



SPACE CYBERSECURITY WEEKLY WATCH

Week 4

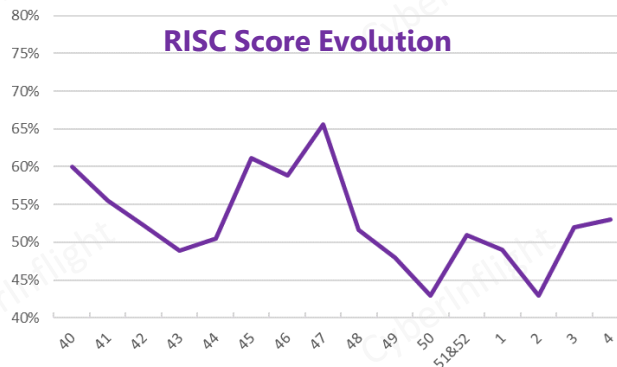
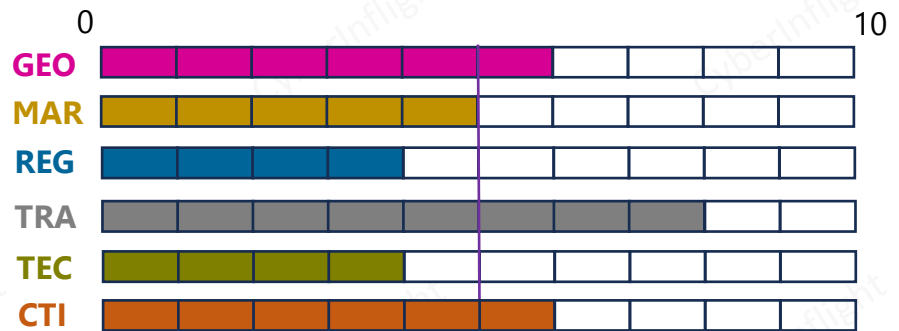
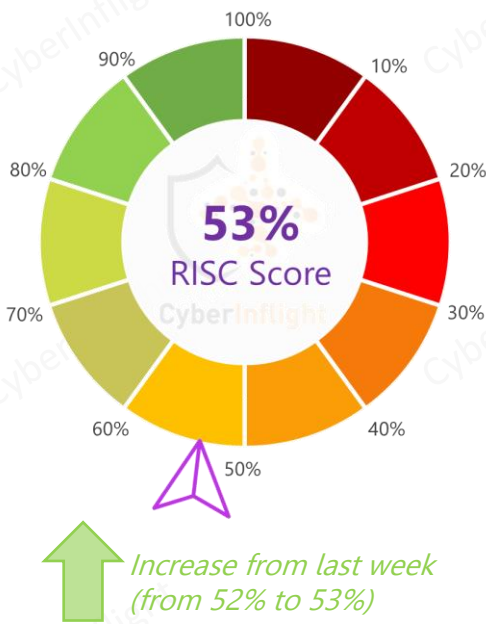
January 23 – 29, 2024

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 : 26
Est. time to read : 40 minutes

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

Overview & RISC Score



After a period of decline since the start of 2024, W3 & W4 show an increase.

This week's RISC Score is 53%. This week, South Korea announced a significant uptick in attempts of cyberattacks by foreign sources, mainly accusing China and North Korea. Also, Ukraine's military intelligence agency (HUR) announced that "Volunteer patriot" hackers of the BO Team launched a cyberattack against the Russian Far Eastern Research Center of Space Hydrometeorology "Planeta," destroying its database and expensive equipment. On the market front, a partnership between EUSPA and Qualinx to develop a consumer-grade, low-power GNSS receiver for the agency's GNSS authentication service. On the technology front, EUSPA and the European Commission have published an updated version of the Galileo OSNMA Internet Data Distribution (IDD) Interface Control Document (ICD) and the Certificate Practice and Certificate Practice Standards (CS/CPS). Last but not least, ESA announced the Space Systems Security challenge as part of its 3S conference, to be held on May 27-28, 2024.



GEPOLITIC



Seoul's spy agency accuses China of major cyber attacks

South Korean spy agency on Wednesday reported a significant uptick in attempts of cyber attacks by foreign sources last year, waged mainly by North Korea and China. Chinese attacks tended to inflict more severe damage than North Korean ones, despite the latter being more frequent. **#SouthKorea #China**

Link: <https://m.koreaherald.com/view.php?ud=20240124000731>



Infrastructure specialist warns attacks, Berlin: "Some strategic common" (Fréd. Space infrastructure under attack, Berlin: "Need common strategy")

With the growing presence of satellite operators and manufacturers of assets in orbit, companies and technologies are being targeted by espionage. The European High Representative for Foreign Affairs and Security Policy calls for more.

Link: <https://www.euractiv.com/en/space/infrastructure-specialist-warns-attacks-berlin-some-strategic-common-need-common-strategy/>



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

According to a detailed report by the deputy national intelligence officer for space at the National Intelligence Council, China's strategy includes sophisticated capabilities, electronic jamming, and potentially employing small robot satellites designed to target U.S. military space assets.

Link: <https://www.intel.com/resources/documents/2024/01/23/chinas-space-warfare-plan-advances-killer-missiles>



MARKET & COMPETITION

Europe sets up space finance initiative

The European Commission is joining forces with the European Space Agency and European investment arm to help more space companies get financing, including from a largely untapped multi-billion dollar fund for strategic investments.

Link: <https://www.euractiv.com/en/space/europe-sets-up-space-finance-initiative/>



Sweden Brings Satellite Monitoring Capabilities to Greece

Sweden is to help set up a new satellite monitoring system in Greece. The company part of the Alion Group will collaborate with the Hellenic Telecommunications and Post Commission (HTPC), and the National Regulatory Authority (NRA) on the project. The NRA, as the Independent Administrative Authority of Greece, seeks to better exercise its responsibilities on satellite spectrum issues, for the benefit of the business and research environment, as well as to cultivate innovation in the field of electronic communications based on satellite broadband networks.

Link: <https://www.satelliteinsights.com/press-releases/2024/01/23/sweden-brings-satellite-monitoring-capabilities-to-greece/>

Belgium Signs Artemis Accords

Belgium has signed the Artemis Accords outlining best practices for responsible behavior in space exploration, becoming the latest major European space power to join.

Link: <https://www.satelliteinsights.com/press-releases/2024/01/23/belgium-signs-artemis-accords/>



Qualinx Partners with EUSPA to Advance GNSS Development

Qualinx, is partnering with the European Union Agency for the Space Programme (EUSPA) under the Fundamental Elements EU R&D funding mechanism to develop a consumer-grade, low-power GNSS receiver for the agency's GNSS authentication service. **#EUSPA #Qualinx**

Link: <https://hardwarebee.com/electronic-breaking-news/qualinx-partners-with-euspa-to-advance-gnss-development/>



REGULATION

Belgium signs Artemis Accords

Belgium has signed the Artemis Accords outlining best practices for responsible behavior in space exploration, becoming the latest major European space power to join.

Link: <https://www.satelliteinsights.com/press-releases/2024/01/23/belgium-signs-artemis-accords/>





TRAINING & EDUCATION

CYSAT – Startup Corner

CyberInflight will be present at this year's CYSAT 2024, in the Startup Corner! There are still places available to join us!
#CYSAT #CyberInflight

Link: https://www.linkedin.com/posts/alexandravallant_cysat-cybersecurity-for-the-space-industry-activity-7153383815300677632-A_Qf?utm_source=share&utm_medium=member_desktop



Space Systems Security Challenge

ESA is happy to announce that in the context of 2024 Security for Space Systems (3S) conference, a hands-on security challenge is organised focusing on the security of space systems. This challenge stands out as the first of its kind to comprehensively cover all layers from RF communication to onboard data handling systems security in a space context.
#3SChallenge #ESA

Link: <https://atpi.eventsair.com/24a06---3s2024/space-systems-security-challenge>



The 2024 Outlook on Cybersecurity in Space: Challenges and Opportunities

Space cybersecurity is a rapidly growing area of interest for the cybersecurity community in space as the industry grows. With the expansion of space exploration and the increasing reliance on satellite technology, addressing cybersecurity challenges in this domain has never been more crucial. **#3SChallenge #ESA**

Link: https://www.esa.int/ESA/Space/Space_Security/Space_Security_in_Space_2024_Executive_Summary

Unlocking the potential of space entrepreneurship by embedding cyber resilience

As the global commercial space sector grows, it becomes increasingly clear that cybersecurity must be at the forefront of all entrepreneurial endeavours from the very beginning. The interconnectedness of space systems, satellites, and ground infrastructure makes vulnerability a multifaceted risk, and its impact. **#SpaceSecurity #ESA**

Link: https://www.esa.int/ESA/Space/Space_Security/Unlocking_the_potential_of_space_entrepreneurship_by_embedding_cyber_resilience

Commercial Space Assets

Space Assets (SA) of Lockheed Telecommunications Corp. is joined by North Star, CEO of OneWeb Technologies, Scott Schreiner, CEO of Intelsat, and Samuel Stone, Tech Fellow with the Aerospace Corporation and Chairman of the Space Act. **#SpaceSecurity #ESA**

Link: https://www.esa.int/ESA/Space/Space_Security/Commercial_Space_Assets

Aerospace Cyber Security

Aerospace cyber security is the process of protecting the information systems and data of the aerospace industry from cyber threats. It involves applying security measures to the design, development, operation, and maintenance of aerospace systems, such as aircraft, satellites, rockets, and ground stations. Aerospace cyber security is important because it ensures the safety, reliability, and resilience of the aerospace sector, which is vital for national security, economic growth, and scientific advancement. **#SpaceSecurity #ESA**

Link: https://www.esa.int/ESA/Space/Space_Security/Aerospace_Cyber_Security

ESA Partners with IATA to Counter Safety Threat from GNSS Spoofing & Jamming

The European Union Aviation Safety Agency (EASA) and the International Air Transport Association (IATA) announced the establishment of a working group today at IATA's headquarters to combat incidents of GNSS spoofing and jamming. The working group will conduct high-level discussions that will involve with satellite-based navigation that provide information on the proper operation of an aircraft. It poses significant challenges to aviation safety. Mitigating these risks requires a multi-faceted and long-term response, beginning with the sharing of incident information and expertise. **#SpaceSecurity #ESA**

Link: https://www.esa.int/ESA/Space/Space_Security/ESA_Partners_with_IATA_to_Counter_Safety_Threat_from_GNSS_Spoofing_and_Jamming



TECHNOLOGY



EUSPA and the European Commission have published an updated version of the Galileo Open Service Navigation Message Authentication OSNMA IDD ICD and the CS/CPS

The publication of an updated version of the Galileo OSNMA Internet Data Distribution (IDD) Interface Control Document (ICD) and the Certificate Practice and Certificate Practice Standards (CS/CPS), together with the OSNMA operational cryptographic material, will allow users and receiver manufacturers to finalize the implementation of the OSNMA protocol in advance of the OSNMA Initial Service provision phase. **#Galileo #OSNMA**

Link: <https://www.gsc-europa.eu/news/updated-documentation-and-cryptographic-material-in-preparation-for-the-galileo-osnma-initial>



Researchers at the Institute for Quantum Computing are leading Canada's first quantum satellite to protect tomorrow's data

The Quantum Cryptography and Secure Communications (QCS) mission will be a demonstration of secure ground-to-space quantum communication. It will be led by a team of researchers from the Institute for Quantum Computing (IQC), which is a member of the national network of quantum research centres. **#Quantum #Canada**

Link: <https://www.iqc.utoronto.ca/news/leading-the-charge-of-quantum-communication-satellite>





THREAT INTELLIGENCE



The top defense news stories of 2023 and what to expect in 2024

The US and other nations are bringing modernization for way they fight. From submarines to satellites to software, upgrading decades old assets to fight, and playing with bleeding edge artificial intelligence. Breaking Defense published an article covering all the major developments in the defense world. #US23 #Defense

Link: <https://breakingdefense.com/2023/12/28/the-top-defense-news-stories-of-2023-and-what-to-expect-in-2024/>

Military intelligence: Cyberattack on Russian scientific research center deals 'devastating' damage

"Volunteer patriot" hackers of the BO Team launched a cyberattack against the Russian Far Eastern Research Center of Space Hydrometeorology "Planeta," destroying its database and expensive equipment, Ukraine's military intelligence agency (HUR) said on Jan. 24. #Cyberattack #Russia

Link: <https://kyivindependent.com/military-intelligence-cyber-attack-on-russian-space-hydrometeorology-research-center-deals-devastating-consequences/>



'Secretive' Russian EW System Could Be Behind NATO GPS Jamming

Russia may be using a 'secretive' electronic warfare (EW) system in its eastern outpost of Kaliningrad as evidenced by reported GPS disruptions plaguing NATO members on the alliance's eastern flank. #Jamming #NATO

Link: <https://www.researchandanalytics.com/news/secretive-russian-ew-system-could-be-behind-nato-gps-jamming/>



Not a new case of GPS spoofing, jamming

New cases of jamming and spoofing appearing at the border of Russia and Poland. #Jamming #Spoofing

Link: <https://www.comsec.com/2023/12/28/new-cases-of-gps-spoofing-jamming/>

Alleged DDoS attack on NASA website

The Great Wall '1.11 Team (GWT)' published on its Telegram channel a recordation of a DDoS attack against the NASA website. #DDoS #NASA

Link: <https://www.111team.com/2023/12/28/ddos-attack-on-nasa-website/>



Satellites and the specter of IoT attacks

Along with threats from old school jamming and interference from terrestrial systems, IoT components make modern spacecraft vulnerable to a new attack vector — other satellites within the horizon and growing network.

#IoT #Satellite

Link: <https://www.comsec.com/2023/12/28/satellites-and-the-specter-of-iot-attacks/>

2023 - The year of GPS jamming and spoofing

They found a YouTube site with over 1000 videos of GPS jamming for 2022, 2023, and the date is 2024. It helped them realize how bad things have gotten. And especially the increase in activity during 2023. #Jamming #GPS

Link: <https://www.inflight.com/2023/12/28/2023-the-year-of-gps-jamming-and-spoofing/>

Russia's Attempts to Deny Ukraine's Access to Starlink Satellites

Russia has been actively trying to deny Ukraine's access to commercial satellites, particularly Starlink provided by Elon Musk's SpaceX. This effort is part of a broader electronic warfare campaign amid the ongoing conflict between the two nations. #Russia #Starlink

Link: <https://www.inflight.com/2023/12/28/russias-attempts-to-deny-ukraines-access-to-starlink-satellites/>



Part 1 - Ground Station Attacks

If a ground station is hacked, it could have serious implications. Here are some potential consequences.

#GroundStation #Attacks

Link: <https://www.inflight.com/2023/12/28/part-1-ground-station-attacks-if-a-ground-station-is-hacked/>

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