



SPACE CYBERSECURITY WEEKLY WATCH

Weeks 51 & 52

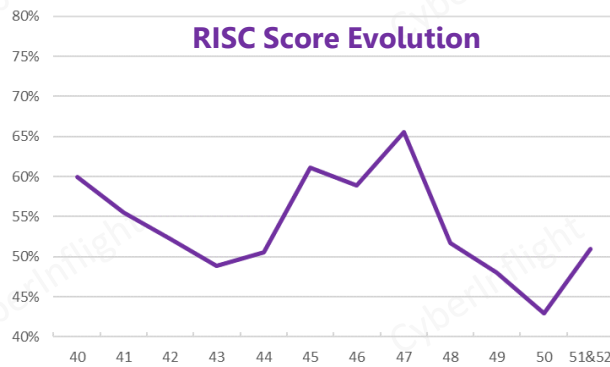
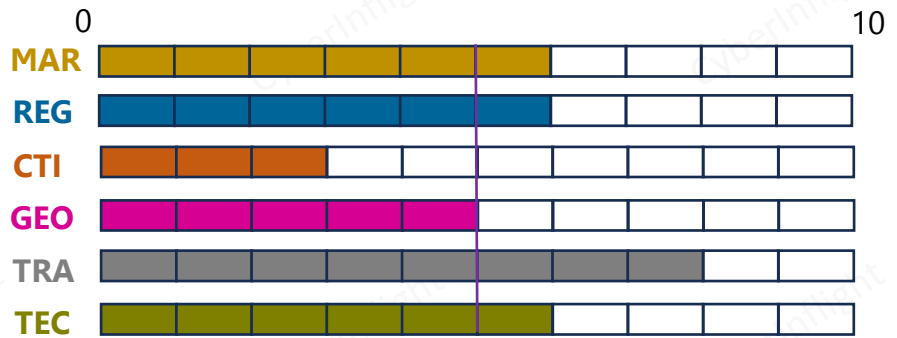
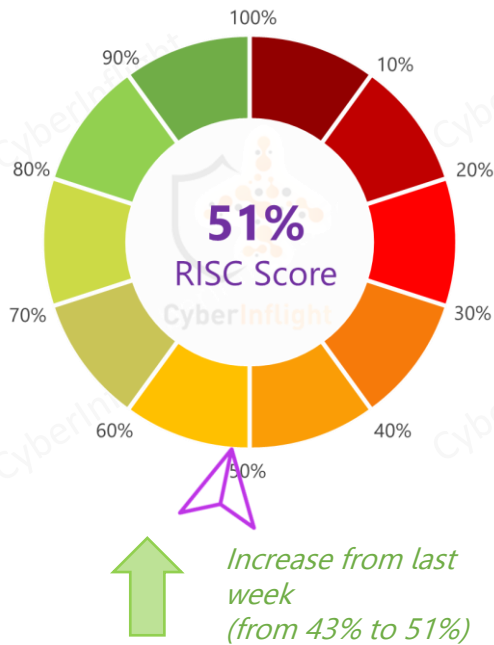
December 12 – December 31, 2023

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

Timeframe : Weekly
of articles identified : 42
Est. time to read : 1h45 min

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

Overview & RISC Score



There was a peak on W47, with a RISC Score of 66%, the highest of the year. The lowest of the year was W50, with a RISC Score of 43%

The RISC Score for this watch is 51%. During this end-of-year period, NASA released its Cybersecurity Guide for Space Industry. On the market front, CYSEC won the ESA PUSH contract to accelerate the adoption of cybersecurity in the space industry. This watch features more threat intel news than average. Among others, the Israeli space agency was attacked on December 25, 2023 by the KETAPANG GREY HAT TEAM. A summary of BlackBerry Research & Intelligence Team research on threat actor AeroBlade was also published. Also during this period, the USSF announced a new component dedicated to SPACECOM. On the technology front, scientists in Russia and China have established quantum communication encrypted with the help of secure keys transmitted by China's quantum satellite. Finally, the ESA Academy has opened registration for its 2024 edition of the Cybersecurity Training Course, which will take place in April.

MARKET & COMPETITION

Star Aerospace Partners with Oneida for Network Expansion

Star Aerospace Industries (SAI), an aerospace and aviation services company headquartered in England, is partnering with Oneida Space Networks to bring highly reliable and secure connectivity services to the commercial, military and general aviation sectors in Thailand and beyond. #SAI #OneidaSpaceNetworks

[Link: https://www.aerospaceintelligencemag.com/star-aerospace-partners-with-oneida-space-networks-20231212/](#)



TrendMicro Partners with SpiderOak to Elevate Security for its CNSS Infrastructure

TrendMicro, an aerospace company dedicated to developing and providing next-generation CNSS products and services, recently announced its strategic partnership with SpiderOak, a leading company in space cybersecurity software. The collaboration aims to elevate TrendMicro's CNSS infrastructure to unprecedented levels of security through SpiderOak's distributed data storage and backup software. #SpiderOak #TrendMicro

[Link: https://www.aerospaceintelligencemag.com/trendmicro-partners-with-spideroak-to-elevate-security-for-cnss-infrastructure-20231212/](#)



Secure and compliant cloud infrastructure in 12 weeks - ESA7

With ESA7's global operations, complex technology, and critical data, it was crucial for the company to ensure security and compliance in their transition to the cloud. Therefore, they were recommended to use OneCloud as their migration partner by Microsoft. #ESA7 #OneCloud

[Link: https://www.aerospaceintelligencemag.com/secure-and-compliant-cloud-infrastructure-in-12-weeks-20231212/](#)



Results of the first CNSS Orbital Systems Cybersecurity Challenge

The pitch day was held on December 14 in Paris, and following the presentations and deliberations of a mixed international CNSS jury, several of the most innovative projects were awarded contracts with CNSS to develop their system. #CNSS #Cybersecurity

[Link: https://www.aerospaceintelligencemag.com/cysec-announces-pitch-day-results-20231212/](#)
[https://www.aerospaceintelligencemag.com/cysec-announces-pitch-day-results-20231212/](#)



Result of the ESA PUSH contract won by CYSEC to accelerate the adoption of cybersecurity in the space industry

PUSH enables companies to offer their innovative space-related products and services to other European companies within the NewSpace ecosystem. ESA Commercialisation Gateway provides funding to facilitate the adoption of these services to future customers. #PUSH #CYSEC

[Link: https://www.linkedin.com/posts/cysecsystems_cybersecurity-space-activity-7142801927536332801-uhhP?utm_source=share&utm_medium=member_desktop](https://www.linkedin.com/posts/cysecsystems_cybersecurity-space-activity-7142801927536332801-uhhP?utm_source=share&utm_medium=member_desktop)



U.S. Military Chooses Kratos for \$179 Million SATCOM Contract

Kratos Defense & Security Solutions has secured an 8-year, \$179 million contract extension from the U.S. Space Force's Space Systems Command to continue supporting ground systems for key U.S. military communications satellites. #Kratos #SATCOM

[Link: https://www.aerospaceintelligencemag.com/kratos-secures-contract-extension-from-us-space-force-20231212/](#)



SpaceSigns Deal to Deliver a Plasma Brake to Spitznagel's Quantum Key Distribution Satellite

SpaceSigns Technologies, a leading French space propulsion systems company, together with Spitznagel, a leading quantum communications technology company, announced the signing of a deal to deliver a Plasma Brake to Spitznagel's test satellite. #SpaceSigns #Spitznagel #QKD

[Link: https://www.aerospaceintelligencemag.com/spacesigns-deal-to-deliver-a-plasma-brake-to-quantum-key-distribution-satellite-20231212/](#)

REGULATION



NASA launches cybersecurity guide for space industry

NASA has published its first Space Security Best Practices Guide, a 57-page document the agency said would help enhance cybersecurity for future space missions. #NASA #Cybersecurityguide

[Link: https://swehb.nasa.gov/display/SWEHBVD/7.22+-+Space+Security%3A+Best+Practices+Guide](https://swehb.nasa.gov/display/SWEHBVD/7.22+-+Space+Security%3A+Best+Practices+Guide)



THREAT INTELLIGENCE



Briefing 16: Analyzing Tactics, Techniques and Procedures Used by Cyber Threat Actors to Access US Space Industry

This article proposes a resume of BlackBerry Research & Intelligence Team research. The team revealed that they had been tracking a long-term cyber campaign targeting the U.S. aerospace sector. The threat actor, tracked as AeroBlade, conducted multiple spearphishing campaigns targeting the same aerospace organization from September 2022 – July 2023.



#USSpaceIndustry #Cyberattack

Link: <https://www.kratosdefense.com/constellations/articles/analyzing-tactics-techniques-and-procedures-used-by-cyber-threat-actors-to-access-us-space-industry>

South Korea's spy satellite vulnerable to North's jamming, cyberattacks

This article proposes a resume of South Korea's capabilities that can affect the operations of South Korea's satellite. The North has tested their efficacy several times, disrupting communications and suspending air and sea traffic in the South.



Link: <https://www.koreatimes.co.kr/www/north/2023/11/131n001.html>

China to lock down GPS data for security concerns

China has recently taken a stringent approach towards applications utilizing Global Positioning System (GPS) across. Concerned about the potential leakage of sensitive information to foreign entities, the Chinese government proposes the lock-down for activities such as precision tracking, surveillance and location-based marketing from Huawei GPS.



Link: <https://www.southchinesea.com/news/2023/11/131n001.html>

ANONYMOUS HACKER targets the website of European Space Agency

The post states that the website of the European Space Agency (ESA) has been targeted by a group called ANONYMOUS HACKER. The proof of ownership for the website is provided through a link. The post was published on Telegram and belongs to the category of a DDoS attack. The victims of this attack are the European Space Agency, specifically the website earth.esa.int.



Link: https://www.esa.int/About_Us

ISAC reports rise in jamming aircraft navigation systems

ISAC has reported a spike of "jamming or jamming" the Global Navigation Satellite System (GNSS) on aircraft in the past few years, according to ISAC.

Link: <https://www.isac.gov.au/news/2023/11/131n001.html>

Inside the Growing Threat of GPS Spoofing

A GNSS Global Navigation Satellite System (GNSS) specialist explains recent consumer cases related to spoofing attacks and why they are a significant threat for automation.

Link: https://www.esa.int/About_Us

The Alarming Surge of GNSS Jamming That's Threatening Flight Safety

GNSS jamming and spoofing is becoming a major threat to flight safety, especially now that we're fully transitioning to Performance Based Navigation (PBN) procedures across the globe. ICAO reported a 200% increase in GNSS interference incidents in 2022, and almost 40% of European air traffic operates through regions that are regularly affected by GNSS jamming and spoofing.

Link: https://www.esa.int/About_Us

Data loss prevention isn't rocket science, but NASA hasn't made it work in Microsoft 365

NASA's Office of Inspector General has run its eye over the aerospace agency's privacy regime and found plenty to like – but improvements are needed. In an audit published on December 19th, the OIG found NASA lacks the data to track and monitor its tools and gave recommendations.



Link: <https://www.irs.gov/audit/2023/11/131n001.html>

Satellite on Earth? or Both: RSCC's Alexey Volin speaks about diversity in TV broadcasting at the Telefamily Day conference

According to Alexey Volin, since the beginning of 2021, Director General of Russian Satellite Communications Company RSCC, has reported about 20 thousand attempts to interrupt TV broadcasting on Russian spacecraft. It seems to prevent interference every day.



Link: <https://www.rscclife.com/en/news/2023/11/131n001.html>

THREAT INTELLIGENCE

THE ANONYMOUS 88 targets News website blog

The ANONYMOUS 88 has targeted the news website blog. The post provides a link as proof of the downtime caused by the attack. The attack is categorized as a DDoS distributed denial of service attack. The victims of this attack include the United States, NATO as an organization, and the website blog name: **NEWS 88888**

Link: [https://www.88888news.com/2023/12/25/anonymous-88-targets-news-website-blog/](#)



THE ANONYMOUS 88 targets the website of News blogs

The ANONYMOUS 88 targets the website of News blogs. The post states that a group called the ANONYMOUS 88 has successfully taken down the website of NEWS on December 24, 2023. **NEWS 88888**

Link: [https://www.88888news.com/2023/12/24/anonymous-88-targets-the-website-of-news-blogs/](#)



★ KETAPANG GREY HAT TEAM targets Israel Space Agency website

KETAPANG GREY HAT TEAM, a threat actor, has targeted the website of the Israel Space Agency. The proof of downtime is provided through a link to a website that shows the reported downtime of the targeted website. The post was published on December 25, 2023, on the Telegram network by the KETAPANG GREY HAT TEAM. The category of the attack is a DDoS attack, and the victims include the Israel Space Agency, with their website space.gov.il/en being targeted.

#IsraelSpaceAgency #DDoS

Link: <https://t.me/KetapangGreyHatTeamV2/920>



Russia's electronic warfare tactics are helping it turn the tide against Ukraine

A report of the electronic warfare tactics being used by the Russian forces provides insight into the tactical protection to Russian forces against drone attacks. **ElectronicWarfare 88888**

Link: [https://www.88888news.com/2023/12/25/russias-electronic-warfare-tactics-are-helping-it-turn-the-tide-against-ukraine/](#)



GEOPOLITIC

Here are the Army's new planned EW, signals programs

Speaking with reporters on Tuesday, Brig. Gen. Ed Barker, program manager for intelligence EW and signals, provided some updates on already established EW programs and new plans planned for fiscal 2025 and beyond. **ElectronicWarfare 88888**

Link: [https://www.88888news.com/2023/12/25/here-are-the-armys-new-planned-ew-signals-programs/](#)



★ USSF Creates New Component for SPACECOM

The name—U.S. Space Forces – Space—may seem a little redundant, but the newest Space Force component will have an outsized role in how the Space Force coordinates with U.S. Space Command. Chief of Space Operations Gen. B. Chance Saltzman revealed the new command Dec. 12 at a conference in Orlando. **#USSF #SPACECOM**

Link: <https://www.airandspaceforces.com/space-force-new-component-spacecom/>



The Space Force's 2024 Resolutions: Forget The 90s—Buy Into The 2020s

This article presents the resolutions for the development of space capabilities for the remainder of the 2020s. **Space Warfare 88888**

Link: [https://www.88888news.com/2023/12/25/the-space-force-2024-resolutions-forget-the-90s-buy-into-the-2020s/](#)



Bridging The Gaps: Protecting The Satellite Constellations In The Era Of Cyber Threats

This article gives a general overview of the risks of cyber threats facing satellite constellations.

ElectronicWarfare 88888

Link: [https://www.88888news.com/2023/12/25/bridging-the-gaps-protecting-satellite-constellations-in-the-era-of-cyber-threats/](#)

TRAINING & EDUCATION

Warning: We Have a Problem: Analyzing the Security of Low Earth Orbit Satellites with Johannes Willbold

In the Chair on the front to back that USA, India, Japan and France's... Johannes Willbold's focus on the security of low Earth orbit (LEO) satellites, Johannes shares his research on satellite vulnerabilities and the challenges in securing satellite systems. They discuss security by obscurity and the lack of standardized protocols in satellite technology.

Warning: We Have a Problem

[Link: https://www.cyberinflight.com/2023/12/12/warning-we-have-a-problem-analyzing-the-security-of-low-earth-orbit-satellites-with-johannes-willbold/](#)



Workshop: A CTF Challenge in Space | Hack a Sat 4 and the State of Space Cybersecurity

In the spirit of building cybersecurity skills, Space Hackers, Logix Hackers, SpaceHackers, and SpaceHackers discuss the history and evolution of the Hack a Sat program, which aims to bridge the gap between the cybersecurity and aerospace communities and increase the capabilities of extreme programming and hacking to secure space systems. The Workshop CTF challenge is the part of the program, which involves real-world attacks on space systems, and the goals draw insights on the different disciplines involved in securing space systems.

Workshop: A CTF Challenge in Space

[Link: https://www.cyberinflight.com/2023/12/12/workshop-a-ctf-challenge-in-space-hack-a-sat-4-and-the-state-of-space-cybersecurity/](#)



Spaceflight Mechanics: The Cornell Space Technology Podcast

Gregory, Assistant Professor at Cornell University, talks with Peter about security in space, testing, cyber crime, and testing space... **Spaceflight Mechanics Podcast**

Spaceflight Mechanics Podcast

[Link: https://www.cornell.edu/2023/12/12/space-technology-podcast/](#)



Cyber security in space and cyber key takeaways from CSOC Live

held at Manchester's Global Summit, the Chartered Institute of Information Security's conference attracted 2000 top minds in cybersecurity, business leaders and people from government circles. The event generated discussions on the challenges and opportunities within the cybersecurity sector ranging from the complexities of regulating online social media platforms to the challenges of cybersecurity in the space industry.

Cyber security in space and cyber key takeaways from CSOC Live

[Link: https://www.cyberinflight.com/2023/12/12/cyber-security-in-space-and-cyber-key-takeaways-from-csoc-live/](#)



Electronic Jamming of the System of Subscriber Terminals of the Starlink Satellite Communication System

This research paper has been published by several Russian universities. It proposes a technique in order to jam the Starlink network in Ukraine.

Electronic Jamming

[Link: https://www.researchgate.net/publication/368275786/figure/fig/1/figure-fig1/368275786-20231212-20231212/](#)

OSPC Senior Advisor Ronald Egan delivered his keynote

OSPC Senior Advisor Ronald Egan delivered his keynote speech at the Embassy of Italy in D.C. at Global Space Summit on the importance of cybersecurity principles in the space domain to our international partners and allies.

OSPC Senior Advisor Ronald Egan

[Link: https://www.ospc.gov/2023/12/12/ospc-senior-advisor-ronald-egan-delivered-his-keynote/](#)

ESA WTA Workshop on Positioning, Navigation, and Timing (PNT) Resilience

This interactive event aims to provide drivers, manufacturers, system suppliers and navigation service providers and institutions to build the necessary skills to Positioning, Navigation, and Timing (PNT) services.

ESA WTA Resilience

[Link: https://www.esa.int/ESA_Media/Workshops_and_Seminars/Workshop_on_Positioning_Navigation_and_Timing_PNT_Resilience](#)

Apply now for the 2024 edition of ESA Academy's Cybersecurity Training Course

ESA Academy is looking for 30 highly motivated Bachelor and Master students to attend the Cybersecurity Training Course 2024. The training course is going to be held from 8 to 12 April 2024 at the ESA Education Training and Learning Facility in ESEC-Galaxia, Belgium.

#EASAcademy #ESEC-Galaxia

Link:

https://www.esa.int/Education/ESA_Academy/Apply_now_for_the_2024_edition_of_ESA_Academy_s_Cybersecurity_Training_Course



Anti-Jamming Technology

Article about some key aspects of anti-jamming technology.

[Link: https://www.cyberinflight.com/2023/12/12/anti-jamming-technology-research-paper/](#)

Cybersecurity in Space: A 2024 Perspective

As we move towards 2024, the focus on cybersecurity in space is becoming increasingly crucial. With the growing importance of space assets to the global economy and national security, space operations must adopt robust cybersecurity measures and remain vigilant against potential cyber threats.

[Link: https://www.cyberinflight.com/2023/12/12/cybersecurity-in-space-a-2024-perspective/](#)



TECHNOLOGY

Space Development Agency looking into alternatives for GPS

The Space Development Agency is working with the Army to provide alternative positioning, navigation and timing (PNT) capabilities that are not dependent on GPS through its Pathfinder Warfighter Space Architecture. **SDA Director David Loomis said: #SpaceDevelopmentAgency #GPS**

Link: <https://www.space.com/space-operations/2023/12/space-development-agency-looking-into-alternatives-to-gps/>



Adrian Space Partners with Kepler Space and Skybeam to Operationalize the World's 1st Orbital Data Center

The Houston-based company Adrian Space has entered agreements with Kepler Communications LLC Inc. and Skybeam Global Corp. to integrate and demonstrate high data rate Optical Interconnect (OI) links on the first module of Adrian Space's commercial space station. Adrian Space is parallel, the Adrian Space team is building the world's first scalable, cloud technology enabled, commercial orbital data center to be hosted on Adrian Station.

#AdrianSpacePartnersKeplerSpace

Link: <https://www.adrian.space/news/orbital-data-center/>

Successful Space Demonstration of QNNC PQC Module with Squaredot

Squaredot and Squaredot Technologies have successfully demonstrated a light-weight prototype of Post-Quantum Cryptography (PQC) key exchange between a nano-satellite, Squaredot, and a Singapore Ground Station using key generated by an on-board quantum random number generator (QNNC) output. **#PQC #Space #Squaredot**

Link: <https://www.squaredot.com/news/space-demonstration-of-qnnc-pqc-module-with-squaredot/>

Introducing NNNLink Security: elevating communication with enhanced security

On December 20th, NNNLink 1 announced the release communication subsystem NNNLink 1, NNNLink 2, as its name suggests, is based on the star topology and light protocol NNNLink architecture, but further extended with an unmatched communication security feature using PQC for cryptography. **#N3Link #NNNLink Security**

Link: <https://www.adrian.com/introducing-annlink-security-elevating-communication-with-enhanced-security/>

Benefits of modernized GNSS signals for timing applications in communications networks

This article gives an overview of the benefits of modern GNSS signals for modern terrestrial applications.

#GNSS #Timing #Applications

Link: <https://www.adrian.com/news/2023/12/benefits-of-modernized-gnss-signals-for-timing-applications-in-communications-networks/>

GPS anti-jamming system to be installed on South Korean helicopters

South Aerospace Industries (SAI) has signed a contract with Korea Aerospace Industries (KAI) to provide its GPS anti-jamming systems for the light armed helicopter (LAH) and Phase Production, the company announced in a statement.

#Korea #AntiJamming

Link: <https://www.adrian.com/news/2023/12/gps-anti-jamming-system-to-be-installed-on-south-korean-helicopters/>



China and Russia test 'hack-proof' quantum communication link for Brics countries

Scientists in Russia and China have established quantum communication encrypted with the help of secure keys transmitted by China's quantum satellite, showing that a BRICS quantum communication network may be technically feasible. **#Quantum #Encryption**

Link: <https://www.scmp.com/news/china/science/article/3246752/china-and-russia-test-hack-proof-quantum-communication-link-brics-countries?module=inline&pgtype=article>



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