



From Simulation to Operations: Smallsat Security in the Space Cyber Range

BY SPACEIT, CYBEXER TECHNOLOGIES, CGI ESTONIA, CR14



The **Space Cyber Range** offers a comprehensive virtual environment for:

- **Testing, validation, and certification of various space assets and processes.**
- **Cybersecurity training and exercises.**
- **Industry knowledge sharing and networking.**

This environment aims to increase the reliability and security of industry participants' solutions while promoting education and knowledge sharing within the space ecosystem.

The Problems We're Solving

Testing, Validation, Certification

- Alteration or corruption of satellite data
- Command injection leading to loss of control
- Faulty orbit and maneuver planning validation
- Verification of secure data exchange between ground & space
- Accreditation according to standards (EU space law)

Cybersecurity Training and Exercises

- Simulating DDoS attacks on mission control centers
- Practicing response to GNSS spoofing and jamming scenarios
- Training teams to detect and counter data exfiltration attempts
- Ransomware and malware drill challenges in ground systems
- Coordinated multi-satellite cyberattack scenarios

Use-Cases in Development

Communications Testing

Connecting FlatSat to the SCR with a virtual Mission Control System and simulated Ground Station. CubeSat manufacturers can test communications, automate protocol checks and evaluate resilience to attacks as delays, replays, and unauthorized commands.

Collision Avoidance Operations

Simulating satellite operators training in collision-avoidance procedures. Attacks aim to raise collision risk or trigger unnecessary maneuvers. Two scenarios: overwhelming operators with false warnings, corrupting data, hide/invent threats.

Remote Integration & Pre-Ait Validation

Enabling remote testing of satellite HW/SW interfaces through a FlatSat setup connected via VPN to the Space Cyber Range. This setup simulates the Assembly, Integration and Test (AIT) phase and supports early procedure development and compatibility checks without needing all hardware in one location.



Space Cyber Exercise

Integrating cybersecurity into traditional spacecraft operations training to simulate cyber-attacks (from Ground IT system to Satellite C&C), defence scenarios, to build skills to detect, analyze and respond to cyber incidents in satellite systems.

Critical Infrastructure Exercise

Testing resilience of critical-infrastructure operators to GNSS timing disruptions. Simulated threats like jamming, spoofing, and signal loss show how timing failures impact Time Servers and cascade through the broader CI network.

Satellite Operator Training

Targeting satellite operations in a simulated Mission Control System, exposing operators to internal system malfunctioning and malicious attacks: Coworker Account Hijack, Unexpected Power Drain, Forgotten Ground Watchdog Reset, Intentional System Modification.

A Growing European Collaboration

- **SCR** officially kicked off in **January 2025**.
- SCR will reach Initial Operational Capability in **Q2 2026**.
- **Development according to the initial plan.** Technology Phase/CDR successfully completed, Product phase started in September 2025.
- Some of the SCR technologies are already in use in leading cybersecurity exercises, including **NATO CCDCOE's Locked Shields** (over 4,000 participants).
- SCR has also been included in various other European space cybersecurity related initiatives.



Developing Consortium



SPACEIT

CybExer

CGI

CR14

- Spaceit delivers software solutions for satellite operations and space cybersecurity. Company's software ensures satellite missions benefit from automated operations, low latency, high data rates, and robust security. It is also utilized in large-scale live-fire cyber defense exercises. Spaceit operated OPS-SAT ORIOLE mission will launch in 2026 and will feature a thermal camera and an optical communication terminal in space and on the ground.
- Provides sophisticated cybersecurity training platforms with a focus on cyber capability development. The company has a strong technical and organizational foundation in developing and maintaining advanced cyber security solutions, incl. organizing and executing complex cyber drills, exercises, and hackathons for NATO, the EU, and national entities.
- Developing software for space applications since 2010, focusing on mission-critical and security-relevant elements. The company works extensively with ESOC, ESRIN, and ESAC, creating a strong network in the European space sector, particularly in Estonia and Finland, incl. designing the second-generation ground segment for Galileo, contributing key management facilities, security components.
- Established by the Estonian Ministry of Defence to offer cybersecurity-related research and development for both domestic and international partners. Over 12 years of experience in cybersecurity training, exercises, testing, validation, and experimentation with a focus on military-grade cyber range, incl. collaborations with private and public sector partners globally.

Thank you!



Cybersecurity

ESA Funds New Estonian Space Cyber Testing and Training Ground

By Mark Holmes | January 24, 2025

APPLICATIONS

Estonia to host Europe's new space cybersecurity testing ground

