Satellite Security and Post-Quantum-Cryptography

22 JUNE 2025

Heiko Radde



Heiko Radde

Protecting Satellites from Threats: A Post-Quantum Cryptography Field Test
Timeframe: 01/01/1990 – 22/06/2025
France · Conflict Prevention · Issue VII

Key Insights

- Is current satellite cybersecurity sufficient to address emerging threats, especially with rising space reliance? Most commercial satellites still rely

on outdated or minimal cybersecurity measures. Many use “security by obscurity,” and standard communication protocols either lack security or use weak static keys. Meanwhile, satellites are becoming critical infrastructure and increasingly targeted in cyber conflicts. Current satellite security is inadequate – it must be strengthened.

Definition

A KEM is a triple of algorithms KEM = (KeyGen, Encaps, Decaps)

Spacecrafts are in essence embedded systems

Documents: ☐ Full Publication (PDF) ☐ Source Document

DOI 10.69790/epis07.32892

EPIS