

SPACE CYBERSECURITY WEEKLY WATCH

Week 49

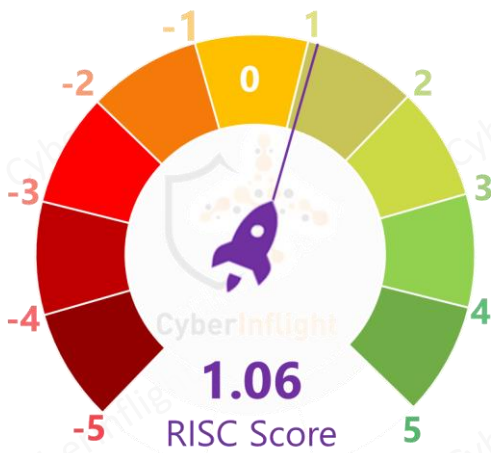
December 03 - 09, 2024

Timeframe: Weekly
of articles identified: 41
Est. time to read: 1 hour

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

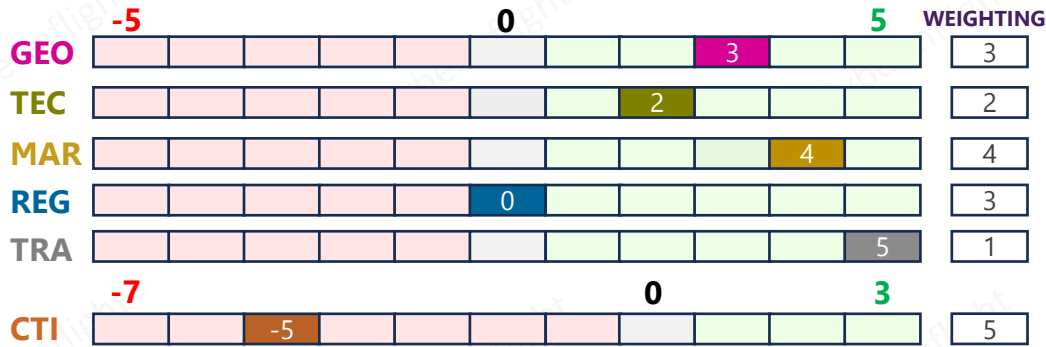
- **GEOPOLITICS**
- **TECHNOLOGY**
- **MARKET INTELLIGENCE**
- **REGULATION**
- **TRAINING & EDUCATION**
- **THREAT INTELLIGENCE**
- ★ **IMPORTANT NEWS**

RISC Score Assessment

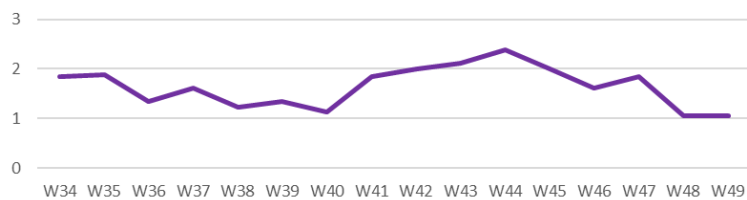


This week's RISC score is 1.06, reflecting the same risk as last week. This similarity is attributed to an important threat climate, equilibrated with several articles referring to contracts and market aspects, as well as training documents.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score Evolution



On the geopolitical side, an article from IARI (Istituto Analisi Relazioni Internazionali) about space has been published where it states that the militarization and weaponization of space have led to the development of anti-satellite weapons and that increasing cyber threats further complicate space security. On the threat intel side, an awareness article about spacecraft, satellites, and space-based systems that, in recent years, have increasingly become targets for malicious actors, including nation-sponsored hacker groups, raising serious concerns about mission safety and national security came up. Moreover, Interpol tipped off South Korean authorities about a suspicious shipment of satellite receivers from a Korean firm to an overseas company known for illegal broadcasting. Analysis confirmed that the receivers either came preloaded with malicious software enabling DDoS attacks or were configured to install it during firmware updates. The affected devices had been shipped between January 2019 and September 2024, with an earlier batch of nearly 98,000 units already infected at the time of sale. On the market front, RTX Raytheon will build 13 Next Generation Jammer Mid-Band (NGJ-MB) airborne EW systems for US Navy and Australian EA-18 Growler combat jets under terms of a \$591m contract announced in late November. On the technological side, Jesse Morehouse, Lockheed Martin's director of business development and strategy for positioning navigation and timing, said the ecosystem often overlooks security upgrades and technological innovations being developed to enhance GPS. Lastly, on board the ISS and the European Columbus module, DropCoal is performing its daily tasks that require real-time protection and adhere to rigorous cybersecurity standards set by ESA and NASA.

GEOPOLITICS

Space Balance Overview

Space balance overview: The space balance overview is a key concept in space geopolitics, referring to the distribution of power and influence among space-faring nations. It encompasses various factors such as satellite capabilities, launch capabilities, and space-based assets. The balance of power in space is constantly shifting as more countries enter the space domain.

[Link: https://www.space.com/54888-space-balance-overview.html](#)



The evolving strategic importance of space in modern military operations

Since the mid-1950s, the number of space actors has proliferated, with more countries now actively participating in space activities. This interest highlights the critical role of satellites and space technologies in both the military and commercial sectors. Nations are investing heavily in advanced space capabilities to strengthen military power and protect strategic assets, making space a contested and competitive domain. **#Awareness #Military**

Link: <https://iari.site/2024/12/07/the-evolving-strategic-importance-of-space-in-modern-military-operations/>

US working with partners for space security

The United States is working with its partners to enhance space security. This includes sharing intelligence, conducting joint operations, and developing common standards. The goal is to ensure the safety and security of space activities for all nations. The US is also leading efforts to address the growing challenges of space security, including the development of space-based anti-satellite capabilities and the establishment of a space-based early warning system.

[Link: https://www.defense.gov/Newsroom/Record/Article/348441/US-working-with-partners-for-space-security](#)



Today's Cold War: space, cybersecurity and geopolitical strategy

Today's Cold War: space, cybersecurity and geopolitical strategy. The current geopolitical landscape is characterized by a new Cold War between the United States and China. This rivalry extends to space, where both nations are competing for dominance. Space is seen as a critical domain for national security, and the competition for space-based assets and capabilities is intensifying. This competition is also driving advances in cybersecurity and artificial intelligence.

[Link: https://www.space.com/54888-space-balance-overview.html](#)

TECHNOLOGY

Space 2024: Overview of the Space Industry and Key Developments in 2024

Space 2024: Overview of the Space Industry and Key Developments in 2024. The space industry has seen significant growth in 2024, with new launches, commercial space flights, and advancements in satellite technology. Key developments include the launch of the Artemis moon lander, the first commercial space station, and the deployment of new satellite constellations. The industry is also seeing increased competition and collaboration between nations and private companies.

[Link: https://www.space.com/54888-space-balance-overview.html](#)



Lockheed Martin challenges narrative on GPS vulnerability

Lockheed Martin is challenging the prevailing narrative that military users of the Global Positioning System (GPS) are dangerously vulnerable to service disruptions and is emphasizing the advanced security features set to debut with the upcoming GPS III F satellites. While GPS is widely viewed as an indispensable backbone of the global economy, it is simultaneously seen as a fragile technological system vulnerable to sophisticated electronic warfare techniques and signal disruption. Jesse Morehouse, Lockheed Martin's director of business development and strategy for positioning navigation and timing, said this narrative overlooks security upgrades and technological innovations being developed to enhance GPS. **#LockheedMartin #GPS**

Link: <https://spacenews.com/lockheed-martin-challenges-narrative-on-gps-vulnerability/>



THREAT INTELLIGENCE

Western Intelligence Agencies Warn of a Cyberwar

Western intelligence agencies have issued a warning of a potential cyberwar between the United States and China. The agencies cite the increasing sophistication of Chinese cyber operations and the growing reliance on technology in both nations. The warning is based on the belief that a cyberwar could have significant global consequences, including the disruption of critical infrastructure and the loss of sensitive information.

[Link: https://www.space.com/54888-space-balance-overview.html](#)



European Space Agency Warns of Space Threats

The European Space Agency (ESA) has issued a warning of space threats, including the risk of satellite collisions and the potential for space-based anti-satellite weapons. The agency is calling for international cooperation to address these threats and ensure the safety and security of space activities. ESA is also working to develop space-based early warning systems and anti-satellite capabilities to protect its own assets.

[Link: https://www.space.com/54888-space-balance-overview.html](#)



THREAT INTELLIGENCE

Countering Navigation and Timing Satellites and their reliance on GPS

Countering Navigation and Timing Satellites and their reliance on GPS



Countering Navigation and Timing Satellites and their reliance on GPS

GPS spoofing and jamming: High altitude platforms to counter GPS jamming

GPS spoofing and jamming: High altitude platforms to counter GPS jamming



GPS spoofing and jamming: High altitude platforms to counter GPS jamming

It's time to defend ourselves in space

It's time to defend ourselves in space



It's time to defend ourselves in space

2024-2026 US Space Security Strategy

2024-2026 US Space Security Strategy



2024-2026 US Space Security Strategy

GPS spoofing and jamming: High altitude platforms to counter GPS jamming

GPS spoofing and jamming: High altitude platforms to counter GPS jamming



GPS spoofing and jamming: High altitude platforms to counter GPS jamming

★ Orbit under siege: The cybersecurity challenges of space missions

In recent years, spacecraft, satellites, and space-based systems have increasingly become targets for malicious actors, including nation-sponsored hacker groups, raising serious concerns about mission safety and national security. According to a 2024 Deloitte report, the number of active satellites in orbit is approaching 10,000 and is expected to double every 18 months. This rapid growth increases the risk of cyberattacks on satellites, ground stations, and communication links.



#Awareness #SpaceMissions

Link: <https://www.cysecurity.news/2024/12/orbit-under-siege-cybersecurity.html>

Countering navigation spoofing: High altitude platforms to counter GPS jamming

Countering navigation spoofing: High altitude platforms to counter GPS jamming

Countering navigation spoofing: High altitude platforms to counter GPS jamming

China's rapid space militarization raises concerns

China's rapid space militarization raises concerns



China's rapid space militarization raises concerns



THREAT INTELLIGENCE

APT28 targets semiconductor firms, launches attacks on aerospace and semiconductor industries in multiple countries

APT28, also known as Fancy Bear, has been targeting semiconductor firms in a global group headed by the Russian government. The group has been active in multiple countries, including the United States, Europe, and Asia. The group has been targeting semiconductor firms in multiple countries, including the United States, Europe, and Asia. The group has been targeting semiconductor firms in multiple countries, including the United States, Europe, and Asia.

Link: [https://www.cisa.gov/news-events/press-releases/details?id=A192401](#)



Long Range Countering China's (LRCC) threat to US critical infrastructure and military systems

The LRCC threat to US critical infrastructure and military systems is a significant concern. The group has been targeting critical infrastructure and military systems in multiple countries, including the United States, Europe, and Asia. The group has been targeting critical infrastructure and military systems in multiple countries, including the United States, Europe, and Asia.

Link: [https://www.cisa.gov/news-events/press-releases/details?id=A192401](#)



US military systems and software in the process of cyberattacks capabilities of adversaries (that) targeted for sophisticated and dangerous cyberattacks

The US military systems and software are in the process of cyberattacks capabilities of adversaries. The group has been targeting military systems and software in multiple countries, including the United States, Europe, and Asia. The group has been targeting military systems and software in multiple countries, including the United States, Europe, and Asia.

Link: [https://www.cisa.gov/news-events/press-releases/details?id=A192401](#)



Korean firm busted for Selling DDoS-enabled satellite receivers

The investigation began in July 2024 when Interpol tipped off South Korean authorities about a suspicious shipment of satellite receivers from a Korean firm, B Corporation, to an overseas company, A Corporation, known for illegal broadcasting. Interpol suspected that the devices included malicious software enabling DDoS attacks. Subsequent analysis confirmed that the receivers either came preloaded with the malware or were configured to install it during firmware updates. The affected devices had been shipped between January 2019 and September 2024, with an earlier batch of nearly 98,000 units already infected at the time of sale. **#SouthKorea #DDoS**

Link: <https://cyberinsider.com/korean-firm-busted-for-selling-ddos-enabled-satellite-receivers/>



Cybersecurity in space safeguarding the food basket

The cybersecurity in space is a significant concern for the food basket. The group has been targeting space systems and infrastructure in multiple countries, including the United States, Europe, and Asia. The group has been targeting space systems and infrastructure in multiple countries, including the United States, Europe, and Asia.

Link: [https://www.cisa.gov/news-events/press-releases/details?id=A192401](#)



Space satellite network cyberattacks 2024

The space satellite network cyberattacks in 2024 are a significant concern. The group has been targeting satellite networks and infrastructure in multiple countries, including the United States, Europe, and Asia. The group has been targeting satellite networks and infrastructure in multiple countries, including the United States, Europe, and Asia.

Link: [https://www.cisa.gov/news-events/press-releases/details?id=A192401](#)



Russia 'breaks out' cyberattacks target aerospace firms

Russia has broken out cyberattacks targeting aerospace firms. The group has been targeting aerospace firms and infrastructure in multiple countries, including the United States, Europe, and Asia. The group has been targeting aerospace firms and infrastructure in multiple countries, including the United States, Europe, and Asia.

Link: [https://www.cisa.gov/news-events/press-releases/details?id=A192401](#)



MARKET & COMPETITION

Defense and Military agencies announce partnership, announce first software defined satellite communication satellite in 2026 launch date

Defense and Military agencies announce partnership to support the development and delivery of the first software defined satellite communication satellite in 2026 launch date. The partnership will support the development and delivery of the first software defined satellite communication satellite in 2026 launch date. [Defense Weekly](#)



USCIS announces new program for public service activities, announced for software defined satellite communication satellite in 2026 launch date

Europe's first satellite in orbit and Europe

Europe's first satellite in orbit and Europe. The satellite is the first of its kind and will be used for a variety of purposes, including navigation, communication, and data collection. The satellite is the first of its kind and will be used for a variety of purposes, including navigation, communication, and data collection. [Space Daily](#)



Defense's Signal Corps uses US Navy contract

Defense's Signal Corps uses US Navy contract. The contract is for the development and delivery of the first software defined satellite communication satellite in 2026 launch date. [Space Daily](#)



Navy asks RTX Raytheon for 13 airborne electronic warfare (EW) jammers for US and Australian combat jets

RTX Raytheon will build 13 Next Generation Jammer Mid-Band (NGJ-MB) airborne EW systems for US Navy and Australian EA-18 Growler combat jets under terms of a \$591m contract announced in late November. The NGJ midband is an advanced electronic attack system that denies, disrupts, and degrades enemy communications and air-defense radar systems. [EW #Raytheon](#)



Link: <https://www.militaryaerospace.com/sensors/article/55247123/raytheon-technologies-corp-airborne-electronic-warfare-ew-jammers>

Space program with capability to strengthen public sector IT cybersecurity

Space program with capability to strengthen public sector IT cybersecurity. The program is designed to provide the public sector with the tools and resources needed to protect their information systems from cyber threats. [Space Daily](#)



USCIS announces new program for public service activities, announced for software defined satellite communication satellite in 2026 launch date

USCIS announces new program for public service activities, announced for software defined satellite communication satellite in 2026 launch date. The program is designed to provide the public sector with the tools and resources needed to protect their information systems from cyber threats. [Space Daily](#)



USCIS announces new program for public service activities, announced for software defined satellite communication satellite in 2026 launch date

USCIS announces new program for public service activities, announced for software defined satellite communication satellite in 2026 launch date. The program is designed to provide the public sector with the tools and resources needed to protect their information systems from cyber threats. [Space Daily](#)

USCIS announces new program for public service activities, announced for software defined satellite communication satellite in 2026 launch date. The program is designed to provide the public sector with the tools and resources needed to protect their information systems from cyber threats. [Space Daily](#)



USCIS announces new program for public service activities, announced for software defined satellite communication satellite in 2026 launch date

USCIS announces new program for public service activities, announced for software defined satellite communication satellite in 2026 launch date. The program is designed to provide the public sector with the tools and resources needed to protect their information systems from cyber threats. [Space Daily](#)

MARKET & COMPETITION

France is expected to add jobs in space as satellite operators will increase (Post-Action is 100 jobs in France in its space and military activities)

The Ministry of Defense is expected to add jobs in space as satellite operators will increase (Post-Action is 100 jobs in France in its space and military activities)



USA: The space industry is expected to add jobs in space as satellite operators will increase

USA: The space industry is expected to add jobs in space as satellite operators will increase

The space industry is expected to add jobs in space as satellite operators will increase



USA: The space industry is expected to add jobs in space as satellite operators will increase

TRAINING & EDUCATION

What 2024 ISS Success: Establishing the future of life and space power

The success of the ISS is a testament to the power of international cooperation and the future of space exploration



The International Space Station: A platform for 2024 space exploration and ISS-based research

The International Space Station is a platform for 2024 space exploration and ISS-based research



Spaceport Village - ISS-2024 Mission Success: Launch 2024-2025 ISS

Spaceport Village - ISS-2024 Mission Success: Launch 2024-2025 ISS



What cybersecurity on the ISS teaches us about defending critical systems

400 kilometers above the Earth, on board the International Space Station and inside the European Columbus module, DropCoal—a complex scientific experiment developed by the Romanian InSpace Engineering (RISE)—is performing its daily tasks, relying on real-time operations from the ground. However, real-time operations require real-time protection that adheres to rigorous cybersecurity standards set by both the European Space Agency (ESA) and the National Space Administration (NASA). #ISS #DropCoal

Link: <https://www.bitdefender.com/en-us/blog/businessinsights/what-cybersecurity-on-the-iss-teaches-us-about-defending-critical-systems>

USA: The space industry is expected to add jobs in space as satellite operators will increase

The space industry is expected to add jobs in space as satellite operators will increase



USA: The space industry is expected to add jobs in space as satellite operators will increase



TRAINING & EDUCATION

2024 Space Force official series of Space Cybersecurity Month
The 2024 series of space operations for the 2024 Space Force Cyber Month includes a host of events, including the monthly Space Cyber Security Challenge, which is a series of challenges and puzzles designed to challenge the skills of participants in cyber security. The 2024 Space Cyber Security Challenge is a series of challenges, puzzles, and quizzes designed to challenge the skills of participants in cyber security. The 2024 Space Cyber Security Challenge is a series of challenges, puzzles, and quizzes designed to challenge the skills of participants in cyber security.



2024 Space Force Cyber Security Challenge
The 2024 Space Force Cyber Security Challenge is a series of challenges and puzzles designed to challenge the skills of participants in cyber security. The 2024 Space Force Cyber Security Challenge is a series of challenges, puzzles, and quizzes designed to challenge the skills of participants in cyber security.



2024 Space Force Cyber Security Challenge
The 2024 Space Force Cyber Security Challenge is a series of challenges and puzzles designed to challenge the skills of participants in cyber security. The 2024 Space Force Cyber Security Challenge is a series of challenges, puzzles, and quizzes designed to challenge the skills of participants in cyber security.



2024 Space Force Cyber Security Challenge
The 2024 Space Force Cyber Security Challenge is a series of challenges and puzzles designed to challenge the skills of participants in cyber security. The 2024 Space Force Cyber Security Challenge is a series of challenges, puzzles, and quizzes designed to challenge the skills of participants in cyber security.

2024 Space Force Cyber Security Challenge
The 2024 Space Force Cyber Security Challenge is a series of challenges and puzzles designed to challenge the skills of participants in cyber security. The 2024 Space Force Cyber Security Challenge is a series of challenges, puzzles, and quizzes designed to challenge the skills of participants in cyber security.

*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*

