



SPACE CYBERSECURITY WEEKLY WATCH

Week 36

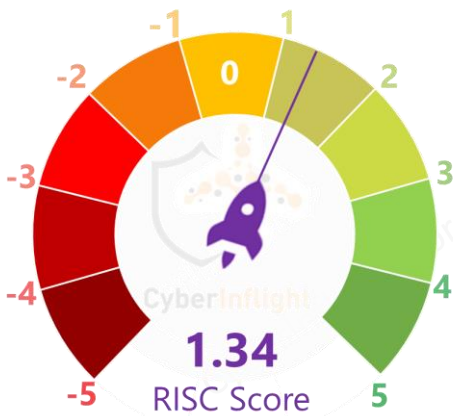
September 3 - 9, 2024

Timeframe : Weekly
of articles identified : 33
Est. time to read : 45 minutes

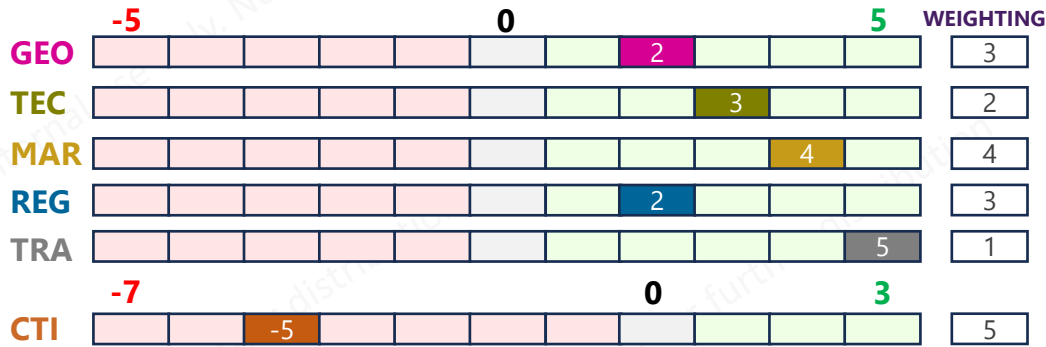
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

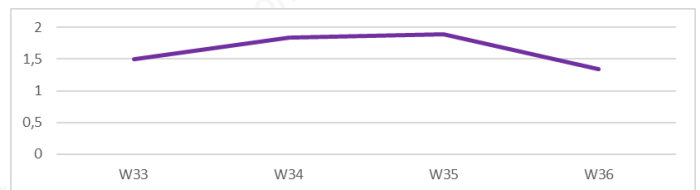
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score Evolution



↓ This week's RISC score is 1.34, a decrease from last week, mainly due to a high-threat climate.

On the geopolitical front, according to an internal investigation obtained by Navy Times, the senior enlisted leaders among the US littoral combat ship Manchester's gold crew installed and secretly used their very own Wi-Fi network during a deployment last year. On the technological side, EUSPA has completed the testing of the Galileo Open Service Navigation Message Authentication (OSNMA) and is now gearing up for its operational launch. On the market front, Applied Dynamics International (ADI) announced the successful completion of a major project to modernize the National Oceanic and Atmospheric Administration's (NOAA) satellite emulator systems. This project sets a new benchmark for cybersecurity and operational longevity in mission-critical satellite systems. On the regulatory front, an article about the proposed Spacecraft Cybersecurity Act has been published. If passed, the legislation would mandate NASA to overhaul the way it procures and builds its spacecraft. On the threat intel side, in a joint advisory released by the FBI, the CISA, and NSA, it was revealed that the Russian GRU hackers, often junior officers from GRU's 161st Specialist Training Center, have been involved in cyber sabotage since 2020. These officers are accused of conducting cyber operations that have harmed critical US infrastructure, with particular emphasis on energy, government, and aerospace sectors. Lastly, on Tuesday September 10 in Brussels, ONERA - The French Aerospace Lab, with the support of the Permanent Representation of France to the European Union, is organizing a conference on strengthening the competitiveness and defense of the European Union. The event will focus on the role of dual-use technologies and their importance for competitiveness and strategic autonomy.



GEOPOLITICS



How Navy chiefs conspired to get themselves illegal warship Wi-Fi

For a variety of reasons, including operational security, a crew's internet access is regularly restricted while underway, to preserve bandwidth for the mission and to keep their ship safe from nefarious online attacks. But the senior enlisted leaders among the littoral combat ship Manchester's gold crew knew no such privation last year, when they installed and secretly used their very own Wi-Fi network during a deployment, according to a scathing internal investigation obtained by Navy Times. **#USSF #Starlink**

Link: <https://www.navytimes.com/news/your-navy/2024/09/03/how-navy-chiefs-conspired-to-get-themselves-illegal-warship-wi-fi/>



USCIB chief says foundation stone for US's Cyber National Security Research Center

US Cyber Intelligence Board (USCIB) Chief, Admiral Michael S. Rogers, announced the foundation stone for the US Cyber National Security Research Center (USCNSRC) during a ceremony at the US Cyber Command (USCIB) headquarters in Fort Belvoir, Colorado. The center will focus on research and development in the field of cyber intelligence, and will be a key component of the US's cyber defense strategy.



Insights: Assessing the call for space superiority

In a recent report, the US Cyber Intelligence Board (USCIB) has highlighted the importance of space and cyberspace in the US's national security strategy. The report states that space and cyberspace are critical domains for the US, and that the US must maintain a strong presence in these domains to ensure its national security. The report also calls for the US to invest in research and development in the field of space and cyberspace, and to develop a space superiority strategy.



TECHNOLOGY



Galileo is getting ready for the upcoming OSNMA operational declaration

The European Union Agency for the Space Programme (EUSPA) has completed the testing of the Galileo Open Service Navigation Message Authentication (OSNMA) and is now gearing up for its operational launch. Access and knowledge to perform spoofing attacks are increasing, resulting in disruption or denial incidents being more frequently observed. The Galileo Programme has therefore developed and integrated an Open Service Navigation Message Authentication (OSNMA) capability into the Galileo infrastructure and operations. **#Galileo #OSNMA**

Link: <https://www.euspa.europa.eu/newsroom-events/news/galileo-getting-ready-upcoming-osnma>



USCIB chief says foundation stone for US's Cyber National Security Research Center

US Cyber Intelligence Board (USCIB) Chief, Admiral Michael S. Rogers, announced the foundation stone for the US Cyber National Security Research Center (USCNSRC) during a ceremony at the US Cyber Command (USCIB) headquarters in Fort Belvoir, Colorado. The center will focus on research and development in the field of cyber intelligence, and will be a key component of the US's cyber defense strategy.



Integrating the complex landscape of aerospace cybersecurity and new engine technology

In the past decade, there has been a significant increase in the number of aerospace cybersecurity incidents, and this trend is expected to continue. The complexity of aerospace systems, combined with the increasing use of new engine technology, is making it difficult for aerospace organizations to keep up with the latest threats. This report explores the challenges of aerospace cybersecurity and provides insights into how organizations can better protect their systems.





MARKET & COMPETITION

★ Viasat awarded potential \$153m BFT network services contract by DISA

"Viasat is honored to continue its history of providing support for the global L-Band BFT network and systems, and the continued modernization of how critical situational awareness is made available across the tactical edge at scale," said David Schmolke, Vice President of Mission Connections and Cybersecurity Department at Viasat. **#Contract #DISA**



Link: <https://news.satnews.com/2024/09/05/viasat-awarded-potential-million-bft-network-services-contract-by-disa/>

Business Continuity: Acquisition of New Systems, Expanding Company's National Security Support Portfolio



★ ADI completes successful modernization of NOAA satellite emulators

Applied Dynamics International (ADI), a global leader in industrial computing and connectivity, announced the successful completion of a major project to modernize the National Oceanic and Atmospheric Administration's (NOAA) satellite emulator systems. This project sets a new benchmark for cybersecurity and operational longevity in mission-critical satellite systems. **#NOAA #Compliance**



Link: <https://finance.yahoo.com/news/adi-completes-successful-modernization-noaa-130000005.html>

ADI Systems Has completed Modernization



Business Continuity and System expansion update



Space Force Cybersecurity Policy Update



ADI Modernizing NOAA Operations Undergraduate Update



REGULATION

★ NASA science mission spacecraft are at risk from hackers, but a new law could help protect them

NASA missions are prime targets for cyberattacks. In a move to counter the escalating threat of these attacks, U.S. congressmen Maxwell Alejandro Frost and Don Beyer have proposed the Spacecraft Cybersecurity Act. If passed, the legislation would mandate NASA to overhaul the way it procures and builds its spacecraft. **#NASA #ProtectingSpace**



Link: <https://www.space.com/nasa-science-missions-at-risk-from-hackers-new-law-could-protect>

US 10th Anniversary of Cybersecurity for Space (C4S) The Military Program Law as Instrument of Confidence for the Ground Force



US 10th Anniversary of Cybersecurity for Space (C4S) The Military Program Law as Instrument of Confidence for the Ground Force



TRAINING & EDUCATION



Renforcer la compétitivité et la défense de l'Union européenne (Trad. Strengthening the competitiveness and defense of the European Union)

On Tuesday September 10 in Brussels, ONERA - The French Aerospace Lab, with the support of the Permanent Representation of France to the European Union, is organizing a conference on strengthening the competitiveness and defense of the European Union. The event will focus on the role of dual-use technologies in space, and their importance for competitiveness and strategic autonomy. **#Security #Europe**

Link: https://www.linkedin.com/posts/laurent-leylekian_mardi-10-septembre-%C3%A0-bruxelles-lonera-activity-7237070255880085504-m0S4?utm_source=share&utm_medium=member_desktop



TRAINING & EDUCATION

Government Technology Magazine September 2024
Article: The new space cyber security standards in the new publication of the Government Technology Magazine
September 2024
[Link: https://www.gtmagazine.com/...](#)

THREAT INTELLIGENCE

South Korea's National Intelligence Service (NIS) has released a report on the activities of North Korean hackers targeting South Korean government agencies and private sector entities in the last quarter of 2023.

The report details the activities of North Korean hackers, including the use of advanced malware and social engineering tactics, to steal sensitive information and disrupt government operations.



The report also notes the increasing threat to satellites and ground operations.

The number of cyberattacks against South Korean government agencies and private sector entities has increased significantly in the last quarter of 2023, with a notable increase in the number of attacks targeting satellites and ground operations.



The report also notes the increasing threat to satellites and ground operations.

Space Information Sharing and Analysis Center (Space ICSA) is announcing an update to its threat level assessment as a TLP (C) public release.

Considering recent developments in space security, Space ICSA is updating its threat level assessment to reflect the current state of space security. The update is intended to provide more accurate and timely information to the public and to help organizations better understand the risks to their space assets.



[Link: https://www.space-icsa.com/...](#)

★ Russian Cyber Unit 29155 exposed: targeting NATO and allied nations

In a joint advisory released by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and National Security Agency (NSA), it was revealed that the GRU hackers, often junior officers from GRU's 161st Specialist Training Center, have been involved in cyber sabotage since 2020. These officers are accused of carrying out cyber operations that have harmed critical US infrastructure, with particular emphasis on energy, government, and aerospace sectors. **#Russia #CriticalInfra**



Link: <https://thecyberexpress.com/russian-cyber-unit-29155-exposed/>

But the British, New Zealand, and other allies have also been targeted by the GRU hackers, often junior officers from GRU's 161st Specialist Training Center, have been involved in cyber sabotage since 2020.

The report details the activities of North Korean hackers, including the use of advanced malware and social engineering tactics, to steal sensitive information and disrupt government operations.



The report also notes the increasing threat to satellites and ground operations.

South Korea's National Intelligence Service (NIS) has released a report on the activities of North Korean hackers targeting South Korean government agencies and private sector entities in the last quarter of 2023.

The report details the activities of North Korean hackers, including the use of advanced malware and social engineering tactics, to steal sensitive information and disrupt government operations.



The report also notes the increasing threat to satellites and ground operations.

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

