SPACE CYBERSECURITY WEEKLY WATCH

W9

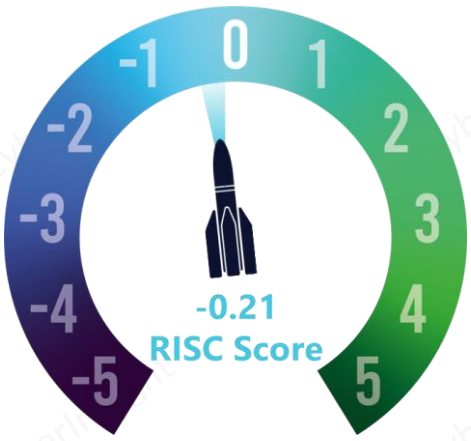
February 24 – March 2, 2026

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.

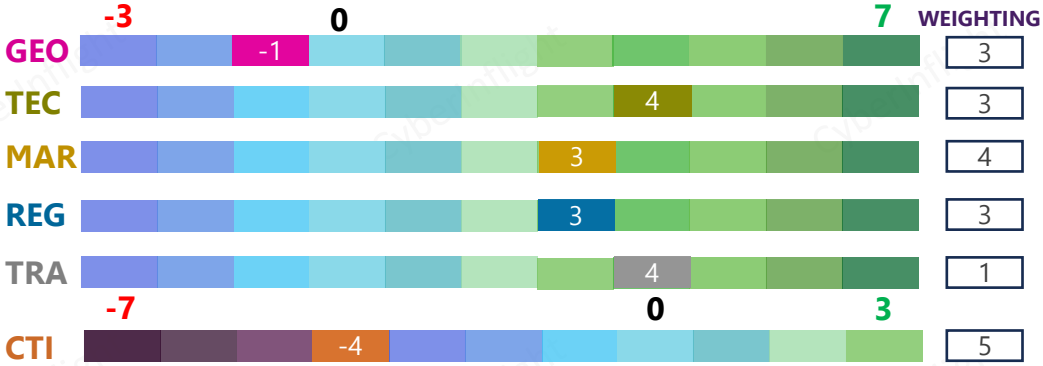
GEOPOLITICS
TECHNOLOGY
MARKET & COMPETITION
REGULATION
TRAINING & EDUCATION
THREAT INTELLIGENCE
IMPORTANT NEWS

RISC Score Assessment

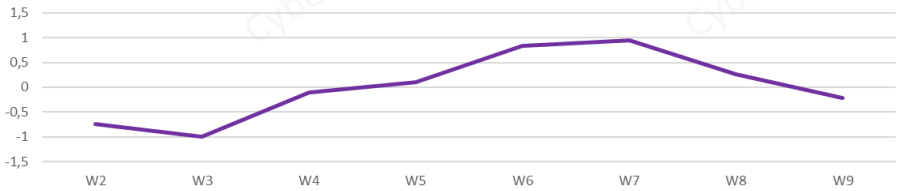


The RISC score for this watch is -0.21, down from last week, due to a poor geopolitical and threat climate.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



This week, **Iran's state television networks were reportedly hacked**, with footage of U.S. President Donald Trump and Israeli Prime Minister Benjamin Netanyahu briefly interrupting regular broadcasts. The incident, though unconfirmed by Iranian authorities, highlights the vulnerability of state-controlled media to cyber disruptions and the potential for information warfare to escalate regional tensions. On the regulatory side, **India's CERT-In and SIA-India collaborated to develop a comprehensive framework and guidelines for space cybersecurity.** This initiative aims to secure India's space communication assets and strengthen the resilience of its space ecosystem, reflecting a broader trend of nations formalizing cybersecurity standards for critical space infrastructure. On the market front, **Germany announced a €35bn investment in low Earth orbit (LEO) resilience and non-kinetic deterrence capabilities through 2030.** On the threat landscape, **GPS jamming in the Middle East surged dramatically between February 27 and March 1**, according to data from Flightradar24. The expansion of high-interference zones threatens aircraft navigation and underscores the urgent need for resilient positioning, navigation, and timing (PNT) solutions in conflict-prone regions. On the technological side, **ESA successfully tested a new verification service for Galileo that mitigates spoofing threats in real-world environments.** By confirming the authenticity of Galileo's satellite navigation data, this service enhances the system's robustness against deception. On the academic front, **researchers demonstrated a single-satellite-based method for geolocating GNSS spoofers from low Earth orbit.** This innovation leverages LEO-based receivers to detect and pinpoint interference sources, offering a scalable solution for persistent GNSS threat monitoring and response.

GEOPOLITICS

Iran State TV Network Hacked? Trump and Netanyahu Footage 'Appear' Amid Broadcasts

Several social media commentators reported on Sunday that Iran's state television networks had been "hacked", with US President Donald Trump and Israeli Prime Minister Benjamin Netanyahu appearing briefly between regular broadcasts. **#Iran #Hijacking**

Source: Times Now World, SOC Radar

REGULATION

CERT-In and SIA-India collaborate to develop a framework and guidelines for space cyber security

The Indian Computer Emergency Response Team (CERT-In), under the Ministry of Electronics and Information Technology (MeitY), in collaboration with SIA-India has developed a comprehensive framework and guidelines for space cyber security for securing space communication assets and contributing towards the resilience of India's space ecosystem. **#Framework #India**

Source: Indian Infrastructure, CERT-In

MARKET & COMPETITION

[redacted]

[redacted]

Germany Commits €35 Billion to LEO Resilience and Non-Kinetic Deterrence

On Saturday, Feb. 28, technical details emerged regarding Germany's massive €35 billion ($41 billion) pivot toward sovereign military space capabilities. The investment, which runs through 2030, signals a departure from purely defensive postures as Berlin prepares for a "sharply more contested" orbital environment involving Russian and Chinese counterspace activities. **#GermanSpaceCommand #NATO**

Source: Satnews

THREAT INTELLIGENCE

[redacted]

[redacted]

THREAT INTELLIGENCE

[redacted]

GPS jamming map shows sharp rise in Middle East interference from February 27 to March 1

GPS disruption across the Middle East has intensified dramatically, according to tracking data visualized on the Flightradar24 GPS jamming map. The heatmap, which monitors satellite navigation interference affecting aircraft positioning systems, shows a noticeable expansion of high-interference zones between February 27 and March 1, 2026.

#Jamming #MiddleEast

Source: Business Upturn

TECHNOLOGY

Galileo vs. spoofing: ESA tests in real-world environments

For the last seven months, a new verification service for Galileo has mitigated the threat of spoofing in the Open Service by confirming that the satellite navigation data used for positioning originated in the Galileo system. **#Galileo #Spoofing**

Sources: ESA, AeroMorning

[redacted]

[redacted]

[redacted]

TRAINING & EDUCATION

Single-Satellite-Based Geolocation of Broadcast GNSS Spoofers from Low Earth Orbit

This paper presents an analysis and experimental demonstration of single-satellite single-pass geolocation of a terrestrial broadcast Global Navigation Satellite System (GNSS) spoofer from Low Earth Orbit (LEO). The proliferation of LEO-based GNSS receivers offers the prospect of unprecedented spectrum awareness, enabling persistent GNSS interference detection and geolocation. Accurate LEO-based single-receiver emitter geolocation is possible when a range-rate time history can be extracted for the emitter. **#Paper #Spoofing**

Source: Cornell University

TRAINING & EDUCATION

[redacted]

[redacted]

[redacted]

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 researches and cybersecurity awareness training.
Contact us at: research@cyberinflight.com