

SPACE CYBERSECURITY WEEKLY WATCH

W21

May 19 – May 25, 2026

Timeframe: Weekly

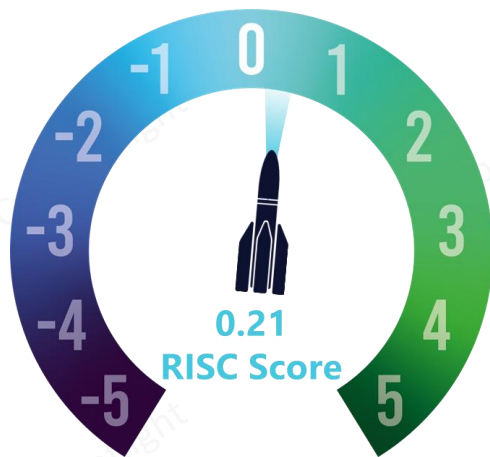
of articles identified: 23

Est. time to read: 45 minutes

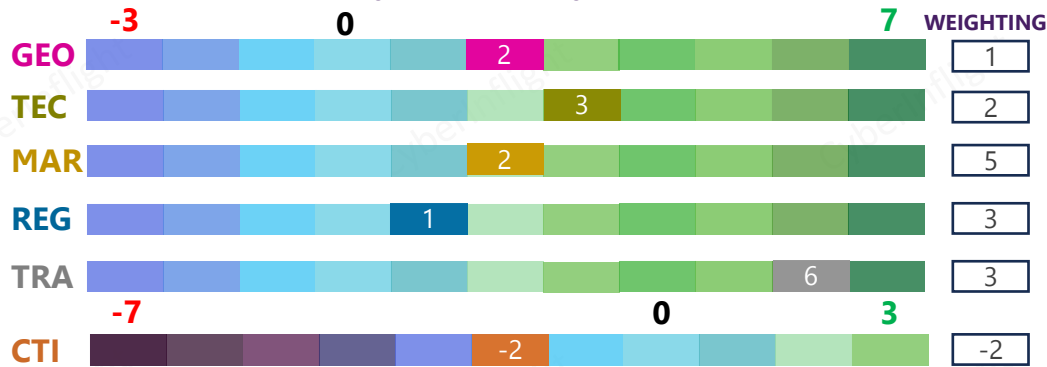
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

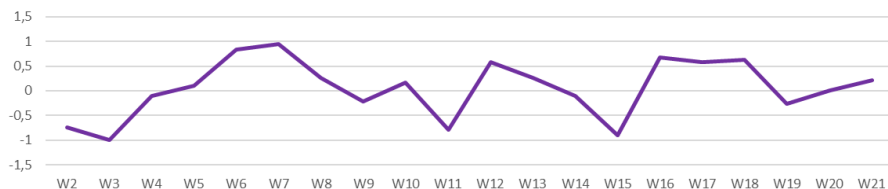
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



The RISC score for this watch is 0.21, up 0.21 from last week. This is due to still a small number of news outlets overall, but a good training and education climate, with several conferences and events held.

This week, **CyberInflight attended CYSAT 2026 in Paris and COMET by CNES in Toulouse!** Discover some of our best insights!

On the geopolitical front, **Chinese and Russian leaders Xi Jinping and Vladimir Putin used a summit in Beijing to deepen their "good neighborliness and friendly cooperation,"** which, among other initiatives, includes plans to expand collaboration on satellite internet, AI, and cybersecurity. On the regulation side, an article highlights the **EU Space Act proposal and its implications for cybersecurity, market access, and non-EU space operators.** On the market front, **York Space Systems LLC has agreed to acquire UK satellite communications company ALL.SPACE Networks Ltd.** in a transaction that deepens York's position in military connectivity infrastructure while underscoring growing investor focus on resilient communications systems designed for contested operating environments. On the threat intel aspect, according to Integrity ISR, a U.S.-based defense and intelligence firm, **Russian assets closed in on ICEYE-36, a radar satellite operated by ICEYE that delivers reconnaissance data to U.S. and European governments** — including Ukraine, which uses the data as it defends itself against Russian aggression. On the technological side, an article by Stratosphere Lab studies how we can **maintain and guarantee the integrity of satellite and payload data against threats while operating within the extreme resource constraints of small satellites.** Lastly, on the training side, **a 2-day course at DEFCON 2026 by VisionSpace** aims to teach how to analyze and exploit satellite and ground-station systems using software only in a safe lab environment.

CYBERINFLIGHT'S NEWS

CyberInflight attended CYSAT 2026 and COMET by CNES!

CyberInflight team had the pleasure of attending this year's CYSAT conference, a key gathering for the space cybersecurity ecosystem. The week continued with the COMET Cyber session at CNES premises, dedicated to CTI, with the support of the Space ISAC. **#CyberInflight #CYSAT**

Source: [LinkedIn](#)



GEOPOLITICS

Xi and Putin pledge closer cooperation on AI, cyberspace, and satellite systems

Chinese leader Xi Jinping and Russian President Vladimir Putin used a summit in Beijing to deepen their "good neighborliness and friendly cooperation," which, among other initiatives, includes plans to expand collaboration on satellite internet, artificial intelligence, cybersecurity, and internet governance. **#Cyber #Satellite**

Source: [The Record](#)



REGULATION

The EU Space Act proposal in the legislative process: Cybersecurity, market access, and implications for non-EU space operators

A new space age is looming – and the EU Commission has already made a first bold legislative move for it: the proposal of an EU Space Act aims to establish common EU rules for the safety, resilience, and sustainability of space activities and for the provision of space-based data and space services in the EU. Since the Commission proposal in June 2025, the Parliament rapporteur's draft and the Council Presidency's compromise text of March 2026 have revealed material divergences on key issues, including cybersecurity requirements, market access, and third-country operators. This article summarizes the key differences between the emerging institutional approaches and explains what they may mean for space operators active in the EU market. **#EUSpaceAct #Cybersecurity**

Source: [JDSupra](#)



MARKET & COMPETITION

USCIS announces regulatory changes to support and promote small business capabilities

USCIS is announcing regulatory changes to support and promote small business capabilities. The changes include streamlining the process for small businesses to obtain visas and other immigration benefits. USCIS is also launching a new initiative to provide technical assistance and training to small businesses. **#USCIS #SmallBusiness**

Source: [USCIS](#)



Government to lead India's space program

The Indian government is leading the country's space program, which includes the development of a new space agency, the Indian Space Research Organisation (ISRO). The government is also launching a series of initiatives to promote space technology and innovation. **#India #Space**

Source: [ISRO](#)



MARKET & COMPETITION



York Space Systems to acquire ALL.SPACE in defense communications expansion

York Space Systems LLC has agreed to acquire satellite communications company ALL.SPACE Networks Ltd. in a transaction that deepens York's position in military connectivity infrastructure while underscoring growing investor focus on resilient communications systems designed for contested operating environments. The deal, announced alongside ALL.SPACE financier Rochefort Asset Management LLC, comes as defense agencies and contractors accelerate investment in multi-orbit satellite connectivity capable of maintaining communications across increasingly complex battlefield and intelligence operations. **#YorkSpaceSystems #All.Space**

Source: [Citybiz](#)



THREAT INTELLIGENCE

Chinese aerospace engineers sentenced to 15 years in prison for espionage report

An article shared on Weibo by Xinhuanet, the official news outlet of China, reported that 15 Chinese aerospace engineers were sentenced to 15 years in prison for espionage. The article also mentioned that the engineers were involved in providing technical information and documents to foreign intelligence agencies.

Source: [Xinhuanet](#)



Cybersecurity report warns Iran could target U.S. and defense industry

A new report from the U.S. House of Representatives' Select Committee on Intelligence warns that Iran is increasingly active in cyber operations targeting U.S. and defense industry. The report states that Iran has conducted several cyberattacks against U.S. and defense industry targets in the past few years.

Source: [U.S. House of Representatives](#)



Commercial satellite supplying intel to Ukraine is cornered by 4 Russian spacecraft — US Space Force can only watch as Russia threatens 'quasi-civilian' targets

Open-source orbital tracking data revealed that 4 Russian satellites have expended considerable fuel to approach an American-Finnish satellite. According to Integrity ISR, a U.S.-based defense and intelligence firm, Russian assets closed in on ICEYE-36, a radar satellite operated by ICEYE that delivers reconnaissance data to U.S. and European governments — including Ukraine, which uses the data as it defends itself against Russian aggression. **#ICEYE #Russia**

Source: [tom's Hardware](#)



Space Branch 6666: Space Research Center

Project involves use of Space Branch 6666: Space Research Center. **#Space Branch 6666**

Source: [Xinhuanet](#)



Space Branch 66

Project involves use of Space Branch 66: Space Research Center. **#Space Branch 66**

Source: [Xinhuanet](#)



Learning and spending on intelligence with an ISIRI researcher

How can a satellite intelligence system be improved? How can we protect ourselves against it? In this interview, the author discusses the challenges of satellite intelligence and the potential for future developments. The author also discusses the importance of satellite intelligence in the context of national security and the need for continued investment in the field.

Source: [Xinhuanet](#)



TECHNOLOGY

ISIRI launches a 200 program to combat navigation signal threats

The Islamic Revolutionary Guard Corps (IRGC) has launched a 200 program to combat navigation signal threats. The program involves the development of a new satellite navigation system that is resistant to jamming and spoofing. The IRGC also plans to conduct tests of the system in the near future.

Source: [Xinhuanet](#)



TECHNOLOGY



Security of an in-orbit satellite: Detection of compromise through integrity

When malware runs on a satellite in orbit, there are minimal mechanisms to protect satellite data or provide visibility to mission control. This is especially critical for low-cost, open-hardware satellites that lack sophisticated security features. Traditional security approaches either consume excessive resources on small satellite platforms or require hardware that adds weight, cost, and complexity to missions. The question we set out to answer: How can we maintain and guarantee the integrity of satellite and payload data against threats while operating within the extreme resource constraints of small satellites? **#StratosphereLab #In-orbitDetection**

Source: [Stratosphere Lab](#)

ISIRI develops a system for detecting interference in satellite communications

ISIRI is developing a new satellite system with advanced security features, including a secure communications and control system. The system is designed to detect and respond to threats in the satellite communication system. The project is funded by the European Space Agency (ESA) through its Horizon Europe program. **#ISIRI**

Source: [ISIRI](#)



ESA's Space is preparing a next generation of satellites, planned to launch in 2026

ESA's Space is preparing a next generation of satellites, planned to launch in 2026. The satellites are designed to provide a range of services, including navigation, communication, and Earth observation. The project is funded by the European Space Agency (ESA) through its Horizon Europe program. **#ESA**

Source: [ESA](#)



TRAINING & EDUCATION

ESA's Space Cybersecurity Course

ESA's Space Cybersecurity Course is a 2-day course designed to provide participants with a comprehensive understanding of space cybersecurity. The course covers topics such as satellite security, ground station security, and space mission security. The course is funded by the European Space Agency (ESA) through its Horizon Europe program. **#ESA**

Source: [ESA](#)



ESA's Space is preparing a next generation of satellites, planned to launch in 2026

ESA's Space is preparing a next generation of satellites, planned to launch in 2026. The satellites are designed to provide a range of services, including navigation, communication, and Earth observation. The project is funded by the European Space Agency (ESA) through its Horizon Europe program. **#ESA**

Source: [ESA](#)



ESA's Space is preparing a next generation of satellites, planned to launch in 2026

ESA's Space is preparing a next generation of satellites, planned to launch in 2026. The satellites are designed to provide a range of services, including navigation, communication, and Earth observation. The project is funded by the European Space Agency (ESA) through its Horizon Europe program. **#ESA**

Source: [ESA](#)



VS: S-RAD (Satellite-Radio Analysis & Disruption) - Andrzej Olchawa, Ricardo Fradique & André Cirne- DCTLV2026

As space systems become increasingly critical to communications, navigation, and national infrastructure, understanding their unique protocols, RF characteristics, and operational dependencies is vital for identifying risks before adversaries do. This 2-day course will teach you how to analyze and exploit satellite and ground station systems using software only in a safe lab environment. We will go over satellite architecture and common link protocols, as well as SDR fundamentals. The hands-on labs cover protocol analysis and exploitation, simulated attacks, and how they can be combined with more traditional vulnerabilities to compromise space missions. By the end of the course, participants will be able to demonstrate a complete, nondestructive red-team chain of compromise in a controlled environment and produce actionable remediation and detection recommendations. **#VisionSpace #Defcon**

Source: [Defcon](#)



