SPACE CYBERSECURITY WEEKLY WATCH

Week 34

August 20 – 26, 2024

Timeframe : Weekly

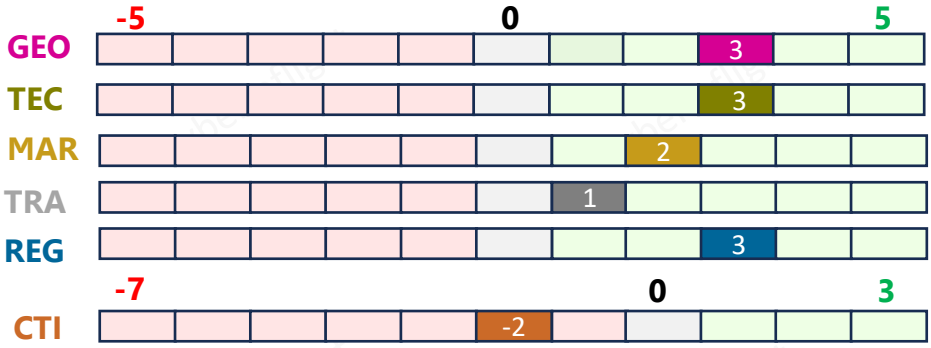
# of articles identified : 41

Est. time to read : 75 minutes

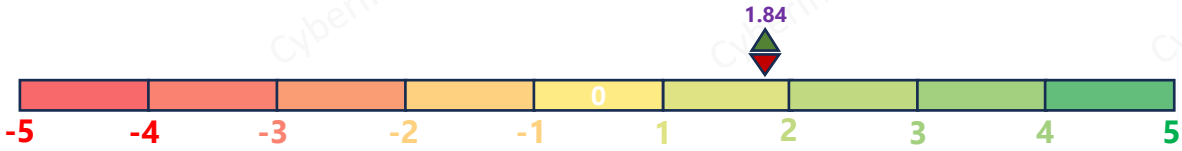
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score Assesment



This week's RISC score is 1.84, a slight increase from last week, mainly due to geopolitical factor as nation shows more interest in buying satellite technology.

On the geopolitical front, Japan and India have held their latest "2+2" ministerial dialogue, focusing on cybersecurity cooperation and joint efforts. This partnership is seen as a strategic move to counter regional threats and ensure a free and open Indo-Pacific. On the technological side, Chinese researchers have successfully demonstrated space-to-ground communications using a lightweight quantum satellite, advancing Quantum Key Distribution (QKD) technology. This innovation is a significant leap in secure communications, potentially revolutionizing global cybersecurity. On the market front, the UK is investing £20 million in a state-of-the-art anti-jamming test facility to enhance the resilience of GPS and other critical infrastructure against electronic warfare threats. This facility aims to support the development of advanced anti-spoofing and jamming technologies essential for national security and defense operations. On the Threat Intel side, Defence and Security multinational Thales released its 2024 Critical Infrastructure report, and it makes for some grim reading. One of the key figures is that ransomware attacks on critical infrastructure (CI) entities have increased year on year, with 24% reporting an attack in the last 12 months, compared to 21% for the previous reporting period. On the regulatory front, HR 8965, the Spacecraft Cybersecurity Act which would require NASA acquisition processes to include guidelines and controls for managing cybersecurity risks. Lastly, a informative BALPA's webinar is being organized which covers the important and topical issue of GPS jamming and spoofing.

GEOPOLITICS

Japan, India to accelerate space, cyber security cooperation; set to confirm revision of joint declaration at 2+2 meeting

Japan and India have held their latest "2+2" ministerial dialogue, focusing on cybersecurity cooperation and joint efforts in regional geopolitics. This partnership is seen as a strategic move to counter regional threats and ensure a free and open Indo-Pacific. **#Japan #India**

Link: https://japannews.yomiuri.co.jp/politics/defense-security/20240817-205556/

MARKET & COMPETITION

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

UK to build $20M anti-jamming test facility

The UK is investing £20 million in a state-of-the-art anti-jamming test facility to enhance the resilience of GPS and other critical infrastructure against electronic warfare threats. This facility aims to support the development of advanced anti-spoofing and jamming technologies essential for national security and defense operations. **#UK #AntiJamming**

Link: https://rntfnd.org/2024/08/23/uk-to-build-huge-new-20m-anti-jamming-test-facility-uk-defense-journal/

TECHNOLOGY

[redacted]

[redacted]

China advances QKD with Lightweight quantum satellite

Chinese researchers have successfully demonstrated space-to-ground communications using a lightweight quantum satellite, advancing Quantum Key Distribution (QKD) technology. This innovation is a significant leap in secure communications, potentially revolutionizing global cybersecurity. **#QuantumSecurity #QKDInnovation**

Link: https://syntony-gnss.com/news/tech/the-crucial-role-of-gnss-testing-against-spoofing-attacks

TECHNOLOGY

Protecting military space technology from bad actors

The crucial role of GNSS testing against spoofing attacks

Furuno to participate in Jammertest 2024, the world's largest GNSS resilience testing event

GPS Spoofing With HackRF One

Global quantum key encryption: Nano-Satellite QUBE launches into Space

The military applications of Artificial Intelligence in space

Ingalls Information Security to showcase cutting-edge cybersecurity solutions at 2024 Air, Space & Cyber Conference

Ground Control to Major Threat: Hacking the Space Link Extension Protocol

2024 Africa Aerospace & Defence Conference

REGULATION

[redacted]

[redacted]

Review - HR 8965 introduced – NASA cybersecurity

Last month, Frost introduced HR 8965, the Spacecraft Cybersecurity Act. The bill would require NASA acquisition processes to include guidelines and controls for managing cybersecurity risks. Frost is a member of the House Science, Space, and Technology Committee to which this bill was assigned for consideration. This means that there may be sufficient influence to see the bill considered in Committee. Nothing in this bill would engender any organized opposition but it is suspected that there would be bipartisan support for the bill to be approved in Committee.
#NASA #Act

Link: https://chemical-facility-security-news.blogspot.com/2024/08/review-hr-8065-introduced-nasa.html

[redacted]

[redacted]

[redacted]

TRAINING & EDUCATION

BALPA's GPS Spoofing and Jamming Webinar

BALPA webinar covering the important and topical issue of GPS Jamming and Spoofing. Combined with representatives from Boeing and Airbus, BALPA's Stuart A. Clarke will be moderating the webinar before introducing presentations from Ian Goodwin and Dr. Kirk Vining, followed by a Q&A session. **#Webinar #Spoofing**

Link: https://www.youtube.com/watch?v=2kkIA-gRZVw

[redacted]

[redacted]

THREAT INTELLIGENCE

[redacted]

Thales 2024 critical infrastructure report reveals a rise in ransomware and a lack of readiness

Defence and security multinational Thales released its 2024 Critical Infrastructure report last week, and it makes for some grim reading. One of the key figures is that ransomware attacks on critical infrastructure (CI) entities have increased year on year, with 24 per cent reporting an attack in the last 12 months, compared to 21 per cent for the previous reporting period. **#Thales #CriticalInfra**

Link: https://www.cyberdaily.au/security/10980-thales-2024-critical-infrastructure-report-reveals-a-rise-in-ransomware-and-a-lack-of-readiness

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]