



SPACE CYBERSECURITY WEEKLY WATCH

Week 3

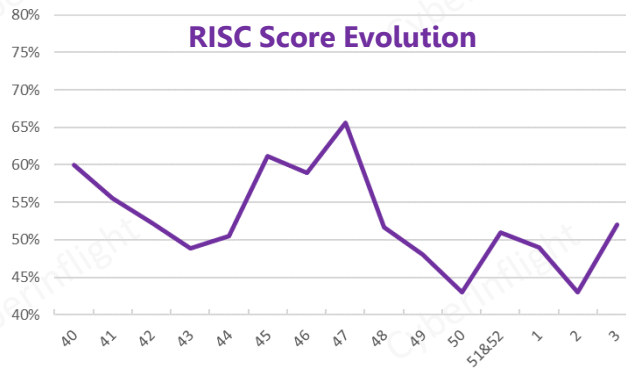
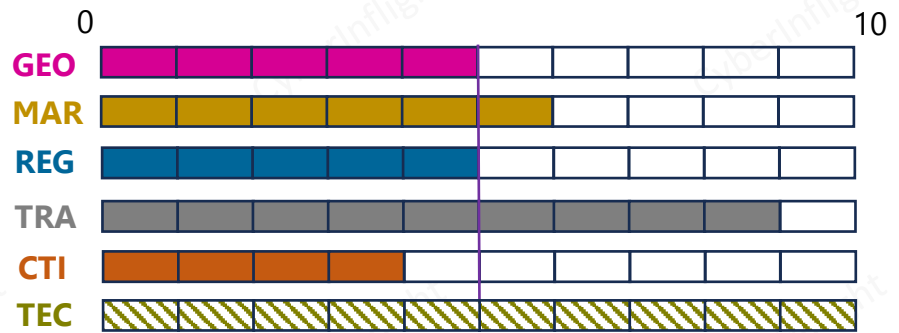
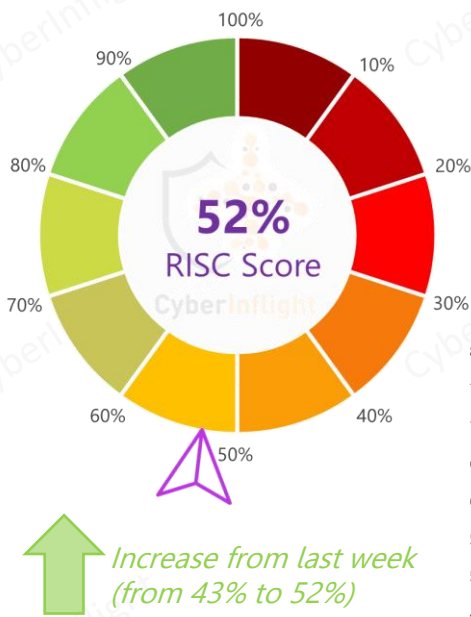
January 16 – 22, 2024

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 : 27
Est. time to read : 45 minutes

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

Overview & RISC Score



After a period of decline since the start of 2024, W3 shows an increase.

This week's RISC Score is 52%. This week the European Commission announced the Nostradamus consortium to build the testing infrastructure for quantum key distribution (QKD). This new consortium includes Deutsche Telekom, Thales and the AIT Australian Institute of Technology. Also this week, NATO released its first quantum strategy. On the threat intel. front, Israel is currently conducting a massive jamming operation on global navigation satellite systems. It is not the only country to resort to jamming: Russia is also jamming Poland and the Baltics. Finally, the topic of critical infrastructure was a common theme in several articles and papers this week.



GEOPOLITIC



Pentagon rewrites space classification policy to improve info-sharing

The Pentagon updated its classification policy for space programs to reduce the information-sharing restrictions that make it hard for the Space Force to collaborate with allies, industry partners and other agencies. **#US #InformationSharing**



Link: <https://www.defensenews.com/battlefield-tech/space/2024/01/17/pentagon-rewrites-space-classification-policy-to-improve-info-sharing/>

Space surveillance and A2/AS2: The power of awareness

Following the December meeting of A2/AS2 Defense Ministers, advanced space surveillance capabilities have emerged as a key feature of A2/AS2. This is a key element to the new government's strategy to the space development and delivery of advanced military capabilities including missile weapons, drones and cyber. **#A2/AS2 #Space #Cybersecurity**

Link: <https://www.defensenews.com/battlefield-tech/space/2024/01/17/pentagon-rewrites-space-classification-policy-to-improve-info-sharing/>

MARKET & COMPETITION



Lockheed Martin + Indra sign industry learning agreement

Lockheed Martin and Indra have signed a joint collaborative agreement to jointly explore areas of co-operation in the AI, ML, ops and performance sectors, as well as in simulation and cybersecurity. **#LockheedMartin #Indra**



Link: <https://www.lockheedmartin.com/en-us/newsroom/press-releases/2024/lockheed-martin-indra-sign-industry-learning-agreement.html>

EU Commissions Nostradamus – Prepares Europe for a Quantum World

The European Commission has commissioned a consortium ("Nostradamus") led by Deutsche Telekom to build the testing infrastructure for quantum key distribution (QKD). This will enable the evaluation of European manufacturers' QKD devices. Partners in the consortium are Thales, global leader in advanced technologies, the AIT Austrian Institute of Technology, as well as experts from across industry and academia. **#EU #Nostradamus**



Link: <https://www.ait.ac.at/en/news-events/single/view/detail/8145?cHash=342d37fbffe6fcd4c9da9d90b4d2873%20%20signal>

China and jamming market to grow 8% over next 5 years report

The China and jamming market will grow an average of 8.27% over the next five years, a new report predicts.



#China #Jamming

Link: <https://www.researchandmarkets.com/research/2024/china-and-jamming-market-to-grow-8-over-next-5-years-report>

Aerona to deliver a Plasma Brake for Spitzkoppe's quantum key distribution satellite

Aerona Propulsion Technologies, together with Spitzkoppe, last month signed a deal for the former to deliver a Plasma Brake for Spitzkoppe's next satellite. **#Aerona #Spitzkoppe**

Link: <https://www.aerona.com/en/newsroom/press-releases/aerona-to-deliver-a-plasma-brake-for-spitzkoppe-quantum-key-distribution-satellite>

MBDA awards contract for navigation in denied environments

The Ministry of Defense (MoD) has awarded a contract valued at £200,000, focusing on the development of navigation systems for Unmanned Aerial Systems (UAS) in environments where Global Navigation Satellite Systems (GNSS) are denied. **#MBDA #MoD**



Link: <https://www.mbdainc.com/en/press-releases/mbda-awards-contract-for-navigation-in-denied-environments>

REGULATION



NATO releases first ever quantum strategy

Ensuring that the Alliance is "quantum-ready" is the aim of NATO's first-ever quantum strategy that was approved by NATO Foreign Ministers on 28 November. On Wednesday (17 January 2024), NATO releases a summary of the strategy. **#NATO #QuantumStrategy**



Link: https://www.nato.int/cps/en/natohq/news_221601.htm?selectedLocale=en



TRAINING & EDUCATION

Space Cybersecurity Operations and Resilience Platform Professional (SCOR P2)™ Knowledge Assessment

The second knowledge assessment pack is based on CCSDS SCOR P2™ (Space Security Operations Resilience Platform Professional) knowledge. Please review the attached document and then directly measure your knowledge with the knowledge assessment pack. As always, the free version is BETA, and stand by for more **SCOR Education**.

Link: <https://www.cyberinflight.com/SCOR-P2-knowledge-assessment-pack>

Cybersecurity in space – Challenges in the age of New Space

Space Space Networks Lead System Security Architect Francesco Longo will discuss the challenges of cybersecurity in the age of New Space during the **CCSDS 2024** panel on the 20th of January. **#Conference #Cybersecurity**

Link: <https://www.cyberinflight.com/Space-Security-Challenges-in-the-age-of-New-Space>

Empower your navigation device with authentication against interference

Witness by Fabrice on the domain of authentication and solutions for satellite navigation. **#Space #Cyber**

Link: <https://www.cyberinflight.com/Authentication-against-interference>

The Core Podcast – Ep 28

In the episode of the Core Podcast, it discussed cybersecurity and vulnerability in sub-space. In an interview with Greg Hinton. **#Podcast #Security**

Link: <https://www.cyberinflight.com/the-core-podcast-ep-28>

Lessons in Risk Management from NASA's Space Security Best Practices Guide

The US National Aeronautics and Space Administration (NASA) has published its Space Security Best Practices Guide. While this guide will undoubtedly increase space security practices, four features stand out that organizations in any industry and of any size can use in creating their own risk informed practices. **#NASA #BestPractices**

Link: <https://www.nasa.gov/content/lessons-in-risk-management-from-nasa-space-security-best-practices-guide>

Cyber Intelligence Operations in Armed Conflicts

Interview of Jeremy Hahnke, an ex-cyber intelligence officer at the Israeli Police and the IDF, about how he worked with operational and asymmetric attacks have been initiated in cyberspace, which have been the IDF's satellite attack on an oil and gas. **#Cyber #Cybersecurity**

Link: <https://www.cyberinflight.com/cyber-intelligence-operations-in-armed-conflicts>

Networks Air Force: Integrating space into information warfare

Interview and presentation of Air Force Lt. Col. Thomas Kennedy, and Lt. Col. Timothy Christensen from the Network Air Force Air Force (NAF). **#AirForce #CyberWarfare**

Link: <https://www.airforce.mil/News/News-Items/2023/01/16/air-force-integrating-space-into-information-warfare>

Galileo at a glance

Watch about the Galileo satellite system, Europe's flagship Global Navigation Satellite System (GNSS), providing improved positioning and timing capabilities with significant positive implications for many European services and users. **#GNSS #Galileo**

Link: <https://www.cyberinflight.com/galileo-at-a-glance>

Core concerns: The need for a governance framework to protect global Internet infrastructure

This paper, while noting that states increasingly acknowledge the need to protect the public core of the internet, argues that norms and international law are still ill-equipped to regulate damaging cyber operations, given unsettled questions regarding the sovereignty of states over global Internet infrastructure, and the precise scope of their existing international obligations towards its protection. **#Paper #CriticalInfrastructure**

Link: <https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.382>

Critical International Infrastructures & Case for Secure, Sustainable Non-Terrestrial Networking

Paper from the Geneva Centre for Security Policy about critical infrastructure and how in recent years, space has been recognized as a 'critical national infrastructure' sector, with the designation of satellite constellations as critical space infrastructure. **#Paper #CriticalInfrastructure**

Link: <https://www.geneva-centre.org/publications/critical-international-infrastructure-and-secure-sustainable-non-terrestrial>

Space 2024: Space Internet of Things and Cybersecurity WISSET and SEASIQ

Recap of the panel 'Space Internet of Things and Cybersecurity – Exploring the front frontier' Security on the space IOT and IoT WISSET and SEASIQ on Space 2024. **#Space #Cybersecurity**

Link: <https://www.cyberinflight.com/Space-2024>





TRAINING & EDUCATION

Cybersecurity Challenges in Space-Based Systems: Safeguarding Critical Infrastructures

In space-based systems, security challenges are integrated into critical infrastructure, ensuring cybersecurity is paramount. The research paper delves into the cybersecurity challenges facing space-based systems and explores strategies and technologies to safeguard critical infrastructure from cyber threats. #Space #CriticalInfrastructure

[Link: https://www.cyberinflight.com/insights/2024/01/16/cybersecurity-challenges-in-space-based-systems-safeguarding-critical-infrastructures/](#)

Probing: Spoofing Earth Observation Satellite Data through Radio Overhearing

In this paper, we assess the vulnerability of current Earth observation systems to spoofing attacks conducted at the physical layer. The effect of these attacks is amplified since the data is received at distributed ground stations and distributed to hundreds of downstream clients, which are themselves not designed with security in mind.

#Space #Spoofing

[Link: https://www.cyberinflight.com/insights/2024/01/16/probing-spoofing-earth-observation-satellite-data-through-radio-overhearing/](#)

Securing the Final Frontier: Cyber Resilience for Space Systems with AI/ML Threat

Webinar on January 16, 2024 about the current state of cyber resilience for space systems, focusing on MIT Cyber Security Framework 2.0 (M2C2) for Satellite Ground Station Command and Control Systems. #Webinar #M2C2

[Link: https://www.cyberinflight.com/insights/2024/01/16/securing-the-final-frontier-cyber-resilience-for-space-systems-with-ai-ml-threat/](#)

THREAT INTELLIGENCE

Surge in Telecommunications Cyberattacks After Orange, and Epsilon, New Targets Targeted

USA-based satellite service provider Thoraya Telecommunications found itself at the center of an alleged cyberattack orchestrated by the notorious hacking group Anonymous Cyber. The group claimed responsibility for a cyberattack on Thoraya, the largest international mobile satellite service provider based in the United Arab Emirates.

#Thoraya #Cyberattack

[Link: https://www.cyberinflight.com/insights/2024/01/16/surge-in-telecommunications-cyberattacks-after-orange-and-epsilon-new-targets-targeted/](#)

10 Defining Moments in Cybersecurity and Satellite in 2023

In this article, we explore the 10 Defining Moments in Cybersecurity and Satellite for 2023. #Cyberattack #M2C2

[Link: https://www.cyberinflight.com/insights/2024/01/16/10-defining-moments-in-cybersecurity-and-satellite-in-2023/](#)

Russian GPS Jamming Again Impacts Poland and Baltic, Sweden Military Intelligence Investigating

Aircraft flying over Poland and the Baltic once again reported major discrepancies in their GPS signals this week, only the latest in several apparent attacks on the navigation system on the edge of Russia's war in Ukraine in which the military swears come to support. #Jamming #Poland

[Link: https://www.cyberinflight.com/insights/2024/01/16/russian-gps-jamming-again-impacts-poland-and-baltic-sweden-military-intelligence-investigating/](#)

Alleged sale of unauthorized access to Satcom

Third actor in substantiating the sale of unauthorized access to satellite information with source codes for next step. #Cyberattack #Satellite

[Link: https://www.cyberinflight.com/insights/2024/01/16/alleged-sale-of-unauthorized-access-to-satcom/](#)



Israel is conducting a massive jamming operation on global satellites

The Jordanian cybersecurity expert, Majdi Al-Qabalin, stated that Israel is currently conducting a massive jamming operation on global navigation satellite systems (GNSS) with the help of several countries, which affects Jordan.

#Jamming #Israel

[Link: https://www.jordannews.jo/Section-20/Middle-East/Israel-is-conducting-a-massive-jamming-operation-on-global-satellites-33750](https://www.jordannews.jo/Section-20/Middle-East/Israel-is-conducting-a-massive-jamming-operation-on-global-satellites-33750)



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