Trusted and Resilient Earth Observation Infrastructures – Cybersecurity as a Foundation for Reliable Decision-Making

Annual Meeting CAETS 2026

Claudia Eckert, President acatech

acatech

NATIONAL ACADEMY OF SCIENCE AND ENGINEERING

Agenda

1. Why is the topic strategically important now?
2. Earth Observation (EO) Infrastructure and it‘s Terrestrial Impact
3. EO Infrastructure: a Complex System of Systems
4. Attack Surface
5. Protecting EO Infrastructure
6. Take Home Message

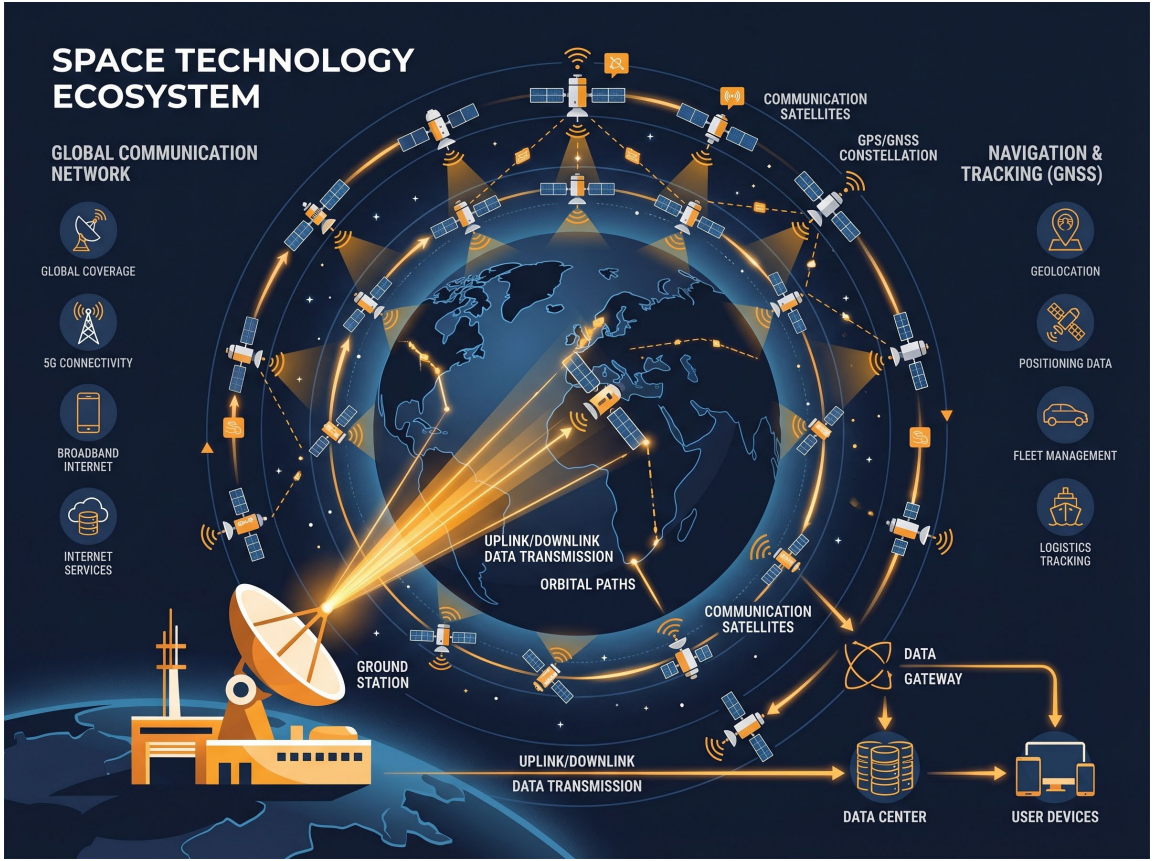
1. Why is the topic strategically important now?
Conflicts and hybrid threats increasingly extend into space systems

- 2022: attack by Russian hackers on the Viasat KA-SAT network at the beginning of Russia's full-scale invasion disrupted communications in Europe.
- 2026: Recent geopolitical conflicts have been accompanied by increased cyber activity targeting satellite and ground-based space infrastructure.
- Threats directed at (small) satellites and at ground stations as well as disruptions to GNSS signals;
  space debris, space weather and dependencies on external providers.

- **Space is not only an operational domain.**
  It is part of a networked critical infrastructure.
- **Compromised components, data, information leakages have immediate consequences on Earth.**

acatech

2. Earth Observation Infrastructure and it‘s Terrestrial Impact



2. Earth Observation Infrastructure and it‘s Terrestrial Impact

Why trusted space-based information matters on earth

Communication

Resilient connections, redundancy in the event of terrestrial network failures and reaching remote regions

Navigation & Timing

PNT for transport, logistics, financial market timing and synchronization of technical systems

Energy & Grids

Earth observation for routes, leaks and changes in critical facilities

Transport & Logistics

Routes, fleets, maritime situational awareness and supply chains

Environment & Agriculture

Detecting drought, vegetation, wildfire risk and resource management; enabling precision farming

Crisis Management

Situational awareness, early warning and coordination of disaster response and rescue operations.

3. EO Infrastructure: a Complex System of Systems

Many Components and Dependencies

Orbit

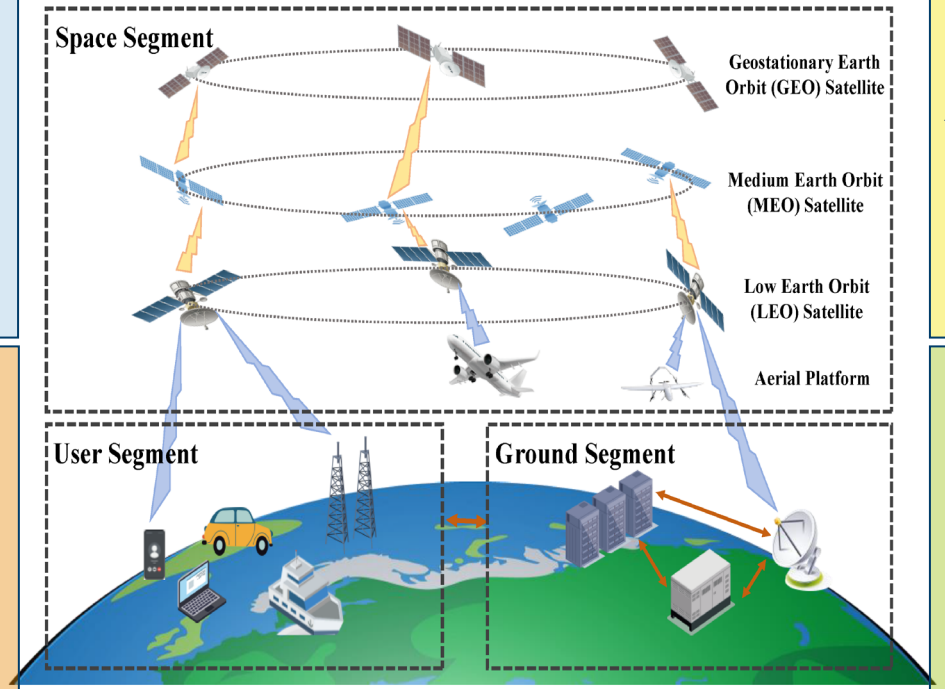
Space Segment: e.g.

- Satellites (e.g. LEO)
- Electrical Power Subsystem
- Communication, Control

Ground

Ground Segment

- Ground stations
- Antennas
- Telemetry, tracking and control
- Data processing



Source: Wang, B. et al.. A Comprehensive Literature Review of Cybersecurity in Satellite. *Aerospace* **2026**, *13*, 249. https://doi.org/10.3390/aerospace13030249

Users / Critical Services

Applications on Earth

- Public sector
- Infrastructure operators
- Industry and economy
- Citizens and society

Data & Services

Processing and distribution

- Data storage (on-premise and cloud)
- Analytics, value-added services

Challenge: Expanding and Evolving Attack Surface!

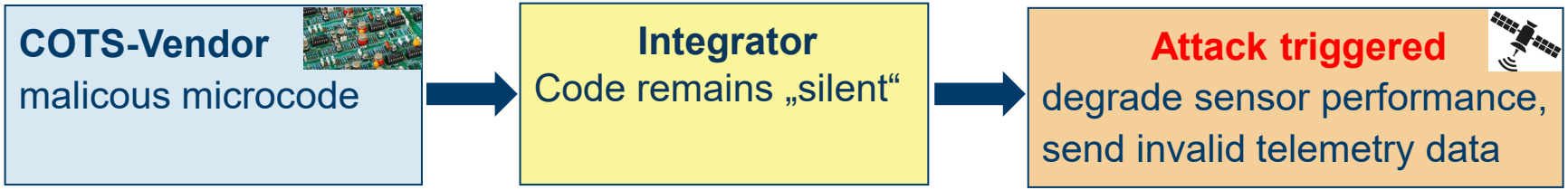
acatech

4. Attack Surface: Expanding and Emerging

Democratized space leads to an emerging threat landscape

1. Satellites: >12,000 active satellites

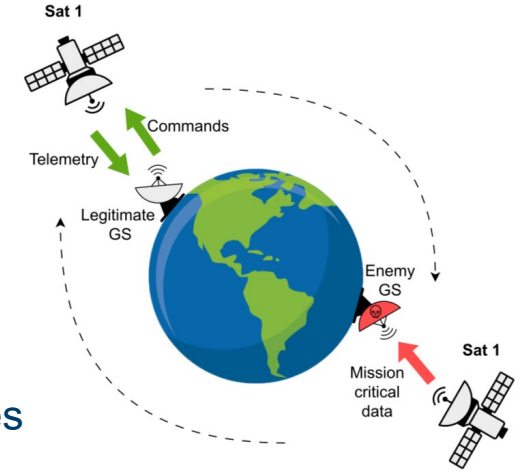
- **COTS** (*commercial of the shelf*) components replace custom-made, trusted hardware:
  - Lacking verified trust: implicit trust in multi-national supply-chains
    Operational impact: Bypassing network detection, unauthorized takeover



- **Vulnerable Onboard Computers:** exploited e.g. via firmware updates
  - Lacking internal separation: unsafe update paths, disable critical functions

acatech

4. Attack Surface: Expanding and Emerging



2. Ground Stations:

- **Vulnerable Gateways:** exploited e.g. via fake ground endpoints
  - Lacking authenticated ground components: loss of control
- **Vulnerable Data processing:** exploited e.g. via corrupted data
  - Lacking integrity checks: attacked ML triggers false activities

3. Communication:

- **Vulnerable: TT&C:** exploited e.g. via command injection over legacy links
  - Lacking link authentication: altering of attitude, disabling subsystems
- **Vulnerable Inter-Satellite-Links** (for coordination)**:** exploited e.g. via link flooding
  - Lacking rate-limitations, lacking isolation: overloading ISLs, bypass defence

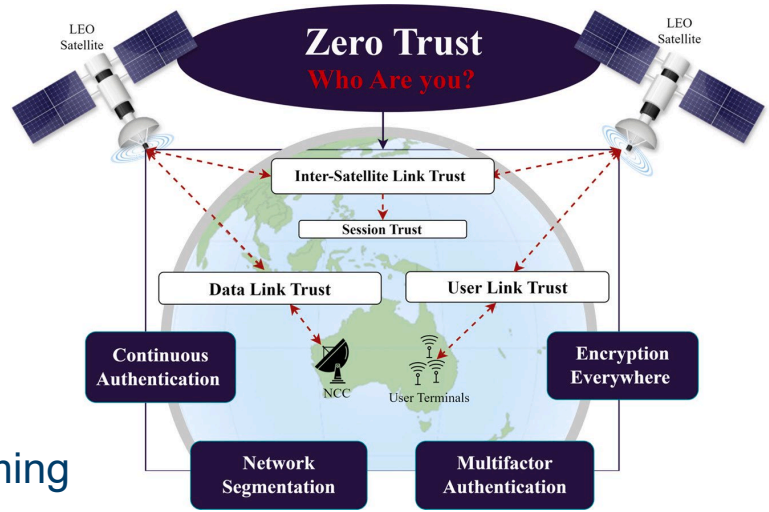
Security needs are obvious: Authentication, isolation, integrity checks. Learn from Enterprise Security Architectures and just do it?

Source: Vanlyssel et al., SpyChain: Multi-Vector Supply Chain Attacks on Small Satellite Systems, *arXiv* **2025**, https://doi.org/10.48550/arXiv.2510.06535

5. Protecting EO Infrastructure

Terrestrial Security Measures (e.g. NIST 800-53)

- Zero-Trust: *Never Trust, Always Verify paradigm*
- Trusted Hardware, Verified Software Artefacts
- Strong Authentication with Multi-Factors
- End-to-End Encryption with state-of-the art Crypto
- Vulnerability Management



Positive: lost of standard solutions applicable

- Hardware Security, Application Isolation, Anti Jamming

Negative: Resource-limitations require adaptions

- Security-per-Watt Paradigm
- Limited Contact Windows
- Distributed Security Paradigm

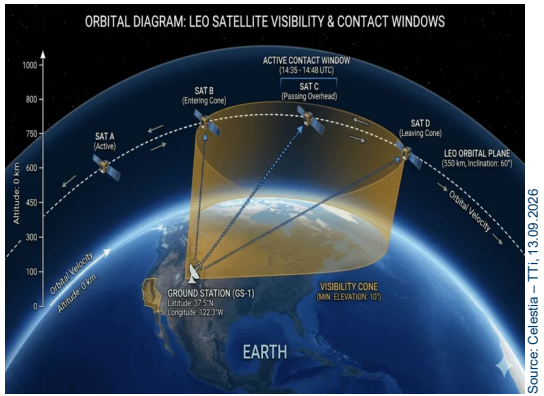
Source: Farrea et al., Zero trust-based authentication for Inter-Satellite Links in NextGen Low Earth Orbit networks, *Ad Hoc Networks* **2025**, 174, 103817, 10.1016/j.adhoc.2025.103817

acatech

5. Protecting EO Infrastructures

Selected Constraints and their impact on security

- **Security-per-Watt (SpW) Paradigm** versus expensive traditional security protocols
  - lightweight yet effective countermeasures tailored to orbital constrains, e.g. SDLS
- **Limited Contact windows** (8-12 minutes)
  - Adapting Zero Trust Architectures (ZTA) to **Event-of-Contact-Driven** ZTA
  - Bundled operation for authentication, keys exchange



Source: Celestia – TTI, 13.09.2026

- **Distributed Security Paradigm**:
  - limited contacts, big delays: **decentralised incident handling capabilities** required
  - **Signed artifacts**: updates, configuration changes must be cryptographically signed.
  - **Rate-limiting**: Bounding the impact of compromised nodes
  - **Control-payload partitioning**: Separating commands from payload data

acatech

Open Research Challenges: The Frontiers of Orbital Trust

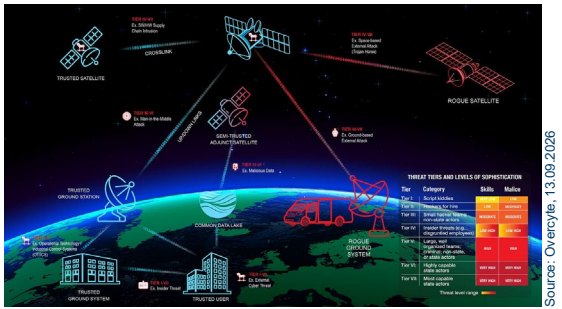
Security baselines are insufficient for long-term mission assurance

- **Lightweight Post-Quantum Cryptography (PQC):**
  - Defence against “store now, decrypt later”, current solutions are not appropriate
- **Autonomous AI-Driven Threat Detection:**
  - New measures for robust AI to provide trustworthy data
- **Zero-Trust for Dense LEO Swarms:**
  - New lightweight but trustworthy protocols to manage identities and authorization in swarms of thousands of satellites
- **Protecting Edge-AI Pipelines:**
  - Onboard processing using AI will increase.
  - New methods to protect the pipelines against adversarial inputs that try to trick models into misclassifying terrestrial features.

Take Home Message

Today:

- Compromised Components of EO-Infrastructure directly affect vital terrestrial sectors.
- Democratized space leads to an emerging threat landscape.



Source: Overcyte, 13.09.2026

Tomorrow:

- Standard security solutions are directly applicable: **apply them**!
- Special adaptations are required: **develop them**!

The way forward:

- Defense against "store now, decrypt later" with lightweight PQC solutions.
- Protect onboard Edge-AI processing across dense LEO satellite swarms with robust AI.

Securing the full pipeline – from orbit to ground stations, data processing, and end-users – is vital for long-term mission assurance

acatech

Thank You for your Attention

Contact
Claudia Eckert, President acatech
Claudia.Eckert@acatech.de

acatech
NATIONAL ACADEMY OF SCIENCE AND ENGINEERING