



SPACE CYBERSECURITY WEEKLY WATCH

Week 12

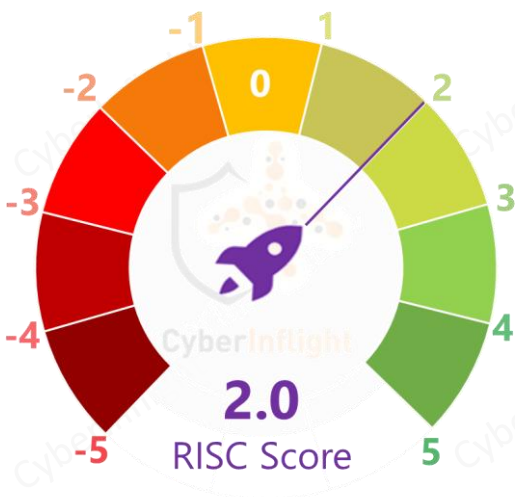
March 18 – 24, 2025

Timeframe: Weekly
of articles identified: 27
Est. time to read: 60 minutes

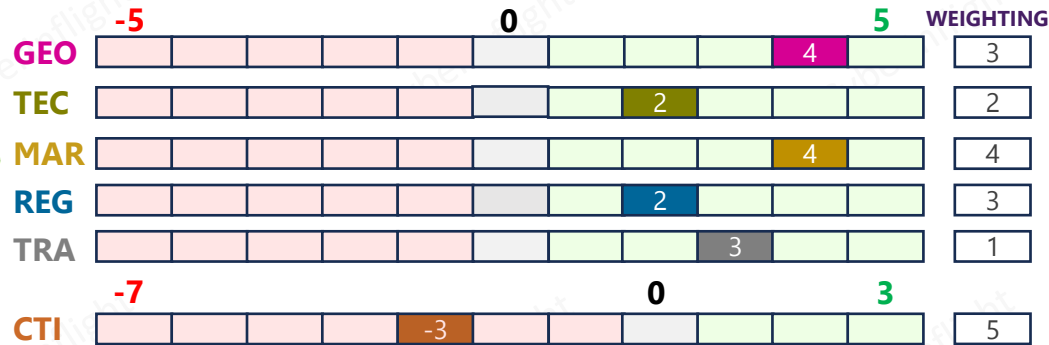
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

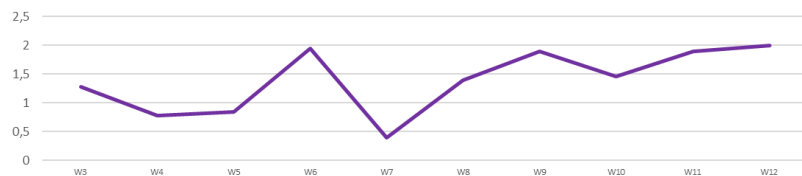
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



The RISC score for this watch is 2.0, a little increase from last week. This score is due to some positive geopolitical strategies, a high amount of news on the market, and few threats.

This week's geopolitics news includes the 5th edition of the French military space exercise AsterX. Organized by the French Space Command (CDE), the event will bring together 170 French and foreign civilian and military participants at the Centre national d'études spatiales (CNES) in Toulouse from March 17 to 28. On the regulation front, while the ReArm Europe Plan/Readiness 2030 strengthens pan-European defense capabilities with new financial means, the White Paper frames a new approach to defense and identifies investment needs. On the market side, Liverpool City Region and Greater Manchester mayors have signed a groundbreaking agreement with Axiom Space, developer of the first commercial space station. On the threat intel side, a hacker group called Lab Dookhtegan said it had disrupted the communication networks of 116 ships belonging to two major Iranian shipping companies in one of the most significant attacks against Iranian maritime operations critical to oil sales. On the technical front, encryption of transmitted data is an ever-growing concern as more critical functions depend on safe and secure data links. Quantum encryption is specifically designed to detect if any third party is even trying to eavesdrop, with any interference automatically detected thanks to fundamental rules of quantum physics. Lastly, a research paper proposes a novel spoofing detection technique for the global navigation satellite system (GNSS), which leverages satellite trajectory information and array antenna-based direction of arrival (DoA) estimation.



REGULATION



Commission unveils the White Paper for European Defence and the ReArm Europe Plan/Readiness 2030

While the ReArm Europe Plan/Readiness 2030 strengthens pan-European defense capabilities with new financial means, the White Paper frames a new approach to defense and identifies investment needs. **#WhitePaper #EuropeanDefence**

Link: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_793



MARKET & COMPETITION



Mayors sign space deal to 'unlock billions' for North West

Liverpool City Region Mayor and Greater Manchester Mayor have signed a groundbreaking agreement with Axiom Space, developer of the first commercial space station. The Memorandum of Understanding (MoU) will establish a framework for collaboration on space-based research, development, and manufacturing, helping to position the North West as a global centre for innovation in microgravity science and space technology. **#Collaboration #AxiomSpace**

Link: <https://businesscloud.co.uk/news/mayors-sign-space-deal-to-unlock-billions-for-north-west/>



The future of space cybersecurity is one of innovation and growth

The future of space cybersecurity is one of innovation and growth. The industry is seeing a surge in investment and activity, with many companies now offering comprehensive cybersecurity solutions for space-based systems. This is driven by the increasing number of satellites in orbit and the growing reliance on space-based services. **#SpaceCybersecurity #Innovation**

Link: [https://businesscloud.co.uk/news/the-future-of-space-cybersecurity-is-one-of-innovation-and-growth/](#)



Spanish Space and Foreign Agencies receive €10m to build next gen rocket engine

Spanish Space and Foreign Agencies have received a €10m grant to build next generation rocket engines. This funding is part of a broader effort to support the development of advanced space technologies and to enhance the competitiveness of the Spanish space industry. **#SpaceTechnology #Innovation**

Link: [https://businesscloud.co.uk/news/spanish-space-and-foreign-agencies-receive-10m-to-build-next-gen-rocket-engine/](#)



Los Angeles Air Force Base, Space Systems Command sign a contract with Space Systems

Los Angeles Air Force Base, Space Systems Command has signed a contract with Space Systems. This contract is for the development and testing of advanced space-based systems, including the next generation of rocket engines. **#SpaceSystems #Contract**

Link: [https://businesscloud.co.uk/news/los-angeles-air-force-base-space-systems-command-sign-a-contract-with-space-systems/](#)



Space Force joins with US Space Administration

The US Space Force is joining with the US Space Administration. This move is part of a broader effort to streamline space operations and to enhance the effectiveness of the space force. **#SpaceForce #USSpaceAdministration**

Link: [https://businesscloud.co.uk/news/space-force-joins-with-us-space-administration/](#)



Space Force will add 100 jobs in 2025 to boost military readiness

The Space Force will add 100 jobs in 2025 to boost military readiness. This increase in personnel is part of a broader effort to enhance the capabilities of the space force and to ensure that it is prepared for the challenges of the future. **#SpaceForce #MilitaryReadiness**

Link: [https://businesscloud.co.uk/news/space-force-will-add-100-jobs-in-2025-to-boost-military-readiness/](#)



Space Systems and Space Administration will partner to deliver next gen navigation system

Space Systems and Space Administration will partner to deliver next generation navigation systems. This partnership is part of a broader effort to enhance the accuracy and reliability of space-based navigation services. **#SpaceSystems #SpaceAdministration**

Link: [https://businesscloud.co.uk/news/space-systems-and-space-administration-will-partner-to-deliver-next-gen-navigation-system/](#)





THREAT INTELLIGENCE

US analysis of the Russian satellite tracking done at (C)SST 2025 with the (C)SST 2025 'Secret Russia'

The article discusses the (C)SST 2025 'Secret Russia' report from the perspective of 'Space satellite tracking done at (C)SST 2025, mainly by means of ground and space-based communications. #Space #Russia

Link: [https://www.cyberinflight.com/2025/03/18/secret-russia-satellite-tracking-at-csst-2025-with-the-csst-2025-secret-russia/](#)



US states and Ukraine report Russia's interference with satellites in the US - Break public knowledge

The article reports on the US states and Ukraine's report on Russia's interference with satellites in the US. It discusses the impact of such actions on national security and the need for improved satellite security measures. #Space #Russia #Ukraine

Link: [https://www.cyberinflight.com/2025/03/18/us-states-and-ukraine-report-russias-interference-with-satellites-in-the-us-break-public-knowledge/](#)



Space tracks (C)SST 2025 with the satellite detection

The article discusses the (C)SST 2025 with the satellite detection, focusing on the use of satellite tracking technology to monitor and identify potential threats in space. #Space #Satellite #Tracking

Link: [https://www.cyberinflight.com/2025/03/18/space-tracks-csst-2025-with-the-satellite-detection/](#)



★ Cyber group says it disrupted Iranian shipping communications

A hacker group called Lab Dookhtegan said it has disrupted the communication networks of 116 ships belonging to two major Iranian shipping companies in one of the biggest attacks against Iranian maritime operations, critical to the country's oil sales. Some reports indicate that NITC's fleet relies on VSAT (Very Small Aperture Terminal) satellite technology for offshore coordination. #LabDookhtegan #VSAT

Link: <https://www.iranintl.com/en/202503182119>



US Space Force reveals Chinese satellite performing 'highlighting' operations in orbit

The article reports on the US Space Force's discovery of a Chinese satellite performing 'highlighting' operations in orbit. It discusses the implications of such activities for space security and the need for improved satellite tracking capabilities. #Space #China #Satellite

Link: [https://www.cyberinflight.com/2025/03/18/us-space-force-reveals-chinese-satellite-performing-highlighting-operations-in-orbit/](#)



TRAINING & EDUCATION

Space Foundation announces recipient of National Space U. 2025 to new generation national security leadership

The article announces the recipient of the National Space U. 2025 award, which recognizes individuals who have demonstrated exceptional leadership and commitment to national security in the space domain. #Space #NationalSecurity #Leadership

Link: [https://www.cyberinflight.com/2025/03/18/space-foundation-announces-recipient-of-national-space-u-2025-to-new-generation-national-security-leadership/](#)



US Space Force announces recipient of National Space U. 2025 to new generation national security leadership

The article reports on the US Space Force's announcement of the recipient of the National Space U. 2025 award, highlighting the individual's contributions to space security and national defense. #Space #NationalSecurity #Leadership

Link: [https://www.cyberinflight.com/2025/03/18/us-space-force-announces-recipient-of-national-space-u-2025-to-new-generation-national-security-leadership/](#)





TRAINING & EDUCATION

Research to assess the effectiveness of GNSS spoofing detection techniques in the context of satellite navigation systems, GNSS, and the associated cyber threat. This paper discusses the effectiveness of GNSS spoofing detection techniques, including trajectory-based detection, array antenna-based direction of arrival (DoA) estimation, and machine learning-based detection. The paper also discusses the effectiveness of GNSS spoofing detection techniques in the context of satellite navigation systems, GNSS, and the associated cyber threat.

Link: [https://ieeexplore.ieee.org/document/10827561](#)



Robust GNSS spoofing detection based on prior information of satellite trajectories

In this paper, we propose a novel spoofing detection technique for the global navigation satellite system (GNSS), which leverages trajectory information of satellites and array antenna-based direction of arrival (DoA) estimation.

#Spoofing #Detector

Link: <https://ieeexplore.ieee.org/document/10827561>



The satellite navigation system (GNSS) is a global network of space-based navigation satellites that provide location and time information to users. GNSS systems are vulnerable to spoofing attacks, which can be used to deceive users and disrupt critical services. This paper discusses the effectiveness of GNSS spoofing detection techniques, including trajectory-based detection, array antenna-based direction of arrival (DoA) estimation, and machine learning-based detection. The paper also discusses the effectiveness of GNSS spoofing detection techniques in the context of satellite navigation systems, GNSS, and the associated cyber threat.

Link: [https://ieeexplore.ieee.org/document/10827561](#)

Research to assess the effectiveness of GNSS spoofing detection techniques in the context of satellite navigation systems, GNSS, and the associated cyber threat. This paper discusses the effectiveness of GNSS spoofing detection techniques, including trajectory-based detection, array antenna-based direction of arrival (DoA) estimation, and machine learning-based detection. The paper also discusses the effectiveness of GNSS spoofing detection techniques in the context of satellite navigation systems, GNSS, and the associated cyber threat.

Link: [https://ieeexplore.ieee.org/document/10827561](#)



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