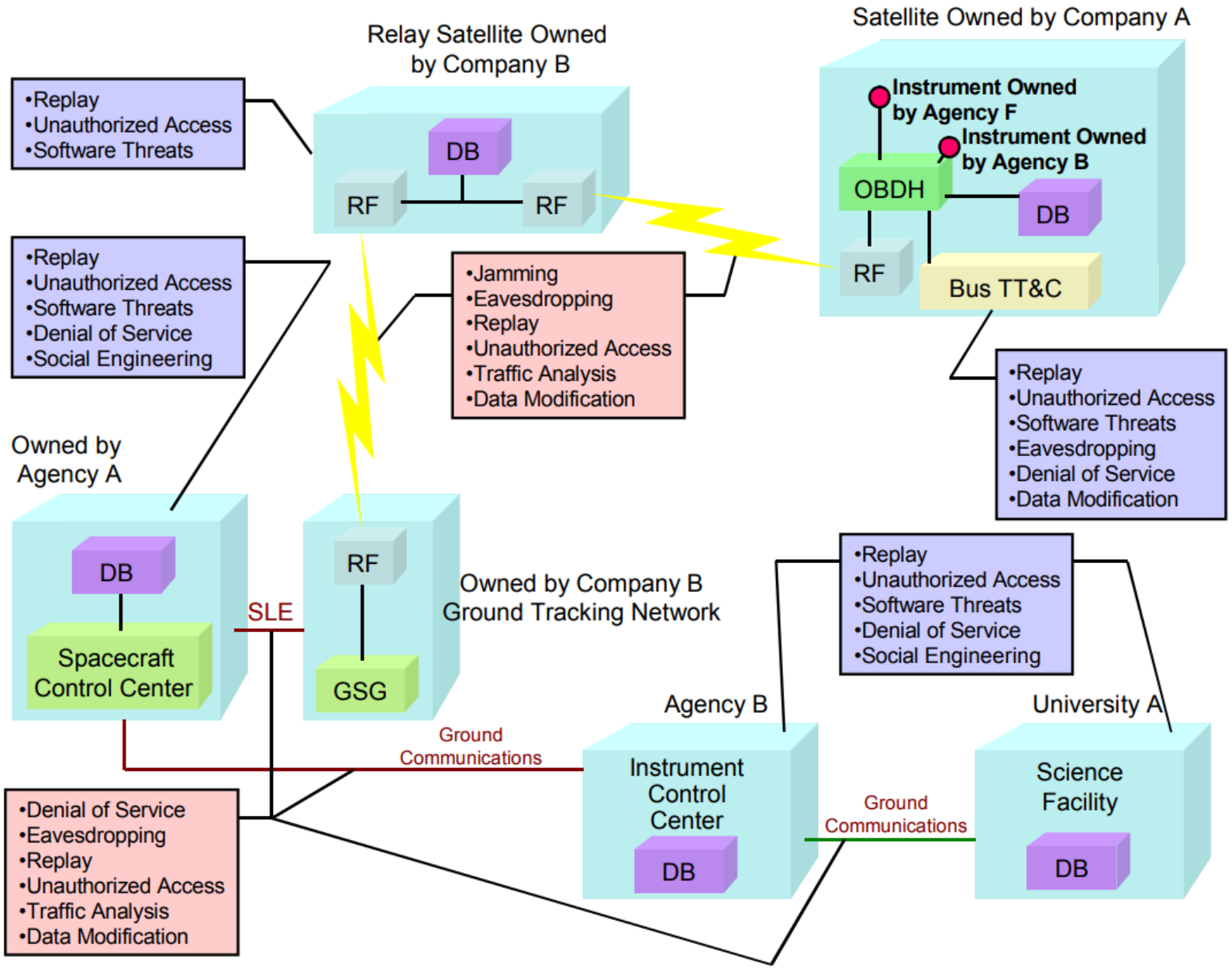
SSEG	
Physical and Electromagnetic Damage	Weapons, Environmental damages Space-based attack
Cybersecurity Attacks	Cryptographic Attacks Exploit vulnerabilities DoS, Malware injection Payload control, Process Lineage Analysis

USEG	
Physical Security Attacks	Environmental or accidental damage Unauthorized physical access Deliberate damage
Attacks on the network	Modification Interference, Interception
Attacks on users	Prevent personnel availability Misuse, Exfiltration of information
Logical security Attacks	Cryptographic Attacks Password, credential and session attacks Exploit vulnerabilities Drive-by-Download Process Lineage Analysis



GSEG	
Physical Security Attacks	Environmental or accidental damage Unauthorized physical access Deliberate damage
Attacks on the network	Modification Interference, Interception
Side-channel attacks	Attacks to the working environment Supply Chain Threats
Attacks on personnel	Prevent personnel availability Misuse, Exfiltration of information
Logical security Attacks	Cryptographic Attacks Password, credential and session attacks Exploit vulnerabilities Drive-by-Download Process Lineage Analysis

SECURITY THREATS



CCSDS 350.1-G-3

System / Network

- Replay
- Link Jamming
- Interception (theft)
- Unauthorized Access
- Software Threats
- Traffic Analysis
- Data Modification
- Hardware Failures
- Supply Chain Threats

Space Elements

- Space Debris
- Replay
- Link Jamming
- Unauthorized Access
- Software Threats
- Data Modification
- Hardware Failures
- Supply Chain Threats

Users

- Interception
- Software Threats
- Social Engineering
- Physical Attacks

Control

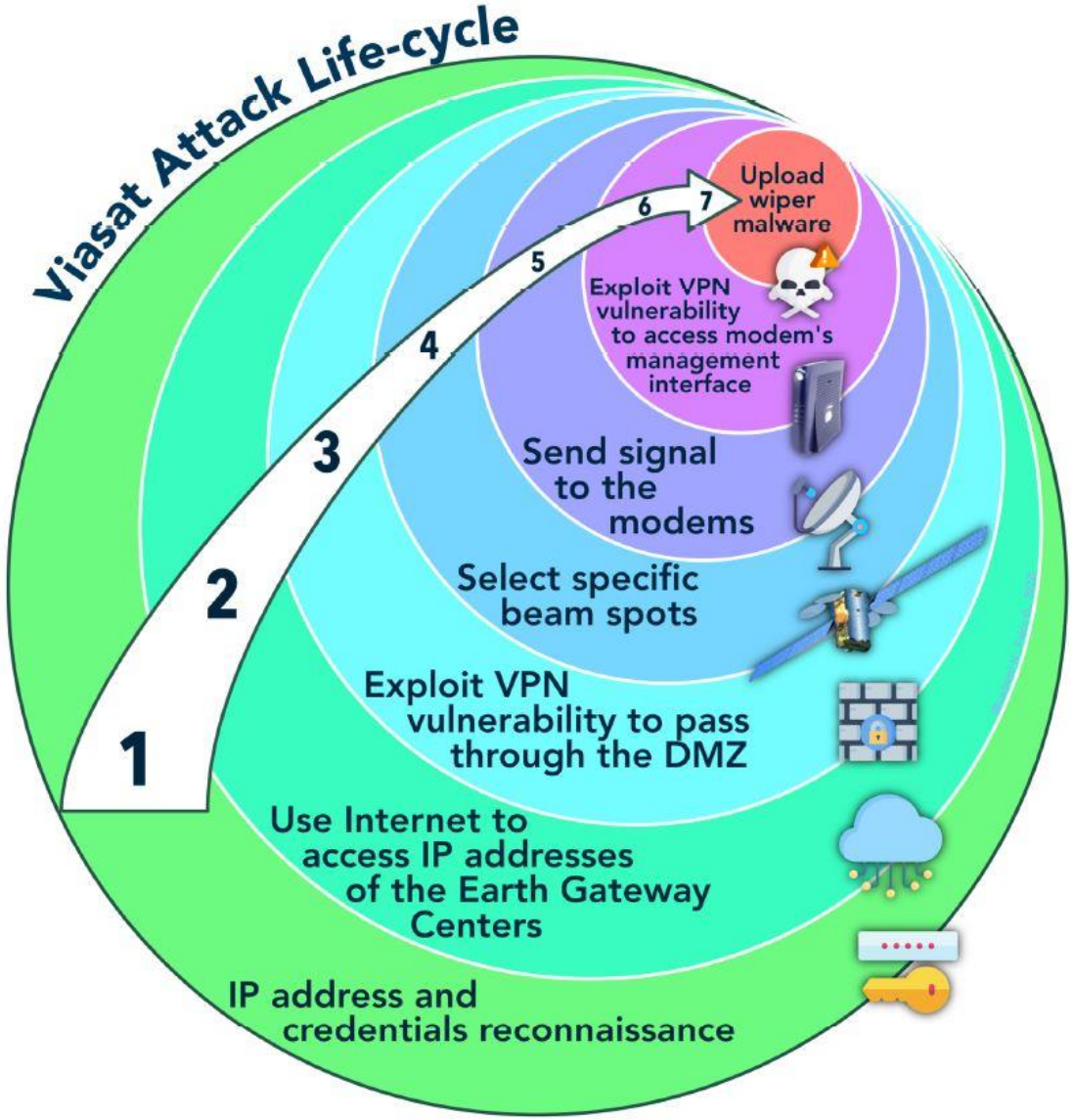
- Replay
- Unauthorized Access
- Software Threats
- Social Engineering
- Physical Attacks
- Data Modification
- Hardware Failures
- Supply Chain Threats

SECURITY THREAT EXAMPLE

- The VIASAT cyberattack in Feb. 2022
  - Viasat offers mobile two-way satellite broadband telecom services (it can support military applications)
  - 23 Feb. 2022. Hackers gain access to mng services through a VPN installation in a mng center in Italy.
    - Exploitation of a misconfiguration in a VPN appliance to gain remote access to the trusted management segment of the KA-SAT network
    - Lateral movement through this trusted network to a specific network used to manage and operate the network.
    - Upload wiper malware (AcidRain) to specific modems.
  - 24 Feb. 2022. Russia invades Ukraine
- Impact [1]
  - Thousands of Viasat modems went offline → loss of internet access
  - Potential to threaten government or military objects
  - Impacted the civilian population and civilian objects
  - Impacted a major German energy company who lost remote monitoring access to over 5,800 wind turbines
  - In France nearly 9,000 subscribers of a satellite internet service provider experienced an internet outage.
  - In addition, around a third of 40,000 subscribers of another satellite internet service provider in Europe (Germany, France, Hungary, Greece, Italy, Poland) were affected

SECURITY THREAT EXAMPLE

- Detailed information on the attack
  - An analysis of the Viasat cyber attack with the MITRE ATT&CK® framework (link)
    - Mapping to TTPs of MITRE ATT&CK framework
  - Space Cybersecurity Lessons Learned from The ViaSat Cyberattack from Nicolò Boschetti (Cornell University), Nathaniel Gordon (Johns Hopkins University) and Gregory Falco (Cornell University) (link)
  - AcidRain | A Modem Wiper Rains Down on Europe by SentineOne Team (link)



4.

Security standards and practices

STANDARDS, GUIDELINES, BEST-PRACTICES

- Nowadays there is no a single “Security Standard”
- Agencies and organizations defines applicable requirements for the missions / programs (tailored)
- Standards (e.g., CCSDS) exist for some aspects (e.g., protocol, operations)
- There are several good source of guidelines and practices
- There is a strong push to evolve existing engineering standards to include safety aspects

[ECSS-E-ST-80C – Space engineering – Security in space systems lifecycles (1 July 2024)]

STANDARDS, GUIDELINES, BEST-PRACTICES

Reference	Takeaways
BSI TR-3184 Infosec for Space Systems	• Satellite lifecycle process • Reference Architecture • 53 threats vs 59 security measures
SP800-53r5	• Good source of control language & control cross-reference
ISO/IEC 27000 FAMILY / ISO 27002:2022	• Manageable control framework • considerable overlap between its “Organisational” and “Technological” controls
US SPD-5	• 6 areas for SV protection
SPARTA / ATT&ACK / D3FEND / ESA SPACE-SHIELD	• Validation of attack patterns & check countermeasures
NASA Best Practices Guide	• Threat Actor Capabilities / Tactics • Architecture for Space Mission vs Ground Mission
NIST CSF 1.1/2.0	• Breakout of Governance as its own Function • Function alignment for defensive measures
CCSDS Green/Magenta Books	• Alignment of threat models to satellite missions • Mapping of threats to mission impacts • CCSDS Security framework aligned to ISO 27001
AEROSPACE TOR-2021-01333-REV.A	• Satellite attack patterns aligned to defensive measures • Satellite Vehicle requirements architecture (43 requirements in 7 groups)
CYBERSECURITY IN SPACE (KAVALLIERATOS)	• Space Threat taxonomy chart (not quite an attack tree)
SATCOM Terminal Hacking Paper	• Threat model regarding SATCOM user devices (not discussed much elsewhere)
CIS-18	• Overall framework and assessment methodology

Thank you!

Carlo Sarto
carlo.sarto@qascom.it

EVALUATION TEST

1. What does "TT&C" stand for in the context of satellite operations? (single answer)
   a) Telemetry, Tracking, and Command
   b) Telecommands, Telemetry and Control
   c) Threat, Tracking, and Countermeasures
   d) Transmission, Targeting, and Control

2. Why is zero-day vulnerability exploitation particularly dangerous in the space sector? (multiple answer)
   1. Satellites are often physically inaccessible for patching.
   2. The long communication delays make rapid response difficult.
   3. The potential impact of a successful attack is very high.
   4. All of the above.

3. What are the main phases of a space mission life-cycle? Can you give an example of threats during the production/manufacturing phase?

4. What are the main segments of a generic SATCOM mission? Which of these is/are most important to protect? Why?