



SPACE CYBERSECURITY WEEKLY WATCH

Week 45

November 5 – November 11, 2024

Timeframe: Weekly
of articles identified: 27
Est. time to read: 45 minutes

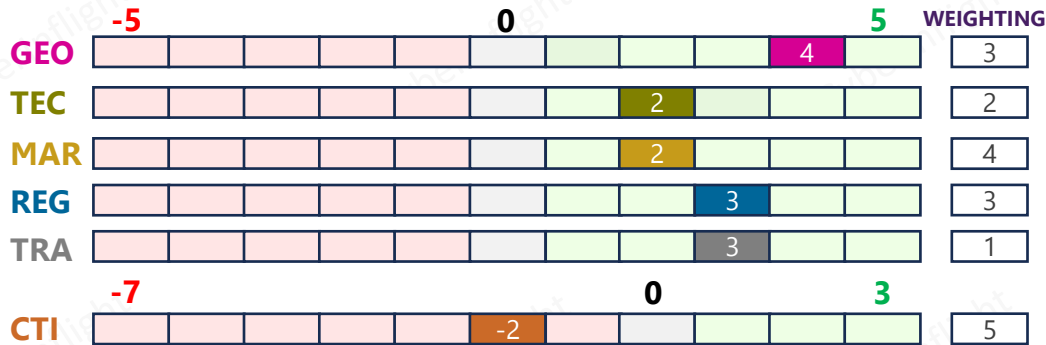
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

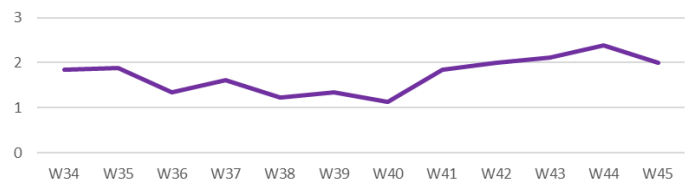
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score Evolution



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.

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/>



UK and South Korea strengthen cybersecurity cooperation

UK and South Korea have agreed to a new cyber security partnership, with a focus on addressing digital infrastructure risks. The agreement will focus on knowledge sharing, mutual support, and capacity building across sectors. The partnership supports UK-South Korean cybersecurity goals and will be a key element of the UK-South Korea Strategic Partnership. **#UKSC #SouthKorea**

Link: <https://www.gov.uk/government/news/uk-and-south-korea-agree-cyber-security-partnership>



UK strengthens space defence ties with China

The UK Space Command (UKSC) has announced a new partnership with China, focusing on military satellite security and cyber resilience. The agreement is part of the UK's strategy to build a resilient space and military capability for global defence projects. The UK-China defence partnership is the UK's growing role in global space security. **#UKSC #China**

Link: <https://www.gov.uk/government/news/uk-space-command-announces-partnership-with-china>



US Space Force to enhance command & control by 2030

The US Space Force is working to enhance its command and control capabilities by 2030, focusing on better resilience and cyber defence capabilities. The plan includes a new command and control architecture, and more advanced satellite capabilities. The initiative aims to improve the resilience and effectiveness of US operations. The enhanced cyber support efforts will be a key element of the US's growing role in global space security. **#USSF**

Link: <https://www.defence.gov/newsroom/defense-features-us-space-force-command-and-control-by-2030>



India's critical need for a quantum technology vision

The quantum revolution is set to transform the global security landscape, with quantum computing and quantum communication and quantum sensing. India's quantum technology vision is a key element of its growing role in global space security. The quantum technology vision is a key element of India's growing role in global space security. **#India**

Link: <https://www.defence.gov/newsroom/india-quantum-technology-vision>



US military general warns of China's growing military space capabilities

A top US military general has warned that China's growing military space capabilities pose a significant threat to US operations. The general stated that China's military space capabilities are a key element of its growing role in global space security. **#USSF**

Link: <https://www.defence.gov/newsroom/us-military-general-warns-of-chinas-growing-military-space-capabilities>





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>

US's cyber warfare skills still up with rising tensions

The United States' cyber warfare capabilities remain strong despite rising tensions with North Korea, according to a report from the House of Representatives. The report highlights the US's advanced cyber warfare skills and its ability to respond to threats from North Korea. It also notes that the US is working to improve its cyber warfare capabilities and to ensure that its cyber warfare operations are effective and efficient.

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

Western military technology faces challenges against Russia

Western military technology faces challenges against Russia, according to a report from the House of Representatives. The report highlights the US's advanced military technology and its ability to respond to threats from Russia. It also notes that the US is working to improve its military technology and to ensure that its military operations are effective and efficient.

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

Cyber espionage risk exposed in Japan's Space Agency leak

A leak from Japan's Space Agency has exposed a cyber espionage risk, according to a report from the House of Representatives. The report highlights the US's advanced cyber espionage capabilities and its ability to respond to threats from Japan. It also notes that the US is working to improve its cyber espionage capabilities and to ensure that its cyber espionage operations are effective and efficient.

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



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/>

CISA issues report of resilience measures for critical infrastructure

The Cyber and Information Security Administration (CISA) has issued a report on resilience measures for critical infrastructure. The report highlights the US's advanced resilience measures and its ability to respond to threats from critical infrastructure. It also notes that the US is working to improve its resilience measures and to ensure that its resilience operations are effective and efficient.

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

Defense contractors prepare for CMMC 2.0 cybersecurity compliance

Defense contractors are preparing for CMMC 2.0 cybersecurity compliance, according to a report from the House of Representatives. The report highlights the US's advanced cybersecurity capabilities and its ability to respond to threats from defense contractors. It also notes that the US is working to improve its cybersecurity capabilities and to ensure that its cybersecurity operations are effective and efficient.

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





MARKET & COMPETITION

US Space Command's commercial cooperation will be given budget of \$1.5 billion
US Space Command's commercial cooperation will be given budget of \$1.5 billion. The additional cooperation is intended to be used to support various activities, including the development of a new set of rules to regulate private space activities in order to ensure safety and security. The program will also support efforts to ensure that private space activities are conducted in a safe and secure manner.



US Space Command's commercial cooperation will be given budget of \$1.5 billion

US Space Command's commercial cooperation will be given budget of \$1.5 billion
US Space Command's commercial cooperation will be given budget of \$1.5 billion. The additional cooperation is intended to be used to support various activities, including the development of a new set of rules to regulate private space activities in order to ensure safety and security. The program will also support efforts to ensure that private space activities are conducted in a safe and secure manner.



US Space Command's commercial cooperation will be given budget of \$1.5 billion

US Space Command's commercial cooperation will be given budget of \$1.5 billion
US Space Command's commercial cooperation will be given budget of \$1.5 billion. The additional cooperation is intended to be used to support various activities, including the development of a new set of rules to regulate private space activities in order to ensure safety and security. The program will also support efforts to ensure that private space activities are conducted in a safe and secure manner.



US Space Command's commercial cooperation will be given budget of \$1.5 billion

US Space Command's commercial cooperation will be given budget of \$1.5 billion
US Space Command's commercial cooperation will be given budget of \$1.5 billion. The additional cooperation is intended to be used to support various activities, including the development of a new set of rules to regulate private space activities in order to ensure safety and security. The program will also support efforts to ensure that private space activities are conducted in a safe and secure manner.



US Space Command's commercial cooperation will be given budget of \$1.5 billion

★ 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-subsiary-wisesat-space-prepares-for-a-january-2025-launch-of-next-generation-satellite-supporting-european-satellite-independence-and-iot-connectivity/>

WiseSat prepares satellite launch for European IoT connectivity
WiseSat prepares satellite launch for European IoT connectivity. The new generation of satellites is 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 prepares satellite launch for European IoT connectivity



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>



How quickly advanced an cyberthreat can spread
The workshop will focus on the importance of the cybersecurity resilience in the space sector, addressing the specific challenges and opportunities. The event, featuring interactive and practical sessions, will explore the latest trends in space cybersecurity, with a particular emphasis on satellite and space-based systems. The workshop will provide a unique opportunity to learn from the experiences of experts in the field.

With leading experts and practitioners
An exclusive panel of leading experts has been selected, providing insights to enhance cyber resilience from multiple perspectives. The panel will discuss the latest trends in space cybersecurity, including satellite and space-based systems. The workshop will also feature a series of practical sessions, including a hands-on exercise, to provide participants with a deeper understanding of the challenges and opportunities in space cybersecurity.

Open to European and non-European participants
The workshop is open to all participants, regardless of their location. It is a unique opportunity to learn from the experiences of experts in the field and to foster cooperation between UK and EU stakeholders in digital security. The workshop will provide a unique opportunity to learn from the experiences of experts in the field.

The workshop is a unique opportunity to learn from the experiences of experts in the field
The workshop will provide a unique opportunity to learn from the experiences of experts in the field. It will feature a series of practical sessions, including a hands-on exercise, to provide participants with a deeper understanding of the challenges and opportunities in space cybersecurity. The workshop will also feature a series of practical sessions, including a hands-on exercise, to provide participants with a deeper understanding of the challenges and opportunities in space cybersecurity.

Open to European and non-European participants
The workshop is open to all participants, regardless of their location. It is a unique opportunity to learn from the experiences of experts in the field and to foster cooperation between UK and EU stakeholders in digital security. The workshop will provide a unique opportunity to learn from the experiences of experts in the field.

*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*