



SPACE CYBERSECURITY WEEKLY WATCH

W51, W52, W1

December 16 – January 5, 2025

Timeframe: Weekly
of articles identified: 40
Est. time to read: 80 minutes

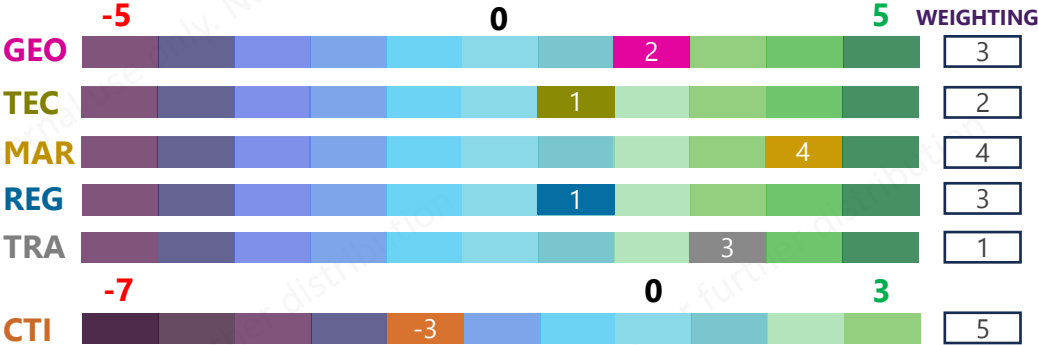
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

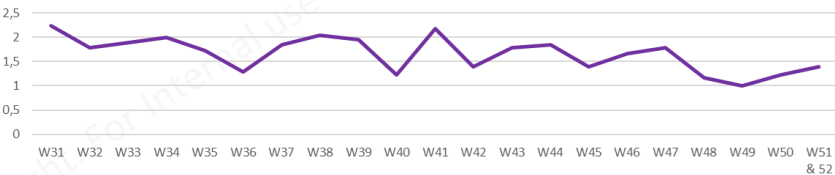
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



↑ The RISC score for this watch is 1.39, a slight increase from W50, due to improvements in the Market and Threat Intel fronts.

Happy New Year! As we step into 2026, this special watch brings together key developments from the end of 2025 and the first week of January. CyberInflight wrapped up the year with an initiative at TBS Education, delivering a lecture on space cybersecurity to Aerospace Master's students. On the geopolitical front, France and the United States conducted close-proximity satellite maneuvers under the joint Operation Olympic Defender. These illustrate strengthened bilateral coordination and France's capacity to conduct dynamic and responsible space operations aimed at deterring adversarial actions. On the regulatory front, Japan formally adopted a new national cybersecurity strategy that will guide policy over the next 5 years. This aims to enhance coordination among civilian, law enforcement, and defense institutions in response to growing and increasingly sophisticated cyber-threats. On the technological side, Leonardo DRS completed the first on-orbit test of its next-generation software-defined radio with integrated advanced cryptography. On the market front, Sopra Steria announced exclusive negotiations to acquire Starion and Nexova through its subsidiary CS Group. The proposed acquisition aims to strengthen Europe's sovereign capabilities by creating a leading player in secure digital services for the space and cybersecurity sectors. On the threat side, ESA confirmed a cybersecurity incident affecting a limited number of external servers. While investigations are ongoing, preliminary findings indicate a contained impact, highlighting the persistent exposure of space organizations to cyber risks beyond core networks. Lastly, a recent academic study analyzed how orbital altitude affects cyber-threats to LEO, MEO, and GEO systems, identifying weak encryption and command-path vulnerabilities as consistent factors that enable adversarial success across all orbital regimes.



CYBERINFLIGHT'S NEWS

CyberInflight at TBS Education: Space Cybersecurity in action!

We had the pleasure of delivering a lecture on Space Cybersecurity to the Aerospace Master of Science students at TBS Education. Our market analysts Héloïse Do Nascimento Cardoso and Valentine Crepineau shared insights on cyber-threats, geopolitical challenges, market dynamics, and regulatory frameworks, providing students with a holistic view of the space cybersecurity ecosystem. **#Cyberdefense #CyberInflight**

Source: [LinkedIn](#)



GEOPOLITICS

France, US practice up-close satellite maneuvers under joint space war plan

The bilateral rendezvous and proximity operation "illustrates France's ability to conduct dynamic and responsible operations to deter adversaries from acting against its space interests," according to France's Space Command.

#OlympicDefender #SpaceWarfare

Source: [Breaking Defense](#)



The German government's Space Safety and Security Strategy

On 16 November 2025, the Federal Ministry of Defense and the Federal Space Office presented the first national space safety and security strategy, which aims to ensure all security-related space activities, including satellite operations, are carried out in a secure and reliable manner while ensuring sustainability. It particularly focuses on ensuring a resilient and reliable security-related infrastructure and capabilities in space. **#GermanSpaceStrategy**

Source: [JPRS.com](#)



Space Force to focus training on orbital warfare, joint integration

The Space Force is getting the green light to focus training on orbital warfare, joint integration, and ensuring a space-ready war-fighting posture in the future. **#SpaceForce #OrbitalWarfare**

Source: [DefenseNews](#)



Cybersecurity and new frontiers in wireless technology: Underwater, Space, and Earth at the Atlantic Foundation conference

The first day of the conference, meeting 100 guests from the first session, opened with a look at the progress of the cyber industry in the Atlantic Foundation. The focus is on cybersecurity in the underwater, terrestrial, and space domains. In the presence of the Secretary of Defense, the Atlantic Foundation will host a series of events. **#AtlanticFoundation #Cybersecurity**

Source: [JPRS.com](#)



Building space Europe: steps up security of satellites

In the European Space Agency (ESA) framework, member states are building defense-related capabilities, as well as creating security-based space assets. It will use a number of tools, such as security to ensure the security of its satellites, as well as providing an early warning system. It will also be putting space communication to the test of the first mission. **#EuropeanSpaceAgency**

Source: [JPRS.com](#)



REGULATION

EU Space Act to update space information policy, a 15-year paradigm revision set to redefine what, how, and where data goes in critical information and the new regulatory paradigm for space activities

The European Space Agency (ESA) is a critical transformation of the space domain, which is intended to be a new space-based information system, a coordinated, comprehensive set of measures to ensure the security of its satellites, as well as providing an early warning system. It will also be putting space communication to the test of the first mission. **#EuropeanSpaceAgency**

Source: [JPRS.com](#)



Japan adopts new cybersecurity strategy to counter rising cyber-threats

The Japanese government has formally adopted a new cybersecurity strategy that will guide national policy over the next five years. The decision aims at strengthening Japanese cybersecurity coordination across civilian, law enforcement, and defense institutions. **#NationalStrategy #Japan**

Source: [The Cyber Express](#)



REGULATION

Indian government releases roadmap for radio frequency spectrum allocation

The Union Minister for Information and Public Relations, Government of India, announced the release of the Roadmap for Radio Frequency Spectrum Allocation. The roadmap outlines the government's strategy for managing the radio frequency spectrum, which is a finite resource, and ensuring its efficient use for various applications, including telecommunications, broadcasting, and defense. The roadmap also emphasizes the need for international cooperation in spectrum management.

Keywords: Spectrum Allocation, Radio Frequency, Government of India

Source: [Ministry of Information and Public Relations](#)



TECHNOLOGY



Leonardo DRS Achieves Major Milestone with First Space-Based Test of Next-Generation Secure Data Transport Capability

Leonardo DRS, Inc. announced today the successful completion of the first on-orbit test of its revolutionary multi-channel software-defined radio (SDR) with integrated advanced cryptography. This milestone marks a significant advance in validating a technology poised to establish a new standard for secure U.S. military satellite data transport at the tactical edge. #Leonardo #Secure

Source: [Leonardo DRS](#)



European Software and Cyber Dependencies

European Software and Cyber Dependencies (ESCD) is a project aimed at reducing the European Union's dependence on non-EU software and hardware. The project focuses on identifying critical dependencies and developing strategies to mitigate risks. The project also aims to promote the development of European software and hardware capabilities.

Keywords: Software, Cyber, Dependencies, European Union



The State of Satellite Navigation

A new study of satellite navigation systems indicates the continued growth of satellite-based navigation systems and services. The study highlights the increasing reliance on satellite navigation for various applications, including transportation, agriculture, and disaster management. The study also discusses the challenges and opportunities associated with the development and deployment of satellite navigation systems.

Keywords: Satellite, Navigation, Systems, Study

MARKET & COMPETITION

Space Force begins first network overhaul as cybersecurity demands grow

The U.S. Space Force is beginning its first major network overhaul, a project that will modernize the network infrastructure used by the Space Force and its partners. The project is being led by the Space Force's Network Operations Center and is expected to be completed by 2028.

Keywords: Space Force, Network, Overhaul, Cybersecurity

Source: [Space Force](#)



Space operations next-generation global to local network to support national government missions

The U.S. Space Force is developing a next-generation global to local network to support national government missions. The network will enable the Space Force to provide secure and reliable communication services to government agencies and the public. The network is being developed by the Space Force's Network Operations Center and is expected to be completed by 2028.

Keywords: Space Force, Network, Operations, Government



AI shipping introduces flexible 5G communication... ensuring both connectivity and security

AI shipping introduces flexible 5G communication, ensuring both connectivity and security. The system uses artificial intelligence to manage the 5G network, allowing for dynamic allocation of resources and ensuring that the network remains secure and reliable. The system is being developed by the Space Force's Network Operations Center and is expected to be completed by 2028.

Keywords: AI, Shipping, 5G, Communication, Security



The cyber vulnerability of space is not in orbit, it is on the ground

The cyber vulnerability of space is not in orbit, it is on the ground. This statement highlights the fact that the ground-based infrastructure that supports space operations is often the most vulnerable to cyber attacks. The statement also emphasizes the need for robust cybersecurity measures to protect the ground-based infrastructure and ensure the security of space operations.

Keywords: Cyber, Vulnerability, Space, Ground





MARKET & COMPETITION



Proposed acquisition of Starion and Nexova, European specialists in space systems engineering and cybersecurity

Sopra Steria, a major tech player in Europe, has announced that it is in exclusive negotiations to acquire Starion and Nexova on behalf of its subsidiary, CS Group. This acquisition aims to create a leading European operator in secure, sovereign digital services and solutions for the space and cybersecurity sectors. **#SopraStoria #Nexova**

Sources: [Sopra Steria](#) [Quantum Zeitgeist](#)



USAF, NASA announce \$100m research effort on AI cybersecurity

The Department of Defense and NASA announced that they will partner with the NSA to conduct a \$100m research effort on AI cybersecurity. The effort will focus on developing new AI-powered cybersecurity tools and techniques to protect the nation's critical infrastructure. **#USAF #NASA #NSA**



Germany awards COTS, Manneded aircraft \$100m for new COTS development

The German Ministry of Defense has awarded a \$100m contract to develop a new COTS (Commercial Off-The-Shelf) aircraft. The contract is for the development of a new COTS aircraft that will be used for a variety of missions, including reconnaissance, surveillance, and intelligence gathering. **#Germany #COTS #Manneded**



Portugal signs 10-year military agreement to strengthen positioning, proposed services

Portugal has signed a 10-year military agreement with the United States to strengthen its positioning and provide proposed services. The agreement is part of a larger effort to enhance the defense capabilities of the United States and its allies. **#Portugal #Military #Agreement**



France's new \$100m Portugal funding plan includes 'enhanced cybersecurity' for Cyber Command, here's what we know

The new \$100m Portugal funding plan includes 'enhanced cybersecurity' for Cyber Command. The plan is part of a larger effort to enhance the defense capabilities of the United States and its allies. **#France #Portugal #Cybersecurity**



US Space partners with Canada defense department and Telus to deliver next generation military satellite

The US Space Force has partnered with the Canadian defense department and Telus to deliver the next generation military satellite. The partnership is part of a larger effort to enhance the defense capabilities of the United States and its allies. **#USSpace #Canada #Telus**



THREAT INTELLIGENCE

Canadian Forces Command creates new Ops Center for NATO and US

The Canadian Forces Command has created a new Operations Center for NATO and the United States. The center is part of a larger effort to enhance the defense capabilities of the United States and its allies. **#Canada #NATO #US**



Chinese Space command creates data hub

The Chinese Space Command has created a new data hub. The hub is part of a larger effort to enhance the defense capabilities of the United States and its allies. **#China #Space #Data**



THREAT INTELLIGENCE

Alleged Confidential Status of Spacecraft are Leaked

Confidential status information for various spacecraft is leaked to the public, raising concerns about the security of space operations.

Reported by: [Source]

Source: [TheCyberExpress](#), [Red Hot Cyber](#)



Refugees target the satellites of European Space Agency

Refugees have targeted the satellites of the European Space Agency (ESA) in an attempt to disrupt its operations.

Reported by: [Source]

Source: [TheCyberExpress](#), [Red Hot Cyber](#)



U.S. and European Space Agencies (ESA) agree to discuss attacks, raising flight hazard

The United States and the European Space Agency (ESA) have agreed to discuss attacks on spacecraft, raising concerns about the safety of space operations.

Reported by: [Source]

Source: [TheCyberExpress](#), [Red Hot Cyber](#)



European Space Agency confirms cybersecurity breach on external servers

The European Space Agency (ESA) has confirmed a cybersecurity breach involving servers located outside its corporate network. This confirmation comes following threat actor claim that they had compromised ESA systems and stolen a large volume of internal data. In an official statement shared on social media, the European Space Agency said it is aware of the cybersecurity issue and has already launched a forensic security investigation, which remains ongoing. According to ESA, preliminary findings indicate that only a very small number of external servers were impacted. **#ESA #DataBreach**

Sources: [X](#), [TheCyberExpress](#), [Red Hot Cyber](#)



Alleged unauthorized access to the NASA U.S. satellite system

An alleged unauthorized access to the NASA U.S. satellite system is reported, raising concerns about the security of the system.

Reported by: [Source]

Source: [TheCyberExpress](#), [Red Hot Cyber](#)



Why U.S. and Chinese satellites are highlighting in orbit

The U.S. and Chinese satellites are highlighting in orbit, raising concerns about the security of the system.

Reported by: [Source]

Source: [TheCyberExpress](#), [Red Hot Cyber](#)



TRAINING & EDUCATION

Space Cybersecurity: A systematic overview of attacks against space infrastructure

Space infrastructure represents an emerging domain that is critical to the global economy and society. However, the domain is vulnerable to attacks, in the cyber, space, and physical domains. This report provides a systematic overview of attacks against space infrastructure.

Reported by: [Source]

Source: [TheCyberExpress](#), [Red Hot Cyber](#)



Cybersecurity has always been a critical focus in the Aerospace and Defense industry

Cybersecurity has always been a critical focus in the Aerospace and Defense industry. This report provides a systematic overview of attacks against space infrastructure.

Reported by: [Source]

Source: [TheCyberExpress](#), [Red Hot Cyber](#)



Optimal satellite architecture for spaceborne jamming attacks

Optimal satellite architecture for spaceborne jamming attacks is discussed, highlighting the importance of the system design.

Reported by: [Source]

Source: [TheCyberExpress](#), [Red Hot Cyber](#)



TRAINING & EDUCATION



The Global Frontier of Security: The impact of space security with the President
The President's address to the nation on space security was a landmark moment, marking the first time a U.S. President has explicitly addressed the global security implications of space. The speech outlined the critical nature of space as a domain of competition, the threat of unprovoked space aggression, and the urgent need for a robust security posture. It emphasized the importance of international cooperation and the role of the United States in leading the world in space security.

Source: [CyberInflight](#)



Space Cybersecurity in Asia in the spotlight of CNA's Asia 2025
The Asia 2025 conference, an annual event for Asia-Pacific leaders, has spotlighted space cybersecurity as a critical issue. The conference featured a panel discussion on the topic, with experts from the U.S., Japan, and South Korea. The panelists discussed the challenges of space cybersecurity in the Asia-Pacific region and the need for international cooperation to address these challenges.

Source: [CyberInflight](#)



Satellite Cybersecurity Across Orbital Altitudes: Analyzing Ground-Based Threats to LEO, MEO, and GEO

The researchers characterize how orbital altitude dictates attack feasibility and impact. Their evaluation reveals distinct threat profiles: GEO systems are predominantly targeted via high-frequency uplink exposure, whereas LEO constellations face unique risks stemming from limited power budgets, hardware constraints, and susceptibility to thermal and radiation-induced faults. The results demonstrate that weak encryption and command path irregularities are the most consistent predictors of adversarial success across all orbits. **#Paper #Awareness**



Source: [Cornell University](#), [Quantum Zeitgeist](#)

Strategic Disruption from Space: Operation Range of Motion and the Future of Regional Space Warfare
The concept of strategic disruption from space is a new paradigm in warfare, one that involves the use of space-based assets to disrupt an adversary's military and economic activities. The U.S. has been developing this capability, and it is expected to play a major role in future regional space warfare. The article discusses the challenges of this new paradigm and the need for international cooperation to address these challenges.

Source: [CyberInflight](#)



SpDRM: Space Satellite Intrusion Detection Using Reproducible Machine Learning for Near-Realtime Satellite Communication Networks
Space and satellite communication networks are becoming increasingly vulnerable to cyber threats. The SpDRM project is a new approach to detecting and preventing these threats. It uses machine learning to analyze satellite communication data and identify suspicious activity. The project is currently in the testing phase, and it is expected to be deployed in the near future.

Source: [CyberInflight](#)



The 6th Space Summit - Summary 2025 to 2026
The 6th Space Summit was held in Washington, D.C. in 2025. It was the largest gathering of space leaders in the world, with over 100 participants from 30 countries. The summit focused on the challenges of space security and the need for international cooperation to address these challenges. The summit also discussed the future of space exploration and the role of the United States in leading the world in space.

Source: [CyberInflight](#)



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