SPACE CYBERSECURITY WEEKLY WATCH

Week 45

November 5 – November 11, 2024

Timeframe: Weekly

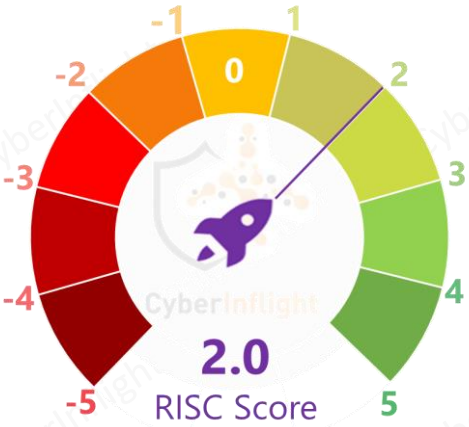
# of articles identified: 27

Est. time to read: 45 minutes

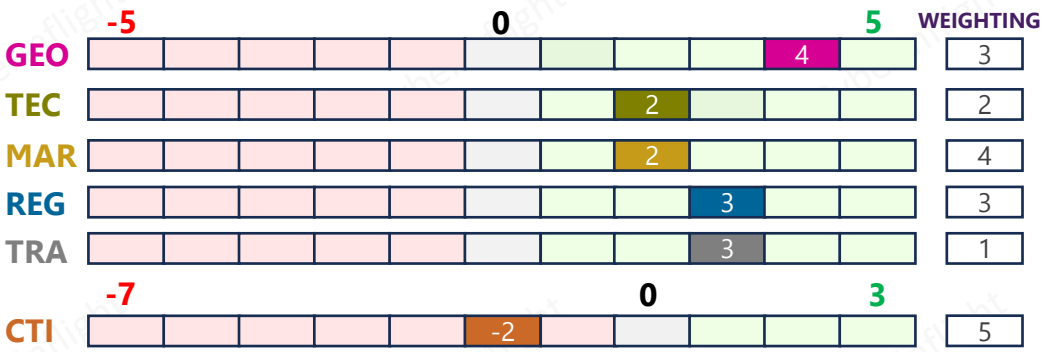
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

RISC Score Assesment

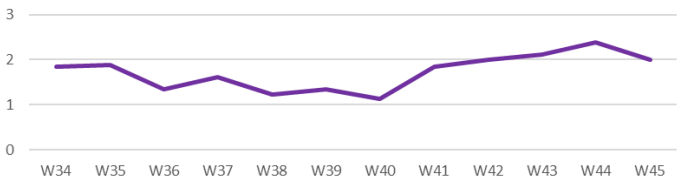


Overview & Resilience Index for Space Cybersecurity (RISC)



This week's RISC score is 2.0, down from the previous week. This decline is primarily driven by less favorable technological developments and updates in market conditions.

RISC Score Evolution



On the geopolitical front, the UK Space Command (UKSC) and the US Space Force (USSF) are strengthening ties to enhance defense capabilities in space, targeting potential adversarial threats. This partnership covers collaborative activities, from monitoring space activities to potential joint missions, positioning both nations as leaders in space. On the technological side, Swiss company WiseSat, part of WiseKey, is set to launch a new generation of satellites designed to support IoT connectivity across Europe, featuring quantum-resistant cryptographic keys; these satellites will boost Europe's satellite independence and security. On the market front, the European Union Agency for the Space Programme (EUSPA) shared recent successes and laid out ambitious targets under the Horizon Europe initiative. These projects aim to drive innovation in Europe's space sector, focusing on sustainable technology and market resilience. On the threat intel side, North Korea has conducted more than 300 GPS jamming attacks on South Korea over a single month, raising severe concerns about regional security and aviation safety. South Korean officials warn that these disruptions, primarily targeting Seoul's air and maritime traffic, may also impact critical infrastructure. On the regulatory front, the National Institute of Standards and Technology (NIST) has revised its guidelines for supply chain cybersecurity, addressing current vulnerabilities and risks. The updated guidelines provide organizations with new frameworks to secure their supply chains, particularly in response to increasing cyberattacks. Lastly, the Body of European Regulators for Electronic Communications (BEREC), in collaboration with the European Union Agency for Cybersecurity (ENISA), invites participants to an upcoming workshop on enhancing network resilience.

CYBERINFLIGHT'S NEWS

CyberInflight to participate in Cybersecurity Business Convention 2024

Florent Rizzo from CyberInflight will be moderating a session "Cybersecurity Governance of Space Programmes: Enhancing Security throughout the Value Chain" at the Cybersecurity Business Convention (CBC) 2024, on November 28. CBC is a major event dedicated to cybersecurity governance. This conference will cover trends and challenges in cybersecurity, with industry leaders discussing the evolving security landscape and solutions. CyberInflight's participation highlights its active role in the space cybersecurity industry. **#CBC #CybersecurityConference**

Link: https://www.linkedin.com/posts/cbc-cybersecurity-business-convention_programme-2024-gouvernance-de-la-cybers%C3%A9curit%C3%A9-activity-7259505894923628544-7UVY?utm_source=share&utm_medium=member_desktop

GEOPOLITICS

British and American space forces work together

In a recent strategic move, the UK Space Command (UKSC) and the US Space Force (USSF) are strengthening ties to enhance defense capabilities in space, targeting potential adversarial threats. This partnership covers collaborative activities, from monitoring space activities to potential joint missions, positioning both nations as leaders in space. The alliance reflects a shared vision to uphold security amid evolving global tensions. **#USSF #UKSC**

Link: https://ukdefencejournal.org.uk/british-and-american-space-forces-work-together/

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

THREAT INTELLIGENCE

North Korea's GPS jamming threats escalate

North Korea has conducted more than 300 GPS jamming attacks on South Korea over a single month, raising serious concerns about regional security and aviation safety. South Korean officials warn that these disruptions, primarily targeting Seoul's air and maritime traffic, may also impact critical infrastructure. Such GPS jamming incidents are considered aggressive provocations, and South Korea is working to counter these risks while monitoring its neighboring state's activities closely. **#GPSJamming #CriticalInfra**

Link: https://www.theepochtimes.com/world/north-korea-carried-out-300-gps-jamming-attacks-in-a-month-says-seoul-5757569

[redacted]

[redacted]

[redacted]

[redacted]

REGULATION

NIST SP 800-161r1-upd1 document updates cybersecurity guidelines to tackle supply chain risks

The National Institute of Standards and Technology (NIST) has revised its guidelines for supply chain cybersecurity, addressing current vulnerabilities and risks. The updated guidelines provide organizations with new frameworks to secure their supply chains, particularly in response to increasing cyber-attacks. This regulatory move emphasizes the importance of resilience in interconnected systems critical to national infrastructure. **#NIST #SupplyChainSecurity**

Link: https://industrialcyber.co/threats-attacks/nist-sp-800-161r1-upd1-document-updates-cybersecurity-guidelines-to-tackle-supply-chain-risks/

[redacted]

[redacted]

MARKET & COMPETITION

[redacted]

[redacted]

[redacted]

[redacted]

EUSPA's new projects achieve big results and set ambitious goal

The European Union Agency for the Space Programme (EUSPA) shared recent successes and laid out ambitious targets under the Horizon Europe initiative. These projects aim to drive innovation in Europe's space sector, with a focus on sustainable technology and market resilience. EUSPA's work exemplifies Europe's commitment to advancing space capabilities. **#EUSPA #HorizonEurope**

Link: https://www.linkedin.com/posts/euspa_big-results-even-bigger-expectations-activity-7259858494567170048-Dnxb?utm_source=share&utm_medium=member_desktop

TECHNOLOGY

WiseSat prepares satellite launch for European IoT connectivity

Swiss company WiseSat, part of WiseKey, is set to launch a new generation of satellites designed to support IoT connectivity across Europe. Featuring quantum-resistant cryptographic keys, these satellites will boost Europe's satellite independence and security. The launch aligns with broader European goals of advancing IoT capabilities while prioritizing robust encryption standards. **#WiseSat #IoT**

Link: https://news.satnews.com/2024/11/04/wisekey-subsidiary-wisesat-space-prepares-for-a-january-2025-launch-of-next-generation-satellite-supporting-european-satellite-independence-and-iot-connectivity/

[redacted]

TRAINING & EDUCATION

BEREC cybersecurity workshop opens for registration

The Body of European Regulators for Electronic Communications (BEREC), in collaboration with the European Union Agency for Cybersecurity (ENISA), invites participants to an upcoming workshop focused on enhancing network resilience. The event will provide hands-on cybersecurity training and foster cooperation between UK and EU stakeholders in digital security. As cyber threats increase across industries, this workshop represents a critical effort to build stronger defense strategies across national boundaries. **#CyberResilience #ENISA**

Link: https://www.berec.europa.eu/en/news/latest-news/berec-network-resilience-workshop-registration-open

[redacted]

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