SPACE CYBERSECURITY WEEKLY WATCH

Week 25
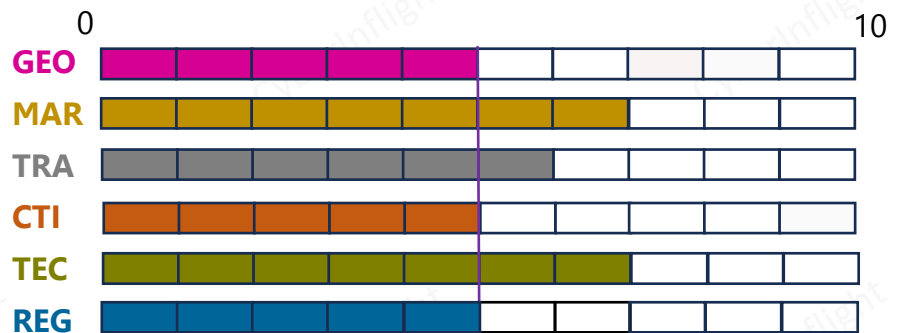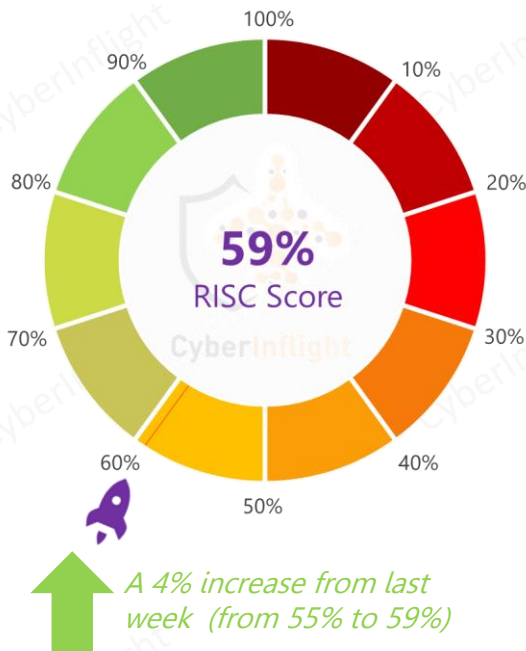
June 18 – 24, 2024

Timeframe : Weekly

# of articles identified : 30

Est. time to read : 50 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 INTELLIGENCE**

■ **TRAINING & EDUCATION**

■ **THREAT INTELLIGENCE**

■ **TECHNOLOGY**

■ **REGULATION**

★ **IMPORTANT NEWS**

Overview & Resilience Index for Space Cybersecurity (RISC)

59%
RISC Score

A 4% increase from last week (from 55% to 59%)

	0									10
GEO										
MAR										
TRA										
CTI										
TEC										
REG										

RISC Score Evolution

After declining from W18 to W20, as well as in W23 and W24, the RISC score (the tool assessing space cybersecurity resilience) struggled to recover. However, it rose slightly in W22 and W25.

This week's RISC score is 59%. This week, USSF launched programs to modernize satellite ground systems. The private sector and the cloud are being called upon to carry out this program for ground operator resilience. On the regulation front, as a veteran of data protection, NIS2 has witnessed first-hand the evolution of digital threats and the increasing sophistication of cyber adversaries. As such, the launch of NIS2 is a giant step in redefining the cybersecurity landscape for essential and digital services. On another front, AQNav was released by SandboxAQ, which is a technology designed for navigation when GPS systems are jammed or not available. AI algorithms, powerful quantum sensors, and the Earth's crustal magnetic field in AQNav make it resistant to interference. On another news, a paper entitled "Outer space cyberattacks: generating novel scenarios to avoid surprise" published by California Polytechnic University, prepares policy makers and technical specialists for the future of cybersecurity in space by helping them to create hypothetical threat scenarios for anticipation. Regarding the market front, a contract is signed for the supply of Safran's Geonyx inertial navigation and pointing systems to the Polish Armed Forces by Safran Electronics & Defense and Wojskowe Zakłady Elektroniczne. This contract is aimed at enhancing the resilience of Polish satellites against jamming and spoofing. Lastly, the head of the Space ISAC has warned that the commercial space industry is facing an assault of cyber attacks and other threats, but lacks the resources and coordination to adequately defend itself.

GEOPOLITIC

Five Eyes' Critical 5 nations focus on adapting to evolving cyber threats to boost critical infrastructure security resilience

Cybersecurity agencies from the 'Five Eyes' alliance provided updates on the evolving risks to critical infrastructure and described how the nations within the Critical 5 partnership are updating their strategies to protect critical infrastructure. The narrative highlighted sharp methods to enhance the security and resilience of their critical infrastructure within their borders. **#FiveEyes #CriticalInfrastructure**

Link: https://industrialcyber.co/critical-infrastructure/five-eyes-critical-5-nations-focus-on-adapting-to-evolving-cyber-threats-to-boost-critical-infrastructure-security-resilience

Newest NATO member Sweden says Russia disrupting its satellite networks

Swedish authorities say Russia is behind "harmful interference" deliberately targeting the Nordic country's satellite networks that it first noted days after joining NATO earlier this year. **#Sweden #Russia**

Link: https://therecord.media/nato-member-sweden-says-russia-disrupting-its-satellite-networks

⭐ ## Space Force takes another swing at modernizing satellite ground systems

The US Space Force has embarked on yet another attempt to modernize ground systems used to command and control military satellites. This time, it's turning to the commercial sector and the cloud with a program called Rapid Resilient Command and Control (R2C2). The goal of this modernization is to bolster resiliency by allowing ground operators to rapidly respond to attacks, jamming, cyber intrusions and other disruptions that could cripple satellite networks. **#USSF #R2C2**

Link: https://spacenews.com/space-force-takes-another-swing-at-modernizing-satellite-ground-systems/

REGULATION

⭐ ### NIS2 directive explained: duty of care for data

The introduction of the Network and Information Security Directive 2 (NIS2) by the European Union marks a significant milestone in the journey toward a safer, more stable digital ecosystem. As data protection veterans, we have witnessed firsthand the evolution of digital threats and the increasing sophistication of cyber adversaries. It is against this backdrop that we delve into the importance of NIS2 and its potential to redefine the landscape of cybersecurity for essential and digital services. **#NIS2 #Cybersecurity**

Link: https://www.veeam.com/blog/nis2-directive-explained.html

GAO raises red flag over supply chain issues and delays in DoD space programs

The Pentagon remains sluggish in fielding innovative weapons systems even as security risks intensify. The congressional watchdog's report examined 19 major weapons systems across the military services. GAO flags several hiccups in Space Force programs, including long-standing issues with the GPS's ground system and user equipment. It also cites supply chain challenges and technical risks for the Space Development Agency planned constellation of satellites in LEO. **#GAO #SpacePrograms**

Link: https://spacenews.com/gao-raises-red-flag-over-supply-chain-issues-and-delays-in-dod-space-programs/

TECHNOLOGY

Awesome DIY Raspberry Pi satellite hacking cyberdeck version 2.0

The article provides a presentation of a satellite hacking cyberdeck powered a Raspberry Pi mini PC, and created by YourCyber spaceforcepoints to showcase it at the Open Source 2024 in San Francisco. **#SatelliteHacking #DIY**

Link: https://www.pcity.ge/go/pi/ro/satellite-hacking-cyberdeck

BAE Systems preparing warfighters for M-Code

BAE Systems has updated nearly all of its GPS receivers with M-Code capability, giving warfighters access to equipment that is more resistant to spoofing and jamming - something that's becoming increasingly critical on today's battlefields. BAE offers various M-Code capable receivers, including the DIMA-M for precision strike and other crucial applications. And these receivers have been proven to protect against spoofing and jamming in various testing scenarios.

#BAESystems #MCode

Link: https://insidegnss.com/bae-systems-preparing-warfighters-for-m-code

GNSS Technologies a focus on detecting and mitigating PNT threats

GNSS TechSolve solution detects spoofing and jamming in a matter of seconds. This solution leverages advanced multi-element digital signal processing to spatially identify and separate real GPS signals from fake ones. It calculates the angle of arrival (AOA), making it possible to determine if the signal is from a valid satellite or a specific.

#GNSSTechnologies #PNT

Link: https://insidegnss.com/gnss-technologies-a-focus-on-detecting-and-mitigating-pnt-threats

⭐ ## Commercial Real-Time Navigation System Powered by AI and Quantum to Address GPS Denial, Jamming and Spoofing

SandboxAQ is officially announcing AQNav, a breakthrough technology designed for navigation across air, land and sea when Global Positioning Satellite (GPS) systems are jammed or not available. AQNav is a geomagnetic navigation system that leverages proprietary AI algorithms, powerful quantum sensors, and the Earth's crustal magnetic field. AQNav will provide an unjammable, all-weather, terrain-agnostic, real-time navigation solution in situations where GPS signals are unavailable, denied, or spoofed. **#AQNav #GPS**

Link: https://giscafe.com/nbc/articles/view_article.php?articleid=2077939

New counter drone solution with GNSS spoofing capabilities

SaTran Electronics & Defense has launched Skystriker, a counter-drone solution designed to protect battlespaces and sensitive installations from rogue drone threats. Skystriker replaces the hostile drone's satellite guidance signals with modified signals designed to deceive the drone about its position in order to disrupt or interrupt its mission. **#SaTran #GNSS**

Link: https://www.unmannedsystemstechnology.com/2024/06/new-counter-drone-solution-with-gnss-spoofing-capabilities

Joint Navigation Conference

Joint Navigation Conference was held from June 3 to 6. It is the largest U.S. military Positioning Navigation and Timing (PNT) conference of the year with joint service and government participation. The event focused on technical advances in PNT with emphasis on joint development, test and support of affordable PNT systems, logistics and integration. From an operational perspective the conference will focus on advances in battlefield applications of GPS, critical strengths and weaknesses of field navigation devices, warfighter PNT requirements and solutions, and navigation warfare.

#Conference #PNT

Link: https://www.jnc.org/nc/

TRAINING & EDUCATION

⭐ **Outer space cyberattacks: generating novel scenarios to avoid surprise**
This report aims to help policymakers and tech specialists prepare for the future of cybersecurity in outer space. The report, called Outer Space Cyberattacks, from California Polytechnic State University's Ethics and Emerging Sciences Group think tank. It highlights different manners and motivations for cyberattacks in space, and includes a tool helping cybersecurity teams create hypothetical threat scenarios. **#Cybersecurity #Space**
Link: https://arxiv.org/abs/2406.12041

MARKET & COMPETITION

Safran and Wojskowe Zakłady Elektroniczne join forces to support Polish Defense

Safran Electronics & Defense and the Polish company Wojskowe Zakłady Elektroniczne (WZE S.A.) signed for the first time a contract for the supply of Safran's Geonyx inertial navigation and pointing systems to the Polish Armed Forces during the Eurosatory exhibition. This inertial navigation technology is resilient to jamming and spoofing of satellite navigation signals to Polish Armed Forces. **#Safran #Poland**

Link: https://www.edrmagazine.eu/%E2%96%BA-safran-and-wojskowe-zaklady-elektroniczne-join-forces-to-support-polish-defense

THREAT INTELLIGENCE

Backing up ground stations and satellite control centers: a comprehensive security guide

[text obscured/blurred] **#GroundStationsSecurity**

Link: *[text obscured/blurred]*

⭐ ### Space industry group warns of escalating cyber threats, outmatched defense

The commercial space industry is facing a onslaught of cyber attacks and other threats, but lacks the resources and coordination to adequately defend itself, the head of the Space ISAC warned. She said that 100 cyberattacks against critical infrastructures related to space systems were recorded every week. Most space companies would have a difficult time defending against well-orchestrated cyber attacks by a nation-state. **#CyberThreats #Space**

Link: https://spacenews.com/space-industry-group-warns-of-escalating-cyber-threats-outmatched-defenses/

The GPS jamming/spoofing in the eastern Black Sea and eastern Mediterranean Sea is still going strong

[text obscured/blurred] **#Crimea #Israel**

Link: *[text obscured/blurred]*

Navigating the Atlantic: first ever GPS jamming on commercial flights

[text obscured/blurred] **#Atlantic #GPS**

Link: *[text obscured/blurred]*

Israel's GPS signal jamming not affecting flight safety, says Minister

[text obscured/blurred] **#Israel #GPS**

Link: *[text obscured/blurred]*

UK aviation agency raises grave concern over North Korea's GPS signal jamming

[text obscured/blurred] **#Jamming #NorthKorea**

Link: *[text obscured/blurred]*

Japan's space agency reports cyberattacks, possible data leak

[text obscured/blurred] **#JAXA #Cybersecurity**

Link: *[text obscured/blurred]*