CYBERSECURITY CHALLENGES IN SATELLITE SYSTEMS

Monika Adamczyk
Cybersecurity Expert
monika.adamczyk@enisa.europa.eu

22 05 2024
Our mission is to achieve a high common level of cybersecurity across the Union
AREAS OF WORK

Cloud and Big Data
COVID19
Critical Infrastructures and Services
CSIRT Services
CSIRTs and communities
CSIRTs in Europe
Cyber Crisis Management
Cyber Exercises
Cybersecurity Education
Data Protection
National Cybersecurity Strategies
NIS Directive
Standards and Certification
Threat and Risk Management
Cyber Crisis Management
IoT and Smart Infrastructures
Trust Services
Trainings for Cybersecurity Specialists
ENISA GUIDANCE FOR SATELLITES
SPACE CYBERSECURITY EU POLICIES

EECC Directive

• Commercial satellite operations are part of the telecommunication sector
• Appropriate and proportionate technical and organizational measures to manage the risks posed to the security of public electronic communications networks and services

NIS2 Directive

• Space (operators of ground-based infrastructure) is included as one of the critical sectors
• Appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems which essential and important entities use for their operations or for the provision of their services

EU Space Strategy for Security and Defence

• Creation of an annual classified space threat landscape
• Establishment of an EU Space ISAC
• Proposal for an EU Space Law to cover the part of the space sector, which is not in scope of NIS2
## NIS2 CYBERSECURITY REQUIREMENTS

- Policies on risk analysis and information system security
- Incident handling
- Business continuity (backup and crisis management, disaster recovery)
- Supply chain security
- Security in network and IS acquisition, development and maintenance
- Policies and procedures on effectiveness of risk-management measures
- Basic cyber hygiene practices and cybersecurity training
- Policies and procedures regarding the use of cryptography and encryption
- Human resources security, access control policies and asset management
- Use of multi-factor authentication or continuous authentication solutions
The European Commission and EUSPA are spearheading the formation of the EU Space Information Sharing Centre (ISAC).

Who Can Join?

• **Founding Participants**: those dedicated to shaping the governance of EU Space ISAC. They play a pivotal role in its inception, driving its initial activities and promoting wider participation.

• **Members**: private entities from the EU Space sector, EU academic institutions, and other recognized institutions contributing space sector security knowledge.

• **Public Partners**: entities like EU institutions, bodies and agencies, European Space Agency, national space agencies, and National Computer Emergency Response Teams.

This network-based information-sharing platform promotes collaboration, awareness and best practices among private entities to ensure the safety of our space systems and the networks they rely on.
THREATS, RISKS, CHALLENGES
## USES OF SATELLITE SYSTEMS

<table>
<thead>
<tr>
<th>Application</th>
<th>Example of implementation</th>
<th>Economy Sectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoT</td>
<td>Location tracking of a containers and alerting in case of an anomaly (e.g. door opening)</td>
<td>Transport / Rail</td>
</tr>
<tr>
<td>Network interconnection</td>
<td>Backup trans-national network for the monitoring of European power grids</td>
<td>Energy / Electricity</td>
</tr>
<tr>
<td>Telephony</td>
<td>Satellite-enabled telephony for assessment teams during a disaster with potential destruction / saturation of the terrestrial cell phone networks</td>
<td>Public administration</td>
</tr>
<tr>
<td>M2M</td>
<td>Monitoring and remote operation of hydroelectric plants in remote areas</td>
<td>Energy / Electricity</td>
</tr>
<tr>
<td>Internet access</td>
<td>Backup of terrestrial-based Internet access for the logistics department of a hospital</td>
<td>Health / Healthcare providers</td>
</tr>
</tbody>
</table>
LIFECYCLE

- Design and development
- Assembly
- Prelaunch
- Launch
- On orbit check
- Operations
- Decommissioning
ASSETS
THREATS

Non malicious

- Collisions with other bodies
- Mis-computed manoeuvre
- Platform mis-configured
- Untested COTS components
- Non-compliance to radio regulations
- Payload mis-configured

Malicious

- IT, networks, users
  - Phishing
  - Network traffic sniffing
- Space specific
  - Signal jamming
  - Platform hijacking
- Supply chain
  - Sabotage
  - Software / hardware backdoor
  - Payload mis-configured
  - Non-compliance to radio regulations
ASSOCIATED RISKS

**Technical**
- Degradation/outage of commercial services
- Information theft, forgery
- Hijacking of communication capabilities
- Damage or destruction of assets

**Commercial**
- Harm to the company reputation
- Loss/degradation of competitive advantage
- Loss of commercial capabilities
- Financial loss because of penalties
CHALLENGES

• Shift from analogue to digital, use of COTS and complex supply chain has exposed satellites to a spectrum of cyberthreats ("standard" terrestrial and space specific)

• Coordinated approach in satellite security (physical and cyber) is difficult to achieve

• Effective protection of satellites requires risk based approach and security measures, which must be present in every stage of a satellite lifecycle

• Despite the fact that some of system elements are located thousands kilometres away from Earth does not mitigate their exposure to cyber-attacks

• Cybersecurity in satellites extends beyond the technical realm, affecting international relations, cooperation, and competition
THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Agamemnonos 14, Chalandri 15231
Attiki, Greece

+30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu