SPACE CYBERSECURITY WEEKLY WATCH

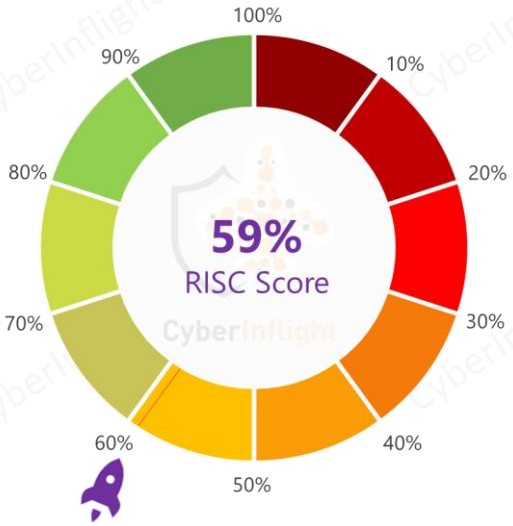
Week 29
July 16 – 22, 2024

Timeframe : Weekly
# of articles identified : 38
Est. time to read : 75 minutes

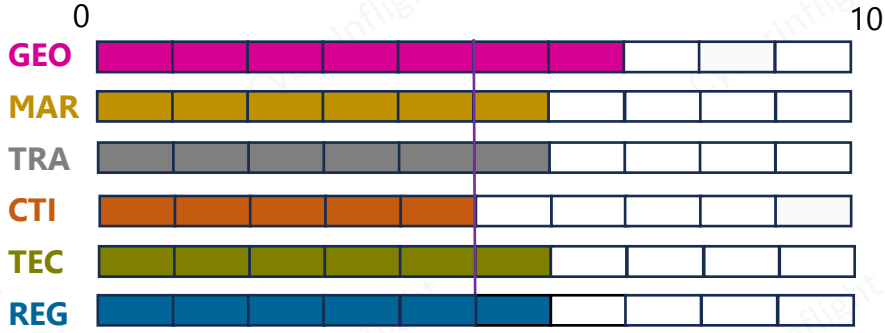
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

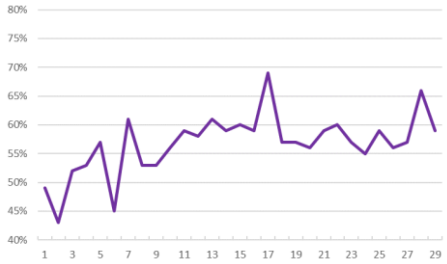
Overview & Resilience Index for Space Cybersecurity (RISC)



7 percentage points of decrease from last week (from 66% to 59%)



RISC Score Evolution



After struggling to recover since the drop from W18 and finally rising on W28, the RISC score (the tool used to assess cybersecurity resilience in space) is back down slightly.

This week's RISC score is 59%. In geopolitical news, the US Space Force revealed that the US is installing a new ground-based jammer designed to prevent Chinese or Russian satellites from sharing information, about US forces, during an attack. The first 11 of 24 of these devices will be deployed in undisclosed locations before the end of the year. On the technology front, after two Finnair planes flying to Estonia recently had to return to Helsinki due to GPS spoofing, Finnair is now beginning to implement real quantum navigation systems to prevent such incidents from occurring in the future. On the market front, the US Department of Transportation has awarded contracts to nine suppliers specializing in complementary PNT technologies. These contracts are designed to enhance the safety and reliability of GPS and improve the resilience of PNT by instrumenting, testing, and evaluating complementary PNT technologies at various field test sites. In other news, the Aspen Security Forum was held July 16-19 in Colorado. There was a panel on "Infinity and Beyond: Space and National Security," which focused on opportunities and threats in space. On the regulatory front, the UK will introduce a Cyber Security and Resilience Bill to strengthen the nation's cyber defenses and secure critical infrastructure. This initiative aims to protect businesses that rely on cyberspace. Lastly, 2024 Olympics are approaching, and given their heavy reliance on satellites, this event is an attractive target for malicious actors with different motivations. Strong and broad mitigation measures are needed to address these threats.

GEOPOLITIC

US prepares jamming devices targeting Russia, China satellites

The Space Force disclosed that the US is about to deploy a new ground-based jammer designed to blunt Chinese or Russian satellites from transmitting information about US forces during a conflict. These devices aren't meant to protect US satellites from Chinese or Russian jamming but "to responsibly counter adversary satellite communications capabilities that enable attacks. **#China #Russia**

Link: https://www.bnnbloomberg.ca/business/international/2024/07/19/us-prepares-jamming-devices-targeting-russia-china-satellites/

Russia is ready to counter US plans for 'satellite jammers' in space

[redacted]

The US Space Force: pioneering America's military dominance in the final frontier

[redacted]

Putin and China 'both developing weapons to attack US assets in space'

[redacted]

The latest information on China's cyberwarfare capabilities and the Strategic Support Force

[redacted]

Rising tensions over outer space – a new diplomatic hot zone

[redacted]

TECHNOLOGY

[redacted]

Opinion: Reliable GPS is coming to an end – but new quantum technologies could show the path forward

Using a quantum-assured navigation system, a vehicle may be able to position itself precisely even when GPS is not available for very long periods. To prevent a repeat of the Finnair event, real quantum navigation systems are now starting to undergo field testing. **#QuantumNavigation #Finland**

Link: https://www.thestar.com.my/tech/tech-news/2024/07/19/opinion-reliable-gps-is-coming-to-an-end---but-new-quantum-technologies-could-show-the-path-forward

[redacted]

[redacted]

MARKET & COMPETITION

US DOT awards contract for complementary PNT technology

The US Department of Transportation (DOT) has awarded contracts to nine vendors specializing in complementary positioning, navigation, and timing (PNT) technologies. These contracts aim to enhance the security and reliability of the GPS, totaling more than $7.2 million. They will fund the instrumentation, testing, and evaluation of Complementary PNT technologies at various field test ranges. This initiative, executed through the Volpe Center in response to the DOT Complementary PNT Action Plan, aims to facilitate the adoption of these technologies to improve PNT resiliency. **#DOT #PNT**

Link: https://www.militaryaerospace.com/communications/article/55126099/us-dot-awards-contracts-for-complementary-pnt-technology

[redacted]

[redacted]

[redacted]

TRAINING & EDUCATION

Military experts highlight space opportunities, threats at Aspen Conference

The 15th Annual Aspen Security Forum was held July 16-19. There was a panel on "Infinity and Beyond: Space and National Security," which focused on opportunities and threats in space. **#Conference #Space**

Link: https://www.defense.gov/News/News-Stories/Article/Article/3843526/military-experts-highlight-space-opportunities-threats-at-aspen-conference/

REGULATION

[redacted]

[redacted]

UK set to debut Cyber Security and Resilience Bill to boost national cyber defenses, secure critical infrastructure

The U.K. government is poised to introduce the Cyber Security and Resilience Bill into Parliament in the coming months. The move is expected to 'strengthen the UK's cyber defenses, ensure that critical infrastructure and the digital services that companies rely on are secure. **#UK #CriticalInfrastructure**

Link: https://industrialcyber.co/regulation-standards-and-compliance/uk-set-to-debut-cyber-security-and-resilience-bill-to-boost-national-cyber-defenses-secure-critical-infrastructure/

THREAT INTELLIGENCE

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

THREAT INTELLIGENCE

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Cybersecurity at major global events: satellite security insights for the 2024 Olympics

Satellites play a strategic role in supporting various aspects of the Olympics, ranging from communication, navigation, and security surveillance, to broadcasting. However, this dependence also opens up opportunities for various types of cyber-attacks. An event as large as the Olympics will always be a prime target for various motives, such as sabotage, espionage, political disinformation, undermining the host's reputation, spreading fear and anxiety worldwide, and financial gain. **#2024Olympics #SpaceCybersecurity**

Link: https://moderndiplomacy.eu/2024/07/19/cybersecurity-at-major-global-events-satellite-security-insights-for-the-2024-olympics/

[redacted]

[redacted]

[redacted]

[redacted]

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