



SPACE CYBERSECURITY WEEKLY WATCH

W12

March 17 – 23, 2026

Timeframe: Weekly
of articles identified: 21
Est. time to read: 55 minutes

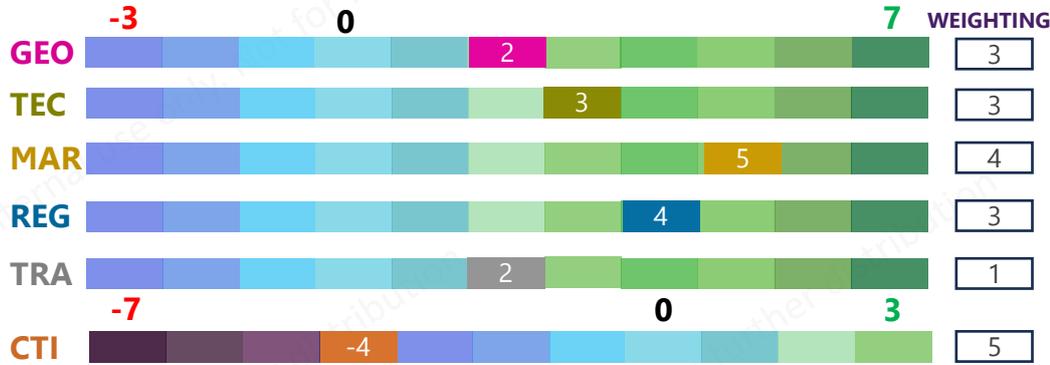
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

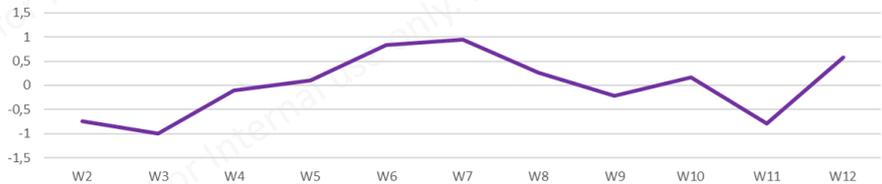
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



↑ The RISC score for this watch is 0.58, up from last week due to a good market and technological climate.

This week, **Iran is leveraging Chinese Beidou technology to intensify GPS spoofing and jamming** across the Middle East, significantly enhancing the precision of its missile strikes and targeting capabilities. This collaboration underscores the growing convergence of regional conflicts and space-based warfare, with Beijing's satellite systems enabling Tehran's military operations. Shifting to the regulatory side, there are **increasing questions about the cyber weaponization of the space domain**, where algorithmic warfare, such as GNSS signal manipulation and satellite command hijacking, challenges traditional notions of sovereignty. Furthermore, these multi-domain operations (MDO) operate at speeds and scales that outpace conventional legal frameworks, demanding urgent updates to international space law and cyber norms. On the market front, **the USSF has established new acquisition portfolios dedicated to space control and orbital warfare**, signaling a strategic shift toward proactive capabilities in contested space environments. These portfolios will streamline the development of technologies to counter adversarial threats, from electronic warfare to kinetic operations. Regarding the threat landscape, **experts warn that AI-driven attacks could compromise satellite control systems as early as the coming years**, leading to catastrophic collisions and debris cascades in Earth's orbit. Aging satellites, often lacking robust cybersecurity, are particularly vulnerable to jamming, spoofing, and command takeover, posing risks to both commercial and military operations. Turning to technological advancements, **Spain's GMV Aerospace & Defence, in partnership with ENAIRE and ESA, has developed the STAGER system**, a cost-effective solution for detecting and localizing GNSS spoofing and jamming threats. Lastly, on the training front, **new research introduces i-SDT (intelligent Self-Defending Digital Twins)**, a framework designed to discriminate between cyberattack types in industrial cyber-physical systems.



GEO POLITICS

★ Iran is using Chinese technology to 'spoof' satellite navigation signals

GPS jamming and spoofing by Iran have intensified dramatically since the outbreak of conflict in the Middle East, creating critical vulnerabilities for both commercial aviation and military operations, according to Jack Hidary, CEO of SandboxAQ. In an interview with CNBC, Hidary warned that Iran is now receiving access to China's Beidou satellite navigation system, enabling greater accuracy in missile strikes and targeting across the region. **#Iran #China**

Source: [MSN](#)



REGULATION

★ Cyber weaponization of space domain: legal aspects of algorithmic warfare

The least dominant of these triads is the Sixth-Domain Warfare, which violates sovereignty by crossing boundaries, undermining Global Navigation Satellite System (GNSS) signals, algorithmically manipulating Critical Information Infrastructure (CII), and exploiting weaknesses in satellite command and control (C2) systems. It is a space of multi-domain operations (MDO) that is faster and less visible than conventional war, designed to inhabit the real world of tangible things with state and nation-states, and is obsolete. **#Opinion #Cyberwarfare**

Source: [Cyber Blog India](#)



MARKET & COMPETITION

★ New Space Force acquisition portfolios to cover space control, orbital warfare

The Space Force now has put into place all of its mission-focused acquisition portfolios, including offices dedicated to space control and orbital warfare, according to the top space acquisition officer. Tom Ainsworth, who is performing the duties of the Air Force assistant secretary for Space Acquisition and Integration, told the annual McAleese Defense Programs Conference today that while the department is "still working through the detail of which programs specifically go into each one," the final seven portfolio acquisition executive (PAE) offices now are being put in place.

#USSF #Acquisitions

Source: [Breaking Defense](#)



MARKET & COMPETITION

UK continues to strengthen security partnership with expansion of One Cyber bill to the UK

The UK has continued to strengthen security partnership with the US under the One Cyber bill, which is a significant step forward for the UK in the area of cybersecurity. The bill is a landmark piece of legislation that will help to protect the UK's critical infrastructure and data from cyber threats. The bill is a key part of the UK's strategy to become a global leader in cybersecurity. The bill is a key part of the UK's strategy to become a global leader in cybersecurity.



UK, US, and NATO continue to strengthen security partnership with expansion of One Cyber bill to the UK

The UK, US, and NATO continue to strengthen security partnership with the expansion of the One Cyber bill to the UK. This is a significant step forward for the UK in the area of cybersecurity. The bill is a landmark piece of legislation that will help to protect the UK's critical infrastructure and data from cyber threats. The bill is a key part of the UK's strategy to become a global leader in cybersecurity.



UK, US, and NATO continue to strengthen security partnership with expansion of One Cyber bill to the UK

The UK, US, and NATO continue to strengthen security partnership with the expansion of the One Cyber bill to the UK. This is a significant step forward for the UK in the area of cybersecurity. The bill is a landmark piece of legislation that will help to protect the UK's critical infrastructure and data from cyber threats. The bill is a key part of the UK's strategy to become a global leader in cybersecurity.



UK, US, and NATO continue to strengthen security partnership with expansion of One Cyber bill to the UK

The UK, US, and NATO continue to strengthen security partnership with the expansion of the One Cyber bill to the UK. This is a significant step forward for the UK in the area of cybersecurity. The bill is a landmark piece of legislation that will help to protect the UK's critical infrastructure and data from cyber threats. The bill is a key part of the UK's strategy to become a global leader in cybersecurity.



THREAT INTELLIGENCE

UK, US, and NATO continue to strengthen security partnership with expansion of One Cyber bill to the UK

The UK, US, and NATO continue to strengthen security partnership with the expansion of the One Cyber bill to the UK. This is a significant step forward for the UK in the area of cybersecurity. The bill is a landmark piece of legislation that will help to protect the UK's critical infrastructure and data from cyber threats. The bill is a key part of the UK's strategy to become a global leader in cybersecurity.



UK, US, and NATO continue to strengthen security partnership with expansion of One Cyber bill to the UK

The UK, US, and NATO continue to strengthen security partnership with the expansion of the One Cyber bill to the UK. This is a significant step forward for the UK in the area of cybersecurity. The bill is a landmark piece of legislation that will help to protect the UK's critical infrastructure and data from cyber threats. The bill is a key part of the UK's strategy to become a global leader in cybersecurity.



AI attacks could cause incidents in space as early as the coming years — Space

According to experts, attackers could gain control of satellites and steer them into collisions with other spacecraft. This could trigger a cascade of debris and render Earth's orbit unsafe for future use. Experts also highlight the problem of aging satellites operating without adequate cybersecurity. They can become easy targets for attacks—ranging from signal jamming to command spoofing. **#AI #Satellites**

Sources: [SPACE](#), [UA News](#)



THREAT INTELLIGENCE

2025 Report warns of rising cyber threats to critical infrastructure from China, Russia, Iran, and North Korea

The report highlights growing cyber threats to critical infrastructure from China, Russia, Iran, and North Korea. It notes that these nations are increasingly targeting critical infrastructure and using cyber espionage to gain insights into military activities in a region. The assessment stresses that cyber threats to critical infrastructure are rising sharply, especially with regard to energy, water, and space systems, using concerns for the protection of space systems. [Read More](#)



Analysts claim to have breached a Chinese espionage network and stolen 10 petabytes of sensitive military data

A report published earlier this month by the National Security Agency (NSA) claims to have breached a Chinese espionage network and stolen 10 petabytes of sensitive military data. The report states that the network was used to collect and analyze intelligence on the United States and its allies. According to the report, the network was used to collect and analyze intelligence on the United States and its allies. The report also mentions that the network was used to collect and analyze intelligence on the United States and its allies. [Read More](#)



TECHNOLOGY

A Framework for Designing U.S. Space Operations Capabilities

The report discusses the need for a framework to guide the design of U.S. space operations capabilities. It notes that the current framework is outdated and does not account for the growing number of space-faring nations. The report also mentions that the current framework is outdated and does not account for the growing number of space-faring nations. [Read More](#)



New GMV Monitoring System Detects and Localizes GNSS Spoofing and Jamming

Spain's GMV Aerospace & Defence, together with ENAIRE, has developed a cost-effective system capable of detecting and localizing radio-frequency threats to satellite navigation, including spoofing and jamming. Supported by the European Space Agency (ESA) NAVISP program, the STAGER ('Sophisticated GNSS Threats Protection') project addresses the growing challenge posed by deliberate and accidental disruptions to satellite navigation services, an issue of increasing concern for both civil and military sectors. **#STAGER #SILENT**

Source: [InsideGNSS](#)



2025 Complete design of equipment for technology demonstration satellite aimed at creating Japan's first space communication satellite network

The Japanese government has announced a plan to launch a technology demonstration satellite in 2025. The satellite is designed to demonstrate the capabilities of a new space communication system. The satellite is designed to demonstrate the capabilities of a new space communication system. [Read More](#)



TRAINING & EDUCATION

Full-time Cybersecurity Degree Symbolic National Learning for International Operations in 2025 Global Education

The report discusses the need for a full-time cybersecurity degree program. It notes that the current program is outdated and does not account for the growing number of space-faring nations. The report also mentions that the current program is outdated and does not account for the growing number of space-faring nations. [Read More](#)





TRAINING & EDUCATION



Cyber-Resilient Digital Twins: Discriminating Attacks for Safe Critical Infrastructure Control

Industrial Cyber-Physical Systems (ICPS) face growing threats from cyber-attacks that exploit sensor and control vulnerabilities. Digital Twin (DT) technology can detect anomalies via predictive modelling, but current methods cannot distinguish attack types and often rely on costly full-system shutdowns. This paper presents i-SDT (intelligent Self-Defending DT), combining hydraulically-regularized predictive modelling, multi-class attack discrimination, and adaptive resilient control. **#Paper #DigitalTwins**

Source: [Cornell University](#)



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