SPACE CYBERSECURITY WEEKLY WATCH

Week 33

August 13 – 19, 2024

Timeframe : Weekly

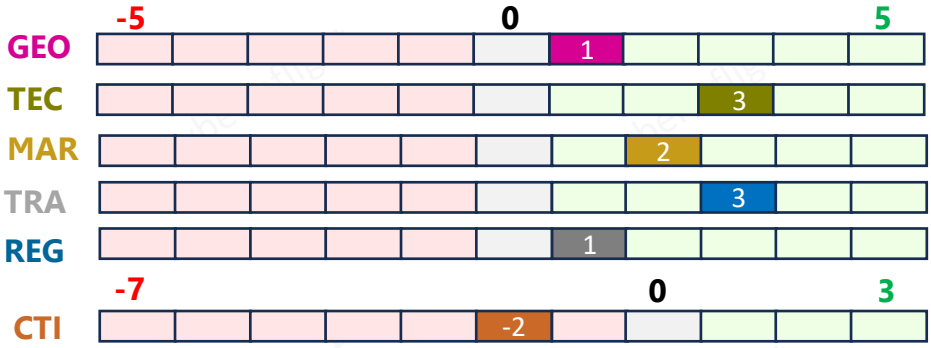
# of articles identified : 26

Est. time to read : 45 minutes

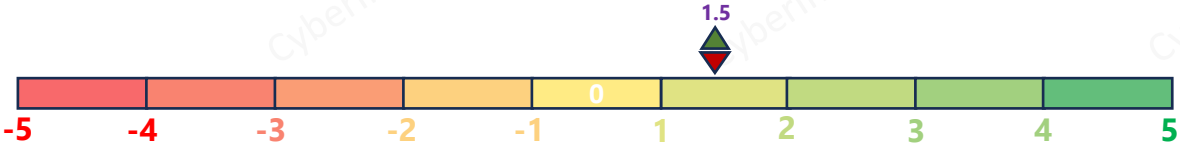
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score Assesment



Methodology Change : In our latest weekly watch, we've refined our approach to assessing the RISC score by incorporating advanced analytics and updated metrics. This enhanced methodology allows for a more accurate and comprehensive evaluation of emerging threats with most reliable and actionable insights.

This week's RISC score is 1.5. On the geopolitical front, South Korea is preparing to launch a new spy satellite as part of its efforts to bolster national security and surveillance capabilities. This satellite will play a critical role in monitoring regional activities, particularly concerning North Korea. On the technological side, there is growing trend in the adoption of satellite enabled Industrial Internet of Things (IIoT) connectivity. Companies are increasingly utilizing these technologies to optimize Supervisory Control and Data Acquisition (SCADA) systems, particularly in remote or challenging environments where traditional connectivity options fall short. On the market front, industry experts from across government, defence, business and academia will take part in the conference and exhibition at SEC Glasgow from 11-12 September. On the regulatory front, The National Institute of Standards & Technology officially released the long-awaited final versions of three new post-quantum encryption algorithms. On the Threat Intel, according to a military spokesperson, Ukraine's military attacked and destroyed an idle gas platform off Crimea, which Russian units had used as a broadcasting station for GPS interference equipment. Lastly, an informative read, as spoofing is becoming a prevalent threat to the users of Global Navigation Satellite Systems (GNSS). It is important to deepen our understanding of spoofing attacks and develop resilient techniques to effectively combat this threat. Detecting and mitigating these attacks requires thorough testing, typically conducted in a laboratory environment through the establishment of a spoofing test-bed.

GEOPOLITICS

[redacted]

South Korea to launch spy satellite for enhanced surveillance amid rising tensions

South Korea is preparing to launch a new spy satellite as part of its efforts to bolster national security and surveillance capabilities. This satellite will play a critical role in monitoring regional activities, particularly concerning North Korea. The mission represents a significant step in South Korea's strategy to enhance its intelligence-gathering abilities and maintain a strategic edge in the region. The satellite is expected to provide real-time data and high-resolution imagery, supporting both military operations and broader national security objectives. **#NationalSecurity #Surveillance**

Link: https://www.straitstimes.com/asia/east-asia/south-korea-s-spy-satellite-to-start-full-fledged-mission

MARKET & COMPETITION

[redacted]

Space expo in Glasgow set to welcome over 3,000 attendees

Industry experts from across government, defence, business and academia will take part in the conference and exhibition at SEC Glasgow from 11-12 September. The programme agenda includes: The UK's leadership in space, strategic goals for scotland's space sector, investment in the new space economy, space law symposium, cyber-security.

#Conference #Glasgow

Link: https://futurescot.com/space-expo-in-glasgow-set-to-welcome-over-3000-attendees/

[redacted]

[redacted]

[redacted]

TECHNOLOGY

Satellite-enabled IIoT connectivity gains traction

FreeWave's research reveals a growing trend in the adoption of satellite-enabled Industrial Internet of Things (IIoT) connectivity. Companies are increasingly utilizing these technologies to optimize Supervisory Control and Data Acquisition (SCADA) systems, particularly in remote or challenging environments where traditional connectivity options fall short. **#IIoT #SCADA**

Link: https://www.satcom.digital/news/new-freewave-research-reveals-satellite-enabled-iiot-connectivity-gains-traction-as-senior-leaders-look-to-optimize-productivity-scada-and-data

THREAT INTELLIGENCE

[redacted]

Ukraine destroys an offshore platform used for GPS spoofing

Last week, the Ukrainian Navy launched an operation to fight back against Russian GPS spoofing with force. According to a spokesperson, Ukraine's military attacked and destroyed an idle gas platform off Crimea, which Russian units had used as a broadcasting station for GPS interference equipment. **#Ukraine #GPS**

Link: https://rntfnd.org/2024/08/16/ukraine-destroys-an-offshore-platform-used-for-gps-spoofing-maritime-executive/

[redacted]

[redacted]

REGULATION

'No time to waste': NIST formally issues standards for defense against quantum hacking

The National Institute of Standards & Technology officially released the long-awaited final versions of three new post-quantum encryption algorithms, with additional, more specialized algorithms on the way. They are all designed to defend against future hacks carried out by quantum computers, an unproven but rapidly developing threat that could quickly crack the kinds of encryption used almost universally today, including those used in the most sensitive Pentagon systems. **#NIST #Quantum**

Link: https://breakingdefense.com/2024/08/no-time-to-waste-nist-formally-issues-standards-for-defense-against-quantum-hacking/

[redacted]

[redacted]

[redacted]

[redacted]

TRAINING & EDUCATION

An open GNSS spoofing data repository: characterization and impact analysis with FGI-GSRx open-source software-defined receiver

Spoofing is becoming a prevalent threat to the users of Global Navigation Satellite Systems (GNSS). It is important to deepen our understanding of spoofing attacks and develop resilient techniques to effectively combat this threat. Detecting and mitigating these attacks requires thorough testing, typically conducted in a laboratory environment through the establishment of a spoofing test-bed. **#GNSS #Spoofing**

Link: https://link.springer.com/article/10.1007/s10291-024-01719-2

[redacted]