SPACE CYBERSECURITY WEEKLY WATCH

W7

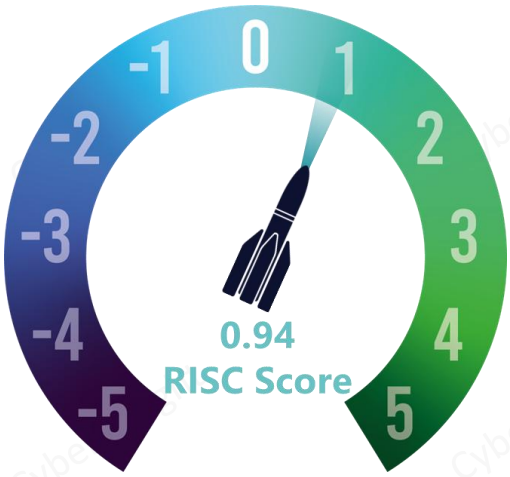
February 10 – 16, 2026

Timeframe: Weekly
# of articles identified: 25
Est. time to read: 55 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.

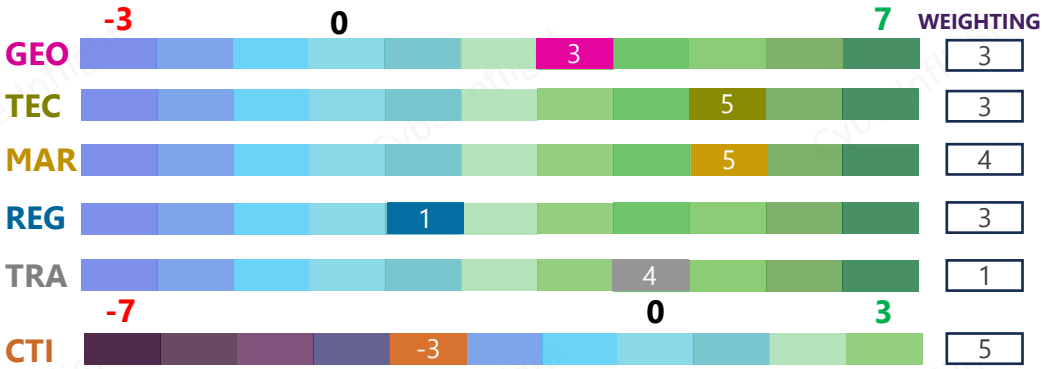
GEOPOLITICS
TECHNOLOGY
MARKET & COMPETITION
REGULATION
TRAINING & EDUCATION
THREAT INTELLIGENCE
IMPORTANT NEWS

RISC Score Assessment

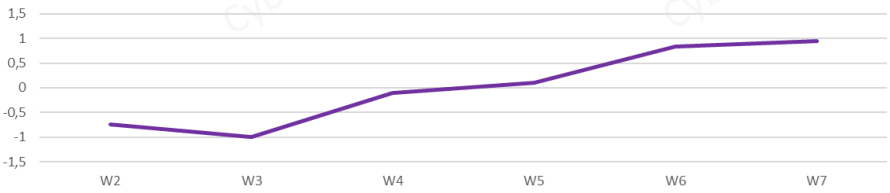


The RISC score for this watch is 0.94, up from last week, driven by stronger scores in the Technology and a less active threat climate.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



This week, **Russia and Iran condemned Elon Musk's Starlink at a United Nations meeting**, accusing the satellite constellation of violating international law. Both countries criticized its use in conflicts, signaling a growing pushback against the militarization of commercial space infrastructure and the influence of private actors in global security dynamics. On the regulatory side, the **European Union Agency for Cybersecurity (ENISA) updated its international strategy** to strengthen the EU's cybersecurity cooperation beyond Europe. The revised approach aligns with the EU's long-term objectives, emphasizing partnerships with global actors to address cross-border cyber threats and enhance collective resilience. On the market front, **Japan announced plans to subsidize the development of anti-jamming technology for satellite signals**, aiming for commercialization by 2033. The initiative, funded through JAXA's Space Strategy Fund with subsidies of up to 2.5 billion yen ($16 million), underscores Tokyo's commitment to securing its satellite communications against growing electronic threats. On the threat landscape, a re**port revealed how Chinese PLA satellites enabled Iran's hybrid kill chain during the 2025 Twelve-Day War with Israel**. Beijing's orbital surveillance fused with Tehran's strike capabilities, demonstrating a new model of cross-regional military cooperation that reshapes power dynamics in the Middle East and beyond. On the technological side, the **UK launched the TOUCAN project** to test an alternative to GNSS timing signals. This two-way satellite time and frequency transfer (TWSTFT) system, linking the UK's official timekeeping authority with its eLoran navigation system, aims to reduce dependency on vulnerable satellite-based timing infrastructure. Lastly, **new research explored adversarial attacks on satellite fingerprinting systems**.

GEOPOLITICS

[redacted]

Russia, Iran blast Musk's Starlink during UN space meeting

Officials from Russia and Iran blasted Elon Musk's Starlink at a Monday United Nations meeting held by the Committee on the Peaceful Uses of Outer Space. Both countries alleged that Musk's satellite internet constellation service program was operating in violation of international law. **#UN #SpaceX**

Source: The Hill

[redacted]

REGULATION

ENISA updates its international strategy to strengthen EU's cybersecurity cooperation

The European Union Agency for Cybersecurity has released an updated international strategy to reinforce the EU's cybersecurity ecosystem and strengthen cooperation beyond Europe's borders. The revised ENISA International Strategy refreshes the agency's approach to working with global partners while ensuring stronger alignment with the European Union's international cybersecurity policies, core values, and long-term objectives. **#ENISA #EUCooperation**

Source: The Cyber Express

MARKET & COMPETITION

[redacted]

[redacted]

[redacted]

MARKET & COMPETITION

[redacted]

Japan to subsidize anti-jamming tech that protects satellite signals

The Japanese government plans to support the development of technology that prevents satellite telecommunication signals from jamming attacks, looking to commercialize the devices around 2033, Nikkei has learned. Financial support will be provided through the Space Strategy Fund, operated by the Japan Aerospace Exploration Agency. The maximum amount for each subsidy will be 2.5 billion yen ($16 million). **#SpaceStrategyFund #AntiJamming**

Source: Nikkei Asia

THREAT INTELLIGENCE

[redacted]

[redacted]

[redacted]

[redacted]

Chinese eyes, Iranian fists: how PLA satellites powered Iran's kill chain against Israel in the 2025 Twelve-Day War

The 2025 Twelve-Day War between Israel and Iran did not merely exchange ballistic missiles and drones across contested skies, but instead crystallised a structural transformation in the architecture of modern warfare, as Beijing's orbital surveillance networks fused with Tehran's strike forces to create a hybridised kill chain that has permanently altered the balance of power in the Middle East. **#Iran #China**

Source: Defense Security Asia

TECHNOLOGY

[redacted]

[redacted]

[redacted]

[redacted]

UK to test alternative to GNSS timing signals

A new technology demonstration project in the UK will test a timing link between the country's official timekeeping authority and its eLoran navigation system. Known as a two-way satellite time and frequency transfer (TWSTFT) system, the project is being conducted under the TOUCAN (TWSTFT Capability Demonstration) program. **#GNSS #NAVISP**

Source: Spatial Source

[redacted]

[redacted]

TRAINING & EDUCATION

[redacted]

TRAINING & EDUCATION

SATversary: Adversarial Attacks and Defenses for Satellite Fingerprinting

In this paper, we evaluate a range of attacks against satellite fingerprinting, building on previous works by looking at attacks optimized to target the fingerprinting system for maximal impact. We design optimized jamming, dataset poisoning, and spoofing attacks, evaluating them in the real world against the SatIQ fingerprinting system designed to authenticate Iridium transmitters, and using a wireless channel emulator to achieve realistic channel conditions. We show that an optimized jamming signal can cause a 50% error rate with attacker-to-victim ratios as low as -30dB (far less power than traditional jamming techniques), and demonstrate successful spoofing attacks, with an attacker successfully removing their own transmitter's fingerprint from messages. **#Paper #Fingerprinting**

Source: Cornell University

[illegible]

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