SPACE CYBERSECURITY WEEKLY WATCH

W42

October 13 – October 19, 2026

Timeframe: Weekly

# of news items identified: 37

Est. time to read: 60 minutes

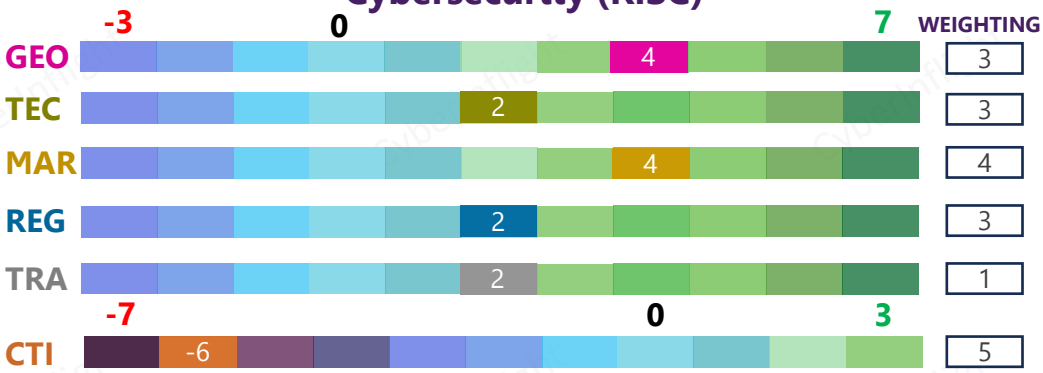
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

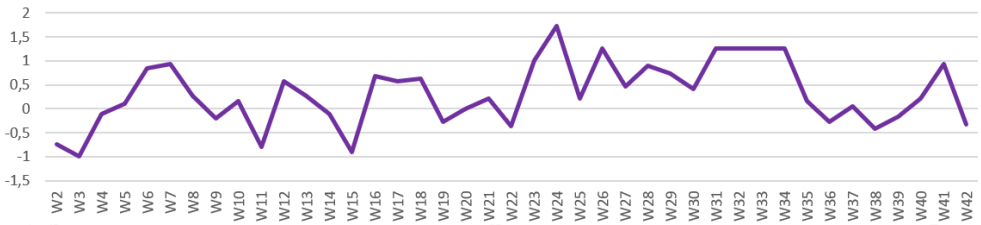
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



The RISC score for this watch is -0.32, a decrease of 1.26 since last week. This decrease is largely due to a more active threat landscape.

CyberInflight has had a busy period, recently publishing its **2026 Space Cybersecurity Market Intelligence Report**. The team is also **seeking an intern in economic intelligence and space cybersecurity** and **will take part in a panel at the upcoming SDSC** in Tallinn, Estonia. On the geopolitical front, **a new study by Clémence Poirier of ETH Zurich's Center for Security Studies** identifies 407 cyber operations targeting the space sector in 2025, a stark indication of the growing exposure of space infrastructure to cyber threats. On the market side, the **UK is reportedly nearing a decision on a contract worth up to £2 billion for its next-generation Skynet military satellites**, with Lockheed Martin among the contenders. The prospect of relying on a US supplier has revived concerns that dependence on foreign technology could constrain Britain's freedom to operate a critical military system. On the regulation front, **a new ECSO paper sets out priority areas for coordinated European investment**, aiming to inform industrial policy and strengthen a space ecosystem that is secure, resilient and competitive. On the threat front, Swiss public broadcaster SRF reports that officials suspect **China was behind the cyberattack on state-owned space company Beyond Gravity**. Separately, **Russia's Cosmos 2612 has maneuvered close to ICEYE-X36**, an Earth-observation satellite operated by Finnish-founded ICEYE. The proximity has raised concern, although the satellite's intent remains unclear. On the technological front, a recent article underscores the **growing importance of key management systems (KMS)**: they help determine when digital intent is granted cryptographic authority, making them a critical part of secure operations. Lastly, next week, the **conference Defence in Space 2026 will be held in London**.

CYBERINFLIGHT'S NEWS

CyberInflight is looking for an intern in economic intelligence and space cybersecurity

We are looking for a curious individual with a strong interest in cybersecurity. Some basic familiarity with technical topics would be a plus. Learn more about the position and how to apply! **#CyberInflight #InternshipOffer**

Source: CyberInflight

CyberInflight is proud to have published its 2026 Annual Space Cybersecurity Report

Drawing on the CyberInflight team's work throughout the year, it brings together research and observations, interview campaigns, and insights gathered through consulting engagements. Across 500 pages, the report examines the evolving threat landscape and the technology, commercial, and regulatory developments shaping the future of space cybersecurity. **#2026Report #4thEdition**

Sources: CyberInflight, CyberInflight

CyberInflight is glad to be a part of a panel at the upcoming SDSC in Tallinn, Estonia

The 6th "Software Defined Space Conference" (SDSC), dedicated to the critical realm of cybersecurity and software development in space, is set to unfold from 27 to 29 October in Tallinn, Estonia. CyberInflight will be on a panel discussing how cybersecurity is addressed in European frameworks. **#SDSC #Panel**

Sources: SDSC

GEOPOLITICS

Space cybersecurity: Why there is a hidden threat to satellites and global infrastructure

The Center for Security Studies at ETH Zurich just released a study identifying 407 cyber operations targeting the space sector in 2025. The incidents affected at least 183 space-related organizations and involved 139 distinct threat actors. **#SpaceCybersecurity #GlobalInfrastructure**

Source: World Economic Forum, IndustrialCyber, ViaSatellite

[redacted]

Source: [redacted]

[redacted]

Source: [redacted]

[redacted]

Source: [redacted]

[redacted]

Source: [redacted]

[redacted]

Source: [redacted]

GEOPOLITICS

[redacted]

MARKET & COMPETITION

[redacted]

Britain poised to award £2bn military satellite deal to U.S. defence giant despite control fears

The Ministry of Defence is on the verge of awarding a contract worth up to £2bn for Britain's next-generation Skynet military satellites to American defence contractor Lockheed Martin. The new deal would replace the current British-built system produced by Airbus in the UK. Concerns that switching from domestically developed technology to a US-sourced alternative could effectively give Washington a veto over how Britain operates the system have intensified sharply.

#Britain #SKYNET

Source: GBNews

[redacted]

REGULATION

EU Cybersecurity Industrial Policy for Space

The paper by ECSO identifies the priority areas in which coordinated European investment is most urgently required, providing a foundation for future industrial policy discussions and initiatives in support of a secure, resilient and competitive European space ecosystem. **#ECSO #SpacePolicy**

Sources: ECSO

REGULATION

[redacted]

THREAT INTELLIGENCE

[redacted]

China suspected in cyberattack on Swiss space company

An investigation by Swiss public television SRF has revealed that company officials suspect China was behind a cyberattack on the Swiss state-owned space company Beyond Gravity. **#BeyondGravity #Switzerland**

Source: SWI

[redacted]

THREAT INTELLIGENCE

[redacted]



[redacted]



[redacted]



[redacted]



[redacted]



Russian military satellite maneuvers into targeting range of NATO reconnaissance satellite supporting Ukrainian strikes



Russian military satellite has maneuvered into an orbit that could allow it to approach a U.S.-registered commercial reconnaissance satellite providing intelligence support to Ukraine, raising concerns over the Russian Armed Forces' potential ability to threaten Western space assets. The Russian spacecraft, Cosmos 2612, has adjusted its orbit to match that of ICEYE-X36, a synthetic aperture radar (SAR) satellite operated by Finnish-founded company ICEYE, which supplies imagery to Ukraine and Western governments. **#RPO #ICEYE-X36**

Source: Military Watch Magazine, Kyiv Post

TECHNOLOGY

[redacted]

From KMS to SpaceKMS: Building a verifiable cryptographic control plane

Modern computing systems depend on cryptographic keys to determine who may sign, decrypt, authenticate, release secrets, provision infrastructure, or authorize high-value actions. A Key Management Service (KMS) is the control plane that governs those keys: where they may exist, who or what may use them, under which policies, and inside which execution environment. As cloud services, financial systems, autonomous software, and AI agents become increasingly action-oriented, KMS becomes critical infrastructure for determining when digital intent is granted cryptographic authority.

#KMS #SpaceKMS

Source: SpaceComputer

TRAINING & EDUCATION

Join Comtech at Defence In Space 2026 in London

On Tuesday, October 27th, Daniel Gizinski, President of Comtech's Satellite and Space Segment, will deliver a keynote on Cyber Resilience. **#DefenceInSpace #Comtech**

Source: Defence In Space

CyberInflight is a Market Intelligence company dedicated to the topic of Space Cybersecurity. The company provides strategic market and research reports, bespoke consulting, market watch & OSINT research, and cybersecurity awareness training.
Contact us at: research@cyberinflight.com