SPACE CYBERSECURITY WEEKLY WATCH

W5

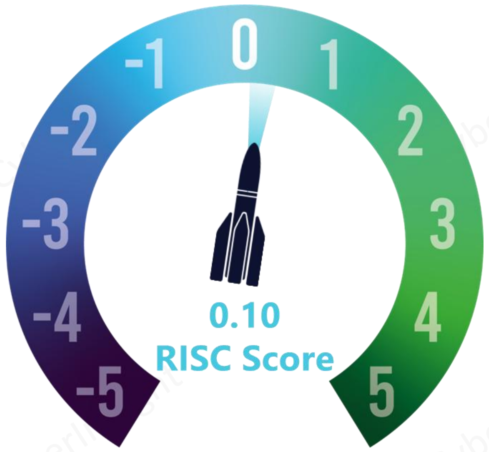
January 27 – February 2, 2026

Timeframe: Weekly
# of articles identified: 18
Est. time to read: 45 minutes

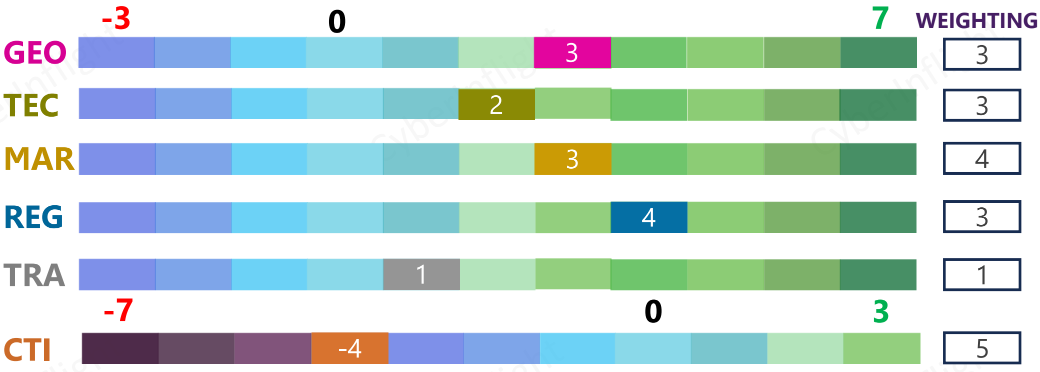
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

- 🟥 **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 0.10, up from last week, notably because of a better threat and geopolitical climate.

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, **SpaceX moved to block Russia's unauthorized use of Starlink on attack drones in Ukraine, following urgent outreach from Ukraine's Ministry of Defense**. The measures highlight the growing role of commercial satellite operators as active stakeholders in modern conflict, as well as the increasing entanglement of private space infrastructure in military and geopolitical dynamics. On the regulatory front, **Pakistan announced plans to develop dedicated cybersecurity regulations for satellite communication services**, aimed at governing how global satellite internet providers operate within the country. On the technological front, **China reached a major milestone in space-based computing with the deployment of Alibaba's Qwen-3 general-purpose AI model in orbit**. Integrated with satellite sensors, the system demonstrates China's growing capabilities in autonomous space operations, reducing reliance on ground infrastructure while lowering latency, bandwidth requirements, and exposure to jamming or cyber disruption. On the threat intel. side, **U.S. defense officials highlighted the role of the new "Cybercom 2.0" force-generation model** in countering Chinese cyber actors who employ "living off the land" techniques. On the market front, **SES and EUSPA confirmed the extension of the EGNOS GEO-1 service agreement through 2030**, with an option to extend to 2032. The decision secures Europe's satellite-based navigation augmentation capability and reinforces the long-term importance of resilient positioning, navigation, and timing services for civil aviation and critical infrastructure. Lastly, on the training and research front, **a decade-long academic study analyzing GNSS-R observations highlighted the global intensification of GNSS signal disruptions due to radio-frequency interference**.

GEOPOLITICS

[redacted]

[redacted]

[redacted]

SpaceX blocks Russian Starlink access on attack drones in Ukraine

SpaceX implemented measures to block Russia's unauthorized use of Starlink on attack drones targeting Ukraine, with Elon Musk announcing on Sunday that the steps proved effective following urgent outreach from Ukraine's Defense Ministry. **#Starlink #Drones**

Source: DataEconomy

REGULATION

[redacted]

Satellite Internet is Coming, But With Strict Security Rules

The Pakistan Telecommunication Authority (PTA) has decided to develop dedicated cybersecurity regulations for satellite communication services to shape how global satellite internet providers operate within the country. **#CybersecurityFrameworks #PTA**

Source: propakistani

TECHNOLOGY

China Deploys Space-Based AI Integrated With Satellite Sensors: A Game Changer For Next Generation Warfare

The Chinese firm Alibaba's Qwen-3 on January 25 was confirmed to have become one of the world's first general-purpose artificial intelligence models to be uploaded and operated in orbit, marking a major milestone in China's emerging leadership in the space-based computing sector. Chinese aerospace start-up Adaspace Technology deployed Qwen-3 to a space computing centre in orbit, where it executed multiple inference tasks in November. The deployment of Qwen-3 strengthens China's position in space-based computing and autonomous satellite operations, dramatically reducing latency, bandwidth demand, and vulnerability to jamming or cyber disruption by almost totally eliminating reliance on ground infrastructure. **#Qwen-3 #AI**

Source: Military Watch Magazine

THREAT INTELLIGENCE

[illegible]

[illegible]

★ Pentagon leaders expect Cybercom 2.0 to help thwart Chinese actors 'living off the land'

Senior officials at the Defense Department say the Pentagon's new cyber force generation model will help the military boot out Chinese threats from America's critical infrastructure networks. A digital tactic known as "living off the land" has been a concern for U.S. officials in recent years as actors linked to China, such as Volt Typhoon, have infiltrated networks in the United States. A key element of the new model is to focus more on cultivating specialization among the cyber workforce rather than rotating people through assignments as generalists. For example, some teams might be trained to defend satellite communications and GPS systems, while others specialize in protecting power grids and transportation networks. **#Cybercom #Cyberthreats**

Source: DefenseScoop

[illegible]

[illegible]

[illegible]

MARKET & COMPETITION

[illegible]

[illegible]

MARKET & COMPETITION

[redacted]

★ EGNOS Secured Until 2030: Why Europe’s Navigation Backbone Matters

SES and the European Union Agency for the Space Programme (EUSPA) have confirmed an extension of the European Geostationary Navigation Overlay Service (EGNOS) GEO-1 satellite service agreement through 2030, with an option to run until 2032. **#Contract #EGNOS**

Source: Alertify

TRAINING & EDUCATION

★ A Decade of GNSS Signal Disruptions in SMAP-R Full-Polarimetric Observations Worldwide

GNSS-R signals enable the analysis of Earth’s surface scattering properties but are highly vulnerable to radio-frequency interference (RFI), especially in conflict zones. The Ukraine–Russia war illustrates an unprecedented intensification of GNSS jamming, impacting both navigation services and remote sensing systems. This study analyzes global RFI using GNSS-R L2c measurements from SMAP-R since 2015, enabling, for the first time, worldwide temporal and polarimetric monitoring. The results reveal strong disturbances over Eastern Europe, Syria, and Burma, with significant signal depolarization, rendering geophysical parameter retrieval unfeasible. **#GNSSDisruptions #RFI**

Source: IEEEXplore

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