

SPACE CYBERSECURITY WEEKLY WATCH

Week 30
July 22 - 28, 2025

Timeframe: Weekly
of articles identified: 23
Est. time to read: 40 minutes

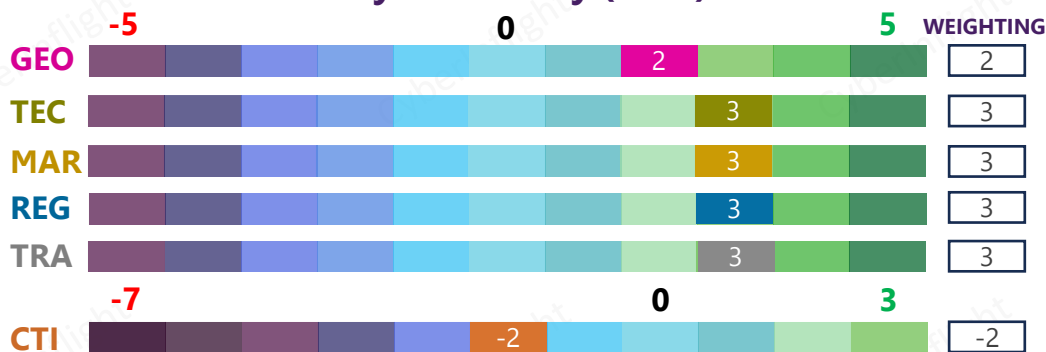
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

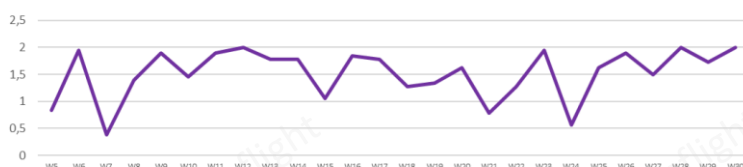
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



↑ The RISC score for this watch is 2. This increase from last week could be explained by security initiatives taken by major actors in space cybersecurity, counterbalancing the threats observed for the week.

This week, the German Space Agency and the German Armed Forces Space Command concluded a joint use agreement to exchange data at the Space Situational Awareness Center. This should contribute to better infrastructure protection. New Zealand's parliament also took a step forward by passing the Outer Space and High-altitude Activities Amendment Bill, establishing a new regulatory framework for ground-based space infrastructure, such as satellite tracking stations and telemetry systems, which support a wide array of orbital and space communication activities. On the technology front, Galileo introduced its Open Service Navigation Message Authentication (OSNMA), a data authentication function for the Galileo Open Service worldwide users, adding a critical layer of security to navigation processes. In parallel, the US Air Force asked RTX Raytheon for secure satellite navigation for positioning, navigation, and timing (PNT) to build and sustain secure, resilient military satellite navigation systems under terms of a \$7.2m contract. Regarding the threats, Lithuania has accused Russia of escalating GPS jamming activities from its Kaliningrad enclave, with aviation safety increasingly at risk. While the deputy chairman of Lithuania's Communications Regulatory Authority said that over 10 sites in Kaliningrad had been identified as sources of interference, the Lithuanian Transport Minister called the situation "worrying," noting that similar disruptions have affected Latvia, Estonia, Poland, Sweden, and Finland. Lately, on the education front, a new paper was published analyzing the range of possible space cyberattack vectors, assessing the efficacy of mitigation measures linked with space infrastructures, and proposing a risk scoring framework.

GEOPOLITICS

U.S. Secretary says Pentagon is taking GPS risks to national security and infrastructure

U.S. Secretary of Defense Pete Hegseth said on Tuesday that the Pentagon is taking GPS risks to national security and infrastructure, and that the U.S. must take action to protect itself. He said that the U.S. must take action to protect itself from GPS spoofing and jamming, which he said is a growing threat to national security and infrastructure. He said that the U.S. must take action to protect itself from GPS spoofing and jamming, which he said is a growing threat to national security and infrastructure.

Link: <https://www.defense.gov/Newsroom/Record/Article/Article-Id/2848484>



★ DLR and Bundeswehr to exchange almost all space data in future

The German Space Agency at the German Aerospace Center (DLR) and the German Armed Forces Space Command have been operating the Space Situational Awareness Center in Uedem together since 2011. However, although both institutions work closely together to identify potential threats in and from space, there have been legal hurdles to joint information processing to date. To overcome these, both parties concluded a joint use agreement on July 22. On this basis, the mutual, almost complete exchange of data should be possible from now on. **#Cooperation #SpaceData**

Link: <https://www.heise.de/en/news/DLR-and-Bundeswehr-to-exchange-almost-all-space-data-in-future-10496308.html>



Signals, noise, and operations: Cyber operations against the space sector and the threat from space

Signals, noise, and operations: Cyber operations against the space sector and the threat from space. The article discusses the growing threat to national security and infrastructure from GPS spoofing and jamming, and the need for the U.S. to take action to protect itself. It also discusses the growing threat to national security and infrastructure from GPS spoofing and jamming, and the need for the U.S. to take action to protect itself.

Link: <https://www.defense.gov/Newsroom/Record/Article/Article-Id/2848484>



Sweden's Swedish internet company leaves its military in dark zone - cyber warfare is considered

Sweden's Swedish internet company leaves its military in dark zone - cyber warfare is considered. The article discusses the growing threat to national security and infrastructure from GPS spoofing and jamming, and the need for the U.S. to take action to protect itself. It also discusses the growing threat to national security and infrastructure from GPS spoofing and jamming, and the need for the U.S. to take action to protect itself.

Link: <https://www.defense.gov/Newsroom/Record/Article/Article-Id/2848484>



REGULATION

★ New Zealand enacts ground-based space infrastructure law to safeguard security

In a swift and decisive move to enhance national security and assert regulatory authority over a critical aspect of modern space operations, the New Zealand Parliament has passed the Outer Space and High-altitude Activities Amendment Bill under urgency. This landmark legislation establishes a new regulatory framework for ground-based space infrastructure, such as satellite tracking stations and telemetry systems, which support a wide array of orbital and space communication activities. **#Law #Sovereignty**

Link: <https://www.devdiscourse.com/article/law-order/3513967-new-zealand-enacts-ground-based-space-infrastructure-law-to-safeguard-security>



TECHNOLOGY

★ Galileo launches OSNMA to combat satellite spoofing threats

In light of the escalating threat landscape, Galileo is set to introduce a groundbreaking protection measure: Open Service Navigation Message Authentication (OSNMA). Scheduled to become fully operational on July 24, 2025, this feature adds a critical layer of security to navigation processes. **#GNSSspoofing #Galileo**

Link: https://defence-industry-space.ec.europa.eu/galileo-leads-way-gnss-spoofing-protection-osnma-2025-07-22_en



Spain launches new space-based radio frequency intelligence capabilities for defense and security. The article discusses the growing threat to national security and infrastructure from GPS spoofing and jamming, and the need for the U.S. to take action to protect itself. It also discusses the growing threat to national security and infrastructure from GPS spoofing and jamming, and the need for the U.S. to take action to protect itself.

Link: <https://www.defense.gov/Newsroom/Record/Article/Article-Id/2848484>



TECHNOLOGY

Quantum computing in the defense and aerospace industry: The next technological frontier

The aerospace sector continues to embrace quantum computing as a critical tool for innovation in aircraft design, mission planning, and supply chain management. One of the most compelling applications of quantum computing in aerospace is its ability to optimize flight paths in real-time, taking into account a vast number of variables such as weather, fuel efficiency, and aircraft performance. This capability is particularly valuable for military operations, where the ability to quickly adapt to changing conditions can be a decisive advantage. Quantum computing is also being used to simulate complex systems, such as engine components and materials, allowing for faster development and testing of new technologies.

Link: [Quantum computing in the defense and aerospace industry: The next technological frontier](#)

QNTA's new satellite quantum navigation solution successfully undergoes first defense trials at QFMA

QNTA, the global leader in quantum infrastructure solutions, today announced groundbreaking developments in its quantum navigation technology. The company's new satellite quantum navigation solution, QNTA-SatNav, has successfully completed its first defense trials at QFMA, demonstrating its ability to provide secure and accurate navigation for military operations. QNTA-SatNav is a next-generation navigation solution that leverages quantum entanglement to provide secure and accurate navigation for military operations. The solution is designed to be resistant to jamming and spoofing, making it ideal for use in high-threat environments. QNTA-SatNav is currently being tested by the Australian Defence Force and is expected to be deployed in the near future.

Link: [QNTA's new satellite quantum navigation solution successfully undergoes first defense trials at QFMA](#)



MARKET & COMPETITION

QNTA, Research, IBM Technology, and Lockheed Shipping Company Partner to deliver quantum navigation and tracking solution for commercial maritime vessels

QNTA, Research, IBM Technology, and Lockheed Shipping Company have entered into a strategic partnership to deliver a quantum navigation and tracking solution for commercial maritime vessels. The partnership aims to leverage the power of quantum computing to provide secure and accurate navigation and tracking for commercial shipping vessels. The solution is designed to be resistant to jamming and spoofing, making it ideal for use in high-threat environments. The solution is currently being tested by the Australian Defence Force and is expected to be deployed in the near future.

Link: [QNTA, Research, IBM Technology, and Lockheed Shipping Company Partner to deliver quantum navigation and tracking solution for commercial maritime vessels](#)

QNTA Space Systems present technology to explore QFMA space opportunities to expand mission delivery and space to ground capabilities

QNTA Space Systems today announced its participation in the QFMA space opportunities to expand mission delivery and space to ground capabilities. The company is currently testing its quantum navigation and tracking solution for commercial maritime vessels. The solution is designed to be resistant to jamming and spoofing, making it ideal for use in high-threat environments. The solution is currently being tested by the Australian Defence Force and is expected to be deployed in the near future.

Registration QFMA

Link: [QNTA Space Systems present technology to explore QFMA space opportunities to expand mission delivery and space to ground capabilities](#)

Space Forge and Lockheed Martin partner to advance U.S. space-based semiconductor manufacturing

Space Forge Inc. announced a strategic partnership with Lockheed Martin to advance U.S. space-based semiconductor manufacturing. The partnership aims to leverage the power of quantum computing to provide secure and accurate navigation and tracking for commercial maritime vessels. The solution is designed to be resistant to jamming and spoofing, making it ideal for use in high-threat environments. The solution is currently being tested by the Australian Defence Force and is expected to be deployed in the near future.

Link: [Space Forge and Lockheed Martin partner to advance U.S. space-based semiconductor manufacturing](#)

International and QNTA Space Partner to deliver Quantum Resilient Secure IoT Network Infrastructure

International and QNTA Space today announced a strategic partnership to deliver Quantum Resilient Secure IoT Network Infrastructure. The partnership aims to leverage the power of quantum computing to provide secure and accurate navigation and tracking for commercial maritime vessels. The solution is designed to be resistant to jamming and spoofing, making it ideal for use in high-threat environments. The solution is currently being tested by the Australian Defence Force and is expected to be deployed in the near future.

Link: [International and QNTA Space Partner to deliver Quantum Resilient Secure IoT Network Infrastructure](#)



MARKET & COMPETITION



Air Force asks RTX Raytheon for secure satellite navigation for positioning, navigation, and timing (PNT)

RTX Corp. will build and sustain secure resilient military satellite navigation systems under terms of a \$7.2m U.S. Air Force contract. Officials of the Air Force Life Cycle Management Center at Robins Air Force Base, Ga., is asking the RTX Raytheon segment in El Segundo, Calif., for Miniaturized Airborne Global Positioning System Receiver (MAGR) production and sustainment. The contract involves MAGR-2K and MAGR-2K-M GPS receivers. **#PNT #Contract**



Link: <https://www.militaryaerospace.com/sensors/article/55305622/raytheon-technologies-corp-satellite-navigation-with-cyber-security-for-positioning-navigation-and-timing-pnt>

THREAT INTELLIGENCE



Lithuania accuses Russia of intensifying GPS jamming operations

Lithuania has accused Russia of escalating GPS jamming activities from its Kaliningrad enclave, with aviation safety increasingly at risk. According to Lithuania's air traffic control company, Oro Navigacija, pilots reported 1,022 cases of GPS interference in June — a dramatic rise from just 46 incidents in the same month last year. **#GPSJamming #Lithuania**



Link: <https://news.az/news/lithuania-accuses-russia-of-intensifying-gps-jamming-operations>

Russian sources of GPS spoofing in Red Sea, sailors urged to rely on alternative systems

US Navy's 7th Fleet, based in the Eastern Mediterranean, has issued an urgent warning to sailors in the Red Sea about GPS spoofing. The spoofing is a form of cyber attack that can cause a ship's GPS to lose accuracy, leading to navigation errors. The spoofing is being carried out by Russian forces. **#GPSJamming #Russia**



Link: <https://www.militaryaerospace.com/sensors/article/55305622/raytheon-technologies-corp-satellite-navigation-with-cyber-security-for-positioning-navigation-and-timing-pnt>

Three years post MS-13 attack, threat now calls for new approach to cybersecurity posture

Three years after the MS-13 attack, threat now calls for new approach to cybersecurity posture. The attack was a major cyber attack that caused significant damage to the company's systems. The attack was carried out by a group of hackers who claimed to be affiliated with the MS-13 gang. **#CyberSecurity #MS13**

Link: <https://www.militaryaerospace.com/sensors/article/55305622/raytheon-technologies-corp-satellite-navigation-with-cyber-security-for-positioning-navigation-and-timing-pnt>

Russian satellite spoofing operations - but Special ops software to thwart

Russian satellite spoofing operations - but Special ops software to thwart. The spoofing is a form of cyber attack that can cause a ship's GPS to lose accuracy, leading to navigation errors. The spoofing is being carried out by Russian forces. **#GPSJamming #Russia**



Link: <https://www.militaryaerospace.com/sensors/article/55305622/raytheon-technologies-corp-satellite-navigation-with-cyber-security-for-positioning-navigation-and-timing-pnt>

Cyber espionage campaign hits Russian aerospace sector using MS-13 tactics

Cyber espionage campaign hits Russian aerospace sector using MS-13 tactics. The campaign is a major cyber attack that caused significant damage to the company's systems. The attack was carried out by a group of hackers who claimed to be affiliated with the MS-13 gang. **#CyberSecurity #MS13**



Link: <https://www.militaryaerospace.com/sensors/article/55305622/raytheon-technologies-corp-satellite-navigation-with-cyber-security-for-positioning-navigation-and-timing-pnt>

TRAINING & EDUCATION

Department issued Notice of HQ and HVT springing into full force for 2025 summer exercises.

Continuing efforts through reports from the global navigation satellite system (GNSS) and other systems to ensure a significant threat to the reliability of secure positioning. Consequently, the detection and resolution of these vulnerabilities are critical to ensure mission success, including the safety and security of the system. The system is being upgraded to ensure high-level security and reliability.



Link: <https://www.militaryaerospace.com/sensors/article/55305622/raytheon-technologies-corp-satellite-navigation-with-cyber-security-for-positioning-navigation-and-timing-pnt>

TRAINING & EDUCATION



SoK: securing the final frontier for cybersecurity in space-based infrastructure

This study analyzes the range of possible space cyber-attack vectors, which include ground, space, satellite, and satellite constellations. In order to address the particular threats, the study also assesses the efficacy of mitigation measures that are linked with space infrastructures and proposes a Risk Scoring Framework. Based on the analysis, this paper identifies potential research challenges for developing and testing cutting-edge technology solutions, encouraging robust cybersecurity measures needed in space. **#Paper #Security**



Link: <https://arxiv.org/abs/2507.17064>



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