

SPACE CYBERSECURITY WEEKLY WATCH

W15

April 7 – 13, 2026

Timeframe: Weekly

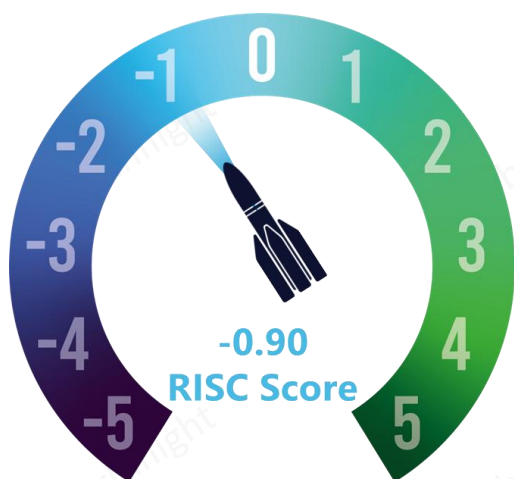
of articles identified: 21

Est. time to read: 50 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.

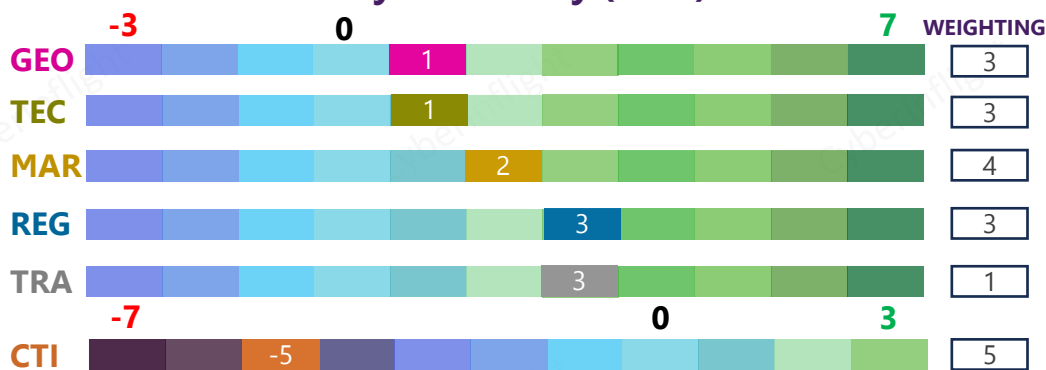
- GEOPOLITICS
- TECHNOLOGY
- MARKET & COMPETITION
- REGULATION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- ★ IMPORTANT NEWS

RISC Score Assessment

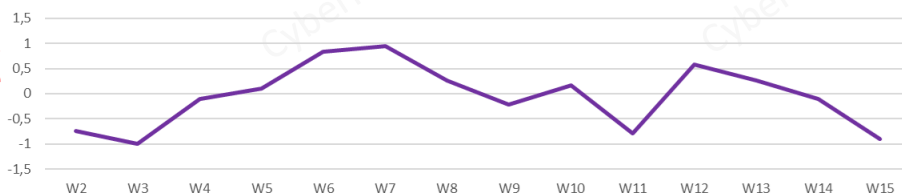


The RISC score for this watch is -0.90, down from last week due to an active threat climate and few geopolitical and market news balanced with updates on the regulation front.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



This week, **Estonia emerged as a cornerstone of Europe's space defense with the Space Cyber Range**, an integrated environment for space cybersecurity simulation, testing, and training. Hosted at Tallinn's CR14 cyber range under ESA's authority, this initiative will provide Europe with one of its first dedicated platforms to prepare for cyber threats in space, reinforcing the continent's commitment to securing its orbital assets. On the regulatory front, the **NSA released a new Cybersecurity Information Sheet (CSI) titled "Securing Space: Cyber Security for Low Earth Orbit Satellite Communications."** Developed in collaboration with Australia's ASD's ACSC and the Australian Space Agency, the report outlines high-level risks and mitigation strategies for LEO SATCOM systems, addressing vulnerabilities in space, ground, and user segments. On the market front, **Redwire secured a quantum satellite contract under the EuroQCI initiative**, marking its transition into a key industrial partner for EU defense missions. On the threat landscape, a **massive 70 GB data leak from Sekisui Aerospace**, a Tier 1 supplier for Boeing, Lockheed Martin, Northrop Grumman, and NASA, was exposed for sale by the threat actor nxe. The compromised files include engineering drawings, material specifications, and Bills of Materials (BoMs) for critical programs, as well as ITAR/EAR-controlled defense technology. This breach not only threatens corporate intellectual property but also national security, compromising supply chain integrity for U.S. defense and space programs. On the technological side, **Deloitte's space business reached new heights with the launch of two satellites carrying payloads for Project Constellation.** This initiative enables software-only, on-orbit cyber defense capabilities, designed to enhance the resilience of legacy satellites already in orbit. On the training front, a podcast with **expert detailed the advanced of the USSF Cyber Resilience On-Orbit (CROO) tool**, a software solution designed to detect and mitigate threats directly on satellites.

GEOPOLITICS



Western Russia provides cyber support and intelligence to Iran

Western Russia has provided cyber support and intelligence to Iran, according to a report from the Russian Ministry of Defense. The report states that Russian cyber forces have been involved in several operations against Iranian targets, including the disruption of Iranian cyber operations and the collection of intelligence on Iranian cyber capabilities.

Source: [RIA Novosti](#)



President: Estonia key to Europe's space defense

The role of space technology in European security is growing, making keeping up with technology developments essential, the head of state said. The Space Cyber Range is a European initiative which officially kicked off in February 2025, under the ESA area of authority. Once it is fully operational, it will be hosted at the CR14 cyber range in Tallinn and will provide one of the first integrated environments in Europe for space cybersecurity simulation, testing, training and validation.

#Estonia #ESTEC

Source: [ERR](#)



REGULATION

NSA is building a better law base without mandatory cybersecurity standards. Here's why that's a bad idea

The National Security Agency (NSA) is building a better law base without mandatory cybersecurity standards. This is a bad idea because it will leave the government vulnerable to cyber attacks. The NSA is currently working on a new law that will give it more power to collect and analyze cyber intelligence. However, this law does not include any mandatory cybersecurity standards for the government. This is a problem because it means that the government will not be able to protect itself from cyber attacks.

Source: [The Hill](#)



Commission moves to strengthen EUPS role in next phase of EU space policy

The European Commission has proposed a new role for the European Union Space Policy Office (EUSPO) in the next phase of the EU space policy. The proposal is to give the EUSPO a more active role in the development and implementation of the EU space policy. This will include the EUSPO being responsible for coordinating the EU's space policy and for ensuring that the EU's space policy is consistent with the EU's overall policy objectives.

Source: [Euronews](#)



NSA reveals details of new LEO security report

The National Security Agency (NSA) along with a number of other parties, has released a new Cybersecurity Information Sheet (CSI), a report that highlights high-level cybersecurity risks and mitigation strategies for users of LEO satellite communication systems. The report is titled "Securing Space: Cyber Security for Low Earth Orbit Satellite Communications." The NSA has worked with the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) in collaboration with the Australian Space Agency on the report. NSA revealed details of the report, March 24. **#NSA #CSI**

Source: [Via Satellite](#)



MARKET & COMPETITION

Boeing Company - Boeing Defense, Space & Security partners with Palantir to accelerate AI adoption across defense, classified programs

Boeing Company - Boeing Defense, Space & Security partners with Palantir to accelerate AI adoption across defense, classified programs. The partnership will focus on developing and deploying AI-powered solutions for defense and intelligence operations. This will include the development of AI-powered tools for threat detection, target identification, and decision-making.

Source: [Boeing](#)



Redwire's ESA quantum satellite deal expands European defense growth story

The project is being led by Redwire's European business units, emphasizing the company's successful transition into a key industrial partner for EU-based missions. This contract is part of the EuroQCI (European Quantum Communication Infrastructure) initiative, which seeks to integrate quantum-secured links into the existing telecommunications fabric of the European Union. For Redwire, this represents a shift toward high-value, specialized defense hardware that moves beyond traditional satellite components into the realm of advanced cybersecurity and national intelligence. **#Contract #EuroQCI**

Source: [SatNews](#)



MARKET & COMPETITION

USAF AFSS becomes a key player in US Space Force ground operations

USAF AFSS is becoming a key player in US Space Force ground operations. The program is designed to provide a secure, reliable, and scalable communication system for the Space Force. The program is designed to provide a secure, reliable, and scalable communication system for the Space Force. The program is designed to provide a secure, reliable, and scalable communication system for the Space Force.



Source: [USAF AFSS](#)

USAF and Space Force Command of the Space Armed Forces complete pilot phase and prepare next generation AFSS for operation planned for November 2026

USAF and Space Force Command of the Space Armed Forces complete pilot phase and prepare next generation AFSS for operation planned for November 2026. The program is designed to provide a secure, reliable, and scalable communication system for the Space Force. The program is designed to provide a secure, reliable, and scalable communication system for the Space Force.



Source: [USAF AFSS](#)

THREAT INTELLIGENCE

How space enabled military operations are vulnerable to cyberattacks

How space enabled military operations are vulnerable to cyberattacks. The program is designed to provide a secure, reliable, and scalable communication system for the Space Force. The program is designed to provide a secure, reliable, and scalable communication system for the Space Force.

Source: [USAF AFSS](#)

Cybersecurity in space is hard to achieve, it's really hard

Cybersecurity in space is hard to achieve, it's really hard. The program is designed to provide a secure, reliable, and scalable communication system for the Space Force. The program is designed to provide a secure, reliable, and scalable communication system for the Space Force.

Source: [USAF AFSS](#)

The alleged leak of China's National Supercomputing Center can have serious geopolitical implications

The alleged leak of China's National Supercomputing Center can have serious geopolitical implications. The program is designed to provide a secure, reliable, and scalable communication system for the Space Force. The program is designed to provide a secure, reliable, and scalable communication system for the Space Force.



Source: [USAF AFSS](#)

As more nations with emerging space capabilities, USF planning also must Report

As more nations with emerging space capabilities, USF planning also must Report. The program is designed to provide a secure, reliable, and scalable communication system for the Space Force. The program is designed to provide a secure, reliable, and scalable communication system for the Space Force.



Source: [USAF AFSS](#)

★ Alleged leak of military and aerospace data (Sekisui Aerospace / Boeing)

A suspected leak of critical intellectual property has been detected. The threat actor nxe has put up for sale a 70 GB package of highly confidential technical data belonging to SEKISUI Aerospace Corporation, a Tier 1 direct supplier for military and commercial programs of Boeing, Lockheed Martin, Northrop Grumman, and NASA. **#DataLeak #NXE**



Source: [X](#)

USAF AFSS becomes a key player in US Space Force ground operations

USAF AFSS is becoming a key player in US Space Force ground operations. The program is designed to provide a secure, reliable, and scalable communication system for the Space Force. The program is designed to provide a secure, reliable, and scalable communication system for the Space Force.



Source: [USAF AFSS](#)

TECHNOLOGY

Deloitte's space business reaches new heights as two new satellites enter orbit

Deloitte's space business has reached new heights as two new satellites enter orbit. The new satellites carry payloads designed to increase space data collection capacity and help meet clients' growing needs for space-based data and insights. Project Constellation enables the engineering and testing of a software-only, on-orbit cyber defense capability designed to be deployed to satellites already in orbit and to improve the cyber resiliency of legacy satellites. #SilentShield #Deloitte

Source: [PR Newswire](#)



Deloitte's space business reaches new heights as two new satellites enter orbit

The new satellites carry payloads designed to increase space data collection capacity and help meet clients' growing needs for space-based data and insights. Project Constellation enables the engineering and testing of a software-only, on-orbit cyber defense capability designed to be deployed to satellites already in orbit and to improve the cyber resiliency of legacy satellites. #SilentShield #Deloitte

Source: [PR Newswire](#)



TRAINING & EDUCATION

Interpreting satellite imagery data: A key to understanding space threats

Interpreting satellite imagery data is a key to understanding space threats. The new training module, "Interpreting Satellite Imagery Data," is designed to help space professionals understand the importance of satellite imagery in space operations and how to use it effectively. The module covers the basics of satellite imagery, including the different types of satellites and the data they collect. It also discusses the challenges of interpreting satellite imagery and provides tips on how to overcome them. #SpaceCybersecurity #Training

Source: [Apple Podcast](#)



USAF spending increases and intelligence based on satellite imagery: A key to understanding space threats

The US Air Force (USAF) is increasing its spending on satellite imagery and intelligence. This is a key to understanding space threats. The new training module, "USAF Spending Increases and Intelligence Based on Satellite Imagery," is designed to help space professionals understand the importance of satellite imagery in space operations and how to use it effectively. The module covers the basics of satellite imagery, including the different types of satellites and the data they collect. It also discusses the challenges of interpreting satellite imagery and provides tips on how to overcome them. #SpaceCybersecurity #Training

Source: [Apple Podcast](#)

Cyber resilience on-orbit a 'nervous system' for detecting threats

Cyber resilience on-orbit is a 'nervous system' for detecting threats. The new training module, "Cyber Resilience On-Orbit: A Nervous System for Detecting Threats," is designed to help space professionals understand the importance of cyber resilience in space operations and how to use it effectively. The module covers the basics of cyber resilience, including the different types of threats and the data they collect. It also discusses the challenges of interpreting cyber resilience data and provides tips on how to overcome them. #SpaceCybersecurity #Training

Source: [Apple Podcast](#)



Cyber resilience on-orbit a 'nervous system' for detecting threats

In this episode of "The Elara Edge," Major General (Ret) Kim Crider, Founding Partner at Elara Nova, and Brigadier General (Ret) Chad Raduege, President of Elara Nova's Cyber, Data, and Communications sector, provide expert perspective on the significance of the Cyber Resilience On-Orbit tool and the broader emergence of the space cyber imperative.

#Podcast #CROO

Source: [Apple Podcast](#)



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