SPACE CYBERSECURITY WEEKLY WATCH

Week 49

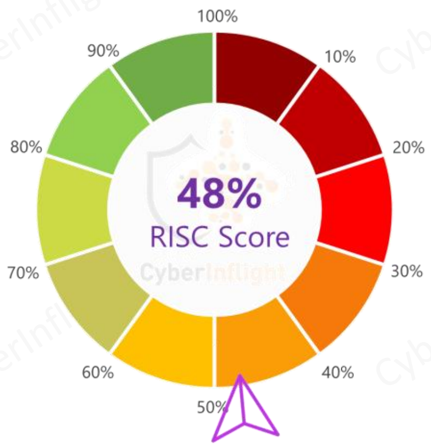
November 28 – December 4, 2023

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

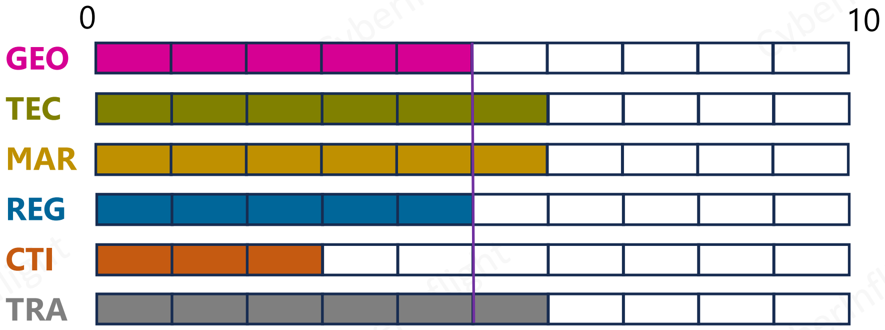
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

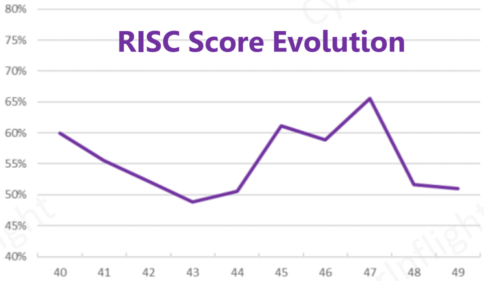
■ GEOPOLITIC
■ TECHNOLOGY
■ MARKET & COMPETITION
■ REGULATION
■ THREAT INTELLIGENCE
■ TRAINING & EDUCATION
★ IMPORTANT NEWS

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 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.

GEOPOLITIC

★ **With formalized MDO doctrine, Army turns focus to space, cyber: Official**

Now that the Army has released its official multi-domain operations doctrine, the service is turning towards integrating the space and cyberspace domains, a “significant” challenge, an official said today. **#US #SpaceCybersecurity**

Link: https://breakingdefense.com/2023/11/with-formalized-mdo-doctrine-army-turns-focus-to-space-cyber-official/

Bengaluru Tech Summit | Cybersecurity for Space has a unique set of challenges: ISRO chief info security officer

[illegible] **#ISRO #SpaceStrategy**

Link: [illegible]

Forget About 'Connecting The Dots' The Next Impending Attack Is Staring Us In The Face

[illegible] **#SpaceCyber #Trends**

Link: [illegible]

US Sanctions North Korean Cyber Unit After Satellite Launch

[illegible] **#US #NorthKorea**

Link: [illegible]

TECHNOLOGY

SDA demos first-ever space-to-ground Link 16 connection

[illegible] **#SDA #Link16**

Link: [illegible]

★ **PNT Makes the World Go Around: The UK’s New Alternative PNT Strategy**

Measures under the new UK strategy for ensuring the continuity of PNT services include the elaboration of a comprehensive crisis plan, to be activated should PNT services become unavailable. This cross-government plan is to be regularly updated, and will include measures for, among other things, identification and implementation of short-term mitigation actions. **#UK #PNT**

Link: https://insidegnss.com/pnt-makes-the-world-go-around-the-uks-new-alternative-pnt-strategy/

Airbus starts Galileo Second Generation satellite production

[illegible] **#Galileo #Airbus**

Link: [illegible]

Toshiba hones quantum encryption as commercialization nears

[illegible] **#Quantum #Toshiba**

Link: [illegible]

MARKET & COMPETITION

IEC Telecom Releases New Cyber Solution Targeting Shipping Customers

IEC Telecom is bringing out a new cybersecurity solution targeting the maritime sector. OptiShield aims to combine advanced cybersecurity software with a remote IT team to ensure protection for onboard networks. IEC Telecom announced the new solution on Nov. 27. IEC Telecom is an international satellite service operator with engineering expertise in low and high-throughput cyber-secure voice and data services for land and maritime use. **#Cybersecurity #SatelliteOperator**

Link: https://www.satellitetoday.com/cybersecurity/2023/11/27/iec-telecom-releases-new-cyber-solution-targeting-shipping-customers/

Axiom Space is all-in with Amazon Web Services

Axiom Space and AWS are also collaborating on the development and demonstration of in-space cybersecurity solutions that set the foundation for operating a cybersecure Axiom Station. **#Axiom #AWS**

Link: https://news.satnews.com/2023/11/28/axiom-space-is-all-in-with-amazon-web-services/

★ 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 ISAC to Enhance Security and Resilience in the Space Sector

The European Commission and the EUSPA jointly initiated the EU Space Information Sharing Centre (ISAC). This platform serves as a nexus for the exchange of information, promoting collaboration, raising awareness, and advocating best practices among private organizations to ensure the robust security of space systems and their interconnected networks. The call for interest is open until October 31th, 2025. **#CallforInterest #EUSpaceISAC**

Link: https://www.thesign.media/blog/unveiling-the-eu-space-information-sharing-centre

Quantum Dice And SpeQtral Unveil Quantum Communication Developments With Zenith QRNG For SpeQtral-1 Mission

Quantum Dice, a spinout from the University of Oxford's quantum optics laboratory, and SpeQtral, a leading quantum communications technology company, proudly announce the launch and use of the Zenith Quantum Random Number Generator (QRNG), a product designed for space, to enable secure quantum communication technologies in the upcoming SpeQtral-1 satellite mission. **#Quantum #QKD**

Link: https://www.quantum-dice.com/quantum-dice-and-speqtral-unveil-quantum-communication-developments-with-zenith-qrng-for-speqtral-1-mission/

The European Space Agency Explores Cybersecurity for Space Industry

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

Link: https://www.darkreading.com/ics-ot-security/european-space-agency-explores-cybersecurity-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. 30, becoming the third African nation to do so. **#Artemis #Angola**

Link: https://spacenews.com/angola-signs-artemis-accords/

EU backs rules to protect digital devices from cyber threats

The European Parliament and EU member states backed new rules to make digital products connected to the internet like fridges, laptops, TVs and toys safer from cyber threats. **#EU #Cybersecurity**

Link: https://www.spacewar.com/reports/EU_backs_rules_to_protect_digital_devices_from_cyber_threats_999.html

THREAT INTELLIGENCE

Cyber Attacks on the GPS Satellites

[illegible]

Movement in the outer space

[illegible]

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

[illegible]

LockBit claims cyberattack on India's national aerospace lab

[illegible]

GPS Spoofing Signals Traced To Tehran

[illegible]

La géopolitique, un accélérateur d'attaques DDoS en EMEA (Trad.: Geopolitics, a gas pedal of DDoS attacks in EMEA)

[illegible]

Ransomware attack on Supply Technologies LLC

[illegible]

Current threats to Global Navigation Satellite Systems

[illegible]

Tracking Interference: The Ukrainian Battlefield Reaches Into Space

[illegible]

Detecting Missile Threats from Space

[illegible]

TRAINING & EDUCATION

[illegible]

★ **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

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]