

SPACE CYBERSECURITY WEEKLY WATCH

Week 49

December 2 - 8, 2025

Timeframe: Weekly

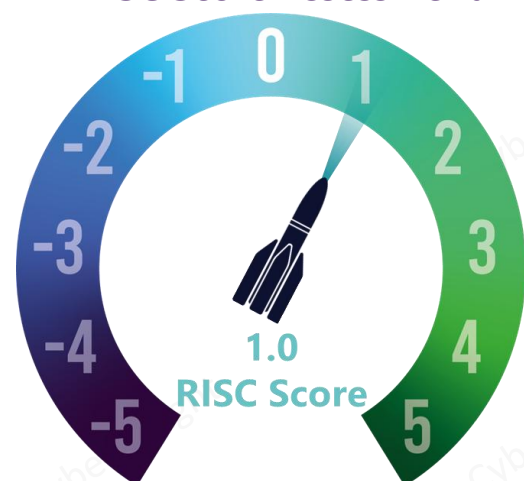
of articles identified: 30

Est. time to read: 60 minutes

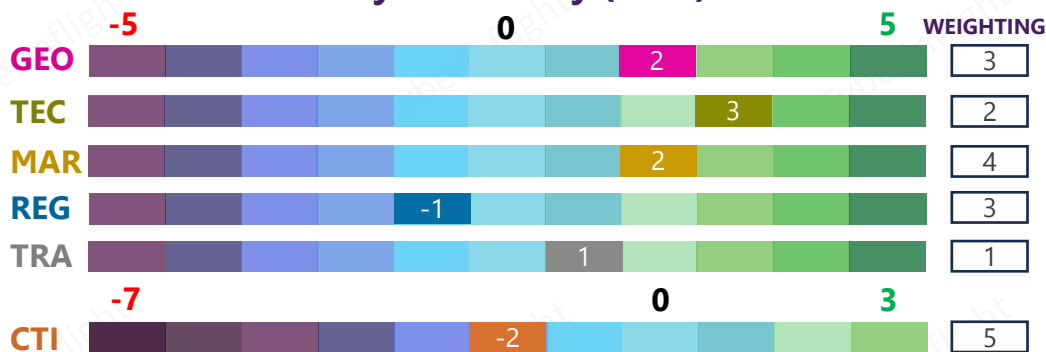
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

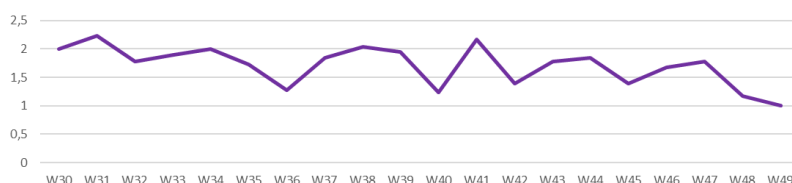
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



↓ The RISC score for this watch is 1.0, a decrease from last week. This difference is due to a drop in geopolitical and regulatory news, balanced by a slight improvement in technological and threat intelligence fronts.

As developments across the space and cybersecurity domains continue to reshape strategic postures, CyberInflight has updated its website to reflect better how our consulting activities complement our research and intelligence products across both traditional space stakeholders and the New Space ecosystem. This week, on the geopolitical side, Poland has formally secured access to the U.S. global military satellite communications network, gaining immediate entry into a system designed to operate under jamming and electronic attack. On the regulatory front, Russian forces in Ukraine continue to use black market Starlink terminals on drones such as the Molniya, extending operational range and lethality despite SpaceX geofencing measures and ongoing U.S. enforcement efforts. On the technological side, the US Space Force's Project Kronos aims to consolidate and modernize legacy systems into a unified software suite offering satellite operators enhanced intelligence and command and control capabilities. On the market side, GomSpace has signed the SECUSAT contract with the European Space Agency for the development of a security-enhanced generation of its NanoCom product line. On the threat side, international space cooperation has taken a new hit as a veteran Russian cosmonaut was abruptly removed from an upcoming SpaceX astronaut mission amid espionage allegations. Lastly, in the training and education section, a recent paper examines how real-world cyberattacks against space infrastructures can be characterized.

CYBERINFLIGHT'S NEWS



Discover our consulting services!

At CyberInflight, we complement our research and intelligence products with tailored consulting services designed to support both traditional space stakeholders and the New Space ecosystem. Discover our approach.

#ConsultingServices #CyberInflight

Source: [CyberInflight](#)



GEOPOLITICS



Poland enters U.S.-led global military satellite network

Poland has formally secured access to the United States' global military satellite communications network, gaining immediate entry into a system designed to operate under jamming and electronic attack. A Memorandum of Understanding was signed on December 4 at the Agency for Geospatial Reconnaissance and Satellite Services in Warsaw by Brigadier General Marcin Górka, Director of the Department of Innovation. The agreement links the Polish Armed Forces to the Wideband Global SATCOM program, a U.S.-led military satellite network providing secure broadband communications worldwide. **#SATCOM #MoU**

Source: [Defense Mirror](#)



REGULATION



Russia evades Starlink bans with black market drone terminals in Ukraine

Russian forces in Ukraine persist in using black market Starlink terminals on drones like the Molniya, enhancing range and lethality despite SpaceX's geofencing and U.S. crackdowns. Illicit supply chains through regions like Sudan evade controls, highlighting challenges in regulating dual-use tech in modern warfare. This raises ethical and geopolitical concerns.

#Crackdowns #BlackMarket

Source: [WPN](#)



TECHNOLOGY



TECHNOLOGY

New technology and tools used to address DDoS/DDP spoofing

A joint effort is underway to develop the new standard for the security of space networks. The effort involves the use of new tools, techniques, and technology, including the use of new tools and techniques to address the problem of DDoS/DDP spoofing.

Source: [CyberInflight](#)

Integrating defense Malaysia for new regional cyber task, strengthening Southeast Asia's cyber resilience

Malaysia is a new regional cyber task, strengthening its position as a leader in technology for security. The integration will allow the country to better protect its critical infrastructure and to better protect its citizens. The integration will also allow the country to better protect its citizens and to better protect its infrastructure.

Source: [CyberInflight](#)

China advances quantum information via Moon satellite for secure networks

China has advanced quantum information, demonstrating a new way to protect data transfer via the Moon satellite using quantum entanglement. The satellite will be used to protect data transfer via the Moon satellite using quantum entanglement. The satellite will be used to protect data transfer via the Moon satellite using quantum entanglement.

Source: [CyberInflight](#)



Space Force wants artificial intelligence (AI) and cybersecurity for space command and control

U.S. Space Force battle-management experts are reaching out to industry for enabling technologies that range from cloud computing infrastructure to software applications, artificial intelligence (AI), and software development services. The Space Force's Project Kronos seeks to consolidate and upgrade legacy systems into a unified software suite that provides satellite operators with intelligence tools and command-and-control capabilities. The project aims to enhance decision-making, accelerate planning and deconfliction, and provide shared situational awareness. **#USSF #KronosProject**

Source: [Military Aerospace Corporation](#)

UK's and US's launch secure satellite on Space station

UK's and US's launch secure satellite on Space station. The satellite will be used to protect data transfer via the Moon satellite using quantum entanglement. The satellite will be used to protect data transfer via the Moon satellite using quantum entanglement.

Source: [CyberInflight](#)

In the U.S. military integrates artificial intelligence, data integrity is the priority

The U.S. military is integrating artificial intelligence, data integrity is the priority. The satellite will be used to protect data transfer via the Moon satellite using quantum entanglement. The satellite will be used to protect data transfer via the Moon satellite using quantum entanglement.

Source: [CyberInflight](#)

MARKET & COMPETITION

Japan to build a satellite for the Japanese Space Agency's new mission

Japan to build a satellite for the Japanese Space Agency's new mission. The satellite will be used to protect data transfer via the Moon satellite using quantum entanglement. The satellite will be used to protect data transfer via the Moon satellite using quantum entanglement.

Source: [CyberInflight](#)

Competition and DDoS Cybersecurity by Israel begins joint research on satellite cybersecurity

Competition and DDoS Cybersecurity by Israel begins joint research on satellite cybersecurity. The satellite will be used to protect data transfer via the Moon satellite using quantum entanglement. The satellite will be used to protect data transfer via the Moon satellite using quantum entanglement.

Source: [CyberInflight](#)

MARKET & COMPETITION



GomSpace signs €1.2m contract with ESA for SECUSAT: A major step forward in secure space communications for a safer world

GomSpace signs SECUSAT contract with the European Space Agency (ESA) for the development of an advanced, security-enhanced generation of its NanoCom product line. The agreement, valued at €1.2m, confirms ESA's confidence in GomSpace's technological leadership and marks a significant milestone in the evolution of secure satellite communications. #SECUSAT #Contract

Source: [GOMSpace](#)



South Korea to improve US Air Space Force M77000 security

South Korea will receive a \$100 million contract to improve the US Air Force's M77000 security. The contract will be awarded to a South Korean company that will provide the necessary hardware and software to enhance the security of the M77000.

Source: [South Korea](#)



IBM and STC Group to address quantum safe solutions for the defense sector

IBM and STC Group have announced a partnership to address quantum safe solutions for the defense sector. The partnership will focus on developing quantum safe solutions for the defense sector, including the development of quantum safe encryption algorithms and the development of quantum safe communication systems.

Source: [IBM](#)



US Cyber Space services IBM working to develop Secure M77000 as a cloud computer

US Cyber Space services IBM working to develop Secure M77000 as a cloud computer. The project will involve the development of a cloud computer that will be able to process and store data in a secure manner. The project will also involve the development of a cloud computer that will be able to process and store data in a secure manner.

Source: [IBM](#)



THREAT INTELLIGENCE

Indian government confirms cyberattacks on Indian airports involving VPN spoofing

The Indian government has confirmed that cyberattacks on Indian airports involving VPN spoofing. The attacks were carried out by a group of hackers who used VPN spoofing to gain access to the airports' internal networks. The government has taken steps to enhance the security of the airports' internal networks.

Source: [India](#)



Communist group threatens killing

A communist group has threatened to kill a person. The group has threatened to kill the person if they do not meet their demands. The group has threatened to kill the person if they do not meet their demands.

Source: [Communist group](#)



Explosion & Espionage! China's bold rocket test ends in fireball, Russian cosmonaut removed from SpaceX

International space cooperation has hit a new low, with a veteran Russian cosmonaut abruptly removed from SpaceX's upcoming astronaut mission amid allegations of espionage. #SpaceX #Espionage

Source: [The Eurasian Times](#)



THREAT INTELLIGENCE

Russia's Roscosmos reports that the US launched and tested a US satellite jammer

On December 1, 2025, Russia's Roscosmos reported that the United States launched and tested a satellite jammer. The jammer was launched from the United States and was used to jam Russian satellites. Roscosmos reported that the jammer was used to jam Russian satellites in the Black Sea, the Mediterranean, and the Atlantic. The jammer was used to jam Russian satellites in the Black Sea, the Mediterranean, and the Atlantic. The jammer was used to jam Russian satellites in the Black Sea, the Mediterranean, and the Atlantic. The jammer was used to jam Russian satellites in the Black Sea, the Mediterranean, and the Atlantic.



Source: [Russia](#)

Play commentators group claims access to NATO Aerospace data is now back with posting

The Aerospace 2025, a US engineering and manufacturing industry group, reported that the defense and aerospace sectors, supported by the US government, group, and NATO, have now gained access to NATO Aerospace data. The group reported that the data is now back with posting. The group reported that the data is now back with posting. The group reported that the data is now back with posting. The group reported that the data is now back with posting.



Source: [Russia](#)

Hundreds of Russian jets in Russia become undetectable due to a malfunction in their factory-installed satellite security system, sources say

Hundreds of Russian jets in Russia became undetectable after their factory-installed satellite security system malfunctioned. Sources say that the system is a satellite security system that is used to protect Russian jets. The system is a satellite security system that is used to protect Russian jets. The system is a satellite security system that is used to protect Russian jets. The system is a satellite security system that is used to protect Russian jets.



Source: [Russia](#)

TRAINING & EDUCATION

Assessment of Artificial Intelligence as an alternative source for cyber threat

The paper, titled "Assessment of Artificial Intelligence as an alternative source for cyber threat", was published by the US government. The paper was published by the US government. The paper was published by the US government. The paper was published by the US government.



Source: [Russia](#)



Characterizing cyberattacks against space infrastructures with missing data: framework and case study

How can we characterize real-world cyberattacks against space infrastructures? This paper addresses the problem by proposing a framework, including metrics, while also addressing the missing-data problem by leveraging methodologies such as the Space Attack Research and Tactic Analysis (SPARTA) and the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) to "extrapolate" the missing data in a principled fashion. **#Framework #Paper**



Source: [Cornell University](#)

Assessing AI-based jamming to US satellite networks using quantum-enhanced deep reinforcement learning

The paper, titled "Assessing AI-based jamming to US satellite networks using quantum-enhanced deep reinforcement learning", was published by the US government. The paper was published by the US government. The paper was published by the US government. The paper was published by the US government.



Source: [Russia](#)

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