



SPACE CYBERSECURITY WEEKLY WATCH

Week 32

August 5 - 11, 2025

Timeframe: Weekly
of articles identified: 26
Est. time to read: 50 minutes

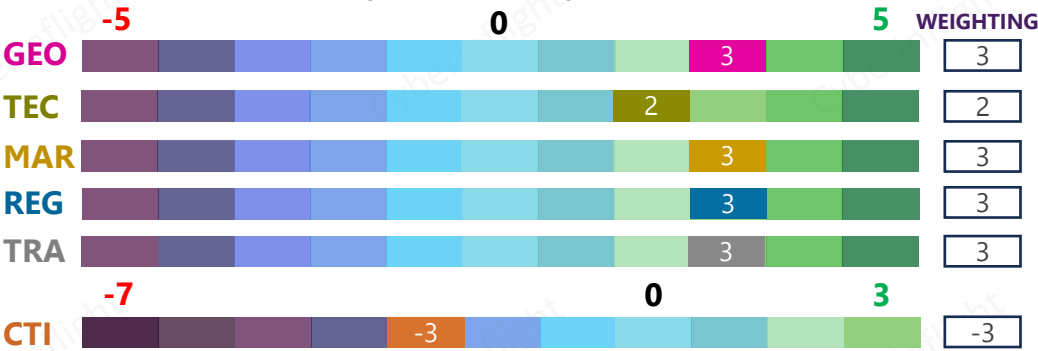
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

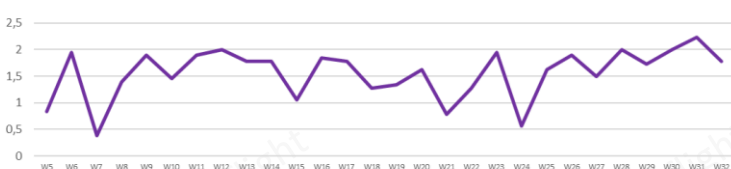
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



↓ The RISC score for this watch is 1.78, a decrease from last week, yet it still reflects a relatively positive outlook. This is due to a predominance of positive news, while negative and threat news are less prevalent.

This week, the geopolitical landscape was predominantly shaped by U.S. developments, notably the launch of the Space Force's annual, future-facing Schriever Wargames, which could help create a framework for better information sharing with allies and partners on sensitive programs and capabilities. On the regulatory front, two U.S. Senators introduced the National Quantum Cybersecurity Migration Strategy Act, a bipartisan bill directing the White House Office of Science and Technology Policy to develop a coordinated national strategy for transitioning federal systems to post-quantum cryptography. In terms of technology, Impulse Space has made several technical improvements to its Mira vehicle, the company's high-thrust, highly maneuverable spacecraft for payload hosting and deployment. Furthermore, India made its mark on the market front, as Infosys, a global leader in next-generation digital services and consulting, announced the launch of its state-of-the-art Infosys Center for Advanced AI, Cybersecurity, and Space Technology at its Hubballi Development Center. On the threat front, Jamco Aerospace Inc., a New York-based engineering and fabrication firm specializing in components for aerospace and aircraft manufacturers, was targeted this week. The company, which supplies parts to aircraft builders used by the U.S. and other governments, was listed on the ransomware site of Play Ransomware. Lastly, on the training front, U.S. Space Force Guardians recently faced off as part of the Resolute Space 2025 exercises, demonstrating their readiness and operational capabilities.

GEOPOLITICS

USF launches competition on cyber force generation

The United States Space Force (USSF) is announcing a competition to select the best cyber force generation concept for the service's cyber force. The competition is open to all U.S. military and civilian organizations, and the winning concept will be used to guide the development of the service's cyber force.

Link: <https://www.defensenews.com/space/2025/08/07/space-force-wargame-could-inform-framework-for-allied-info-sharing/>

Space Force gets new senior leader for cyber and data

The United States Space Force (USSF) has announced the appointment of a new senior leader for cyber and data. The new leader will be responsible for the service's cyber and data operations, and will report to the service's chief of staff.

Link: <https://www.defensenews.com/space/2025/08/07/space-force-wargame-could-inform-framework-for-allied-info-sharing/>

★ Space Force wargame could inform framework for allied info sharing

The Space Force is launching its annual, future-facing Schriever Wargames this week, and the service's chief operations officer said the exercise could help create a framework for better information sharing with allies and partners on sensitive programs and capabilities. **#USSF #SchrieverWargame**

Link: <https://www.defensenews.com/space/2025/08/07/space-force-wargame-could-inform-framework-for-allied-info-sharing/>

REGULATION

★ Senate bill orders White House to create post-quantum cybersecurity roadmap to protect federal systems

Two U.S. Senators introduced the National Quantum Cybersecurity Migration Strategy Act, a bipartisan bill directing the White House Office of Science and Technology Policy to develop a coordinated national strategy for transitioning federal systems to post-quantum cryptography. The legislation builds on the National Quantum Initiative Act of 2018 and the 2022 Quantum Cybersecurity Preparedness Act, aiming to ensure federal systems are resilient against future quantum-enabled cyber threats. **#PostQuantum #Bill**

Link: <https://industrialcyber.co/regulation-standards-and-compliance/senate-bill-orders-white-house-to-create-post-quantum-cybersecurity-roadmap-to-protect-federal-systems/>

Spain sets out 2025-2030 plan to protect federal systems from quantum-enabled cyber threats

The Spanish government has announced a plan to protect federal systems from quantum-enabled cyber threats. The plan is part of the country's broader strategy to enhance its cybersecurity capabilities and is expected to be implemented by 2030.

Link: <https://industrialcyber.co/regulation-standards-and-compliance/senate-bill-orders-white-house-to-create-post-quantum-cybersecurity-roadmap-to-protect-federal-systems/>

Spain completes draft of National Cybersecurity Strategy

The Spanish government has completed the draft of its National Cybersecurity Strategy. The strategy is a comprehensive plan to enhance the country's cybersecurity capabilities and is expected to be implemented by 2030.

Link: <https://industrialcyber.co/regulation-standards-and-compliance/senate-bill-orders-white-house-to-create-post-quantum-cybersecurity-roadmap-to-protect-federal-systems/>

TECHNOLOGY

★ Impulse Space makes technical changes to Mira OTV

Impulse Space has made a number of technical improvements to its Mira vehicle, the company's high-thrust, highly maneuverable spacecraft for payload hosting and deployment. Cybersecurity is at the heart of one of the main upgrades. For example, the design upgrade for Mira integrates NSA Type 1 cryptographic solutions to protect mission data and command links; Mira also complies with CNSSP-12 requirements to ensure end-to-end security for classified information.

#ImpulseSpace #MiraOTV

Link: <https://www.satellitetoday.com/technology/2025/08/06/impulse-space-makes-technical-changes-to-mira-otv/>

TECHNOLOGY

Identifying IT cyber risks through stronger cyber physical security to protect legacy systems and operational continuity

Strong adoption of IT cyber security and IT technologies across various industries is increasingly becoming a critical factor for the global telecommunications network and critical services. As cyber physical security becomes increasingly important, such integration creates a two-pronged challenge, which includes how to keep operational safety in mind while not overlooking the cyber threats that are required to gain to secure legacy systems from dangerous cyber threats. **MIT Magazine**

Link: [https://www.mit.edu/technology/identifying-it-cyber-risks-through-stronger-cyber-physical-security-to-protect-legacy-systems-and-operational-continuity](#)

The global race for space-based quantum sensors

Quantum technology is becoming a key technology for modern science and defense capabilities, and space-based quantum sensors represent the next frontier. Nations around the world are racing to develop quantum sensors, which have the potential to revolutionize navigation, communication, and fundamental physics experiments. With growing competition, countries such as the United States, China, the European Union, Russia, and India are racing to develop these revolutionary sensors to space. **SpaceNews Magazine**

Link: [https://www.spacenews.com/the-global-race-for-space-based-quantum-sensors](#)

MARKET & COMPETITION



Infosys inaugurates center for advanced AI, cybersecurity, and space technology at Hubballi development center

Infosys, a global leader in next-generation digital services and consulting, announced the launch of its state-of-the-art Infosys Center for Advanced AI, Cybersecurity, and Space Technology at its Hubballi Development Center (DC) in Karnataka. This new center is part of 'Infosys Living Labs', a network of over 12 established centers globally designed to help clients accelerate innovation and leverage emerging technologies to future-proof their businesses. **#Infosys #India**

Link: <https://www.infosys.com/newsroom/press-releases/2025/inaugurates-center-advanced-ai-hubballi.html>



AI-powered tools to help make Japan's nuclear facilities more resilient and responsible

AI-powered tools are becoming an important component to provide more secure, resilient, and responsible nuclear power. Japan is currently in the process of upgrading its nuclear facilities with AI-powered tools. The collaboration supports the country's long-term vision of achieving a sustainable and secure energy future. **MIT Magazine**

Link: [https://www.mit.edu/technology/ai-powered-tools-to-help-make-japan-s-nuclear-facilities-more-resilient-and-responsible](#)



What could NATO's commercial space strategy mean for the EU?

NATO's decision to first commercial space strategy is one of the first steps in the alliance's efforts to strengthen its cyber and space capabilities. As a critical component of NATO's overall security strategy, the alliance is working to ensure that its members are able to protect their critical infrastructure and maintain their operational readiness. **MIT Magazine**

Link: [https://www.mit.edu/technology/what-could-nato-s-commercial-space-strategy-mean-for-the-eu](#)



How India is upping China's Beidou navigation system to plug security gaps

India's recent push to up its Beidou navigation system capabilities, which could impact global markets in the future, is a significant development. The alliance is working to ensure that its members are able to protect their critical infrastructure and maintain their operational readiness. **MIT Magazine**

Link: [https://www.mit.edu/technology/how-india-is-upping-china-s-beidou-navigation-system-to-plug-security-gaps](#)



Sweden's Aerospace acquired by Italy's Leonardo and broader Nordic cyber strategy

Sweden's Aerospace, a leading provider of cyber security services, has been acquired by Leonardo, a major Italian defense contractor. This acquisition is part of a broader Nordic cyber strategy to strengthen the alliance's cyber capabilities and ensure that its members are able to protect their critical infrastructure and maintain their operational readiness. **MIT Magazine**

Link: [https://www.mit.edu/technology/sweden-s-aerospace-acquired-by-italy-s-leonardo-and-broader-nordic-cyber-strategy](#)



THREAT INTELLIGENCE

China's cyberattacks on US military and commercial aircraft

Chinese cyberattacks on US military and commercial aircraft have been on the rise in recent years, according to a report from the US Cyber Command. The report states that Chinese hackers have targeted US military and commercial aircraft, as well as other critical infrastructure, in an effort to gain access to sensitive information and disrupt operations. The report also notes that Chinese hackers have used a variety of tactics, including phishing, social engineering, and malware, to carry out these attacks.



Link: [https://www.cyberinflight.com/news/china-cyberattacks-us-military-commercial-aircraft-08-05-2025](#)

Iranian cyberattacks on US military and commercial aircraft

Iranian cyberattacks on US military and commercial aircraft have been on the rise in recent years, according to a report from the US Cyber Command. The report states that Iranian hackers have targeted US military and commercial aircraft, as well as other critical infrastructure, in an effort to gain access to sensitive information and disrupt operations. The report also notes that Iranian hackers have used a variety of tactics, including phishing, social engineering, and malware, to carry out these attacks.



Link: [https://www.cyberinflight.com/news/iran-cyberattacks-us-military-commercial-aircraft-08-05-2025](#)



Major supplier of military and commercial aircraft allegedly hit by Play Ransomware

Jamco Aerospace Inc. is a New York based engineering and fabrication firm that specialises in crafting components for aerospace and aircraft manufacturers, including aircraft builders used by the US and other governments. The company was listed on the ransomware site of Play Ransomware on Wednesday last week, with a ransom payment deadline of Sunday August 10. **#JamcoAerospace #Ransomware**



Link: <https://nationalcybersecurity.com/major-supplier-of-military-and-commercial-aircraft-allegedly-hit-by-play-ransomware-hacking-cybersecurity-infosec-comptia-pentest-ransomware/>

Resolving US military and commercial aircraft

Resolving US military and commercial aircraft is a complex task that requires a combination of technical expertise, legal authority, and diplomatic efforts. The US military and commercial aircraft are often targeted by cyberattacks, and resolving these attacks can be a challenging task. The US military and commercial aircraft are often targeted by cyberattacks, and resolving these attacks can be a challenging task.

Link: [https://www.cyberinflight.com/news/resolving-us-military-commercial-aircraft-08-05-2025](#)

TRAINING & EDUCATION

US Space Force guardians face off as part of Resolute Space 2025

The US Space Force guardians face off as part of Resolute Space 2025, the service's largest ever exercise, designed to train Guardians to operate under contested, degraded and operationally constrained conditions in space. The exercise is a multi-day event that involves a variety of activities, including training, testing, and evaluation. The exercise is a multi-day event that involves a variety of activities, including training, testing, and evaluation.



Link: [https://www.spaceconnectonline.com.au/global/6627-us-space-force-guardians-face-off-as-part-of-resolute-space-2025](#)



US Space Force guardians face off as part of Resolute Space 2025

In warfighting, there's always a foe, real or simulated, designed to push a military force to its limits. Whether in the air, on land, at sea, in cyber space or beyond Earth's atmosphere, testing tactics under pressure is vital to readiness. For the United States Space Force, that challenge came in the form of Resolute Space 2025, the service's largest ever exercise, designed to train Guardians to operate under contested, degraded and operationally constrained conditions in space. **#ResoluteSpace2025 #USSF**



Link: <https://www.spaceconnectonline.com.au/global/6627-us-space-force-guardians-face-off-as-part-of-resolute-space-2025>

US Space Force guardians face off as part of Resolute Space 2025

The US Space Force guardians face off as part of Resolute Space 2025, the service's largest ever exercise, designed to train Guardians to operate under contested, degraded and operationally constrained conditions in space. The exercise is a multi-day event that involves a variety of activities, including training, testing, and evaluation. The exercise is a multi-day event that involves a variety of activities, including training, testing, and evaluation.



Link: [https://www.spaceconnectonline.com.au/global/6627-us-space-force-guardians-face-off-as-part-of-resolute-space-2025](#)

TRAINING & EDUCATION

Interoperability of Quantum Key Distribution Implementations

Quantum key distribution (QKD) is a secure communication method that uses the principles of quantum mechanics to create a shared secret key between two parties. This key can then be used to encrypt and decrypt messages. The interoperability of QKD implementations is a critical challenge for its widespread adoption. This report examines the current state of QKD interoperability, identifying the challenges and opportunities for standardization, testing, and deployment. It also discusses the importance of interoperability for the future of QKD in secure communications. **Page 4/10**

Link: [https://www.cyberinflight.com/research/interoperability-of-quantum-key-distribution-implementations](#)



The great quantum advantage why not by solving tomorrow's problems while retaining today's skills

The quantum advantage is the ability to solve problems that are intractable for classical computers. This advantage is often cited as the primary motivation for investing in quantum computing. However, the quantum advantage is not a single, well-defined concept. It is a collection of different advantages that can be realized in different ways. This report explores the different types of quantum advantage and the challenges of realizing them. It also discusses the importance of retaining classical computing skills while pursuing quantum computing. **Page 4/10**

Market Hypothesis

Link: [https://www.cyberinflight.com/research/the-great-quantum-advantage-why-not-by-solving-tomorrow-s-problems-while-retaining-today-s-skills](#)

The unseen threat: intelligence and security operations in space beyond satellites - how the race for orbital dominance, intelligence surveillance, and cyberflexibility will converge to orbit

The space domain is becoming a critical theater of operations for intelligence and security operations. The convergence of orbital dominance, intelligence surveillance, and cyberflexibility is creating a new paradigm for space operations. This report examines the challenges and opportunities of this convergence, focusing on the unseen threat of intelligence and security operations in space beyond satellites. It also discusses the importance of understanding the convergence of these domains for future operations. **Page 4/10**

Link: [https://www.cyberinflight.com/research/the-unseen-threat-intelligence-and-security-operations-in-space-beyond-satellites-how-the-race-for-orbital-dominance-intelligence-surveillance-and-cyberflexibility-will-converge-to-orbit](#)



System security framework for 5G Advanced/6G and integrated Terrestrial Network-New Terrestrial Network (5G-NTN) with AI enabled cloud security

The integration of Terrestrial Network (TN) and Non-Terrestrial Network (NTN) is a key challenge for 5G Advanced/6G. This integration requires a new system security framework that can address the unique challenges of this integrated network. This report examines the challenges of this integration and the need for a new system security framework. It also discusses the importance of AI-enabled cloud security in this context. **Page 4/10**

Market Hypothesis

Link: [https://www.cyberinflight.com/research/system-security-framework-for-5g-advanced-6g-and-integrated-terrestrial-network-new-terrestrial-network-5g-ntn-with-ai-enabled-cloud-security](#)



Security and resilience of a data space based manufacturing supply chain

The integration of Terrestrial Network (TN) and Non-Terrestrial Network (NTN) is a key challenge for 5G Advanced/6G. This integration requires a new system security framework that can address the unique challenges of this integrated network. This report examines the challenges of this integration and the need for a new system security framework. It also discusses the importance of AI-enabled cloud security in this context. **Page 4/10**

Market Hypothesis

Link: [https://www.cyberinflight.com/research/security-and-resilience-of-a-data-space-based-manufacturing-supply-chain](#)



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