SPACE CYBERSECURITY WEEKLY WATCH

W14

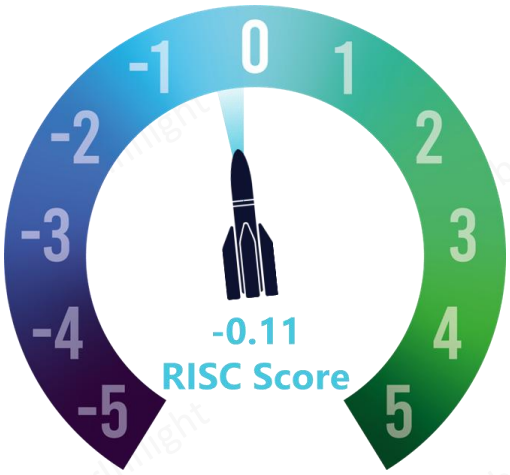
April 1 – 6, 2026

Timeframe: Weekly
# of articles identified: 26
Est. time to read: 65 minutes

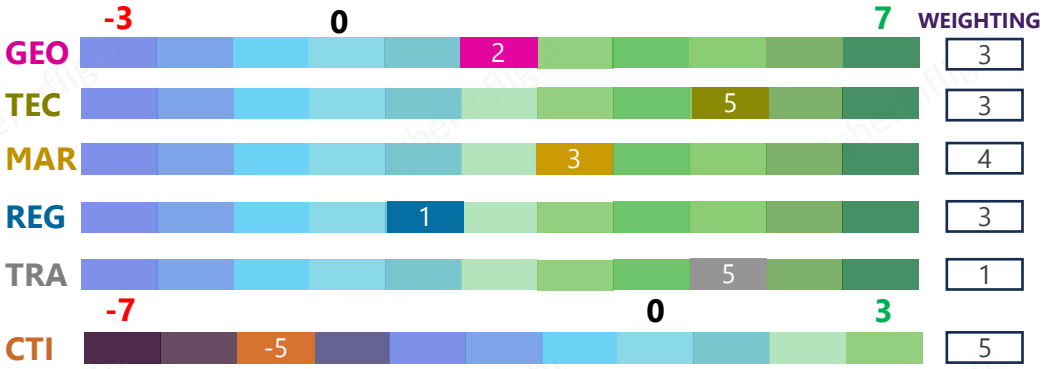
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

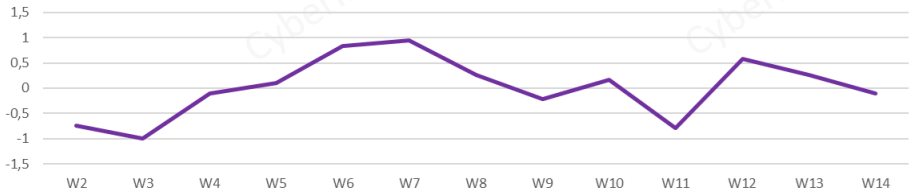
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



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

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 n**ew 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

[redacted]

[redacted]

REGULATION

[redacted]

[redacted]

MARKET & COMPETITION

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

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

[redacted]

[redacted]

[redacted]

[redacted]

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

[redacted]

[redacted]

TECHNOLOGY

[redacted]

[redacted]

[redacted]

China reveals military capabilities in new space solar power plant design

Duan Baoyan, a leading architect of China's "Zhuri" space solar power initiative, wrote in a paper published in Scientia Sinica Informationis last month, that his team had revamped the design of the giant orbital infrastructure. In addition to energy transmission, the new system was required to support a wide range of tasks "such as communication, navigation, reconnaissance, interference and remote control", he said. While designed to improve the efficiency and accuracy of wireless power transmission, these capabilities could, in principle, enable targeted signal transmission, including potential applications such as jamming or securing military communications. **#China #EW**

Source: South China Morning Post

[redacted]

[redacted]

TRAINING & EDUCATION

[redacted]

[redacted]

[redacted]

TRAINING & EDUCATION

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

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