SPACE CYBERSECURITY WEEKLY WATCH

W10

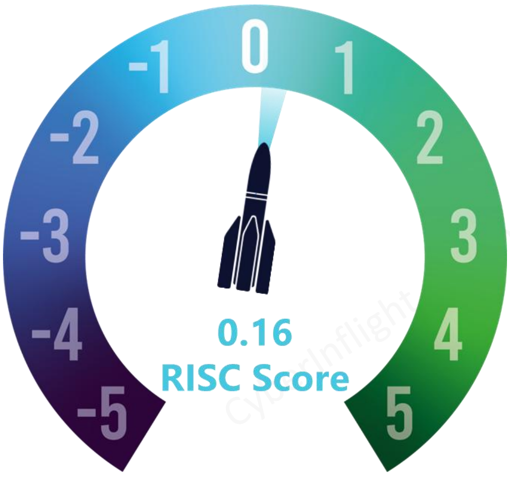
March 3 – 9, 2026

Timeframe: Weekly
# of articles identified: 27
Est. time to read: 65 minutes

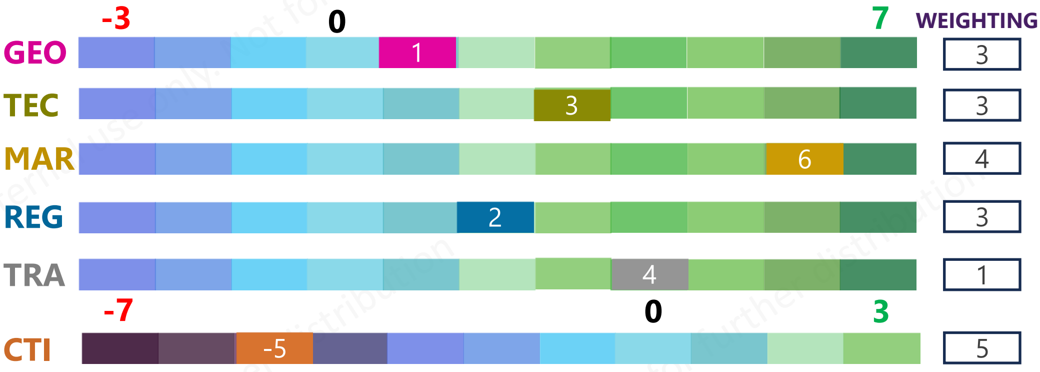
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

RISC Score Assessment

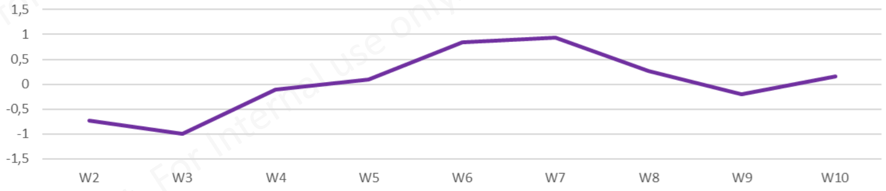


Overview & Resilience Index for Space Cybersecurity (RISC)



The RISC score for this watch is 0.16, up from last week, due to a good market balanced with an active threat and geopolitical climate

RISC Score evolution in 2026



This week, **Israel claimed a targeted strike on a Tehran compound housing Iran's cyber warfare headquarters and Intelligence Directorate**. While the operational impact on Iran's cyber capabilities remains unclear, the attack underscores the blurring line between kinetic and cyber warfare. On the regulatory side, the **Trump Administration unveiled a new U.S. Cyber Strategy**, prioritizing offensive cyber operations, federal network security, and critical infrastructure protection. The strategy also includes an executive order to combat cybercrime and fraud, signaling a shift toward proactive cyber deterrence and workforce strengthening to counter evolving digital threats. On the market front, **Lockheed Martin secured a contract to supply an anti-jamming payload for Japan's next-generation defense communications satellite**, developed by Mitsubishi Electric. This payload will enhance interoperability with allied nations and bolster resistance to electronic interference, reflecting Japan's commitment to securing its military satellite communications in an era of growing orbital threats. On the threat landscape, a **penetration test revealed over 20 security flaws in a satellite receiver widely used by the U.S. Department of Defense, ESA**, and global critical infrastructure operators. The manufacturer, International Data Casting Corporation (IDC), failed to respond to disclosure attempts, exposing a critical gap in supply chain security and the urgent need for vendor accountability in space systems. On the technological side, **DARPA's ROCkN program is advancing GPS-free timekeeping for contested battlefields**. On the academic front, a **Chinese paper proposed a comprehensive literature review of cybersecurity in satellite networks** to propose the Sat-ATT&CK knowledge matrix to model attack chains across physical, network, and user layers.

GEOPOLITICS

[illegible]

[illegible]

★ **Israel claims it 'struck' Iran's cyber warfare headquarters**

Israel has claimed a successful strike on a Tehran-based compound that housed Iran's "cyber warfare headquarters" and the "Intelligence Directorate," among others. The impact of this, however, on Iran's cyber capabilities remains unclear. **#Israel #Iran**

Source: The Cyber Express

[illegible]

[illegible]

REGULATION

[illegible]

★ **Trump Administration Unveils New Cyber Strategy for America**

President Donald Trump released his administration's cyber strategy Friday, promoting offense operations in cyberspace, securing federal networks and critical infrastructure, streamlining regulations, leveraging emerging technologies and strengthening the cybersecurity workforce. Trump also signed an executive order Friday directing agencies to take action to combat cybercrime and fraud. **#CyberStrategy #US**

Sources: CyberScoop, White House, Infosecurity Magazine

MARKET & COMPETITION

[illegible]

MARKET & COMPETITION

★ Lockheed Martin to support Japan's next-generation defense communications satellite with anti-jamming capability

Lockheed Martin, will provide a robust anti-jamming payload for Japan's Next-Generation Defense Satellite Communication System which was awarded to Mitsubishi Electric by the Japan Ministry of Defense. Serving as a mission partner to Mitsubishi Electric, Lockheed Martin's advanced payload will help maximize the satellite's capabilities. The payload will provide interoperability with allied and partner nations and enhance the satellite communications' resistance to interference. **#Contract #AntiJamming**

Sources: Lockheed Martin, Market Screener

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

THREAT INTELLIGENCE

[illegible]

THREAT INTELLIGENCE

GPS jamming is emerging as an increasingly prevalent — and troubling — weapon of war

[illegible]

Source: [illegible]

Symantec reports Iranian Seedworm hackers infiltrate US infrastructure and defense supply chain networks

[illegible]

Source: [illegible]

★ A satellite receiver trusted by Pentagon, ESA has more than 20 security flaws — and the maker never responded

A penetration tester found more than 20 vulnerabilities in a satellite receiver deployed by the U.S. Department of Defense (also referred to as the Department of War), the European Space Agency, and other critical infrastructure operators worldwide — and the device's manufacturer, International Data Casting Corporation (IDC), did not respond to a single disclosure attempt over several months. **#CVE #SFX2100**

Sources: The Cyber Express, CyboWatch

Two key Russian satellite communication providers are 'no longer in touch': Ukrainian hackers attacked Tricolor and Gazprom Space Systems

[illegible]

Source: [illegible]

TECHNOLOGY

★ U.S. Defense Program Advaces GPS-fre timekeeping for contested battlefield

The U.S. DARPA is advancing the ROCkN (Robust Optical Clock Network) program to develop highly precise timekeeping systems that can operate without GPS. The initiative aims to ensure reliable synchronization for military operations in environments where GPS signals may be jammed or denied. By using advanced optical clocks and networked timing technologies, the program seeks to maintain ultra-precise coordination of sensors, communications, and targeting systems on contested battlefields. **#ROCkN #GPS**

Source: Defense Mirror

Austria military's first satellite will hunt for GPS, Galileo interference

[illegible]

Sources: [illegible]

TRAINING & EDUCATION

Mitigating machine-in-the-loop drone attacks on satellite links via atmospheric scintillation analysis

[illegible]

Source: [illegible]

TRAINING & EDUCATION

[illegible]

★ A comprehensive literature review of cybersecurity in satellite networks

Satellite networks are essential to global connectivity yet face severe multidimensional cybersecurity threats. This systematic review conducts a holistic analysis of threats across the physical, network, and user layers. We propose the Sat-ATT&CK knowledge matrix to model satellite-specific attack chains. **#Paper #ThreatModeling**

Source: MDPI

[illegible]

[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