SPACE CYBERSECURITY WEEKLY WATCH

Week 42

October 15 - 21, 2024

Timeframe: Weekly

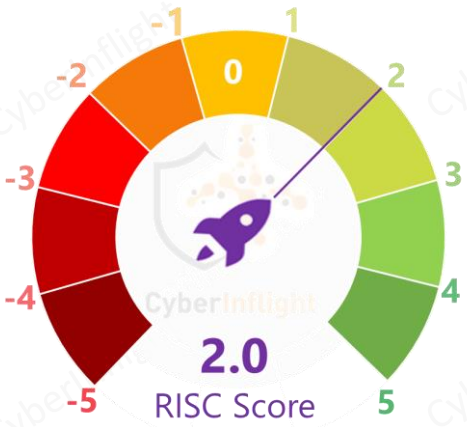
# of articles identified: 36

Est. time to read: 75 minutes

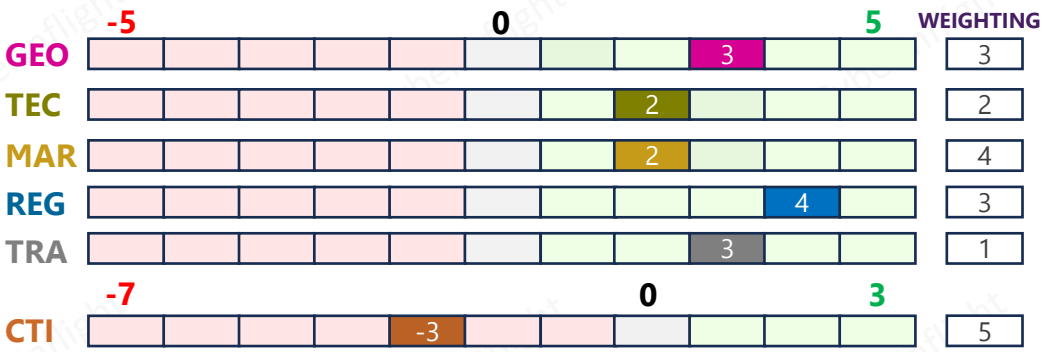
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

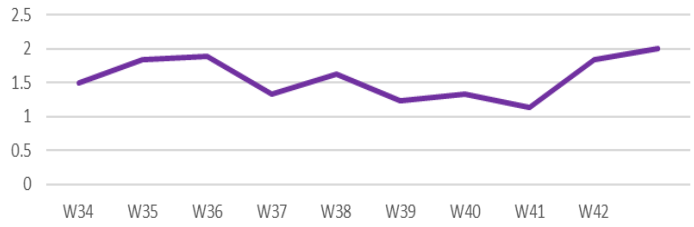
RISC Score Assesment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score Evolution



This week's RISC score stands at 2.0, primarily driven by a favorable geopolitical climate and the implementation of regulatory frameworks that support market growth.

On the geopolitical front, Italy and the US are enhancing their collaboration in space with plans that include joint satellite launches and improved domain awareness. The partnership aims to bolster both nations' space defense capabilities while fostering cooperation in emerging technologies and intelligence sharing. On the technological side, Chinese scientists have made significant strides in quantum computing, using it to crack military-grade encryption like RSA and AES. This quantum breakthrough presents a substantial threat to current encryption standards, potentially undermining the security of sensitive data worldwide. On the market front, CYSEC has been awarded a major contract by the European Space Agency (ESA) to protect satellite operations under its General Support Technology Programme (GSTP). On the threat intel side, the Cybersecurity and Infrastructure Security Agency's (CISA) has issued a warning about Iranian cyber actors using brute force and credential access tactics to compromise critical infrastructure in the US. Meanwhile, Ukraine's GUR cyber unit has successfully carried out a cyberattack targeting Russian satellite communications. On the regulatory front, the EU Commission has adopted new cybersecurity rules to enhance the resilience of critical digital infrastructure under the NIS2 directive, whereas the CISA Cybersecurity Advisory Committee (CSAC) has approved draft reports aimed at strengthening national cyber resilience. These regulations address vulnerabilities in critical infrastructure sectors and propose measures to enhance their defense against cyberattacks. Lastly, space system designers face increasing challenges in embedding cyber resilience into their processes. Insights from recent Australian studies reveal limitations in current design frameworks that make space assets vulnerable to cyberattacks.

GEOPOLITICS

Italy, US space cooperation plan includes launch, domain awareness

Italy and US are enhancing their collaboration in space with plans that include joint satellite launches and improved domain awareness. The partnership aims to bolster both nations' space defense capabilities while fostering cooperation in emerging technologies and intelligence sharing. This marks a significant step in strengthening transatlantic space ties in an increasingly competitive environment. **#Cooperation #Italy**

Link: https://breakingdefense.com/2024/10/italy-us-space-cooperation-plan-includes-launch-domain-awareness/

MARKET & COMPETITION

MARKET & COMPETITION

CYSEC wins European Space Agency contract to protect satellite operations

CYSEC has been awarded a major contract by the European Space Agency (ESA) to protect satellite operations under its General Support Technology Programme (GSTP). The Swiss cybersecurity firm will focus on enhancing the security of satellite communications, addressing the growing need for secure operations in the increasingly competitive space domain. **#CYSEC #ESA**

Link: https://www.cysec.com/gstp/

[redacted]

TECHNOLOGY

[redacted]

[redacted]

[redacted]

[redacted]

Chinese scientists use quantum computers to crack military-grade encryption quantum attack poses a "real and substantial threat" to RSA and AES

Chinese scientists have made significant strides in quantum computing, using it to crack military-grade encryption like RSA and AES. This quantum breakthrough presents a substantial threat to current encryption standards, potentially undermining the security of sensitive data worldwide. The development emphasizes the urgent need for advancements in post-quantum cryptography (PQC) to counter this emerging risk. **#PQC #AES**

Link: https://www.tomshardware.com/tech-industry/quantum-computing/chinese-scientists-use-quantum-computers-to-crack-military-grade-encryption-quantum-attack-poses-a-real-and-substantial-threat-to-rsa-and-aes

REGULATION

CSAC approves draft reports to strengthen national cyber resilience, address critical infrastructure vulnerabilities

The Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Advisory Committee (CSAC) has approved draft reports aimed at strengthening national cyber resilience. These reports address vulnerabilities in critical infrastructure sectors and propose measures to enhance their defense against cyberattacks. The initiative underscores the urgency of protecting essential services from emerging threats in a rapidly evolving cyber landscape. **#CSAC #CriticalInfra**

Link: https://industrialcyber.co/reports/csac-approves-draft-reports-to-strengthen-national-cyber-resilience-address-critical-infrastructure-vulnerabilities/

[redacted]

[redacted]

[redacted]

EU Commission adopts initial cybersecurity rules to enhance critical digital infrastructure resilience

The EU Commission has adopted new cybersecurity rules aimed at enhancing the resilience of critical digital infrastructure under the NIS2 directive. These regulations focus on improving the security posture of essential services, ranging from energy to telecommunications, as the EU steps up efforts to protect its digital ecosystem from growing cyber threats. **#EU #NIS2**

Link: https://industrialcyber.co/regulation-standards-and-compliance/eu-commission-adopts-initial-cybersecurity-rules-to-enhance-critical-digital-infrastructure-resilience/

[redacted]

[redacted]

[redacted]

[redacted]

THREAT INTELLIGENCE

[redacted]

Iranian cyber actors' brute force and credential access activity compromises critical infrastructure organizations

CISA has issued a warning about Iranian cyber actors using brute force and credential access tactics to compromise critical infrastructure in the US. The attackers are focusing on energy, transportation, and healthcare systems, underscoring the urgent need for stronger cybersecurity defenses to mitigate these persistent threats. **#CISA #Iran**

Link: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-290a

[redacted]

[redacted]

[redacted]

[redacted]

GUR cyber specialists attack satellite communications in Russia

Ukraine's GUR cyber unit has successfully carried out a cyberattack targeting Russian satellite communications. This strategic move is part of Ukraine's ongoing efforts to disrupt Russian military operations, demonstrating the increasing role of cyber warfare in modern conflicts. **#Ukraine #GUR**

Link: https://unn.ua/en/news/gur-cyber-specialists-attack-satellite-communications-in-russia

[redacted]

[redacted]

TRAINING & EDUCATION

[redacted]

[redacted]

Cyber resilience limitations in space systems design process: insights from space designers

Designers of space systems are facing increasing challenges in embedding cyber resilience into their processes. Insights from recent studies reveal limitations in current design frameworks that make space assets vulnerable to cyberattacks. The findings suggest a growing need for more robust and adaptable cybersecurity measures to safeguard critical space infrastructure. **#Design #Resilience**

Link: https://www.mdpi.com/2079-8954/12/10/434

[redacted]

[redacted]

[redacted]