SPACE CYBERSECURITY WEEKLY WATCH

W13

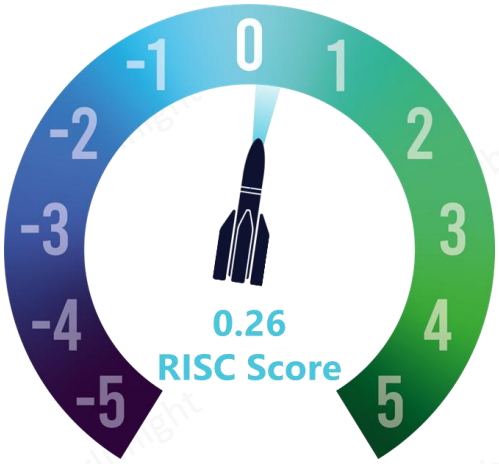
March 24 – 31, 2026

Timeframe: Weekly
# of articles identified: 20
Est. time to read: 50 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.

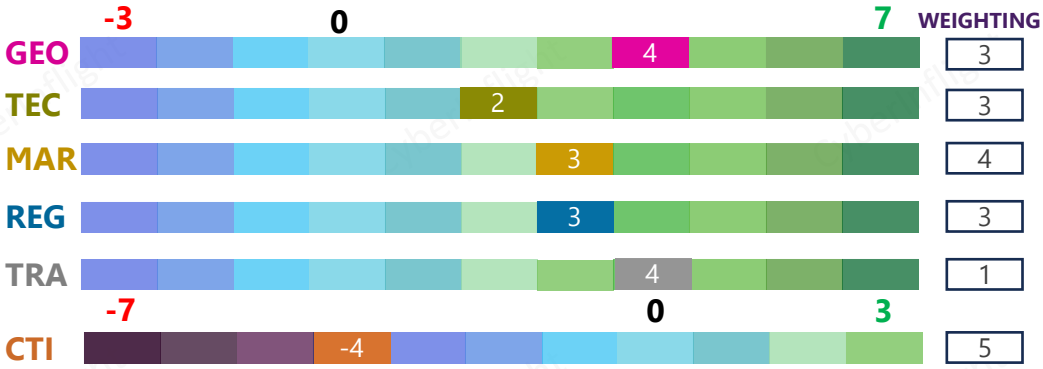
GEOPOLITICS
TECHNOLOGY
MARKET & COMPETITION
REGULATION
TRAINING & EDUCATION
THREAT INTELLIGENCE
IMPORTANT NEWS

RISC Score Assessment

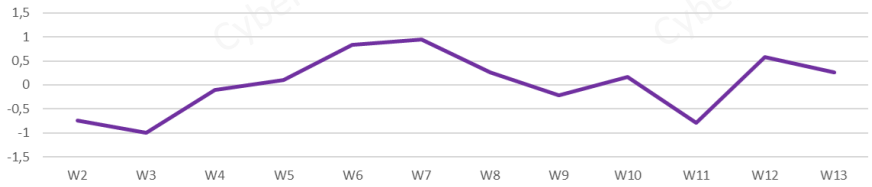


The RISC score for this watch is 0.26, down from last week due to an active threat climate balanced with a lot of geopolitical news

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



This week, the **U.S. Space Force deployed dedicated cyber units to protect rocket launch operations** at Space Launch Delta 30 (Vandenberg) and Delta 45 (Patrick). These squadrons actively monitor and defend against real-time cyber threats during launches, marking a critical step in securing space access amid escalating adversarial risks. On the regulatory side, **the NSA, ASD's ACSC, and allied cyber agencies released joint guidance on risks and mitigations for Low Earth Orbit (LEO) SATCOM** systems. The framework addresses vulnerabilities across space, ground, and user segments, emphasizing supply chain security, data management, and communication link resilience as LEO constellations expand globally. On the market front, **India's new CERT-In cybersecurity rules are set to increase compliance costs for space startups,** mandating rapid incident reporting, dedicated CISOs, and security-by-design principles. While these measures aim to bolster resilience, they also pose operational and financial challenges for emerging players in the sector. On the threat landscape, **tensions between Iran and Israel raise concerns over potential cyberattacks on communication satellites**. Former White House CIO Teresa Payton warned that Iran could target global satellite infrastructure, threatening civilian and commercial operations with cascading disruptions. On the technological side, **the UK advanced its space-based quantum communications mission, building on research from the Quantum Communications Hub and IQN Hub**. This initiative aims to position the UK as a leader in quantum-secure communications, addressing cyber threats posed by next-generation computing technologies .On the training front, **NATO's AVT-417 research meeting explored hybrid space architectures,** integrating space, air, terrestrial, and subsea assets for mission resilience. Key outcomes included requirements for AI-driven autonomy, onboard processing, and standardized interfaces to ensure operational continuity under cyber and kinetic stress.

GEOPOLITICS

Space Force deploys dedicated cyber units to protect rocket launch operations

Two new Defensive Cyber Operations Squadrons are actively monitoring SSC's Launch Ranges during Launch Operations to defend in real time from any adversaries attempting a cyber-attack during launch. The squadrons are located at Space Launch Delta (SLD) 30 at Vandenberg Space Force Base and SLD 45 at Patrick Space Force Base.

#USSF #LaunchOperations

Sources: USSF, Orbital Today

[redacted]

[redacted]

REGULATION

NSA and ASD's ACSC release joint guidance on LEO SATCOM system risks and mitigations

Low Earth Orbit (LEO) satellite communication (SATCOM) services are expanding rapidly, offering new connectivity options but also introducing new cyber security risks. ASD's ACSC, together with the Australian Space Agency, the Canadian Centre for Cyber Security, the National Security Agency, and the New Zealand National Cyber Security Centre have released guidance to help organizations understand these risks and make informed decisions when procuring or using LEO SATCOM services. The guidance outlines risks and mitigations across space, ground and user segments. It also highlights broader risks relating to communication links, supply chains and data management. **#Framework #LEOSATCOM**

Sources: Australian Signal Directorate, NSA

MARKET & COMPETITION

[redacted]

[redacted]

[redacted]

MARKET & COMPETITION

New cyber rules to raise costs for India's space startups

India's new CERT-In cybersecurity framework is set to significantly raise compliance costs for space startups, requiring rapid incident reporting, mandatory CISOs, and security-by-design systems. These rules will force operational restructuring, heavier audits, and governance upgrades, making cybersecurity a core cost center for emerging players.
#Costs #India

Source: Indian Web

[redacted]

THREAT INTELLIGENCE

[redacted]

[redacted]

[redacted]

Iran might start cyberattacks on satellites meant for communication says Ex White House Official

Rising tensions between Iran and Israel are fueling concerns that the conflict could expand beyond traditional military engagement into the digital and space domains. According to former White House Chief Information Officer Teresa Payton, there is a growing risk that Iran may begin targeting satellites used for global communications—an escalation that could have far-reaching consequences for civilian and commercial infrastructure worldwide.
#Iran #SateliteCommunication

Source: Cybersecurity Insiders

TECHNOLOGY

[redacted]

Space mission launch advances UK standing in quantum communications

Emerging from research and development efforts led by the preceding Quantum Communications Hub and later advanced by the IQN Hub - both funded by the Engineering and Physical Sciences Research Council (EPSRC) - the mission brings together five UK research institutions working to strengthen the UK's leadership in space-based quantum communications, addressing cybersecurity threats posed by emerging quantum computing technologies. **#Quantum #SPOQC**

Source: Heriot Watt University

TRAINING & EDUCATION

[redacted]

Platform Implications for Hybrid Space Architectures for NATO Missions

AVT-417 advanced NATO's understanding of how hybrid space architectures that integrate space, air, terrestrial, and subsea assets, can strengthen mission resilience and deterrence. The Research Specialists' Meeting brought together eleven nations to assess platform-level enablers for secure, interoperable, and autonomous hybrid constellations. Key outcomes included identifying requirements for AI-driven autonomy, onboard processing, and standardized interfaces to ensure operational continuity under cyber and kinetic stress. **#Paper #HybridSpaceArchitecture**

Source: NATO