

SPACE CYBERSECURITY WEEKLY WATCH

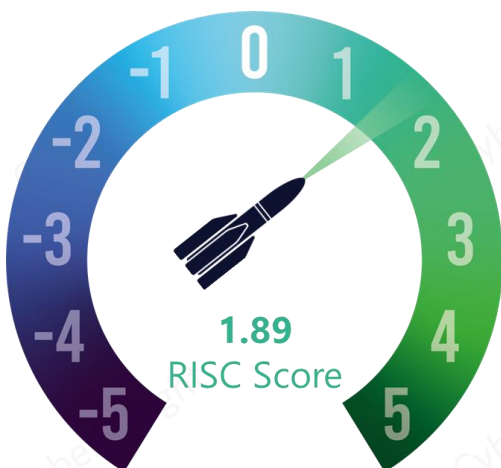
Week 26
June 24 - 30, 2025

Timeframe: Weekly
of articles identified: 41
Est. time to read: 90 minutes

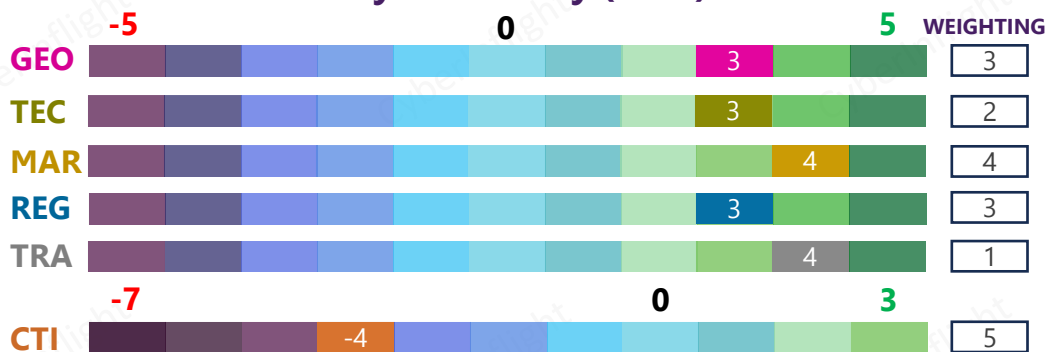
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

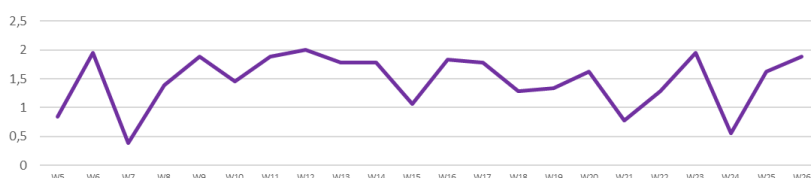
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



↑ The RISC score for this watch is 1.89, an increase from last week. This difference is due to a slight improvement on the threat intel front.

This week, on the regulatory front, the European Commission published the long-awaited proposal for the EU Space Act, establishing a comprehensive regulatory framework to strengthen the resilience, safety, and sustainability of space activities across the Union. CyberInflight is proud to have contributed its space cybersecurity expertise to this critical initiative! On the geopolitical front, the commander of US Space Command, Gen. Stephen Whiting, talks, in an interview, about everything from the Golden Dome to the Commercial Augmented Space Reserve to his worries about Beijing's efforts in space. On the technological side, India's response to the quantum challenge is spearheaded by ISRO (Indian Space Research Organisation) and DRDO (Defense Research and Development Organisation), two agencies driving innovation in secure communication. Moreover, the market is quite dynamic, with the Italian Space Agency (ASI) having awarded Starion Italia the design, development, and implementation of the Cyber Security Operations Center (C-SOC). This innovative facility will protect the agency's space and digital infrastructure. On the threat front, Russian hybrid threats, including sabotage of critical infrastructure, vandalism, weaponized migration, and military intimidation, are highly likely to intensify around the 2025 NATO Summit, especially in the Baltic states, Poland, and Germany. Lastly, the recording of the presentation "Securing the stars: safeguarding space systems" by Chathura Abeydeera, at AUSCERT 2025, is out! (Re)Discover it!

CYBERINFLIGHT'S NEWS

CyberInflight is proud to have contributed to the EU Space Act

The European Commission published the long-awaited proposal for the EU Space Act, establishing a comprehensive regulatory framework to strengthen the resilience, safety, and sustainability of space activities across the Union. CyberInflight is proud to have contributed its space cybersecurity expertise to this critical initiative!

#EUSpace #EUSpaceAct

Link: <https://www.linkedin.com/feed/update/urn:li:activity:7343954382046027776/>

CyberInflight is proud to have attended the EU Space ISAC General Meeting

EU Space ISAC Launches Next Phase with First General Meeting on 4-5 June 2025, marking a key milestone one year after its establishment. With the presence of the European Commission and EUSPA - EU Agency for the Space Programme, the meeting brought together the 50 members from 13 countries across the European space sector.

#EUSpace #SpaceISAC

Link: https://www.linkedin.com/posts/eu-space_eu-space-isac-launches-next-phase-with-activity-7343986467326619649-65hK?utm_source=share&utm_medium=member_desktop&rcm=ACoAAC6ww1MBDUN4xAUPfCv581dgYy1A-7vIm60

GEOPOLITICS

The statement of surprise space and cyber warfare in U.S.-China rivalry

As the United States and China continue to compete for global leadership, the space and cyber domains have emerged as key areas of rivalry. The U.S. and China are both investing heavily in these domains, and the competition is intensifying. This is a sign of the growing importance of space and cyber in the global power struggle.

Link: <https://www.bbc.com/news/technology-68111111>

Canada, EU sign defense pact that could enable joint weapons work

Canada and the European Union have signed a landmark defense pact that could enable joint weapons work. The pact is a significant step towards closer military cooperation between the two sides, and it could have major implications for the global defense industry.

Link: <https://www.reuters.com/world/europe/canada-eu-sign-defense-pact-2025-06-24/>

US Space Command's Gen. Whiting talks Golden Dome, EW and China's space-based kill chain

The commander of US Space Command Gen. Stephen Whiting talks, in this interview, about everything from Golden Dome to the Commercial Augmented Space Reserve to his worries about Beijing's efforts in space. **#SpaceWarfare #U.S.**

Link: <https://breakingdefense.com/2025/06/us-space-commands-gen-whiting-talks-golden-dome-ew-and-chinas-space-based-kill-chain/>

Cyber, electronic warfare key to winning future fights, NATO official says

Cyber and electronic warfare are key to winning future fights, NATO official says. The official emphasized that these domains are critical to the alliance's ability to deter and defeat its adversaries. He also noted that the alliance is working to improve its capabilities in these areas.

Link: <https://www.reuters.com/world/europe/nato-official-cyber-electronic-warfare-key-future-fights-2025-06-24/>

NATO needs a third pillar space

NATO is considering adding a third pillar to its existing pillars of military and political cooperation. The new pillar would focus on space, and it would be a significant step towards a more integrated approach to space security. The alliance is currently in the process of developing a space strategy.

Link: <https://www.reuters.com/world/europe/nato-needs-third-pillar-space-2025-06-24/>

New geopolitical tensions are shaping cyber warfare

New geopolitical tensions are shaping cyber warfare. As the world becomes more interconnected, the risk of cyber attacks is increasing. This is leading to a new era of cyber warfare, and it is important for the world to be prepared for this new challenge.

Link: <https://www.reuters.com/world/europe/new-geopolitical-tensions-shaping-cyber-warfare-2025-06-24/>

Switzerland concerned about Russian satellite interference

Switzerland is concerned about Russian satellite interference. The country has been the target of several Russian satellite operations, and it is worried that this could lead to a full-scale invasion. Switzerland is currently working to improve its defenses against such attacks.

Link: <https://www.reuters.com/world/europe/switzerland-concerned-russian-satellite-interference-2025-06-24/>

GEOPOLITICS

Key priorities for advancing NATO's space mission

NATO has been building up its efforts in the space domain. The alliance has focused on efforts to improve its space domain awareness and cyber threat hunting. The alliance has several military space operations centers and a broad range of allied space capabilities, including the ability to collect and share space data, and are developing a NATO space framework that is expected to be published by 2026. **NATO SpaceMission**

Link: <https://www.nato.int/pr/2025/06/25/key-priorities-for-advancing-natos-space-mission>



REGULATION

EU begins coordinated effort for Member States to collect critical infrastructure to quantify cyber threat mitigation by 2030

The European Union is working to strengthen its cybersecurity position with the adoption of a new security regulatory framework that will create a common and flexible legal framework to the advanced level of protection. All EU Member States are expected to begin the work by the end of 2025, with critical infrastructure required to complete the framework by the end of 2030. **EU Cyber**

Link: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1583



Commission proposes EU Space Act to boost market access and strengthen space safety

The European Commission has proposed the EU Space Act, a new set of ambitious measures to make Europe's space sector cleaner, safer and more competitive in Europe and its export markets. The EU Space Act intends to cut red tape, protect space assets, and create a fair, predictable playing field for businesses. **#EUSpaceAct #Draft**

Link: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1583



Cybersecurity NATO needs to fully implement risk management

Increased cyber space activity and operations in a cyber threat environment with increased risk of attack and impact. To help protect systems of critical importance such as health, the National Institute of Standards and Technology (NIST) has released a new cybersecurity framework. NIST fully implements all steps of the cybersecurity framework. **NATO CyberSecurity**

Link: <https://www.nato.int/pr/2025/06/25/cybersecurity>



TECHNOLOGY



End of cybercrime? How ISRO and DRDO are building India's unhackable quantum network

India's response to the quantum challenge is spearheaded by ISRO (Indian Space Research Organisation) and DRDO (Defense Research and Development Organisation) two agencies driving innovation in secure communication.

#DRDO #ISRO

Link: <https://timesofindia.indiatimes.com/science/end-of-cybercrime-how-isro-and-drdo-are-building-indias-unhackable-quantum-network/articleshow/122025465.cms>



Cybersecurity in NATO: A strategic imperative for defense and government

NATO has been building up its efforts in the space domain. The alliance has focused on efforts to improve its space domain awareness and cyber threat hunting. The alliance has several military space operations centers and a broad range of allied space capabilities, including the ability to collect and share space data, and are developing a NATO space framework that is expected to be published by 2026. **NATO CyberSecurity**

Link: <https://www.nato.int/pr/2025/06/25/cybersecurity>



The ultimate navigation challenge against malicious GPS disruption from Hong Kong

A new study from the National Institute of Standards and Technology (NIST) shows that GPS signals can be disrupted by a small number of malicious GPS receivers. The study shows that GPS signals can be disrupted by a small number of malicious GPS receivers. The study shows that GPS signals can be disrupted by a small number of malicious GPS receivers. **Hong Kong GPS**

Link: <https://www.nist.gov/newsroom/news-releases/2025/06/25/the-ultimate-navigation-challenge-against-malicious-gps-disruption-from-hong-kong>



ISRO's flagship ISAT mission enhances GPS resilience with Galileo PPS and PPS

The Indian Space Research Organisation (ISRO) has launched a new mission to enhance GPS resilience. The mission is designed to enhance GPS resilience by using Galileo PPS and PPS signals. The mission is designed to enhance GPS resilience by using Galileo PPS and PPS signals. The mission is designed to enhance GPS resilience by using Galileo PPS and PPS signals. **ISRO Mission**

Link: <https://www.isro.gov.in/News-Events/Press-Release/2025/06/25/isros-flagship-isat-mission-enhances-gps-resilience-with-galileo-pps-and-pps>



© 2000 Intel Corporation. Intel, the Intel logo, and Pentium are registered trademarks or trademarks of Intel Corporation or its subsidiaries in the United States and other countries. All other trademarks are the property of their respective owners.

Global innovation, only WHO and UNAIDS's question may could secure your investments - and the future of cybersecurity

© 2004 Blackwell Publishing Ltd, *Journal of Internal Medicine* 255: 103–110



MARKET & COMPETITION

Figure 1. A line graph showing the percentage of respondents who reported using various types of mobile devices (e.g., smartphones, tablets, etc.) to access the Internet. The x-axis represents the percentage of respondents, and the y-axis represents the percentage of respondents who reported using the device. The data shows that the majority of respondents (around 70%) reported using smartphones to access the Internet, while a smaller percentage (around 20%) reported using tablets. Other devices like smart TVs and smart speakers are also shown with very low percentages.

© 2015 The Authors. Journal of Internal Medicine © 2015 Blackwell Publishing Ltd

A free, internationally-accessible set of up-to-date, peer-reviewed information is the basis of the Russian Ministry of Foreign Affairs' Foreign Relations Information Project, which was launched in 2004. The project's information system is organized by country, country group, and key identity and interest organizations or "stakeholders" and is available for months of information services for free, including a daily news service, access to key up-to-date and open and press releases, and their analysis, comments, and



Other foreign affairs officials studied a similar provision of President Trump's deal with the State Department of Defense. That budget would have been \$1.1 billion and include large investments in operational, official intelligence, and space-based capabilities. **State Budget**



The effect of the new rules will vary. President Donald Trump's change is more than double others' impact, driving expenditures from 28 to 36% of their gross domestic product by 2035. Some 70% of that funding should be devoted toward your defense, while the remaining 30% should be used to develop other infrastructure such as water systems, education and healthcare.

What Is Happening?

Information of this and related work is available at the <http://www.berkeley.edu> and <http://www.berkeley.edu> websites. The project was supported by the National Science Foundation (NSF) Grant 0000000. The project was also supported by the National Science Foundation (NSF) Grant 0000000.



MARKET & COMPETITION

Establishing the 10th Anniversary of the EU Space Bill

The European Union is celebrating the 10th anniversary of the EU Space Bill, which established the legal framework for the EU's space activities. The bill was adopted in 2015 and has since been amended several times to reflect the evolving space landscape. The anniversary is being marked by a series of events, including a conference in Brussels on June 24-25, 2025, and a report by the European Commission on the progress of the EU's space policy.

Link: [https://ec.europa.eu/commission/presscorner/detail/en/ip-25-1000](#)



Spazio: contratto ASI a Starion Italia per il Cyber Security Operations Center (Trad: Space: ASI contract to Starion Italy for Cyber Security Operations Center)

The Italian Space Agency (ASI) has awarded Starion Italia the design, development and implementation of the Cyber Security Operations Center (C-SOC), an innovative facility that will ensure the protection of the agency's space and digital infrastructure. It was signed by ASI Director General Luca Vincenzo Maria Salamone and Starion Italia CEO Stefano Tatoni in the presence of ASI President Teodoro Valente. **#ASI #Starion**

Link: <https://ageei.eu/spazio-contratto-asi-a-starion-italia-per-il-cyber-security-operations-center/>



How using industry for new technologies in artificial intelligence, AI, hypermedia, and cybersecurity

The article discusses the challenges and opportunities of using industry for new technologies in artificial intelligence, AI, hypermedia, and cybersecurity. It highlights the need for a multi-stakeholder approach involving government, academia, and industry to address these challenges and seize the opportunities.

Link: [https://www.technologyinsights.com/industry-for-new-technologies-in-artificial-intelligence-ai-hypermedia-and-cybersecurity](#)



THREAT INTELLIGENCE

Russia continues electronic warfare with underground DDoS disruption

Russia continues its electronic warfare efforts with underground DDoS disruption. The article reports on a series of DDoS attacks targeting various European countries, including Poland, Germany, and France, which are believed to be part of a larger Russian cyber strategy.

Link: [https://www.technologyinsights.com/russia-continues-electronic-warfare-with-underground-ddos-disruption](#)



Israel's ground war in Gaza continues

Israel's ground war in Gaza continues. The article reports on the ongoing conflict between Israel and Hamas in Gaza, highlighting the impact on the civilian population and the international community's response.

Link: [https://www.technologyinsights.com/israels-ground-war-in-gaza-continues](#)



Russian hybrid threats likely to escalate around 2025 NATO Summit, putting European critical infrastructure at high risk

Recorded Future warns that Russian hybrid threats, including sabotage of critical infrastructure, vandalism, weaponized migration, and military intimidation, are highly likely to intensify around the 2025 NATO Summit. These activities are expected to particularly target European countries, especially if the summit produces decisive outcomes on Ukraine. The Baltic states, Poland, and Germany face the highest risk. **#NATO #Russia**

Link: <https://industrialcyber.co/reports/russian-hybrid-threats-likely-to-escalate-around-2025-nato-summit-putting-european-critical-infrastructure-at-high-risk/>



Major US companies are unlikely to address cyber resilience challenges until 2025

Major US companies are unlikely to address cyber resilience challenges until 2025. The article reports on a survey by Recorded Future showing that most large US companies do not have a formal cyber resilience strategy in place, which could leave them vulnerable to future cyber threats.

Link: [https://www.technologyinsights.com/major-us-companies-are-unlikely-to-address-cyber-resilience-challenges-until-2025](#)



TRAINING & EDUCATION

The monthly meeting of the High Level Group of Experts on China's cyber and space activities is expected to take place in Beijing, involving senior leaders with cyber, space, technology and security expertise. Details on participation in China's cyber and space activities will be discussed.

Link: [https://www.scmp.com/news/china/diplomacy/article/3244444/china-cyber-space-meeting-2025](#)



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