



# SPACE CYBERSECURITY WEEKLY WATCH

Week 49

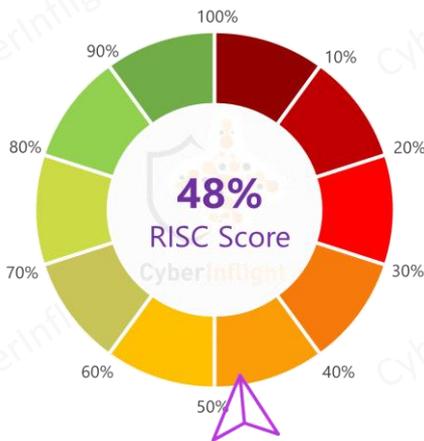
November 28 – December 4, 2023

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

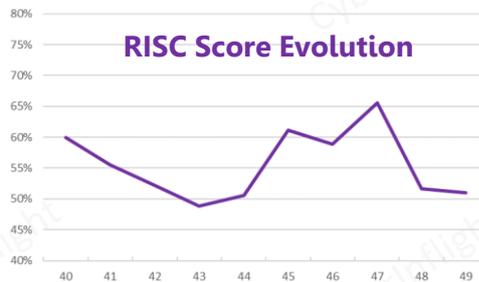
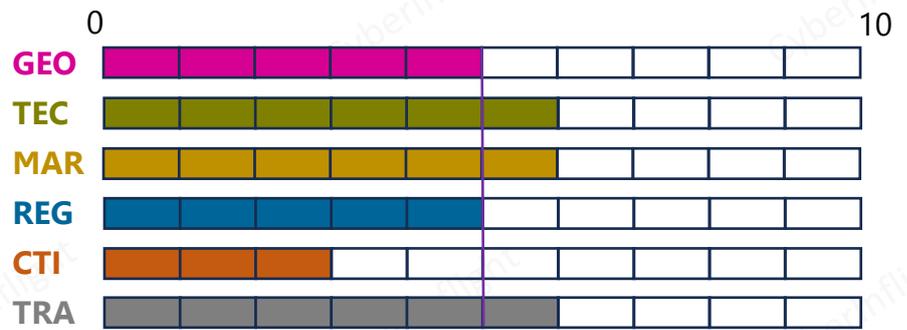
Timeframe : Weekly  
# of articles identified : 35  
Est. time to read : 1h15min

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

## Overview & RISC Score



**↓ Decrease from last week (from 52% to 48%)**



*There was a peak for W47, which had a RISC Score of 66%, the highest of the year so far.*

This week's RISC Score is 48%. Earlier this year, a cyberattack targeted JAXA, the agency then declared this week that the possibility is high that unauthorized access was made to its central server. Also this week, a US Army representative stated that the military is turning towards integrating the space and cyberspace domains to build a military doctrine, which in practice represents a major challenge. On the technology side, measures under the new UK strategy for ensuring the continuity of PNT services require the elaboration of a comprehensive crisis plan to be activated if PNT services become unavailable. This week, the Defense Innovation Unit, USSF and AFRL published a new round of proposals for a space network project. The aim is to connect satellite networks and ground communications systems so military users can get data faster and more securely than is currently possible. A focus on NIST IR 8441 is included in the regulation section of this watch. Finally, an academic paper was published this week on China's use of the eLoran service for its critical infrastructures.





# MARKET & COMPETITION

## EC Telecom Releases New Cyber Solution Targeting Shipping Customers

EC Telecom is bringing out a new cybersecurity solution targeting the maritime sector. Cyphertech aims to combine advanced cybersecurity software with a variety of tools to ensure protection for onboard networks. EC Telecom announced the new solution on Nov. 27. EC Telecom is an international satellite service operator with engineering expertise in low and high throughput cyber services and data services for land and maritime use.

**#Cybersecurity #MaritimeOperator**

**Link:** <https://www.ec-telecom.com/press-releases/2023/11/27/ec-telecom-releases-new-cyber-solution-targeting-maritime-customers/>



## Aviation Space is all in with American Web Services

Aviation Space and AWS are also collaborating on the development and deployment of an open cybersecurity solution that will be the foundation for operating cybersecure future Satcom. **#Aviation #AWS**

**Link:** <https://www.aviationspace.com/2023/11/27/aviation-space-is-all-in-with-aws-with-awscyber/>



## Defense Innovation Unit solicits new round of proposals for space network project

DIU is working with the U.S. Space Force and the Air Force Research Laboratory on efforts to connect satellite networks and ground communications systems so military users can get data faster and more securely than is currently possible. **#US #Security**

**Link:** <https://spacenews.com/defense-innovation-unit-solicits-new-round-of-proposals-for-space-network-project/>



## European Commission Launches Call for Establishing EU Space ISEC to Enhance Security and Resilience in the Space Sector

The European Commission and the EU4SA jointly initiated the EU Space Information Sharing Center (ISEC). The initiative serves as a venue for the exchange of information, promoting collaboration, raising awareness, and addressing joint problems among private organizations to ensure the robust security of space systems and their interconnected networks. The call for interest is open until October 28th, 2023. **#EU #Space #SEC**

**Link:** <https://www.europa.eu/en/press-communication/124684/in-action/eu-space-information-sharing-center>



## Quantum Data And Spectral Small Quantum Communication Developments With Zurich QM&S For Spectral 1 Mission

Quantum Data, a spinoff from the university of Zurich's quantum optics laboratory and Spectral, a leading quantum communications technology company, recently announced the launch and use of the Zurich Quantum Satellite Mission Operator (ZQM&S), a project aimed for space to enable secure quantum communication technologies in the upcoming Spectral 1 satellite mission. **#Quantum #QM&S**

**Link:** <https://www.quantumdata.ch/en/quantum-data-and-spectral-launch-quantum-communication-developments-with-spectral-1-mission/>

## The European Space Agency Explores Cybersecurity for Space Industry

An EU cybersecurity report explains how space-based data and services benefit from public investment in space programs. **#Space #ESA**

**Link:** <https://www.esa.int/en/industry/cybersecurity/cybersecurity-for-space-industry>



# REGULATION



## NIST NCCoE Publishes Cybersecurity Framework Profile for Hybrid Satellite Networks

In late September 2023, the US-based National Institute of Standards and Technology (NIST) published its Cybersecurity Framework Profile for Hybrid Satellite Networks, otherwise known as NIST IR 8441. This blog will explore the reasons behind NIST developing the framework, outline its intentions, and summarize its key points. **#US #NIST**

**Link:** <https://www.tripwire.com/state-of-security/nist-nccoe-cybersecurity-framework-hybrid-satellite-networks>



## Angola signs Artemis Accords

Angola signed the U.S.-led Artemis Accords outlining best practices for space exploration Nov. 28, becoming the third African nation to do so. **#Artemis #Angola**

**Link:** <https://www.esa.int/en/press-communication/124684/in-action/angola-signs-artemis-accords>



## EU backs rules to protect digital devices from cyber threats

The European Parliament and its member states backed new rules to make digital products connected to the internet be cyber-secure. The new rules will help protect digital devices from cyber threats. **#EU #Cybersecurity**

**Link:** <https://www.europa.eu/en/press-communication/124684/in-action/eu-backs-rules-to-protect-digital-devices-from-cyber-threats>





# THREAT INTELLIGENCE

## Cyber Attacks on the GPS Satellites

The past progress and milestones of the methods used in case of a cyberattack against a GPS satellite

### Knowing Hacking

[Link: https://www.timesofindia.indiatimes.com/world/rest-of-world/cyber-attacks-on-gps-satellites/articleshow/105580741.cms?from=mdr](#)

## Placement in the outer space

We've detected a secondary object in close proximity to Oigant, a payload released by Russian satellite COSMOS 2550 around October 11. **Media Watch**

[Link: https://thehindu.com/news-international/space/cosmos-2550-payload/articleshow/105580741.cms?from=mdr](#)

## Japan Space Agency likely penetrated by a cyberattack

The Japan Aerospace Exploration Agency (JAXA) reported to the government that the "possibility is high that unauthorised access was made" to its central server, government spokesman Hirokazu Matsuno told reporters. **#JAXA #Cyberattack**

**Link:** <https://timesofindia.indiatimes.com/world/rest-of-world/japan-space-agency-likely-penetrated-by-cyber-attack/articleshow/105580741.cms?from=mdr>

## Russia and the Growing Danger of Satellite Cyberattacks

While no single agency monitors Russian cyberattacks, the amount of personnel involved in these operations continues to increase. There is a heavy reliance on criminal and civilian involvement to conduct offensive operations. Combining Russian interest in cyber and outer space has led to the "proliferation of hardened (radio frequency) jamming systems (GPS jammers), development of next mobile jammers, and more development and testing of space-based jammers," as reported on by Space Warfare. She also warns that Russia may track American ground control systems in the GPS constellation.

### Media Cyberattack

[Link: https://thehindu.com/news-international/russia-and-the-growing-danger-of-satellite-cyberattacks/articleshow/105580741.cms?from=mdr](#)

## LockBit claims cyberattack on India's national aerospace lab

On Wednesday, LockBit added the National Aerospace Laboratories (NAL) to its dark web leak site, which promises group use to select actions for ransom payments. The group threatened to publish the organization's stolen data if it fails to pay an unspecified amount, according to the listing seen by TechCrunch. **Media Watch**

[Link: https://techcrunch.com/2023/11/28/lockbit-claims-cyberattack-on-indias-national-aerospace-laboratory-announces-attack/articleshow/105580741.cms?from=mdr](#)

## GPS Spoofing Signals Traced To Tehran

A University of Texas student has traced the source of alarming GPS spoofing signals in the Middle East to the eastern suburbs of Tehran. **Media Cyberattack**

[Link: https://www.wired.com/story/gps-spoofing-signals-traced-to-tehran/articleshow/105580741.cms?from=mdr](#)

## La géopolitique, un accélérateur d'attaques DDoS en EPHEA (Trad. Géopolitique, a gas pedal of DDoS attacks in EPHEA)

Cybercriminals stepped up their nefarious activities in the first half of 2023. According to MITRE ATT&CK's latest report, around 73 million distributed denial of service (DDoS) attacks were launched worldwide in the first half of 2023, compared with just over 6 million in the first half of 2022. **Media Cyberattack**

[Link: https://www.computerworld.com/article/3664446/la-geopolitique-un-accelereur-dattaques-ddos-en-ephea-articleshow/105580741.cms?from=mdr](#)

## Ransomware attack on Supply Technologies LLC

Supply Technologies a ransomware attack on Supply Technologies LLC in the US, exfiltrating 7 TB of data including contracts, HR, and technical documents. **Ransomware Cyberattack**

[Link: https://thehindu.com/news-international/usa/ransomware-attack-on-supply-technologies-llc/articleshow/105580741.cms?from=mdr](#)

## Current threats to Global Navigation Satellite Systems

The use of technology, applications, and services associated with GNSS (Global Navigation Satellite Systems) is increasingly widespread, cementing GNSS as a key element of critical industries in both the public and private sectors. This critical dependence on GNSS systems results in an increase of risks and threats that, if not adequately addressed, may have devastating consequences. **Ransomware Threats**

[Link: https://www.gpsworld.com/gnss/articleshow/105580741.cms?from=mdr](#)

## Tracking Interference: The Ukrainian Battlefield Reaches Into Space

Satellite jamming is an acknowledged and expected warfare technique, and industry experts have observed Russia and Ukraine trading blows in space. **Media Watch**

[Link: https://www.kitware.com/insights/ukraine-tracking-interference-the-ukrainian-battlefield-reaches-into-space/articleshow/105580741.cms?from=mdr](#)

## Detecting Missile Threats from Space

This article examines the threats domain, effective missile defense by the West, and all some of the latest US space-based program developments offering missile warning and tracking (MWT) capability to protect against such threats. **Media Watch**

[Link: https://www.army.mil/article/3664446/detecting-missile-threats-from-space/articleshow/105580741.cms?from=mdr](#)





# TRAINING & EDUCATION



Qualifies users for multilateral practitioners paper discussion for advanced satellite systems for strategic use  
Knowledge of IT management of satellites? (Final): What are the best practices for securing satellite  
networks against jamming and spoofing attacks?

Article about the best practices and how to protect satellite networks against jamming and spoofing

**Keywords:** #Workshop

**Link:** <https://www.linkedin.com/pulse/best-practices-securing-satellite-2023>

## China eLoran used for critical infrastructure. Extension to be complete by 2026 - New paper

A paper published yesterday provides more information on China's plans to expand its eLoran service. The paper also confirmed China is using eLoran timing signals to increase the security and reliability of financial, communications, and other infrastructure. **#Paper #GNSS**

**Link:** <https://www.linkedin.com/pulse/china-eloran-used-critical-infrastructure-extension-complete-goward-mzj1e/?trackingId=V8Of1H8JTycBsvXkxOEsBw%3D%3D>

Forum on the economic opportunities - NIS Expert Forum (Final): New Space Economy Forum - NIS Expert Forum

Conference on December 1, 2023 in Rome, on the subject of the transformative power of space technologies, accelerating technology transfer, stimulating economic growth and with sessions on cybersecurity

**Keywords:** #Workshop

**Link:** <https://www.linkedin.com/pulse/forum-on-economic-opportunities-nis-expert-forum-2023>

Quantum Key Distribution for Healthcare Sector" workshop

QKD Workshop on December 27, 2023 about how the groundbreaking QKD technology will enable next-gen cybersecurity for healthcare information **#Workshop #QKD**

**Link:** <https://www.linkedin.com/pulse/qkd-workshop-2023>

4.28 Stars, clouds and deep seas: Ensuring secure and resilient communications infrastructure

The Global Conference on Cyber Capacity Building took place on November 28<sup>th</sup> - 29<sup>th</sup>, 2023 in Accra/Ghana, with a panel on ensuring secure and resilient communications infrastructure **#Conference #Resilience**

**Link:** <https://www.linkedin.com/pulse/4-28-stars-clouds-deep-seas-ensuring-secure-resilient-communications-infrastructure>

Aerospace Cybersecurity: Satellite Hacking | Detecting Attacks and Mitigation Strategies | Part 1

This video tutorial presents how to detect attacks and protect satellite systems. It is a part of our online course Aerospace Cybersecurity: Satellite Hacking by Angeline Tucker **#Course #Cybersecurity**

**Link:** <https://www.linkedin.com/pulse/aerospace-cybersecurity-satellite-hacking-1>

2023 Cybernet in Galileo Program

Cybernet in Galileo is a high-level Europe-wide educational event designed to meet the needs of the cyber ecosystem. Over 3 days, participants will hear from leading figures in the field of cybersecurity on a range of topics, including AI and Cybersecurity, Quantum, Industry and Challenges, Internet of Things, and Mobile Device Protection **#Conference #QKD**

**Link:** <https://www.linkedin.com/pulse/2023-cybernet-in-galileo-program>

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](mailto:research@cyberinflight.com)