SPACE CYBERSECURITY WEEKLY WATCH

W3

January 13 – 19, 2026

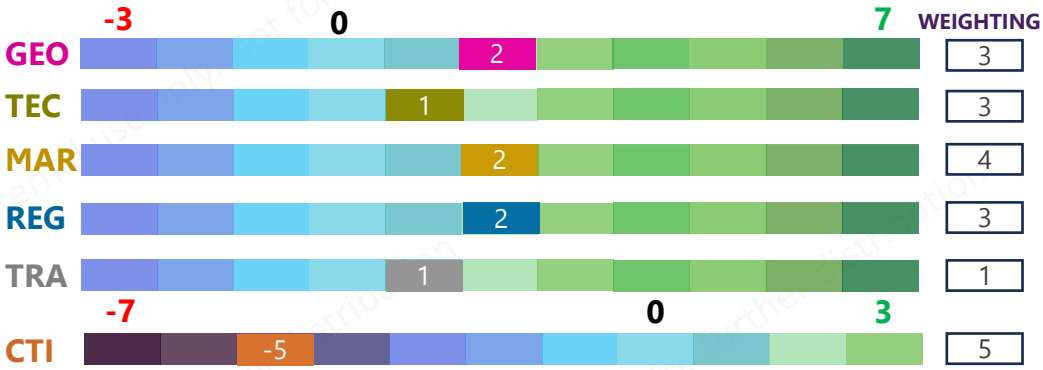
Timeframe: Weekly
# of articles identified: 17
Est. time to read: 35 minutes

Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

- GEOPOLITICS
- TECHNOLOGY
- MARKET & COMPETITION
- REGULATION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- IMPORTANT NEWS

RISC Score Assessment

Overview & Resilience Index for Space Cybersecurity (RISC)



The RISC score for this watch is -1.0, a decrease from last week. This difference is due to a drop in the threat landscape and a tense geopolitical climate. The situation is balanced by some regulatory news.

RISC Score changes in 2026

In 2026, CyberInflight updated its methodology for calculating the RISC Score to better reflect observed realities. The scoring ranges for some categories were adjusted, as these were rarely assessed negatively and more often show moderate to high positive signals. The weighting of Technology was also increased. This change enables the RISC Score to more accurately capture meaningful variations in the risk environment.

This week, **Iran significantly tightened its internet blackout amid nationwide protests, actively targeting satellite-based connectivity**. Authorities reportedly jammed Starlink services and seized satellite dishes to block access to external information, relying on Russian jamming technologies combined with Chinese research support. On the threat intelligence front, **this was considered a state-level electronic warfare operation against Starlink, with technical evidence pointing to coordinated GPS spoofing and jamming** targeting consumer satellite internet terminals. While the service remained partially operational, the attack significantly degraded connectivity, marking a qualitative escalation in the targeting of commercial space services through electronic warfare techniques. On the regulatory front, **China continued to advance its cyber sovereignty strategy**, with amendments to the Cybersecurity Law entering into force on 1 January 2026. The updated framework strengthens security risk monitoring and introduces explicit requirements related to artificial intelligence safety, reflecting Beijing's intent to consolidate legislative control over digital infrastructures while reducing exposure to foreign technologies. On the technological front, **PsiQuantum announced a collaboration with Airbus under the QuLAB project** to explore applications of fault-tolerant quantum computing for aerospace. Regarding the market, **Norway announced plans to establish a national timing service independent of satellite systems**. The initiative aims to reduce reliance on GNSS and enhance national resilience against interference, spoofing, and jamming, reflecting growing awareness of PNT vulnerabilities across critical infrastructures.

GEOPOLITICS

Iran tightens internet blackout, targets Starlink and satellite access amid protests using Russian technology and with Chinese support

As nationwide protests intensify, Iranian authorities have imposed a sweeping internet shutdown, jamming Starlink and seizing satellite dishes to block access to external information. Reports suggest the disruption relies on Russian jamming technology combined with Chinese research, highlighting Tehran's growing technological cooperation with Moscow and Beijing. Starlink has emerged as a key tool for protesters to bypass censorship, drawing criticism from Donald Trump and Elon Musk over Iran's attempts to disrupt the service. On the ground, security forces are also confiscating private CCTV footage to identify and suppress demonstrators. **#Iran #Starlink**

Sources: DNYUZ, Iran International, Opindia

[redacted]

[redacted]

[redacted]

[redacted]

REGULATION

China's Cyber Sovereignty Drive 2025

Key findings reveal a multifaceted escalation in China's cybersecurity posture throughout 2025, characterized by legislative fortification, indigenous capability building, and assertive countermeasures against foreign intrusions. The amendment to China's Cybersecurity Law, approved on 29 October 2025 and effective from 1 January 2026, introduced enhanced security risk monitoring and explicit regulations for artificial intelligence (AI) safety, as a first step. **#China #CybersecurityLaw**

Source: Debug lies

[redacted]

[redacted]

TECHNOLOGY

PsiQuantum collaborating with Airbus to advance quantum computing for aerospace

PsiQuantum announced today that the company is collaborating with Airbus, Europe's largest aeronautics and space company, to advance applications in aerospace for fault-tolerant quantum computers. Under the QuLAB project at Airbus, the two companies are combining their expertise to develop and evaluate quantum algorithms for complex problems in fluid mechanics—illustrating the promise of fault-tolerant quantum computing for aerospace solutions.

#QuLAB #Quantum

Source: HPCWire

[redacted]

THREAT INTELLIGENCE

[redacted]

Iran strikes Musk's Starlink—First 'Electronic Warfare' attack

Cyber investigator Nariman Gharib posted on X Wednesday P.M., claiming the "first documented technical evidence of state-level GPS spoofing against consumer satellite internet." This attack hit its mark. "Starlink stayed online but was barely usable." The attack was detected by analyzing the telemetry from a Starlink terminal in Iran. Gharib says "the data provides direct technical evidence of GPS spoofing/jamming detection." In short, Iran successfully spoofed multiple GPS signals to overwhelm the Starling device and its countermeasures, throwing its steering off course. **#ElectronicWarfare #Starlink**

Sources: Forbes, X

[redacted]

MARKET & COMPETITION

[redacted]

Norway to build non-satellite timing network

Two government agencies in Norway are proposing the establishment of a national time service that does not depend on satellites and are asking for input. Observers tell us this project will go forward, and this request is to help refine how it will be accomplished. **#CallforProposal #AntiInterference**

Sources: RNTND, NKOM

TRAINING & EDUCATION

Research on the Doppler ground simulation system based on spatial coherence laser communication link

Spatial coherence laser communication, characterized by its high-speed data transmission and strong resistance to interference, has emerged as a pivotal technology for future high-speed inter-satellite communication. In satellite laser communication terminals, the Doppler effect caused by high-speed relative movement between satellites significantly affects the performance of the communication link. **#Paper #Communication**

Source: IOP Science