



SPACE CYBERSECURITY WEEKLY WATCH

Week 43

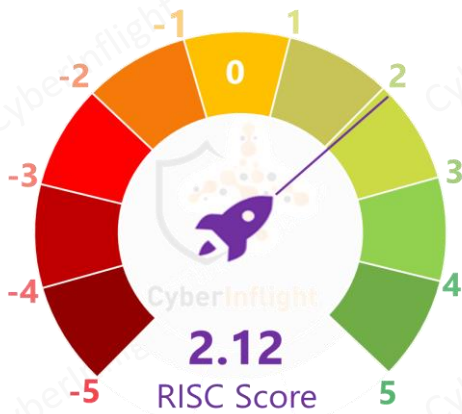
October 22 - 28, 2024

Timeframe: Weekly
of articles identified: 25
Est. time to read: 60 minutes

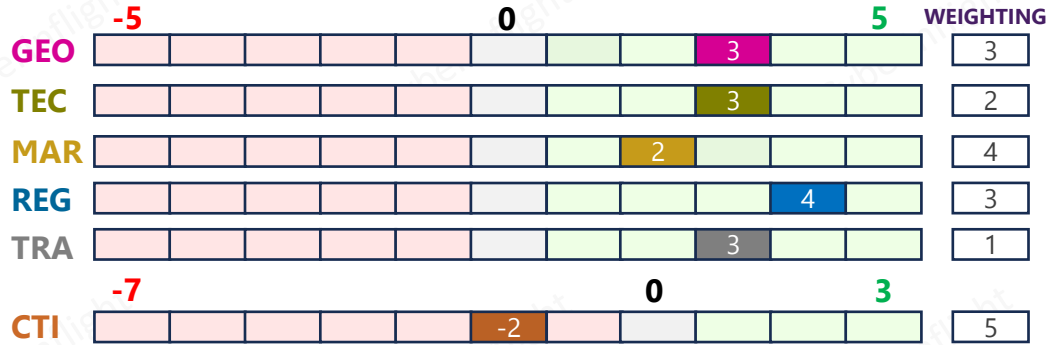
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

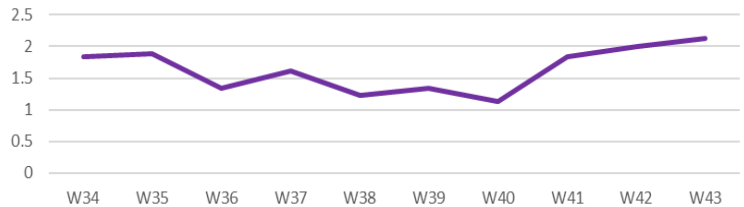
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score Evolution



This week's RISC score is 2.12, an increase from the previous week reflecting a stable yet dynamic environment due to recent technological innovations & decreased presence of high-severity threats in the ecosystem.

On the geopolitical front, the European Space Agency (ESA) has stated it will not comment on the ongoing merger discussions between Airbus Defence & Space and Thales Alenia Space, opting to focus on securing funding for existing and new projects with potential changes in European space industry dynamics. On the technological side, the US Space Force is reportedly advancing its "Meadowlands" project, designed to jam adversarial satellite signals as a countermeasure against potential threats. This jamming technology could disrupt enemy satellites, preventing adversaries from leveraging space-based communication or intelligence capabilities during conflict. On the market front, The European Space Agency (ESA) has selected GMV for the CyberCUBE mission, which aims to tackle cybersecurity threats in space. GMV will work on developing cybersecurity protocols and technologies to protect satellite infrastructure from cyber risks. CyberCUBE will assess vulnerabilities and propose innovative strategies to enhance satellite system resilience, ensuring secure data flow and system integrity in the growing space economy. On the threat intel side, amid rising cyber challenges, the Ukrainian military is exploring the creation of a dedicated cyber army branch. This new initiative is part of Ukraine's response to cyber threats posed by regional adversaries and aims to enhance the country's defensive cyber capabilities. On the regulatory front, NIST is pushing forward with developing post-quantum cryptography (PQC) standards, which are crucial for securing digital data in a future where quantum computing could easily break traditional encryption methods. Lastly, the European Space Agency's 4S Program, focused on supporting secure satellite operations and protecting European space assets, enhances space safety through targeted training initiatives.



CYBERINFLIGHT'S NEWS

Exploring aerospace cybersecurity with 'Tame the Drift' podcast launch episode

Florent Rizzo from CyberInflight joined the Tame the Drift Podcast to share his insights into the evolving landscape of aerospace cybersecurity. In a world where digital threats challenge satellite integrity, critical space assets, and more. Mr. Rizzo delves into the importance of robust threat intelligence and proactive cyber defenses to protect the aerospace ecosystem. **#AerospaceCybersecurity #Podcast**

Link: https://www.linkedin.com/posts/tame-the-drift-podcast_ep-1-tamethedrift-in-aerospace-cybersecurity-activity-7254416246081830912-aKzi?utm_source=share&utm_medium=member_desktop



CyberInFlight's Florent Rizzo nominated for CBC 2024 Cyber Talent award

Florent Rizzo, CEO of CyberInFlight, has been nominated for an award at the upcoming Cybersecurity Business Convention (CBC) 2024 in Toulouse, which celebrates notable advancements and achievements in cybersecurity. The CBC, a key annual event for cybersecurity leaders, promotes innovation, resilience, and the ongoing defense of digital infrastructures. Florent's nomination highlights his contributions to space cybersecurity, reflecting CyberInFlight's ongoing commitment to pioneering cybersecurity in aerospace. The CBC event will also feature discussions, panels, and workshops on critical issues such as emerging threats, regulatory updates, and new security technologies. **#CybersecurityLeadership #CBC2024**

Link: https://groupeladepeche.qualifioapp.com/quiz/1499891_138/cbc-2024-cyberstar.html



CyberInFlight attends IAC, Milan 2024, emphasizing space cybersecurity

CyberInFlight joined global space community at the IAC 2024, where cybersecurity emerged as a core theme. With over 24 papers, two technical sessions, and a plenary discussion dedicated to space cybersecurity, the event underscored the need for proactive measures to protect the growing space ecosystem. CyberInFlight is actively engaging with industry peers to drive solutions for the sector's critical security needs. Let's connect and collaborate to secure space.

#IAC #SpaceCybersecurity

Link: <https://www.linkedin.com/feed/update/urn:li:activity:7254884319549112320/>



GEOPOLITICS

US's rising concerns over GPS jamming and spoofing risks from China

A report from the US Space Force highlights growing concerns over GPS jamming and spoofing risks from China. The report states that China's military and intelligence agencies are increasingly using GPS spoofing and jamming to disrupt US military operations and intelligence gathering. This poses a significant threat to the US's ability to maintain its technological edge in space. The report also notes that China's actions are in violation of international law and could lead to further escalation of tensions between the two nations.

Link: <https://www.spaceintelreport.com/usa-we-wont-weigh-in-on-merger-talks-between-airbus-a-proposed-increase-in-contract-downpayments/>



ESA's stance on Airbus and Thales Alenia Space merger talks

The European Space Agency (ESA) has stated it will not comment on the ongoing merger discussions between Airbus Defence & Space and Thales Alenia Space, opting to focus on securing funding for existing and new projects. With potential changes in European space industry dynamics, ESA's role in negotiating increased contract down payments is seen as essential for advancing its programs amid an evolving landscape of private partnerships. **#ESA #EU**

Link: <https://www.spaceintelreport.com/esa-we-wont-weigh-in-on-merger-talks-between-airbus-a-proposed-increase-in-contract-downpayments/>



China launches new set of classified foreign spy satellite constellations

China has launched a new set of classified foreign spy satellite constellations, marking a significant step in its space intelligence capabilities. The new constellations are designed to provide high-resolution imagery and signals intelligence, enhancing China's ability to monitor global events and military movements. This development is seen as a direct challenge to the US's satellite-based intelligence gathering capabilities and could lead to a new arms race in space intelligence.

Link: <https://www.spaceintelreport.com/usa-we-wont-weigh-in-on-merger-talks-between-airbus-a-proposed-increase-in-contract-downpayments/>



MARKET & COMPETITION



ESA contracts GMV for CyberCUBE space cybersecurity mission

The European Space Agency (ESA) has selected GMV for the CyberCUBE mission, which aims to tackle cybersecurity threats in space. GMV will work on developing cybersecurity protocols and technologies to protect satellite infrastructure from cyber risks. CyberCUBE will assess vulnerabilities and propose innovative strategies to enhance satellite system resilience, ensuring secure data flow and system integrity in the growing space economy. **#ESA #Cybersecurity**

Link: https://www.spacewar.com/reports/GMV_wins_ESA_contract_for_CyberCUBE_space_cybersecurity_mission_999.html



TECHNOLOGY





TECHNOLOGY

★ US Space Force develops "Meadowlands" project to jam enemy satellites

US Space Force is reportedly advancing its "Meadowlands" project, designed to jam adversarial satellite signals as a countermeasure against potential threats. This jamming technology could disrupt enemy satellites, preventing adversaries from leveraging space-based communication or intelligence capabilities during conflict. Focused primarily on countering threats from nations like Russia and China, Meadowlands highlights the strategic importance of satellite jamming in modern defense, emphasizing the U.S. aim to maintain space superiority. **#USSF #SatelliteJamming**



Link: https://www.dailymail.co.uk/sciencetech/article-14001079/Secretive-American-weapon-JAMS-satellites.html?ns_mchannel=rss&ns_campaign=1490&ito=1490



REGULATION

★ NIST advances standards for post-quantum cryptography, securing digital future

NIST is pushing forward with developing post-quantum cryptography standards, which are crucial for securing digital data in a future where quantum computing could easily break traditional encryption methods. These standards are designed to ensure long-term cybersecurity resilience and trust in digital systems as quantum technology advances. This milestone is expected to play a critical role in protecting data across government, finance, and other sensitive sectors. **#PostQuantum #NIST**



Link: <https://decentcybersecurity.eu/nist-advances-post-quantum-cryptography-standards-astrategic-milestone-for-digital-security/>



TRAINING & EDUCATION

US Space Command's Strategic Plan Emphasizes Cyber Training for Space Operations
US Space Command's Strategic Plan (SSP) is a guiding document that serves as a critical component for identifying space needs and prioritizing operational security. With an increasing dependence on satellites for navigation, communications, and intelligence, ensuring the integrity of the data transmitted to and from space assets has become paramount. Training and education are essential to ensure that personnel are equipped with the necessary skills to protect and defend space operations. The SSP outlines a commitment to investing in space cyber training initiatives, ensuring personnel are well-versed in the complex and rapidly evolving space cyber threat landscape.

Key Takeaway:
The SSP emphasizes the importance of investing in space cyber training to ensure personnel are equipped to handle the growing space cyber threat.



Protecting global navigation systems from GNSS spoofing threats
A critical element of modern navigation capabilities is GNSS (Global Navigation Satellite System) systems. These systems are essential for a wide range of applications, from aviation and maritime navigation to precision agriculture and autonomous vehicles. However, GNSS systems are vulnerable to spoofing and jamming threats, which can have significant consequences. Protecting these systems from such threats is a high priority for governments and industry alike. This article explores the challenges of GNSS spoofing and the measures being taken to mitigate these risks.

Key Takeaway:
GNSS spoofing is a growing threat to global navigation systems, and robust security measures are needed to protect these critical infrastructure assets.

ESA's 4S Strategy: Enhancing space operations and safety through training
The European Space Agency (ESA) is committed to ensuring the safety and security of its operations. The 4S Strategy (Safety, Security, Sustainability, and Space) is a key component of this commitment. The strategy focuses on enhancing the resilience of space systems and ensuring the integrity of data transmitted to and from space assets. This includes investing in space cyber training initiatives to ensure personnel are well-versed in the complex and rapidly evolving space cyber threat landscape.

Key Takeaway:
ESA's 4S Strategy is a comprehensive approach to ensuring the safety and security of space operations, with a strong focus on training and education.



ESA's 4S program invests in space system safety training
The European Space Agency's 4S Program is enhancing space safety through targeted training initiatives. Focused on supporting secure satellite operations and protecting European space assets, the program includes simulations and hands-on modules to equip engineers and analysts with advanced skills in space system safety. ESA's commitment to workforce development in this field underlines its goal to strengthen Europe's strategic space infrastructure.

#SpaceSafety #ESA
Link: https://www.linkedin.com/posts/laurence-duquerroy-34183040_esa-europeanspaceagency-funding-activity-7252713221487308802-yV1u?utm_source=share&utm_medium=member_ios



US Space Command and USMC Collaborate on Space Cybersecurity and Safety Workshops
US Space Command and the United States Marine Corps (USMC) are collaborating on space cybersecurity and safety workshops. These workshops are designed to provide personnel with the necessary skills to protect and defend space operations. The workshops cover a wide range of topics, including space cyber threats, satellite operations, and the importance of training and education in this field.

Key Takeaway:
US Space Command and USMC are working together to ensure personnel are well-versed in the complex and rapidly evolving space cyber threat landscape.





THREAT INTELLIGENCE

Russia allegedly provides satellite intelligence to Israeli units for targeting and surveillance
Russia has been providing satellite data to Israeli units, which, along with its targeting intelligence, is being used by the Israeli Defense Forces (IDF) to conduct operations in Gaza. The intelligence is being used to identify and track Hamas targets, as well as to provide real-time updates on the ground situation.



USA: The Department of Defense has authorized the use of satellite intelligence for targeting and surveillance

UK: The Ministry of Defence has authorized the use of satellite intelligence for targeting and surveillance

Recent revelations in the UK and US have highlighted the use of satellite intelligence for targeting and surveillance operations in the surrounding region. The intelligence is being used to identify and track Hamas targets, as well as to provide real-time updates on the ground situation.



USA: The Department of Defense has authorized the use of satellite intelligence for targeting and surveillance



Ukraine Eyes Formation of a New Cyber Army Branch

Amid rising cyber challenges, the Ukrainian military is exploring the creation of a dedicated cyber army branch. This new initiative is part of Ukraine's response to cyber threats posed by regional adversaries and aims to enhance the country's defensive cyber capabilities. If established, this branch would strengthen Ukraine's resilience against cyber warfare, reflecting an increasing global trend toward prioritizing cybersecurity in national defense strategies.



#Ukraine #CyberDefense

Link: <https://www.msn.com/en-us/news/world/ukrainian-military-considering-creation-of-new-cyber-army-branch/ar-AA1sRcjd>

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

