SPACE CYBERSECURITY WEEKLY WATCH

W51, W52, W1

December 16 – January 5, 2025

Timeframe: Weekly

# of articles identified: 40

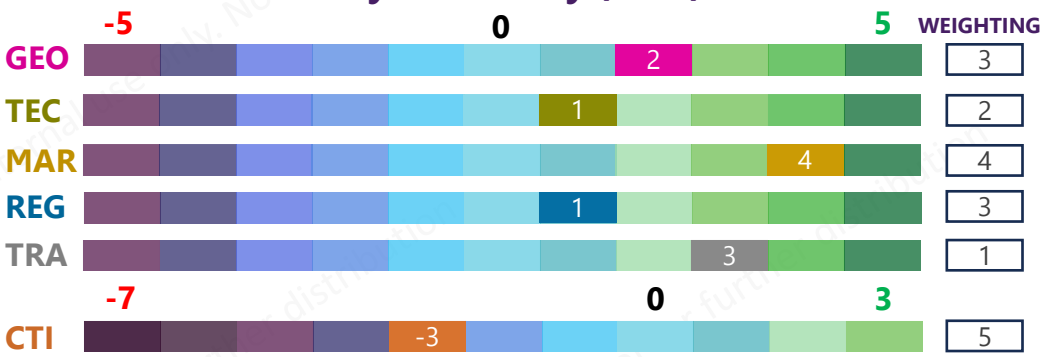
Est. time to read: 80 minutes

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

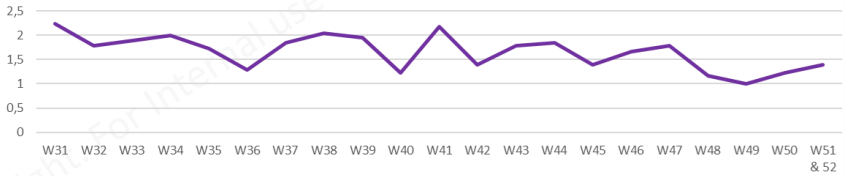
- GEOPOLITICS
- TECHNOLOGY
- MARKET & COMPETITION
- REGULATION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- IMPORTANT NEWS

RISC Score Assessment

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



The RISC score for this watch is 1.39, a slight increase from W50, due to improvements in the Market and Threat Intel fronts.

Happy New Year! As we step into 2026, this special watch brings together key developments from the end of 2025 and the first week of January. CyberInflight wrapped up the year with an initiative at TBS Education, delivering a lecture on space cybersecurity to Aerospace Master's students. On the geopolitical front, France and the United States conducted close-proximity satellite maneuvers under the joint Operation Olympic Defender. These illustrate strengthened bilateral coordination and France's capacity to conduct dynamic and responsible space operations aimed at deterring adversarial actions. On the regulatory front, Japan formally adopted a new national cybersecurity strategy that will guide policy over the next 5 years. This aims to enhance coordination among civilian, law enforcement, and defense institutions in response to growing and increasingly sophisticated cyber-threats. On the technological side, Leonardo DRS completed the first on-orbit test of its next-generation software-defined radio with integrated advanced cryptography. On the market front, Sopra Steria announced exclusive negotiations to acquire Starion and Nexova through its subsidiary CS Group. The proposed acquisition aims to strengthen Europe's sovereign capabilities by creating a leading player in secure digital services for the space and cybersecurity sectors. On the threat side, ESA confirmed a cybersecurity incident affecting a limited number of external servers. While investigations are ongoing, preliminary findings indicate a contained impact, highlighting the persistent exposure of space organizations to cyber risks beyond core networks. Lastly, a recent academic study analyzed how orbital altitude affects cyber-threats to LEO, MEO, and GEO systems, identifying weak encryption and command-path vulnerabilities as consistent factors that enable adversarial success across all orbital regimes.

CYBERINFLIGHT'S NEWS

CyberInflight at TBS Education: Space Cybersecurity in action!

We had the pleasure of delivering a lecture on Space Cybersecurity to the Aerospace Master of Science students at TBS Education. Our market analysts Héloïse Do Nascimento Cardoso and Valentine Crepineau shared insights on cyber-threats, geopolitical challenges, market dynamics, and regulatory frameworks, providing students with a holistic view of the space cybersecurity ecosystem. **#Cyberdefense #CyberInflight**

Source: *LinkedIn*

GEOPOLITICS

France, US practice up-close satellite maneuvers under joint space war plan

The bilateral rendezvous and proximity operation "illustrates France's ability to conduct dynamic and responsible operations to deter adversaries from acting against its space interests," according to France's Space Command. **#OlympicDefender #SpaceWarfare**

Source: *Breaking Defense*

The German government's Space Safety and Security Strategy

On 10 November 2025, the Federal Ministry of Defence and the Federal Foreign Office presented the first national Space Safety and Security Strategy, which aims to cover all security-relevant areas, describe challenges, improve the ability to act in space, and rapidly expand defense capabilities. In particular, the strategy is intended to help ensure security, resilience, and defense capabilities in space. **#German #SpaceStrategy**

Source: LINK Law Now

Space Force to focus training on 'orbital warfare,' joint integration

The Space Force is putting top priority on training Guardians for fighting and winning in space, using both virtual environments and, in the future, a dedicated fleet of live satellites. **#SpaceForce #OrbitalWarfare**

Source: Breaking Defense

Cybersecurity and new frontiers in wireless technology: Underwater, Space, and Earth at the Marconi Foundation conference

The final event in the celebrations marking 130 years since the first wireless signal, and part of the program commemorating the 150th anniversary of Marconi's birth. The focus is on cybersecurity in the underwater, terrestrial, and space dimensions, in the presence of the Director of the ACN Agency, Prefect Bruno Frattasi.

#WirelessTechnology #MarconiFoundationConference

Source: Ansa.it

Hacking space: Europe ramps up security of satellites

In the desolate Arctic desert of Kangerlussuaq, Greenland, European pilots are building defenses against a new, up and coming security threat: space hacks. It's just one example of how Europe is moving to harden the security of its satellites, as rising geopolitical tensions and an expanding spectrum of digital threats are pushing space communications to the heart of the bloc's security policy. **#Europe #SpaceResilience**

Sources: Politico, Voice online, Breaking Defense, Euractiv

REGULATION

EU Space Act: lo spazio come infrastruttura critica e il nuovo paradigma normativo per la resilienza cyber (Trad.: EU Space Act: space as critical infrastructure and the new regulatory paradigm for cyber-resilience)

The EU Space Act represents a European response to a radical transformation of the space domain. When, on February 24, 2022, a few hours before Russia invaded Ukraine, a cyberattack compromised tens of thousands of satellite modems in Viasat's KA-SAT network, the world witnessed the first large-scale demonstration of how orbital infrastructure has become a theater of conflict and how its vulnerability can spread far beyond the borders of the original theater of war. **#EUSpaceAct #SpaceInfrastructure**

Source: ICT Security

Japan adopts new cybersecurity strategy to counter rising cyber-threats

The Japanese government has formally adopted a new cybersecurity strategy that will guide national policy over the next five years. The decision aims at strengthening Japanese cybersecurity coordination across civilian, law enforcement, and defense institutions. **#NationalStrategy #Japan**

Source: *The Cyber Express*

REGULATION

TECHNOLOGY

Leonardo DRS Achieves Major Milestone with First Space-Based Test of Next-Generation Secure Data Transport Capability

Leonardo DRS, Inc. announced today the successful completion of the first on-orbit test of its revolutionary multi-channel software-defined radio (SDR) with integrated advanced cryptography. This milestone marks a significant advance in validating a technology poised to establish a new standard for secure U.S. military satellite data transport at the tactical edge. **#Leonardo #Secure**

Source: *Leonardo DRS*

MARKET & COMPETITION

MARKET & COMPETITION

Proposed acquisition of Starion and Nexova, European specialists in space systems engineering and cybersecurity

Sopra Steria, a major tech player in Europe, has announced that it is in exclusive negotiations to acquire Starion and Nexova on behalf of its subsidiary, CS Group. This acquisition aims to create a leading European operator in secure, sovereign digital services and solutions for the space and cybersecurity sectors. **#SopraStoria #Nexova**

Sources: *Sopra Steria*, *Quantum Zeitgeist*

[redacted]

THREAT INTELLIGENCE

[redacted]

THREAT INTELLIGENCE

[redacted]

[redacted]

[redacted]

European Space Agency confirms cybersecurity breach on external servers

The European Space Agency (ESA) has confirmed a cybersecurity breach involving servers located outside its corporate network. This confirmation comes following threat actor claim that they had compromised ESA systems and stolen a large volume of internal data. In an official statement shared on social media, the European Space Agency said it is aware of the cybersecurity issue and has already launched a forensic security investigation, which remains ongoing. According to ESA, preliminary findings indicate that only a very small number of external servers were impacted. **#ESA #DataBreach**

Sources: *X*, *TheCyberExpress*, *Red Hot Cyber*

[redacted]

[redacted]

TRAINING & EDUCATION

[redacted]

[redacted]

[redacted]

TRAINING & EDUCATION

[redacted]

[redacted]

Satellite Cybersecurity Across Orbital Altitudes: Analyzing Ground-Based Threats to LEO, MEO, and GEO

The searchers characterize how orbital altitude dictates attack feasibility and impact. Their evaluation reveals distinct threat profiles: GEO systems are predominantly targeted via high-frequency uplink exposure, whereas LEO constellations face unique risks stemming from limited power budgets, hardware constraints, and susceptibility to thermal and radiation-induced faults. The results demonstrate that weak encryption and command path irregularities are the most consistent predictors of adversarial success across all orbits. **#Paper #Awareness**

Source: *Cornell University*, *Quantum Zeitgeist*

[redacted]

[redacted]

[redacted]

[redacted]