SPACE CYBERSECURITY WEEKLY WATCH

Week 44
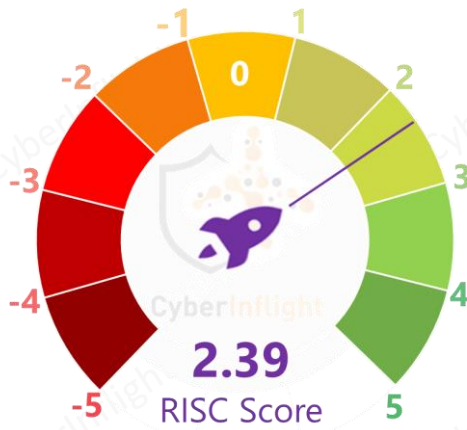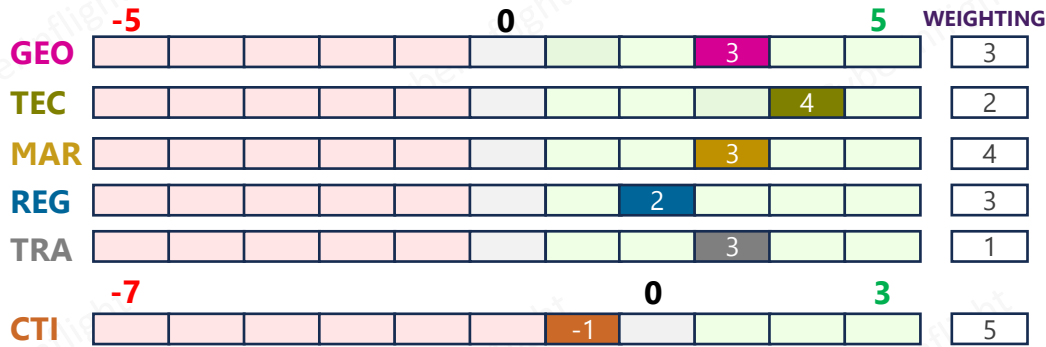
October 29 – November 4, 2024

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

Timeframe: Weekly

# of articles identified: 23

Est. time to read: 45 minutes

- 🟪 **GEOPOLITICS**
- 🟫 **TECHNOLOGY**
- 🟨 **MARKET INTELLIGENCE**
- 🟦 **REGULATION**
- ⬜ **TRAINING & EDUCATION**
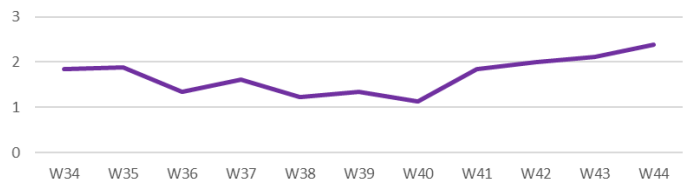- 🟧 **THREAT INTELLIGENCE**
- ⭐ **IMPORTANT NEWS**

RISC Score Assesment

2.39
RISC Score

Overview & Resilience Index for Space Cybersecurity (RISC)

	-5	0	5	WEIGHTING
GEO			3	3
TEC			4	2
MAR			3	4
REG		2		3
TRA			3	1

	-7	0	3	
CTI		-1		5

RISC Score Evolution

This week's RISC score is 2.39, reflecting an increase from the previous week, largely driven by news on technological innovation and positive developments in threat intelligence.

On the geopolitical front, the Space Information Sharing and Analysis Center (Space ISAC) is bolstering its cyber-threat intelligence operations with an expanded network that includes partnerships with key UK stakeholders. This collaborative effort aims to provide real-time alerts and intelligence-sharing to protect critical space infrastructure in both the US and the UK. On the technological side, Safran's new Vision navigation system has achieved a significant breakthrough by developing a jam-proof technology that promises enhanced navigation reliability. This innovation is particularly crucial for military and aerospace applications, where navigation integrity is critical. The system's robust design ensures it can withstand jamming attempts, providing accurate and uninterrupted navigation data. On the market front, the Occitanie region in France has just been selected to host one of the five Maisons du quantique (Quantum Houses) launched by the French government. This ambitious project aims to establish quantum internet via satellite, positioning Occitanie as a leader in this cutting-edge field. On the threat intel side, the US Space Force has restructured its operations with the launch of new Mission Deltas focused on improving Space Situational Awareness (SSA). On the regulatory front, Japan is proposing a new cybersecurity bill aimed at fortifying its critical infrastructure against increasing cyber-threats, particularly from state actors. The legislation would empower the government to set mandatory cybersecurity standards and regulations for industries, particularly those managing essential services such as utilities and telecommunications. Lastly, researchers at ETH Zurich have conducted an extensive study by trawling hacker forums, uncovering critical information about planned and past cyber attacks targeting space infrastructure.

GEOPOLITICS

Allies say 1953 mutual defense treaty extends to cyber, space threats

US and South Korea have reaffirmed their commitment to mutual defense, regarding the 1953 Mutual Defense Treaty to explicitly include cyber and space threats. This extension recognizes the growing importance of digital and extraterrestrial domains in modern warfare. Both nations will work together to counter cyber intrusions, space-based threats, and other challenges posed by adversaries in these domains. **#CyberDefense #SpaceSecurity**

Link: https://www.foxnews.com/news/1953-cyber-say-1953-mutual-defense-treaty-extends-to-cyber-space-threats

US Space Force warns of "mind-boggling" build up of Chinese capabilities

In a recent analysis, the US Space Force raised concerns over China's swift expansion in military space capabilities which includes satellite constellations and counter-space technology. The buildup is perceived as a direct challenge to the United States and its allies, pushing the US to re-evaluate its defense strategies in space. The advancements demonstrate China's increasing investment in space as a contested domain, adding pressure on the US to maintain its technological edge and protect its assets in orbit. **#MilitarySpace #USSF**

Link: https://arstechnica.com/space/2024/11/us-space-force-warns-of-mind-boggling-build-up-of-chinese-capabilities/

⭐ ### Facing growing threats, space industry expands its cyber warding center

The Space Information Sharing and Analysis Center (Space ISAC) is bolstering its cyber threat intelligence operations with an expanded network that includes partnerships with key UK stakeholders. This collaborative effort aims to provide real-time alerts and intelligence-sharing to protect critical space infrastructure in both the US and the UK. As cyber risks to satellites and related assets grow, Space ISAC's enhanced capabilities are expected to improve communication and responsiveness across borders, fostering a cooperative defense approach in the space cybersecurity domain. **#SpaceISAC #UK**

Link: https://www.airandspaceforces.com/facing-growing-threats-space-industry-expands-its-cyber-warning-center/?utm_source=rss&utm_medium=rss&utm_campaign=facing-growing-threats-space-industry-expands-its-cyber-warning-center

THREAT INTELLIGENCE

Interlock ransomware targets FreeBSD and critical infrastructure

The Interlock ransomware variant has recently started to target FreeBSD systems, posing a significant risk to sectors that rely on this open-source operating system, especially within critical infrastructure. Unlike previous ransomware, Interlock exploits unique vulnerabilities in FreeBSD, adding complexity to mitigation efforts. This emerging threat highlights the need for specialized protections within organizations that utilize open-source software to support essential operations. **#InterlockRansomware #Criticality**

Link: https://cybersecuritynews.com/interlock-ransomware-targets-freebsd-and-critical-infrastructure/

Finland faces new jamming threats amid rising tensions

Finland has reported a series of jamming incidents that threaten the security and reliability of its critical infrastructure. These jamming activities, believed to be a result of regional tensions, have disrupted GPS signals and communications, impacting both civilian and defense operations. The Finnish government is now prioritizing the development of anti-jamming measures and strengthening partnerships with neighboring countries to counter these threats. **#Finland #GPSJamming**

Link: https://yle.com/a/f8aaaraaa/status/1b1d534741738384013

⭐ ### Space Force stands up new mission Deltas to oversee SSA, missile tracking

US Space Force has restructured its operations with the launch of new Mission Deltas focused on improving Space Situational Awareness (SSA). These units, designated as Mission Delta 2 and Mission Delta 4, are tasked with monitoring space activity and addressing potential threats. This restructuring underscores the Space Force's commitment to maintaining a clear, real-time picture of the space domain as adversarial activities increase in orbit. **#USSF #SSA**

Link: https://executivegov.com/2024/11/space-force-new-integrated-mission-deltas/

MARKET & COMPETITION

[illegible]

★ L'Occitanie, tête de pont de l'internet quantique par satellite *(Trad: Occitanie Region in France leads quantum internet by satellite initiative)*

The Occitanie region in France is spearheading an ambitious project to establish quantum internet via satellite, positioning itself as a leader in this cutting-edge field. This initiative aims to develop a secure, high-speed quantum communication network that leverages satellite technology. By focusing on quantum internet, Occitanie is set to drive significant advancements in cybersecurity and data transmission, ensuring the region remains at the forefront of technological innovation. **#QuantumInternet #Occitanie**

Link: https://toulouse.latribune.fr/entreprises/business/2024-10-28/l-occitanie-tete-de-pont-de-l-internet-quantique-par-satellite-1009661.html

TECHNOLOGY

★ Unaffected by jamming, the revolutionary French navigation system VISION delivers on its promises

Safran's new Vision navigation system has achieved a significant breakthrough by developing a jam-proof technology that promises enhanced navigation reliability. This innovation is particularly crucial for military and aerospace applications, where navigation integrity is critical. The system's robust design ensures that it can withstand jamming attempts, providing accurate and uninterrupted navigation data. Safran's achievement is a major step forward in secure navigation technology. **#JamProofNavigation #Safran**

Link: https://indiandefencereview.com/french-vision-navigation-system-jam-proof-breakthrough-delivers-promises/

[illegible]

CyberInflight

TECHNOLOGY

Successful demo showcases BAE Systems' next gen M-Code GNSS technology

[blurred text]

Link:
[blurred link]

Royal Navy tests quantum positioning system for GPS-Denied navigation

[blurred text]

Link: [blurred link]

Scientists create a quantum information bridge between photonic and solid state quantum systems

[blurred text]

Link: [blurred link]

Nanosatellites & DeFiN: Spacecoin XYZ to create the first blockchain network in space

[blurred text]

Link: [blurred link]

Logos Space, a new satellite company built for EW Era, launches to provide enterprise connectivity

[blurred text]

Link: [blurred link]

REGULATION

⭐ **Will Japan's cybersecurity bill become a reality?**

Japan is proposing a new cybersecurity bill aimed at fortifying its critical infrastructure against increasing cyber threats, particularly from state actors. The legislation would empower the government to set mandatory cybersecurity standards and regulations for industries, particularly those managing essential services such as utilities and telecommunications. This regulatory push reflects Japan's growing concern about digital vulnerabilities, especially with upcoming international events that could attract cyber adversaries. If passed, the bill would be a landmark shift in Japan's approach to cybersecurity and infrastructure resilience. **#CyberSecurityBill #CriticalInfra**

Link: https://osintcorp.net/will-japans-cybersecurity-bill-become-a-reality/

TRAINING & EDUCATION

Development status and challenges of anti-spoofing technology of GNSS/INS integrated navigation

Recent advances in anti-spoofing technology are proving essential for GNSS/INS navigation systems, which are used widely in both defense and commercial sectors. These developments aim to protect location data from interference and manipulation, which are increasingly common threats. However, integrating anti-spoofing measures within complex GNSS/INS systems poses significant technical challenges. Researchers and developers continue to seek ways to refine these systems, ensuring more resilient and reliable navigation even in electronically contested environments.

#AntiSpoofing #ResearchPaper

Link:

https://www.mdpi.com/article/to/XXXX Development status and challenges of anti-spoofing technology of GNSS/INS integrated navigation

Trawling hacker forums uncovers crucial information on space cyber attacks

Researchers at ETH Zurich have conducted an extensive study by trawling hacker forums, uncovering critical information about planned and past cyber attacks targeting space infrastructure. This investigation highlights how cybercriminals share techniques, vulnerabilities, and tools specific to space systems on these forums. The insights gathered are invaluable for developing more robust cybersecurity defenses **#SpaceCyberAttack #ResearchPaper**

Link: https://interactive.satellitetoday.com/via/november-2024/trawling-hacker-forums-uncovers-crucial-information-on-space-cyber-attacks

Why space cybersecurity needs more imagination

The article discusses the urgent need for innovative approaches in space cybersecurity, citing the Icarus Matrix as a case study. Traditional methods are increasingly inadequate against sophisticated cyber threats targeting space infrastructure. By thinking creatively and leveraging interdisciplinary strategies, cybersecurity experts can better protect space systems. The Icarus Matrix serves as a framework for developing comprehensive defenses that anticipate and mitigate future cyber risks in space. **#SpaceCybersecurity #IcARUSMatrix**

Link: https://interactive.satellitetoday.com/via/november-2024/why-space-cybersecurity-needs-more-imagination

Cyberattacks on critical infrastructure: a ticking time bomb

As cyber attacks on critical infrastructure become more frequent and sophisticated, there is an urgent need for enhanced cybersecurity measures. The article explores recent incidents and the vulnerabilities exposed, emphasizing the importance of regulatory frameworks and proactive defenses. Education and awareness are key components to fortifying these essential systems against potential disruptions. The growing interdependence of global infrastructure makes robust cybersecurity practices a top priority. **#CriticalInfra #CyberDefense**

Link: https://thecybermagazine.com/cybersecurity-for-critical-infrastructure/