

SPACE CYBERSECURITY WEEKLY WATCH

W20

May 12 – May 18, 2026

Timeframe: Weekly

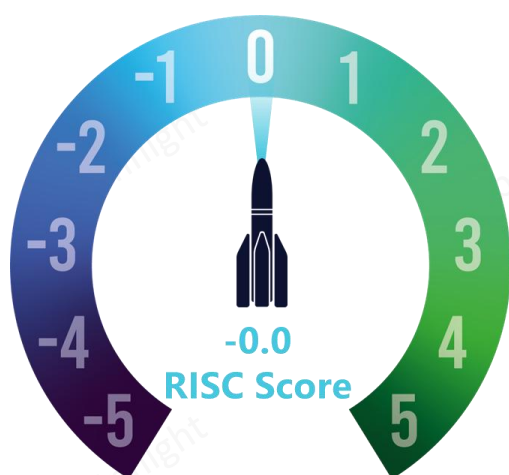
of articles identified: 22

Est. time to read: 40 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

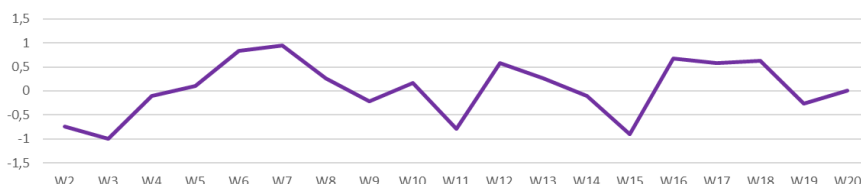


The RISC score for this watch is 0.0, up 0.27 from last week. This neutral score is due to very little news this week, except for Training, which brings the score up a bit compared to last week.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



This week, on the geopolitical front, **U.S. Special Operations Command (SOCOM) is reportedly testing the web-based platform launched by Texas startup SkyFi**, which would provide operators with real-time satellite imagery through integrated commercial satellite networks. On the regulatory side, **the Gibbons Institute of Law, Science & Technology hosted the Workshop on Cybersecurity on Earth and in Space** as an open forum for scholars to present their research in this field and receive peer feedback. On the market front, the **project COSMOS-SECURE represents one of the most strategically forward-looking investments the European Union has made into Slovak deep tech in recent years**. Discover it! On the threat side, **a paper about space hacktivism and the Russo-Ukrainian war has been published**. This paper analyzes primary sources released by NB65, a Ukrainian hacktivist group affiliated with Anonymous, to present a likely kill chain that enabled the claimed intrusion into a ROSCOSMOS ground segment. Building on previously published findings, it proposes a space policy directive to secure space systems from cyberattacks, informed by this analysis, with the aim of enhancing international technical standards for space system cybersecurity. In the technology category, **Surrey Research Park and UK Space Agency strengthen resilience across the UK space supply chain**, as part of proactive action to bolster resilience against threats targeting UK space and space-related companies. Lastly, in the training section, the **SmallSat Europe 2026 Defense Agenda (May 26–28)** brings together military leaders, startup founders, and industry executives for 3 days of keynotes, panels, and tech briefs spanning launch access, resilient communications, AI, missile defense, and the evolving orbital threat environment.

GEOPOLITICS



The Pentagon is transforming U.S. commercial satellites into tactical battlefield infrastructure

For special operations forces (SOF) operating in hostile environments, access to up-to-date geospatial intelligence (GEOINT) can dramatically shape operational decision-making and mission success. The U.S. military is now addressing this challenge. U.S. Special Operations Command (SOCOM) is reportedly testing the web-based platform launched by Texas startup SkyFi, which would provide operators with real-time satellite imagery through integrated commercial satellite networks. **#Pentagon #Battlefield**

Source: [FDD](#)



REGULATION



Workshop on space law and emerging cybersecurity challenges

The Gibbons Institute of Law, Science & Technology at the school hosted the Workshop on Cybersecurity on Earth and in Space on April 16, 2026, as an open forum for scholars to present their research in this field and to receive peer feedback. **#Workshop #SpaceLaw**

Source: [SetonHall](#)



MARKET & COMPETITION



COSMOS-SECURE: Decent cybersecurity leads Europe's push for quantum-safe voice communication in space

The project, formally titled "Bezpečná komunikácia vo vesmírnom výskume" or in English "Secure Communication in Space Research", represents one of the most strategically forward-looking investments the European Union has made into Slovak deep tech in recent years. With total eligible costs of more than €4m and a requested EU contribution of €2m, COSMOS-SECURE will run from January 2026 through December 2029 and is co-financed by the European Union through Program Slovensko 2021 to 2027 and the European Regional Development Fund. **#COSMOS-SECURE #DecentCybersecurity**

Source: [HealSecurity](#)



THREAT INTELLIGENCE



THREAT INTELLIGENCE

Space Threat Intelligence from Strategic Space Task Assessment Report

The report details the findings of the Strategic Space Task Assessment, an analysis of the current state of space security, covering various aspects of space operations, including satellite operations, space-based systems, and space-based threats. The report identifies key areas of concern, such as the potential for space-based cyberattacks, the risk of space-based weapons, and the need for international cooperation to address these threats.

Source: [Space.com](#)



Security experts warn Chinese satellite is suspected spying on US

Security experts warn that a Chinese satellite, believed to be a spy satellite, is suspected of spying on US military and intelligence operations. The satellite, which is believed to be a Chinese-made satellite, is suspected of being used to collect intelligence on US military and intelligence operations. The report identifies key areas of concern, such as the potential for space-based cyberattacks, the risk of space-based weapons, and the need for international cooperation to address these threats.

Source: [The Guardian](#)



Space hacktivism and the Russo-Ukrainian war: an open source space security analysis

In March of 2022, Network Battalion-65 (NB65), a hacktivist group affiliated with Anonymous, claimed responsibility for breaching a ROSCOSMOS ground segment in retaliation for Russia's invasion of Ukraine. NB65 released several primary sources to support its claims, alleging it had disabled ROSCOSMOS's vehicle monitoring system and exposed sensitive proprietary documents. This paper analyzes the primary sources released by NB65 to present the likely kill chain that enabled the claimed intrusion of a ROSCOSMOS ground segment. Building on previously published findings, it proposes a space policy directive for securing space systems from cyberattacks, informed by the results of this analysis, with the aim of enhancing international technical standards for space system cybersecurity. **#Hacktivism #SpaceSecurity**

Source: [Oxford Academic](#)



TECHNOLOGY

How artificial intelligence is reshaping space security

Artificial intelligence (AI) is reshaping space security by enabling more sophisticated threat detection and response capabilities. AI-powered systems can analyze vast amounts of data from various sources, including satellite imagery, ground-based sensors, and open-source intelligence, to identify potential threats and anomalies. This technology is being used to enhance the security of space-based systems and to protect against cyberattacks and other threats to space operations.

Source: [Space.com](#)



Surrey Research Park and UK Space Agency strengthen resilience across the UK space supply chain

Surrey Research Park was delighted to welcome experts from the UK Space Agency's National Security team at the end of April as part of proactive action to bolster resilience against threats targeting UK space and space-related companies. **#UKSpaceAgency #SurreyResearchPark**

Source: [University of Surrey](#)



The key to secure satellite communications

Secure satellite communications are essential for many critical applications, including defense, intelligence, and emergency services. Ensuring the security of these communications is a complex task that involves a combination of technical and operational measures. This article explores the key challenges and solutions for securing satellite communications, highlighting the importance of robust encryption, secure key management, and secure ground stations.

Source: [Space.com](#)



TRAINING & EDUCATION

Space-based intelligence is a critical component of many national security operations. Ensuring the security of this intelligence is a complex task that involves a combination of technical and operational measures. This article explores the key challenges and solutions for securing space-based intelligence, highlighting the importance of robust encryption, secure key management, and secure ground stations.

Source: [Space.com](#)



TRAINING & EDUCATION



Conferences of the SmallSat Europe Event

The SmallSat Europe 2026 Defense Agenda (May 26–28), curated by SpaceNews, brings together military leaders, startup founders, and industry executives for 3 days of keynotes, panels, and tech briefs spanning launch access, resilient communications, AI, missile defense, and the evolving orbital threat environment. **#SmallSatEUROPE #Conference**

Source: [SmallSatEUROPE](#)



Securing the space domain cyber resilience in a contested environment
How can future cyber programs be a future effort to cyber resilience through security, cybersecurity risk, and providing operational capability to space? **SmallSatEurope Agenda**



SmallSat in Space
In 2025, the global small satellite market is projected to reach \$1.5 billion, up from \$1.1 billion in 2024. The growth is driven by the increasing number of small satellites in orbit, which are used for a variety of applications, including Earth observation, communications, and scientific research. **SmallSatEurope Agenda**

Panel: Resilience in space programming strategies for conflict, disruption and espionage
Space is a critical domain for national security and economic activity. As the number of satellites in orbit grows, the potential for conflict, disruption, and espionage increases. This panel will discuss the challenges of space resilience and the need for a comprehensive approach to space security. **SmallSatEurope Agenda**



Panel: AI: Cyber Resilient Systems Engineering for Aerospace
The aerospace industry is facing a new era of challenges, including the need for more resilient systems and the ability to detect and respond to cyber threats. This panel will discuss the challenges of AI in aerospace and the need for a comprehensive approach to space security. **SmallSatEurope Agenda**



Space segment and ground segment in 2025 satellite constellations & space domain perspective
The space segment and ground segment are the two main components of a satellite constellation. This panel will discuss the challenges of space segment and ground segment and the need for a comprehensive approach to space security. **SmallSatEurope Agenda**



Space segment and ground segment in 2025 satellite constellations & space domain perspective
The space segment and ground segment are the two main components of a satellite constellation. This panel will discuss the challenges of space segment and ground segment and the need for a comprehensive approach to space security. **SmallSatEurope Agenda**

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