SPACE CYBERSECURITY WEEKLY WATCH

W6

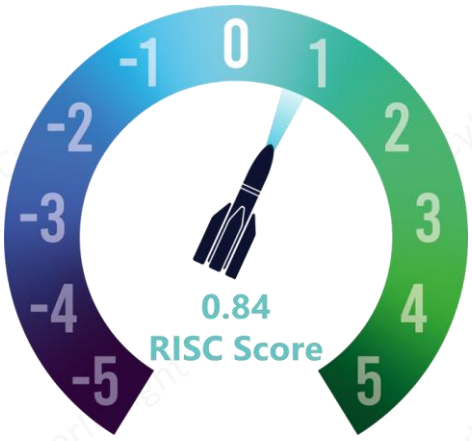
February 3 – 9, 2026

Timeframe: Weekly
# of articles identified: 37
Est. time to read: 80 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.

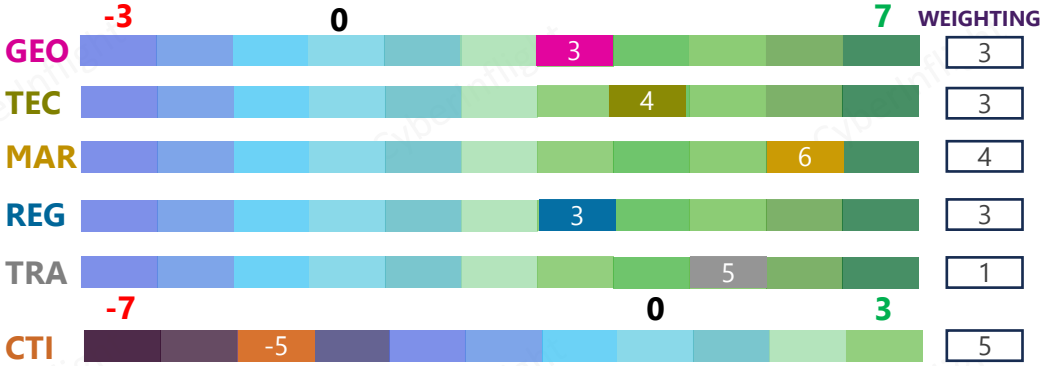
GEOPOLITICS
TECHNOLOGY
MARKET & COMPETITION
REGULATION
TRAINING & EDUCATION
THREAT INTELLIGENCE
IMPORTANT NEWS

RISC Score Assessment



The RISC score for this watch is 0.84, up from last week, driven by stronger scores in the Technology and Market sections. This score is balanced by an active threat climate.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score changes in 2026

In 2026, CyberInflight updated its methodology for calculating the RISC Score to better reflect observed realities. The scoring ranges for some categories were adjusted, as these were rarely assessed negatively and more often show moderate to high positive signals. The weighting of Technology was also increased. This change enables the RISC Score to more accurately capture meaningful variations in the risk environment.

This week, **Starlink cut off Russian troops' access to its satellite internet in Ukraine**, following a direct request from Kyiv. The move disrupted Moscow's frontline communications, highlighting the growing role of commercial space infrastructure in modern conflicts and the strategic leverage of private actors like SpaceX. On the regulatory side, **the White House advanced a draft Executive Order to unify U.S. quantum policy**, establishing a whole-of-government strategy to accelerate innovation, secure supply chains, and maintain American leadership. On the technological front, **China unveiled the TPG1000Cs, the world's first compact high-power microwave weapon capable of disrupting low-Earth-orbit satellites like Starlink**. With a sustained output of 20 gigawatts, this system raises concerns about the vulnerability of satellite constellations to ground-based directed-energy attacks, potentially reshaping the future of electronic warfare in space. Regarding the threat landscape, **European security officials revealed that Russian "inspector" satellites have intercepted communications** from at least a dozen key European spacecraft. These maneuvers, targeting unencrypted command links, risk not only espionage but also potential manipulation of satellite trajectories, underscoring the need for robust space situational awareness and encrypted systems. On the market front, **Spirent partnered with ESA to launch a PNT resilience initiative** for critical national infrastructure. The project will provide UK operators with a comprehensive test framework to measure, track, and enhance the robustness of positioning, navigation, and timing systems against growing disruptions, addressing a long-standing gap in GNSS security. Lastly, a **paper explores distributed anti-jamming strategies for LEO mega-constellations** using game-theoretic beamforming.

GEOPOLITICS

[redacted]

Musk's Starlink blocks Russian troops' internet access at Ukraine's request

Russian troops fighting in Ukraine have reported losing their Starlink satellite internet, according to Russia's pro-war military bloggers, after the SpaceX tycoon Elon Musk acted on a Ukrainian request to curtail access to his network, which Russian soldiers had been using illicitly. **#Starlink #Russia**

Source: DNYUZ

[redacted]

REGULATION

Draft quantum order tasks many agencies with reinvigorating the tech's development

The White House is currently developing a landmark Executive Order focused on quantum information sciences and technology, which is expected to establish a whole-of-government approach to bolstering the U.S. quantum ecosystem. **#Draft #Quantum**

Source: NextGov

[redacted]

[redacted]

TECHNOLOGY

[redacted]

[redacted]

TECHNOLOGY

[redacted]

[redacted]

China unveils microwave weapon capable of disrupting Starlink satellites

Chinese researchers say they have developed the world's first compact high-power microwave weapon capable of sustained output strong enough to disrupt low-Earth-orbit satellites, raising fresh concerns over space security. **#Disruption #TPG1000Cs**

Source: Tipp Insights

[redacted]

[redacted]

THREAT INTELLIGENCE

Russian spy spacecraft have intercepted Europe's key satellites, officials believe

European security officials believe two Russian space vehicles have intercepted the communications of at least a dozen key satellites over the continent. Officials believe that the likely interceptions, which have not previously been reported, risk not only compromising sensitive information transmitted by the satellites but could also allow Moscow to manipulate their trajectories or even crash them. **#SIGINT #Russia**

Source: FinancialTimes, Kyiv Post

[redacted]

[redacted]

THREAT INTELLIGENCE

Ransomware group Sept hits Honeywell Aerospace (Global/USA)

In the latest cybersecurity news, the ransomware group Sept claimed responsibility for a cyberattack on Honeywell Aerospace (honeywell.com), a major U.S. aerospace corporation. The group threatened to leak sensitive avionics software and satellite communication designs unless negotiations are undertaken. #Ransomware #HoneywellAerospace

Source: DarkPitch Defense

US spy satellite agency declassifies high-flying Cold War listening post

The National Reconnaissance Office, the agency overseeing the US government's fleet of spy satellites, has declassified a decades-old program used to eavesdrop on the Soviet Union's military communications signals. CANYON, a now-retired series of eavesdropping satellites that flew from 1971 to 1987 as part of an electronic effort known as Project GAMMA. #CANYON #Eavesdropping

Source: ARS Technica Newspr

Platonychka satellites, robotic arms: former US Space Force Commander warns of Russian, Chinese threats

Cosmos 2558 had been observed shadowing USA 326 ever since being launched in 2021. But now it had hatched a surprise by releasing a smaller module that started moving even closer to the US satellite. #USSF #Russia

Source: RT/DL

Alleged ransomware attack on Yulchon

Ransomware attack hits Yulchon LLP, a leading South Korean aerospace manufacturer partnered with Boeing, Airbus, and Korea Aerospace Industries. The threat actor 'Sweet' claims responsibility. #Ransomware #Sweet

Source: X

MARKET & COMPETITION

From GEO to multi-orbit: how SES NetOps is powering the next phase of Middle East SatCom

Interview with Ali Al Kuwari, Executive CEO of SES NetOps. #Interview #SESNetOps

Source: SatNews International

Furuno and Xona Space Systems sign MoU to develop innovative LEO PNT solutions

Furuno Electric and Xona Space Systems have signed a Memorandum of Understanding (MoU) to collaborate on solutions using Xona Pulse, a low-Earth orbit positioning, navigation and timing (LEO PNT) service for next-generation satellite navigation. #Furuno #LEOPNT

Source: GPSWorld Inside GNSS

Space Force plans to create a contractor pool for 'physical/live' training needs in the summer

The Space Force is planning to issue a new contract this summer to create a pool of qualified vendors to help fill Guardian needs for hands-on training in electronic, cyber, and orbital warfare — with the latter to eventually involve dedicated satellites in orbit, according to service officials leading the effort. #USSF #SpaceCommand

Source: BreakingDefense

Wisekey, Wisesat and Latitude join forces to prepare a future secure IoT satellite constellation

Wisekey, and its subsidiary Wisesat Space AG which focuses on space technology for secure satellite communication, specifically for IoT applications, and Latitude, a French aerospace company designing, manufacturing, and operating an orbital launch vehicle, today announced the signing of a commercial agreement to assess the orbital launch of Wisesat's planned secure IoT satellite constellation. #IoT #Constellation

Source: WiSekey

U.S. intelligence contract for Vantor builds on digital 'living globe' surveillance program

Defense intelligence firm Vantor has captured a $1.1 million contract from the National Geospatial-Intelligence Agency to leverage artificial intelligence for detecting real-time changes from the company's own imaging satellites and space-based sensors. The Vista add Vantor's capabilities aim to provide intelligence "that provides a decisive advantage to policymakers, warfighters, intelligence professionals, and first responders from anywhere in space. #Contract #USG

Source: Washington Times

MARKET & COMPETITION

[redacted]

Spirent partners with ESA to spearhead PNT resilience initiative for critical infrastructure

Spirent Communications, now part of Keysight Technologies, has partnered with the European Space Agency (ESA) to lead an initiative aimed at increasing the resilience of positioning, navigation and timing (PNT) systems used in critical national infrastructure. Under the initiative, Spirent and partners will deliver a comprehensive test framework to drive measurable resilience in PNT systems for users, operators and providers of critical infrastructure in the United Kingdom.

#Contract #NAVISP

Source: GPS World

[redacted]

[redacted]

[redacted]

TRAINING & EDUCATION

[redacted]

[redacted]

TRAINING & EDUCATION

Distributed uplink anti-jamming in LEO mega-constellations via game-theoretic beamforming

Low-Earth-Orbit (LEO) satellite constellations have become vital in emerging commercial and defense Non-Terrestrial Networks (NTNs). However, their predictable orbital dynamics and exposed geometries make them highly susceptible to ground-based jamming. Traditional single-satellite interference mitigation techniques struggle to spatially separate desired uplink signals from nearby jammers, even with large antenna arrays. This paper explores a distributed multi-satellite anti-jamming strategy leveraging the dense connectivity and high-speed inter-satellite links of modern LEO mega-constellations. **#Paper #AntiJamming**

Source: Cornell University

[redacted]

[redacted]