SPACE CYBERSECURITY WEEKLY WATCH

W22

May 27 – June 1, 2026

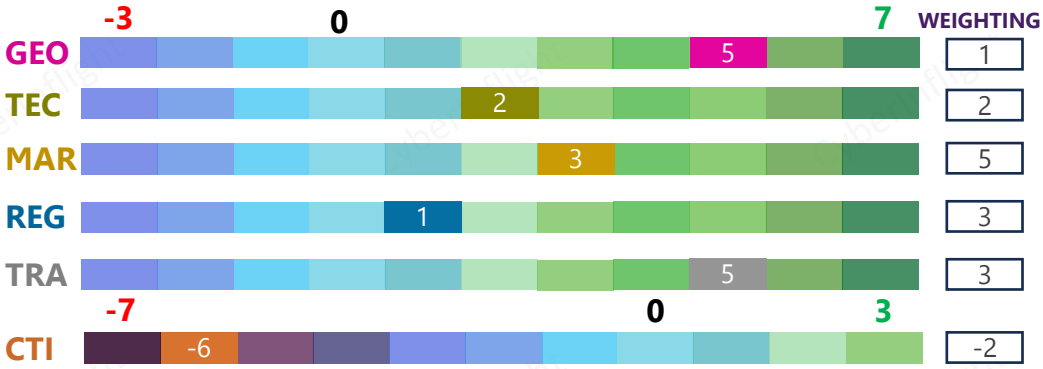
Timeframe: Weekly
# of news identified: 42
Est. time to read: 85 minutes

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

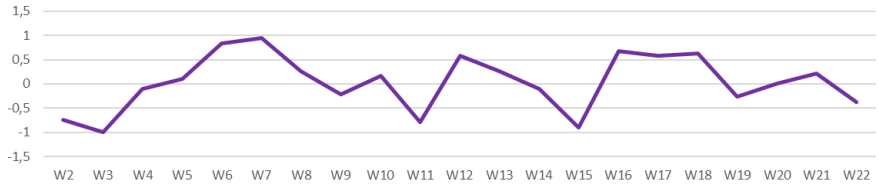
RISC Score Assessment

Overview & Resilience Index for Space Cybersecurity (RISC)



The RISC score for this watch is -0.37, a decrease of 0.58 points compared to the previous week. This is mainly due to a negative climate in Threat intel., with several alleged cyberattacks against the space domain reported.

RISC Score evolution in 2026



This week, on the geopolitical front, **European officials are calling for greater integration of cybersecurity into mission design**. Moreover, in the U.S., the top member on the House Armed Services subcommittee focused on cyber had a stark warning about **how China is positioning itself to overwhelm the U.S. military in cyberspace**. On the regulation side, this year's edition of the **ENISA NIS360 report shows improvement in cybersecurity maturity of EU critical sectors** while the level of criticality in sectors remains comparatively more stable. On the market front, the **EUSPA's EU Space Market Report 2026 was published** and presents key trends, forecasts and insights shaping the evolution of the global space economy. On the threat side, an article highlighting **407 cyberattacks against the space sector in 2025** was published by Air&Cosmos, highlighting that cyber-threats are gradually replacing kinetic threats on the list of concerns. These attacks take various forms and primarily target ground-based systems. Moreover, **a threat actor claims to have successfully breached the Spanish Space Agency and stolen a comprehensive dataset related to the XMM-Newton space telescope**. On the technological side, **experts at SmallSat Europe tried to decipher between the hype and reality of orbital data centers** — in terms of both technology and economics. On the training and education side, a **webinar by GSOA on Cybersecurity in Space: Hardening networks, supply chains & architectures was made available**. The discussion unpacked the evolving space cybersecurity threat landscape, with increasingly powerful threat actors seeking disruption on space infrastructure as it becomes critical for national security. With satellite systems becoming closely integrated with terrestrial networks, new layers of complexity are introduced, increasing the attack surface, but also opening new opportunities.

GEOPOLITICS

[redacted]

[redacted]

Cybersecurity: Critical delay in the European space sector

Cybersecurity has become a top priority amid the trend toward sovereign space infrastructure in Europe, which lags behind China and the United States in this area. Drawing on lessons learned from Ukraine, officials are calling for greater integration of cybersecurity into mission design. **#Cybersecurity #SpaceSector**

Source: Air & Cosmos

[redacted]

[redacted]

In the cyber race against China, CYBERCOM bets on 'quality over quantity.'

The top member on the House Armed Services subcommittee focused on cyber had a stark warning about how America's greatest geopolitical rival is positioning itself to overwhelm the US military in cyberspace. **#CYBERCOM #China**

Source: Breaking Defense

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

REGULATION

ENISA: EU critical sectors improve cybersecurity maturity under NIS2

This year's edition of the ENISA NIS360 report shows improvement in cybersecurity maturity of EU critical sectors while the level of criticality in sectors remains comparatively more stable. The ENISA NIS360 aims to work as an annual assessment tool supporting national authorities, policymakers and other stakeholders in assessing the cybersecurity maturity and criticality of high criticality sectors under the NIS2 Directive. **#NIS2 #ENISA**

Source: Insight EU Monitoring

MARKET & COMPETITION

[redacted]

[redacted]

[redacted]

Unlock the latest EU Space Market insights

The EUSPA's EU Space Market Report 2026 presents key trends, forecasts and insights shaping the evolution of the global space economy. Through data-driven analysis and sector-focused perspectives, the report explores how EO, GNSS, Secure SATCOM, and SSA are transforming industries, enabling resilience and supporting innovation across Europe and beyond. **#EUSPA #EUReport**

Sources: EUSPA, The Brussels Times

THREAT INTELLIGENCE

[redacted]

[redacted]

THREAT INTELLIGENCE

[redacted]

[redacted]

[redacted]

407 cyberattacks against the space sector in 2025

Cyber-threats are gradually replacing kinetic threats on the list of concerns. These attacks take various forms and primarily target ground-based systems. **#SpaceDomain #Cyberattacks**

Source: Air&Cosmos

[redacted]

[redacted]

[redacted]

The alleged database of the Spanish Space Agency is on sale

A threat actor claims to have successfully breached the Spanish Space Agency and stolen a comprehensive dataset related to the XMM-Newton space telescope. **#SpanishSpaceAgency #DataLeak**

Sources: SOCRadar, X

[redacted]

[redacted]

[redacted]

[redacted]

THREAT INTELLIGENCE

[redacted]

TECHNOLOGY

[redacted]

Orbital data centers must tackle chip lifespan, launch availability, and cybersecurity challenges

One of the big topics, especially in light of the SpaceX initial IPO documents, is the future of orbital data centers and the possibilities of moving compute to space. Experts at SmallSat Europe tried to decipher between the hype and reality of orbital data centers — in terms of both technology and economics. **#OrbitalDataCenters #SmallSatEurope**

Source: National Cyber Security

[redacted]

TRAINING & EDUCATION

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Webinar: Cybersecurity in Space: Hardening networks, supply chains & architectures

The discussion unpacked the evolving space cybersecurity threat landscape, with increasingly powerful threat actors seeking disruption on space infrastructure as it becomes critical for national security. With satellite systems becoming closely integrated with terrestrial networks, new layers of complexity are introduced, increasing the attack surface, but also opening new opportunities. **#Webinar #GSOA**

Source: Youtube