SPACE CYBERSECURITY WEEKLY WATCH

Week 3

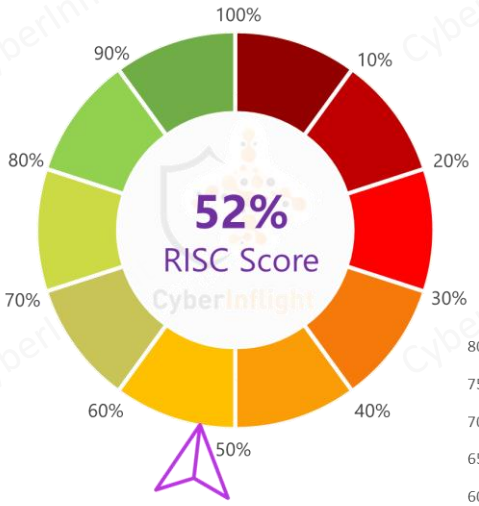
January 16 – 22, 2024

Timeframe : Weekly
# of articles identified : 27
Est. time to read : 45 minutes

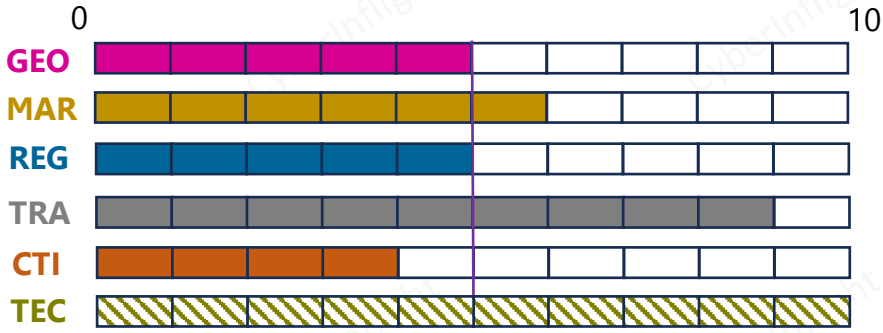
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

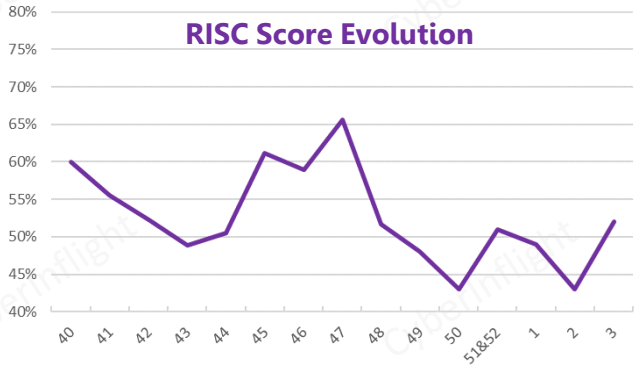
- GEOPOLITIC
- MARKET & COMPETITION
- REGULATION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- IMPORTANT NEWS

Overview & RISC Score



Increase from last week (from 43% to 52%)





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/

[redacted]

MARKET & COMPETITION

[redacted]

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=342d37fbffe6fcdb4c9da9d90b4d2873%20:%20signal

[redacted]

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

[redacted]

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

[redacted]

TRAINING & EDUCATION

Cybersecurity Challenges in Space-Based Systems: Safeguarding Critical Infrastructure
As space-based systems become increasingly integrated into critical infrastructure, ensuring cybersecurity is paramount. This research paper delves into the cybersecurity challenges faced by space-based systems and explores strategies and technologies to safeguard critical infrastructure from cyber threats. **#Paper #CriticalInfrastructure**
Link: https://example.org/public-afcms/preprint/mbrd

Firefly: Spoofing Earth Observation Satellite Data through Radio Overshadowing
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 dedicated ground stations and distributed to hundreds of downstream systems, which are themselves not designed with security in mind.
#Paper #Spoofing
Link: https://www.ndss-symposium.org/ndss-paper/auto-draft-419/

Securing the Final Frontier: Cyber Resiliency for Space Systems with Abhi Therat
Webinar on January 26, 2024 about the current state of cyber resiliency for space systems, focusing on NIST Cyber Security Framework (CSF) IR 8401 for Satellite Ground Station Command and Control Systems. **#Webinar #NIST**
Link: https://www.meetup.com/space-data-hackers/events/298001430/

THREAT INTELLIGENCE

Surge in Telecommunications Cyberattacks After Orange, and Kyivstar, Now Thuraya Targeted
UAE-based satellite service provider Thuraya Telecommunications found itself at the center of an alleged cyberattack orchestrated by the notorious hacking group, Anonymous Sudan. The group claimed responsibility for a cyberattack on Thuraya, the largest international mobile satellite service provider based in the United Arab Emirates.
#Thuraya #Cyberattack
Link: https://therecordmedia.com/cyberattacks-on-telecommunications/

10 Defining Moments in Cybersecurity and Satellite in 2023
In this article, the Satellite identifies 10 Defining Moments in Cybersecurity and Satellite for 2023. **#Cyberattack #2023**
Link: https://www.satellitetoday.com/cybersecurity/2024/01/17/10-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 on which the modern world has come to depend. **#Jamming #Poland**
Link: https://www.breitbart.com/europe/2024/01/19/russian-gps-jamming-again-impacts-poland-and-baltic-sweden-military-intelligence-investigating/

Alleged sale of unauthorized access to Avios
Threat actor is advertising the sale of unauthorized access to satellite information with source codes for most files.
#Cyberattack #Satellite
Link: https://exp.io/threads/106236/

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

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