



SPACE CYBERSECURITY WEEKLY WATCH

Week 33

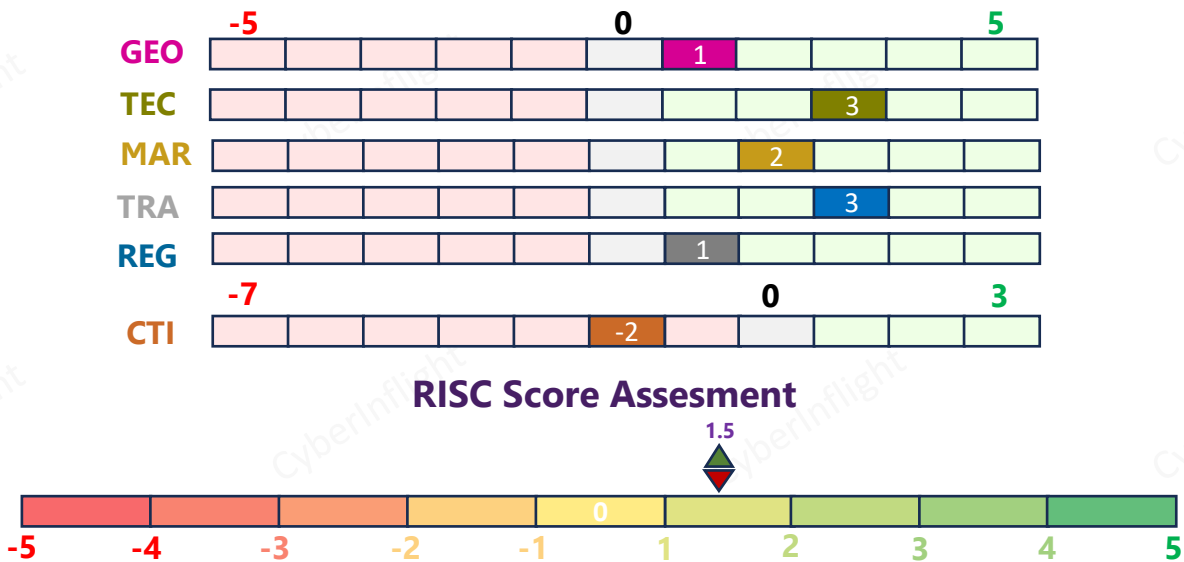
August 13 – 19, 2024

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)



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.



GEO POLITICS

White House advisory group warns US government, full cooperation to US space

The independent White House advisory group on US space is calling the US government to end its policy of allowing its defense contractors to do business with the foreign arms market, and to end its practice of selling advanced military, intelligence, and other US military systems, suggesting that control of US facilities should be under the control of the US government.

Link: [https://www.defenseone.com/analysis/2024/08/13/white-house-advisory-group-warns-us-space-2024/](#)



★ 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

The space - secure satellite communication in the battlefield

Secure satellite communication systems are being developed and tested, offering a significant advantage in military operations. These systems provide a secure and reliable means of communication, even in the face of jamming and interception. The use of satellite communication in the battlefield is becoming increasingly important as the need for secure and reliable communication grows.

Link: [https://www.defenseone.com/analysis/2024/08/13/space-secure-satellite-communication-in-the-battlefield/](#)



★ 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/>



Why Space Force says US military needs to be defense strategy

Space Force is calling for the US military to be a defense strategy, and that's why it's important to have a strong space program. Space is becoming an increasingly important part of the national security strategy, and the US military needs to be prepared to defend its interests in space.

Link: [https://www.defenseone.com/analysis/2024/08/13/why-space-force-says-us-military-needs-to-be-defense-strategy/](#)



Analysis to explore potential benefits from space

Analysis has been conducted to explore the potential benefits from space, including the development of new satellite systems and the use of space for a variety of purposes. The analysis shows that space offers a wide range of opportunities for innovation and growth, and that the US has a significant lead in space technology.

Link: [https://www.defenseone.com/analysis/2024/08/13/analysis-to-explore-potential-benefits-from-space/](#)



USAF expands work partnership with Lockheed

The US Air Force is expanding its partnership with Lockheed Martin, a leading aerospace and defense contractor. The partnership will focus on the development and production of advanced aircraft and missile systems, and will help to strengthen the US military's capabilities in the air and space.

Link: [https://www.defenseone.com/analysis/2024/08/13/usaf-expands-work-partnership-with-lockheed/](#)





THREAT INTELLIGENCE



The growing threat to GPS is a cyber issue

The growing threat to GPS is a cyber issue. According to a report from the House Select Committee on Intelligence, Russian units have used GPS spoofing to interfere with GPS signals and disrupt GPS systems. #GPS #Cyber



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/>



Russia targets the satellites of Israel

Russia has targeted the satellites of Israel. According to a report from the House Select Committee on Intelligence, Russian units have used GPS spoofing to interfere with GPS signals and disrupt GPS systems. #Israel #GPS



Russia targets the satellites of NATO

Russia has targeted the satellites of NATO. According to a report from the House Select Committee on Intelligence, Russian units have used GPS spoofing to interfere with GPS signals and disrupt GPS systems. #NATO #GPS



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/>



The space race the European Union is in

The space race the European Union is in. According to a report from the House Select Committee on Intelligence, the EU is competing with the US and China for leadership in space. #EU #Space



Russia sets new law concerning public-private partnerships (PPPs) in the space sector

Russia sets new law concerning public-private partnerships (PPPs) in the space sector. According to a report from the House Select Committee on Intelligence, the Russian government has passed a law that will allow for more private investment in space. #Russia #Space



Defense-related laws require increased commercial space tech adoption

Defense-related laws require increased commercial space tech adoption. According to a report from the House Select Committee on Intelligence, the US government is pushing for more commercial space tech to be used in defense. #US #Space



US program (NSA) is a key for enhanced cybersecurity

US program (NSA) is a key for enhanced cybersecurity. According to a report from the House Select Committee on Intelligence, the NSA is working on a program to enhance cybersecurity. #NSA #Cyber





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>

[Blurred text from the article abstract, including the title and authors.]



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

