SPACE CYBERSECURITY WEEKLY WATCH

Week 1

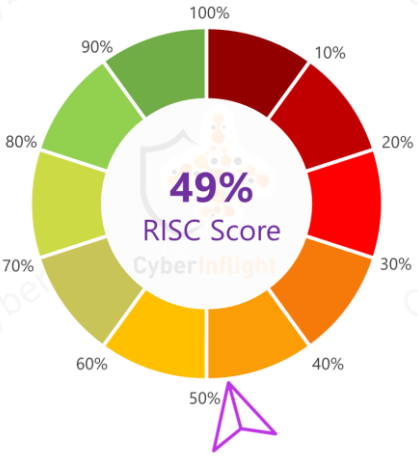
January 1 – 8, 2024

Timeframe : Weekly
# of articles identified : 22
Est. time to read : 30 min

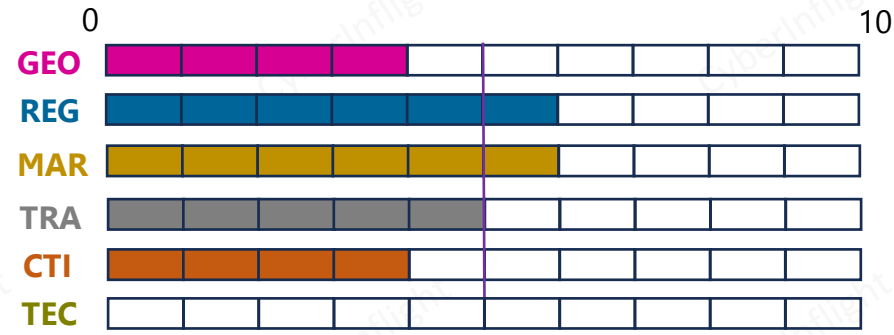
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

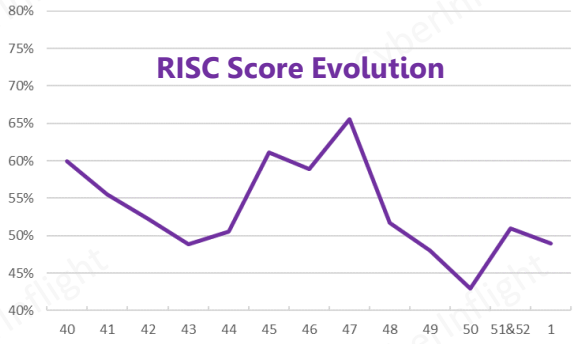
- GEOPOLITIC
- REGULATION
- MARKET & COMPETITION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- IMPORTANT NEWS

Overview & RISC Score



Decrease from last week (from 51% to 49%)





There was a peak on W47, with a RISC Score of 66%, the highest of the year. The lowest of 2023 was W50, with a RISC Score of 43%.

This week's RISC Score is 49%. To mark the new year, NASA has published its "Space Security Best Practices Guide" to bolster mission cybersecurity efforts for the public sector and private sector space activities. This plan has been in preparation for several months and provides guidance specific to missions, programs, and projects not already covered in the existing NPRs (NASA Procedural Requirements) and Standards. An American report published by the Air Force China Aerospace Studies Institute on PLA (People's Liberation Army) Counterspace Command and Control reveals that China's plans for space warfare include cyberattacks and electronic jamming to disrupt and disable U.S. satellite systems. The Airbus acquisition of the cyber IT division of the Atos group has been restarted after a setback in 2023. The deal would be worth around 1.8 billion euros. The Lulz Security Indonesia group, has claimed to have gained access to the WRESAT satellite of Australia. The WRESAT, which stands for Weapons Research Establishment Satellite, was Australia's first satellite. Finally, an interesting podcast episode was released this week, on cybersecurity in outer space.

GEOPOLITIC

Space Force wargames potential satellite refueling plans

As new technologies pave the way for refueling satellites in space, the U.S. Space Force is exploring how to integrate these capabilities into its operations. A tabletop exercise dubbed "Paradise Rising 2.0" shed light on the strategic and logistical considerations involved in this emerging field. **#USSF #Wargames**

Link: https://spacenews.com/space-force-wargames-potential-satellite-refueling-plans/

China's space warfare plan advances killer missiles capable of disabling U.S. satellites

China's plans for space warfare include cyberattacks and electronic jamming to disrupt and disable U.S. satellite systems and, in the future, small robot satellites to grab or crush U.S. military space sensors, according to a senior U.S. intelligence official report. **#Warfare #China**

Link: https://www.washingtontimes.com/news/2024/jan/4/china-space-warfare-includes-cyberattacks-jamming-/

Space security in the Americas can no longer go overlooked

As the space security conversation advances, one region that continues to be largely overlooked is Latin America and the Caribbean (LAC). However, space security should matter to the countries of the region — even to those for whom space is not a recognized priority today — and the United States should realize that with space security gaps mounting, there are important benefits to bringing the conversation closer to home. **#LAC #Resilience**

Link: https://spacenews.com/space-security-americas-no-longer-overlooked/

REGULATION

NASA releases Space Security Best Practices Guide for mission cybersecurity in interconnected space

The U.S. National Aeronautics and Space Administration (NASA) released the first iteration of its Space Security Best Practices Guide to bolster mission cybersecurity efforts for the public sector and private sector space activities, as space missions and technologies grow increasingly interconnected. **#NASA #BestPractice**

Link: https://industrialcyber.co/threats-attacks/nasa-releases-space-security-best-practices-guide-for-mission-cybersecurity-in-interconnected-space/

More Than Just LEO: A Framework for SPD-8 and Space Critical Infrastructure

The argument, thus far, has been stuck on a simple yes or no question: do we designate space as the 17th terrestrial critical infrastructure sector or not? The debate centers on the argument that space assets are so important to terrestrial activities that they should receive such a designation. The space critical infrastructure model must be built around the realities of the environment it governs. As an example, air is not considered critical infrastructure on Earth, but it would be in space. **#CriticalInfrastructure #Framework**

Link: https://spacenews.com/more-than-just-leo-a-framework-for-spd-8-and-space-critical-infrastructure/

Cyber Incident Reporting for Critical Infrastructure – Considerations for the Space Industry

On March 15, 2022, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) into law. Space is not enumerated as a critical infrastructure sector that will be covered by the proposed rules; however, some satellite operators may be required to report cyber incidents because they are integral to critical infrastructure operations, most obviously in sectors such as communications and financial services. **#CriticalInfrastructure #CISA**

Link: https://hfg.org/2024/01/cyber-incident-reporting-for-critical-infrastructure-considerations-for-the-space-industry/

MARKET & COMPETITION

Space economy, il 2024 sarà complesso: investimenti mutevoli e incertezza geopolitica *(Trad.: Space economy, 2024 complex year: changing investments and geopolitical uncertainty)*
What will be the scenario for the space economy in 2024? In this article, analysts at Quilty Space announce their predictions for the new year. **#QuiltySpace #MarketTrends**
Link: https://www.spaceconomy360.it/industria-spaziale/space-economy-il-2024-sara-complesso-investimenti-mutevoli-e-incertezza-geopolitica/

US Air Force Contracts Viasat for Five Year Satellite Tech Overhaul
The contract, named LCMC BA-EXQ by the Pentagon, has a five-year term with a ceiling value of $900 million and requires Viasat to prototype and test systems, hardware, software, and cybersecurity capabilities utilizing satellite services from its Ka-band, S-band, and L-band networks. **#USAirForce #Viasat**
Link: https://www.satellitetoday.com/government-military/2024/01/05/us-air-force-contracts-viasat-for-five-year-satellite-tech-overhaul/

★ **Cybersecurity, Airbus punta sulle attività di Atos: sul piatto fino a 1,8 miliardi *(Cybersecurity, Airbus bets on Atos assets: up to 1.8 billion in the pot)***
Airbus, the European aviation and aerospace giant, aims to buy the cybersecurity unit of the heavily indebted French IT group Atos. The deal is worth between 1.5 billion and 1.8 billion euros. **#Airbus #Atos**
Link: https://www.spaceconomy360.it/difesa-cybersecurity/cybersecurity-airbus-punta-sulle-attivita-di-atos-sul-piatto-fino-a-18-miliardi/

New proposed rule for CMMC 2.0 lays out security requirements, raises some eyebrows
The Defense Department recently released a new proposed rule for its Cybersecurity Maturity Model Certification program, laying out specific security requirements for defense contractors and subcontractors — and resurfacing questions about the balance between bottom-line security and regulatory burden. **#CMMC2.0 #CalltoInterest**
Link: https://breakingdefense.com/2024/01/new-proposed-rule-for-cmmc-2-0-lays-out-security-requirements-raises-some-eyebrows/

Wiseband Partners with Rivada for Network Expansion in the Middle East
Rivada Space Networks, in partnering with Wiseband, an Emirati satellite services company, to bring secure connectivity solutions to the Middle East region. **#Rivada #Wiseband**
Link: https://www.prnewswire.com/news-releases/wiseband-partners-with-rivada-for-network-expansion-in-the-middle-east-302027904.html

TRAINING & EDUCATION

SPACE INTERNET OF THINGS (IOT) AND CYBERSECURITY WISESAT AND SEALSQ "EXPLORING THE FINAL FRONTIER: SECURITY IN THE SPACE IOT ERA"
Webinar by WiSeSat about how the advent of the Space Internet of Things (IoT) opens a new chapter in connectivity and technology, bringing together the vast potential of space exploration with the practicality of IoT. **#Webinar #WiSeSat**
Link: https://www.wisesat.com/news/2024/space-internet-of-things/

★ **Space Invaders: Navigating Cybersecurity in Outer Space**
A podcast episode about cybersecurity in outer space. With increasing satellites orbiting the Earth, space has become a new frontier for cyber attacks. **#Podcast #Satellite**
Link: https://www.ivoox.com/space-invaders-navigating-cybersecurity-in-outer-space-audios-mp3_rf_122108054_1.html

'China developing tools to control foreign satellites': Kenny Huang
Interview of Kenny Huang, CEO of the Taiwan Network Information Center. **#Interview #Taiwan**
Link: https://www.freenet.tv/freenetchina/2024/01/06/taiwan-network-information-centre-ceo-kenny-huang-interview.html

IRIS2 Industry Information Day Presentation
Presentation from the IRIS2 Industry Information Day presenting the different aspects of IRIS2, from regulations to contracts and tender specifications. **#IRIS2 #Presentation**
Link: https://defence-industry-space.ec.europa.eu/system/files/2021-12/IRIS2%20Industry%20Information%20Day%20-%20IRIS2%20Main%20Slides2.pdf

THREAT INTELLIGENCE

Estonia also affected by end-of-year GPS systems jamming

GPS systems across the Baltic Sea region, including Estonia, reported disturbances at the end of last year, monitoring websites show. Russia is to blame, the Consumer Protection and Technical Regulatory Authority (TTJA) said. **#Jamming #Russia**

Link: https://news.err.ee/1609219/01/estonia-also-affected-by-end-of-year-gps-systems-jamming

A new security level against GNSS spoofing

Galileo, Europe's Global Navigation Satellite System, has developed a safety function to strengthen resilience against spoofing attacks. The so-called OSNMA (Open Service Navigation Message Authentication) is a GNSS-embedded anti-spoofing feature that should become attractive for high-end and mass market GNSS receivers. **#Spoofing #Resilience**

Link: https://www.u-blox.com/en/blogs/tech/galileo-spoofing-new-security-level

Lulz Security Indonesia targets access to the WRESAT satellite

Lulz Security Indonesia, a threat actor, has claimed to have gained access to the WRESAT satellite of Australia. The WRESAT, which stands for Weapons Research Establishment Satellite, was Australia's first satellite. The post was published on December 30, 2023, on the Telegram network by Lulz Security Indonesia. The threat actor's claim raises concerns about potential unauthorized access to the satellite. The post does not provide information about any specific victims, organizations, websites, or industries affected by this incident. **#Attack #WRESAT**

Link: https://t.me/lulzsecurityagency/943?single

Five steps to secure the Low Earth Orbit satellite environment

Cybersecurity industry experts have long called for prioritizing satellite communication (SATCOM) security, pointing out vulnerabilities such as those Russia was able to exploit. An analysis published in mid-2023 by German researchers reported the discovery of software vulnerabilities in three satellite systems they studied, including a defect in a code library that they believe is used by multiple other satellite systems. **#Cybersecurity #Satellite**

Link: https://www.c4isrnet.com/opinion/2024/01/04/five-steps-to-secure-the-low-earth-orbit-satellite-environment/

Air Travel Is Not Ready for Electronic Warfare With militaries spoofing GPS signals, civilian planes could get targeted in the crossfire.

Cybersecurity experts warn that it may be possible to maliciously tamper with a plane's navigation system and lead it off course without the flight crew even being aware. Although GPS vulnerabilities have gotten the most attention in recent years, numerous systems aboard modern aircraft are potentially vulnerable to electronic attack. **#Spoofing #EW**

Link: https://spinup.com/blog/agencies/2024/01/air-travel-is-not-ready-for-electronic-warfare.html

Russia Might Be Jamming GPS Signals, Anonymous Researcher Claims

According to the researcher, GPS signals significantly deteriorate over NATO countries near the southern Baltic Sea, and the source of the deterioration appears to be Kaliningrad. **#Jamming #Russia**

Link: https://www.kyivpost.com/post/25328

Exclusive: Russian hackers were inside Ukraine telecoms giant for months

Russian hackers were inside Ukrainian telecoms giant Kyivstar's system from at least May last year in a cyberattack that should serve as a "big warning" to the West, Ukraine's cyber spy chief told Reuters. **#Russia #Ukraine**

Link: https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-06/