



SPACE CYBERSECURITY WEEKLY WATCH

W14

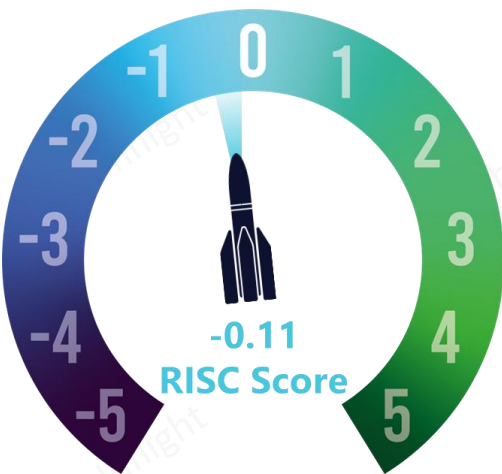
April 1 – 6, 2026

Timeframe: Weekly
of articles identified: 26
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.

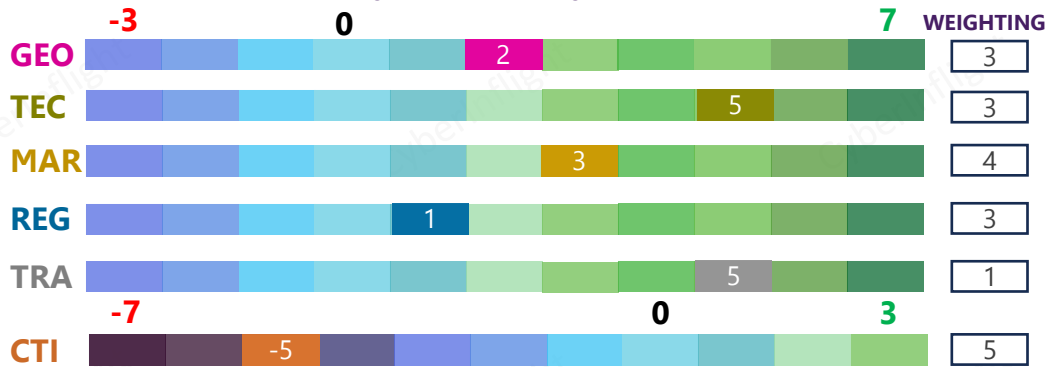
- GEOPOLITICS
- TECHNOLOGY
- MARKET & COMPETITION
- REGULATION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- ★ IMPORTANT NEWS

RISC Score Assessment

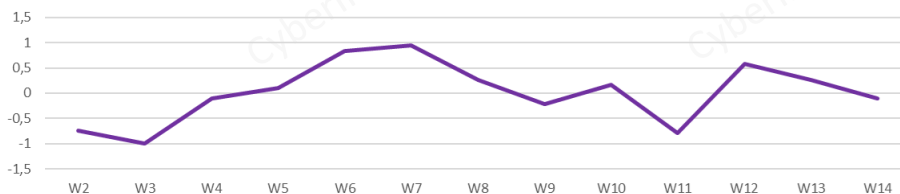


The RISC score for this watch is -0.11, down from last week due to an active threat climate and geopolitical news balanced with a technological innovations

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



This week, the **Russia-Ukraine War continues to reshape perspectives on cyber warfare**, challenging long-held theories about its role in major combat operations. This evolution is prompting militaries worldwide to rethink their cyber doctrine and force structure for future conflicts. On the market front, **the U.S. Military's GPS Next-Generation Operational Control System (OCX) has become an \$8bn debacle**, with costs more than doubling since its inception in 2010. Originally slated for completion in 2016 at \$3.7bn, the program has faced persistent delays. OCX is critical for managing the GPS III satellite constellation, which introduces new signals and jam-resistant capabilities, but its troubled development highlights the challenges of modernizing legacy space systems under budgetary and technical constraints. On the threat landscape, **a critical vulnerability (CVE-2025-47392) in Qualcomm's Snapdragon chips exposes satellite data decoding to memory corruption** via integer overflow. Exploitable from adjacent networks without privileges, this flaw could allow attackers to disrupt GPS-related services in vehicles, IoT devices, and embedded systems. Organizations processing satellite positioning data are urged to treat this as an urgent priority, as compromised inputs could lead to loss of confidentiality, integrity, and availability. On the technological side, **China revealed new details about its "Zhuri" space solar power plant**, designed not only for energy transmission but also for military applications, including communication, navigation, reconnaissance, and signal interference. On the training front, **a new analysis from the U.S. Army's Center for Army Lessons Learned emphasizes the need for resilient communications architectures that combine tactical radios with integrated cyber defense**. Commercial SATCOM, while providing global reach, remains vulnerable to jamming, spoofing, and cyber intrusions.



GEOPOLITICS



From bombers to bytes: rethinking cyber operations in light of the Russia-Ukraine War

The proliferation of computing and the dependency on networking in modern life have only increased their fears of cyber-Pearl Harbors and wars that both begin and end in cyberspace. Fortunately, American theories about the role and nature of cyber warfare in major combat operations remain largely untested due to the lack of a great power conflict.

#Opinion #RussiaUkraineWar

Source: [AFCEA](#)



REGULATION

EU and Europe review EU cybersecurity guidelines as spending rises again

EU cybersecurity guidelines are under review as the Commission considers a new cybersecurity strategy. The Commission is also reviewing the EU Cyber Resilience Act and the EU Cyber Security Strategy. The Commission is also reviewing the EU Cyber Resilience Act and the EU Cyber Security Strategy.

Source: [EU Reporter](#)

Source: [EU Reporter](#)

MARKET & COMPETITION

Encouraging SMEs for quantum communication and supply chain growth

The European Commission is launching a new initiative to support SMEs in the quantum communication and supply chain sectors. The Commission is also reviewing the EU Cyber Resilience Act and the EU Cyber Security Strategy.

Source: [Quantum Europe](#)

Source: [Quantum Europe](#)

Concrete goals over U.S. military satellite supply chain vulnerabilities

The European Commission is launching a new initiative to support SMEs in the quantum communication and supply chain sectors. The Commission is also reviewing the EU Cyber Resilience Act and the EU Cyber Security Strategy.

Source: [Quantum Europe](#)

Source: [Quantum Europe](#)

Reduce SMEs' costs EU quantum secure satellite contract for QSSat Program

The European Commission is launching a new initiative to support SMEs in the quantum communication and supply chain sectors. The Commission is also reviewing the EU Cyber Resilience Act and the EU Cyber Security Strategy.

Source: [Quantum Europe](#)

European supports more SMEs for strategic supply chain support in SMEs

The European Commission is launching a new initiative to support SMEs in the quantum communication and supply chain sectors. The Commission is also reviewing the EU Cyber Resilience Act and the EU Cyber Security Strategy.

Source: [Quantum Europe](#)





MARKET & COMPETITION



The U.S. Military's GPS software Is an \$8bn mess

The GPS Next-Generation Operational Control System, or OCX, is designed for command and control of the military's constellation of more than 30 GPS satellites. It consists of software to handle new signals and jam-resistant capabilities of the latest generation of GPS satellites, GPS III, which started launching in 2018. RTX Corporation, formerly known as Raytheon, won a Pentagon contract in 2010 to develop and deliver the control system. The program was supposed to be complete in 2016 at a cost of \$3.7 billion. Today, the official cost for the ground system for the GPS III satellites stands at \$7.6 billion. **#OCX #Raytheon**

Sources: [DNYUZ](#), [SpaceNews](#)



THREAT INTELLIGENCE

France's military satellites are being hacked

French military satellites are being hacked, according to a report from the French intelligence community. The report states that the hackers are using a sophisticated technique to intercept and manipulate the data being transmitted by the satellites. The report also mentions that the hackers are using a technique called "spoofing" to make the satellites appear to be transmitting false information.



Source: [France 24](#)

North Korea's satellite navigation system is being hacked

North Korea's satellite navigation system is being hacked, according to a report from the South Korean intelligence community. The report states that the hackers are using a sophisticated technique to intercept and manipulate the data being transmitted by the satellites. The report also mentions that the hackers are using a technique called "spoofing" to make the satellites appear to be transmitting false information.



Source: [The Korea Times](#)

US military satellites are being hacked

US military satellites are being hacked, according to a report from the US intelligence community. The report states that the hackers are using a sophisticated technique to intercept and manipulate the data being transmitted by the satellites. The report also mentions that the hackers are using a technique called "spoofing" to make the satellites appear to be transmitting false information.



Source: [The Washington Post](#)

Iranian military satellites are being hacked

Iranian military satellites are being hacked, according to a report from the US intelligence community. The report states that the hackers are using a sophisticated technique to intercept and manipulate the data being transmitted by the satellites. The report also mentions that the hackers are using a technique called "spoofing" to make the satellites appear to be transmitting false information.



Source: [The New York Times](#)

CVE Alert: CVE-2025-47392 – Qualcomm, Inc. – Snapdragon

High risk memory corruption via integer overflow in satellite data decoding, exploitable from an adjacent network with no privileges required; treat as an urgent priority for systems processing potentially tainted positioning data. If an attacker can influence the satellite data inputs, they can drive out-of-bounds memory behaviour leading to loss of confidentiality, integrity, and availability. The practical business impact is service disruption and potential compromise of GPS-related processing in vehicles, IoT, and embedded deployments where positioning feeds drive safety- or location-dependent decisions. **#CVE2025-47392 #Qualcomm**

Source: [RedPacket Security](#), [The Hacker Wire](#)



Warning about satellite communications network being hacked

The report states that the hackers are using a sophisticated technique to intercept and manipulate the data being transmitted by the satellites. The report also mentions that the hackers are using a technique called "spoofing" to make the satellites appear to be transmitting false information.



Source: [The Guardian](#)

Warning about satellite communications network being hacked

The report states that the hackers are using a sophisticated technique to intercept and manipulate the data being transmitted by the satellites. The report also mentions that the hackers are using a technique called "spoofing" to make the satellites appear to be transmitting false information.



Source: [The Guardian](#)





TRAINING & EDUCATION

Resilience through modular, graph-based P2P architectures for satellite-based systems
This article explores how resilient architectures can be achieved through modular, graph-based P2P architectures for satellite-based systems. It discusses the challenges of traditional architectures and how P2P architectures can provide a more resilient and scalable solution. The article also covers the design and implementation of such architectures, including the use of graph-based data structures and distributed algorithms.



High precision geospatial intelligence using an auxiliary location determination configuration for P2P systems
This article discusses the use of auxiliary location determination configurations for P2P systems to achieve high precision geospatial intelligence. It covers the challenges of traditional location determination methods and how P2P systems can provide a more accurate and resilient solution. The article also covers the design and implementation of such configurations, including the use of distributed algorithms and data structures.



The satellite designing secure satellite systems with P2P, I2P, and DHT
This article discusses the design of secure satellite systems using P2P, I2P, and DHT technologies. It covers the challenges of traditional satellite systems and how P2P, I2P, and DHT technologies can provide a more secure and resilient solution. The article also covers the design and implementation of such systems, including the use of distributed algorithms and data structures.



Advanced satellite collaboration with the University of Arizona to reduce atmospheric space operations
This article discusses the collaboration between the University of Arizona and the author to reduce atmospheric space operations. It covers the challenges of traditional space operations and how advanced satellite collaboration can provide a more efficient and resilient solution. The article also covers the design and implementation of such collaborations, including the use of distributed algorithms and data structures.



Beyond SATCOM: how tactical radios and cyber defense forge coalition resilience

To maintain decision advantage in contested environments, commanders must build a resilient communications architecture layered with tactical radios and integrated cyber defense. While commercial SATCOM provides reach, its vulnerabilities to jamming, spoofing, and cyber intrusion demand a robust PACE plan. The U.S. Army Southern European Task Force, Africa (SETAF-AF) G6 actively advances this capability by improving multinational interoperability through research, targeted training, and operational collaboration. **#Paper #CenterforArmyLessonsLearned**



Source: [US Army](#)

*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*