



SPACE CYBERSECURITY WEEKLY WATCH

Week 33

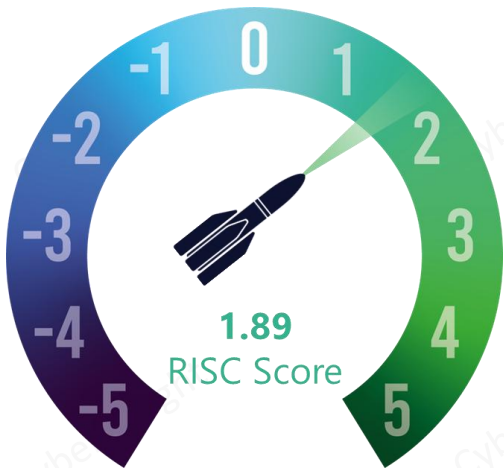
August 12 - 18, 2025

Timeframe: Weekly
of articles identified: 26
Est. time to read: 55 minutes

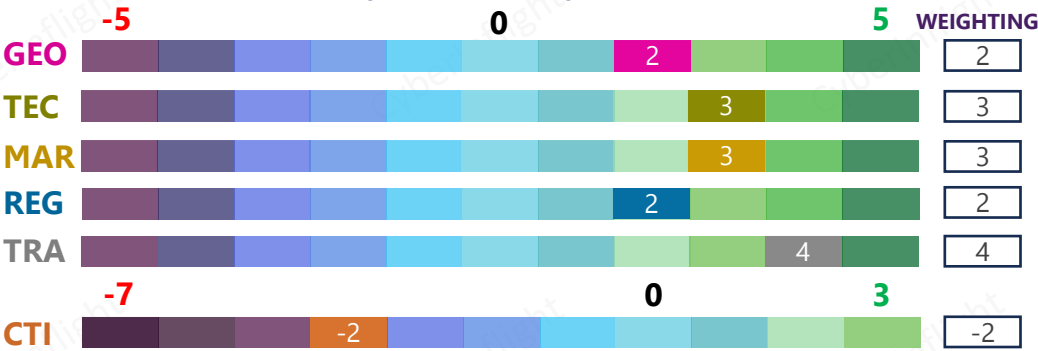
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

RISC Score Assessment

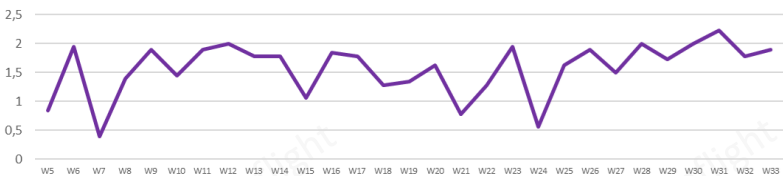


Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025

↑ The RISC score for this watch is 1.89, reflecting a slight increase from last week. This stable situation is due to a calm threat intelligence environment, coupled with initiatives in the geopolitical, regulatory, and market domains, as well as a strong focus on education.



This week was marked by the successful launch of the US Air Force's Navigation Technology Satellite-3 (NTS-3) on a ULA Vulcan rocket, designed to test advanced anti-spoofing signals, a steerable phased-array antenna, and autonomous receivers to enhance national security and PNT capabilities. On the regulatory front, President Donald Trump signed an Executive Order to streamline regulations and foster a competitive commercial space industry, ensuring the United States maintains its leading role in the commercial use of space. Among the Space Policy Directives (SPDs) is one focused on establishing cybersecurity principles for space systems. In the technology sector, NIST finalized its 'lightweight cryptography' standard to safeguard small devices. Four related algorithms are now available to protect data created and transmitted by the Internet of Things and other electronic devices. They provide cyber defense, making it suitable for critical embedded systems in PNT and space applications. Turning to the market front, the French Directorate General of Armaments (DGA) awarded the PALADIN (Positioning and Autonomous Laser Assisted Detection in Near-space) framework agreement to French New Space company Infinite Orbits, with a maximum value of €50m. Regarding threat intelligence, AP News released an analysis highlighting the growing risks of hijacked satellites and orbiting space weapons, emphasizing that space has become a new battlefield in the 21st century. Lastly, an interview with the head of space policy and tech for the Estonian government explained how cybersecurity helped Estonia carve a niche in space.

GEOPOLITICS



US Air Force launches Navigation Technology Satellite-3 to enhance national security and PNT capabilities

The US Air Force Research Laboratory (AFRL) has achieved a significant milestone in enhancing the nation's navigation capabilities with the successful launch of the Navigation Technology Satellite-3 (NTS-3). This satellite was placed into orbit on a United Launch Alliance (ULA) Vulcan rocket from Cape Canaveral Space Force Station in Florida on August 12. The satellite will test new anti-spoofing signals, a steerable phased-array antenna to send signals to ground forces in high-jamming areas, and receivers to help the satellite operate without instructions from ground controllers. **#Vulcan #NTS-3**

Link: <https://newsroom.ulalaunch.com/releases/vulcan-rocket-ushers-in-new-era-of-national-security-space-launch>



REGULATION



President Donald J. Trump enables competition in the commercial space industry

President Donald J. Trump signed an Executive Order to streamline regulations and foster a competitive commercial space industry, ensuring the United States maintains its leading role in the commercial use of space. The White House press release states that President Trump has issued seven Space Policy Directives (SPDs), one of which is aimed at establishing cybersecurity principles for space systems. **#ExecutiveOrder #SpaceIndustry**

Link: <https://www.whitehouse.gov/fact-sheets/2025/08/fact-sheet-president-donald-j-trump-enables-competition-in-the-commercial-space-industry/>



Fact Sheet: Trump 20 Space Policy Directives Streamlining Heavy Burdens on U.S. Space Competitor

The White House today announced a series of seven new Space Policy Directives (SPDs) signed by President Donald J. Trump. The directives are aimed at streamlining regulations and fostering a competitive commercial space industry, ensuring the United States maintains its leading role in the commercial use of space. The directives include: (1) Streamlining regulations to reduce burdens on U.S. space companies; (2) Encouraging innovation and competition in the commercial space industry; (3) Enhancing cybersecurity for space systems; (4) Promoting the development of new space technologies; (5) Encouraging international cooperation in space exploration; (6) Encouraging the development of new space policies; and (7) Encouraging the development of new space laws.



TECHNOLOGY

Implementing space missions with NIST 800-191A compliance

The National Institute of Standards and Technology (NIST) has released a new draft standard, NIST 800-191A, titled "Security and Privacy Controls for Information Systems and Organizations: Cryptographic Protection of Data in Transit." This standard provides a framework for implementing cryptographic protection of data in transit, ensuring the confidentiality and integrity of information systems and organizations. The standard is designed to be flexible and adaptable to various environments, including cloud computing, mobile devices, and IoT devices. It covers a wide range of cryptographic techniques, including symmetric and asymmetric encryption, digital signatures, and key management. The standard also provides guidance on how to implement these techniques in a secure and efficient manner.

Link: <https://www.nist.gov/news-events/news/2025/08/nist-finalizes-lightweight-cryptography-standard-protect-small-devices>



NIST finalizes 'lightweight cryptography' standard to protect small devices

Four related algorithms are now ready for use to protect data created and transmitted by the Internet of Things and other electronics. NIST's newly finalized lightweight cryptography standard provides a defense from cyberattacks for even the smallest of networked electronic devices. The standard uses the Ascon family of algorithms, offering authenticated encryption and hashing functions resistant to side-channel attacks. It protects data, making it suitable for critical embedded systems in PNT and space applications. **#NIST #Cryptography**

Link: <https://www.nist.gov/news-events/news/2025/08/nist-finalizes-lightweight-cryptography-standard-protect-small-devices>



MARKET & COMPETITION



France seeks to safeguard its military assets across space orbits with PALADIN satellite

The Directorate General of Armaments (DGA) awarded the PALADIN (Positioning and Autonomous Laser Assisted Detection in Near-space) framework agreement to French New Space company Infinite Orbits for a maximum value of €50m. The contract tasks Infinite Orbits with delivering a geostationary Earth orbit (GEO) inspection and surveillance service to the French Space Command (CDE) under the national Action and Resilience in Space (ARES) program. The PALADIN satellite, slated for launch in 2027, will build upon the company's Orbit Guard platform and be supported by developments funded through the France 2030 investment plan coordinated by the National Center for Space Studies (CNES). #PALADIN #Contract

Link: <https://armyrecognition.com/news/aerospace-news/2025/france-seeks-to-safeguard-its-military-assets-across-space-orbits-with-paladin-satellite>



Results reported at 50% jumping from across from one island



More than 12,000 operating satellites now orbit the planet, playing a critical role in military operations, navigation systems like GPS, intelligence gathering and economic supply chains. They are also key to early launch-detection efforts, which can warn of approaching missiles. That makes them a significant national security vulnerability, and a prime target for anyone looking to undermine an adversary's economy or military readiness — or to deliver a psychological blow like the hackers supporting Russia did when they hijacked television signals to Ukraine. **#GPSJamming #Vulnerability**

TRAINING & EDUCATION



According to Paul Liias, head of space policy and tech for the Estonian government, the country has played a key role in providing cyber defenses for space programs, including its cyber-range used by NATO for testing defense tools. In this video interview with Information Security Media Group, Liias discussed cybersecurity challenges facing space infrastructure today - at both satellites and ground stations; How to protect aerial drones against GNSS jamming or spoofing; and Preparing Estonia's workforce for space cybersecurity. **#CyberDefense #Interview**



TRAINING & EDUCATION

Canadian Space Agency updates operations for the quantum integration and secure satellite communications

The Canadian Space Agency (CSA) updates its operations for the quantum integration and secure satellite communications. The CSA is the first administration in ground-to-space quantum key distribution (QKD) in Canada. For this update, the existing platform is a microsatellite in low earth orbit and the ground station is located in a ground-based optical quantum network station (GOS). Together, they will enable the creation and exchange of cryptographic keys enabling secure quantum communications at a minimum distance of 100 km. **QKD@CSA**

Link: [https://www.csa.gc.ca/eng/quantum/qkd/2025-08-05](#)



Integrated communication and network serving in 6G satellite network: Protocol, architecture and challenges

In this paper, we explore the integration of communication and network serving in 6G satellite network serving in low earth orbit with satellite network to provide real-time 6G imaging and information transmission. Considering the high mobility characteristics of satellite channels and limited processing capabilities of satellite payloads, we propose an integrated communication and network serving architecture based on an integrated deep transfer learning framework. **Page 1049-1058**

Link: [https://arxiv.org/abs/2507.19111](#)



Measuring Fermi's paradox in single-point quantum walks via local phase-induced spatial heterogeneity

In this work, the authors demonstrate that a quantum walk-based Fermi effect can emerge in discrete-time quantum walks by introducing the local coin operation and introducing a localized phase shift at the origin. Through a series of numerical experiments, they show that this network model without entanglement in high-dimensional coin states outperforms both only in the presence of spatial heterogeneity. **Page 10**

Link: [https://arxiv.org/abs/2507.19111](#)



Advancing America's quantum leadership with next-generation sensors

The next generation quantum technology sensors provide the military with a strategic opportunity to gain significant security and intelligence advantages while maintaining its leadership in the global quantum race. The sensors can provide stable, secure and strong capabilities over long distances, providing a strategic advantage over other military sensors. The sensors are designed to be integrated with existing military systems, such as the current US Navy's Quantum Sensor (QS) in Monterey, August 17, from 10:00 AM to 12:00 PM. A virtual public event exploring quantum sensor technology and its applications in defense and commercial sectors. **QSS@NSA**

Link: [https://www.nsa.gov/quantum/sensors/advancing-america-quantum-leadership-with-next-generation-sensors](#)



Combining self-perceptual QFT profiling through fine-grained trajectory analysis

The literature presents a comprehensive framework for detecting QFT spoofing attacks. Based on this, we propose a self-perceptual QFT spoofing detection framework. This framework can detect QFT spoofing attacks in a more accurate and efficient manner. The framework is designed to be integrated with existing military systems, such as the current US Navy's Quantum Sensor (QS) in Monterey, August 17, from 10:00 AM to 12:00 PM. A virtual public event exploring quantum sensor technology and its applications in defense and commercial sectors. **Page 1049-1058**

Link: [https://arxiv.org/abs/2507.19111](#)



QFT-Space 2025

QFT-Space 2025 is a virtual public event exploring quantum sensor technology and its applications in defense and commercial sectors. The event is designed to be integrated with existing military systems, such as the current US Navy's Quantum Sensor (QS) in Monterey, August 17, from 10:00 AM to 12:00 PM. A virtual public event exploring quantum sensor technology and its applications in defense and commercial sectors. **QSS@NSA**

Link: [https://www.nsa.gov/quantum/sensors/advancing-america-quantum-leadership-with-next-generation-sensors](#)



Secure analysis in cognitive satellite terrestrial networks with untrusted QFT relaying and friendly jamming

The study explores physical layer security in a cognitive satellite terrestrial network where a ground user (GU) network communicates with a terrestrial network (TN) via an untrusted quantum relay (QR) and friendly jamming (FJ). The study explores physical layer security in a cognitive satellite terrestrial network where a ground user (GU) network communicates with a terrestrial network (TN) via an untrusted quantum relay (QR) and friendly jamming (FJ). **Page 1049-1058**

Link: [https://arxiv.org/abs/2507.19111](#)





Contact us at: research@cyberinflight.com