



# SPACE CYBERSECURITY WEEKLY WATCH

Week 42

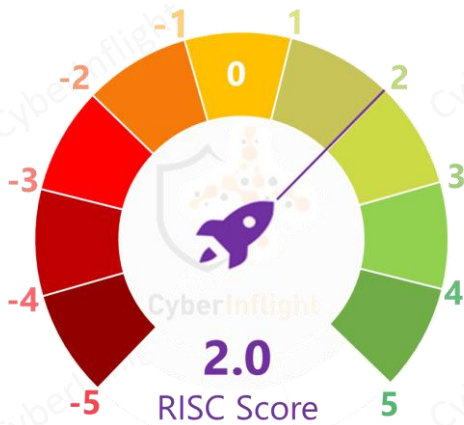
October 15 - 21, 2024

Timeframe: Weekly  
# of articles identified: 36  
Est. time to read: 75 minutes

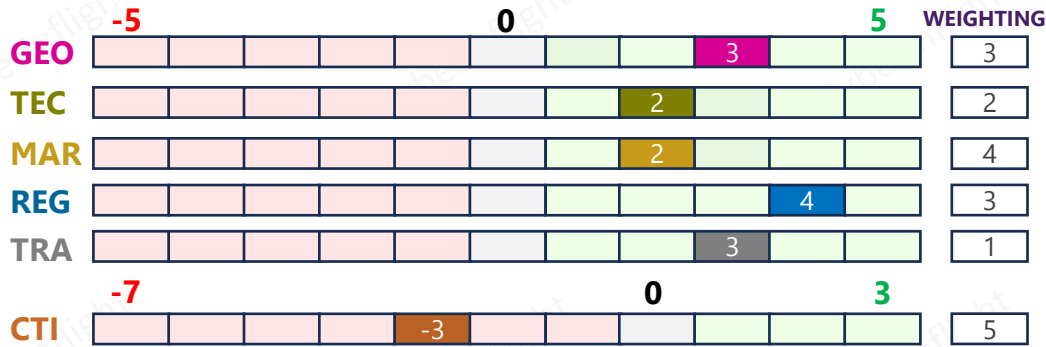
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

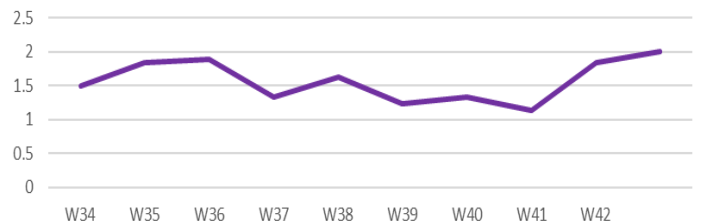
## RISC Score Assessment



## 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

## Space based targeting challenges calling now for NATO Deputy Secretary

The NATO Deputy Secretary General, Alexander Dehaene, has called for a more coordinated approach to space-based targeting challenges. He stated that the current fragmented efforts by individual member states are insufficient to address the growing threat of space-based weapons and surveillance. Dehaene emphasized the need for a unified NATO strategy to ensure the security and resilience of space-based assets.



[https://breakingdefense.com/2024/10/space-based-targeting-challenges-calling-now-for-nato-deputy-secretary/](#)

## OTBAC2024: Canada's CMC gets serious about cyber defense

Canada's Communications and Cyber Centre (CMC) is significantly upgrading its cyber defense strategies in response to the growing cyber threat landscape. The CMC is focusing on enhancing its capabilities to detect, analyze, and respond to cyber threats, particularly those originating from state actors. This includes investing in advanced threat intelligence and improving coordination with other government agencies.



[https://breakingdefense.com/2024/10/otbac2024-canadas-cmc-gets-serious-about-cyber-defense/](#)

## NATO stresses the importance of space in warfare

NATO officials are increasingly stressing the importance of space in warfare, especially as more nations invest in satellite-based capabilities. The alliance is focusing on ensuring the security and resilience of its space-based assets, which are critical for intelligence gathering, communication, and navigation. NATO is also exploring ways to defend against potential threats to these assets.



[https://breakingdefense.com/2024/10/nato-stresses-the-importance-of-space-in-warfare/](#)

## NATO pushes Arctic space plan to member states

NATO is pushing its Arctic space plan to member states, emphasizing the need for enhanced cooperation in the region. The plan focuses on improving space-based capabilities for intelligence and surveillance in the Arctic, which is becoming increasingly strategic due to its natural resources and potential for conflict. NATO is seeking to ensure that all member states are aligned on this approach.



[https://breakingdefense.com/2024/10/nato-pushes-arctic-space-plan-to-member-states/](#)

## ★ 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/>

## India's tie up with US aimed to boost security cooperation - Analysts

The growing strategic partnership between India and the US, which has expanded into space security, is being analyzed by experts. Analysts note that the integration of space-based capabilities into India's defense strategy is a key element of this partnership. This includes joint efforts to enhance domain awareness and improve coordination in space-based operations. The partnership is seen as a significant step towards a more secure and stable global environment.



[https://breakingdefense.com/2024/10/indias-tie-up-with-us-aimed-to-boost-security-cooperation-analysts/](#)

# MARKET & COMPETITION

## Space-based surveillance capabilities for space-based cyber defense

Space-based surveillance capabilities are being developed to enhance space-based cyber defense. These capabilities include advanced sensors and data processing systems that can detect and analyze cyber threats originating from space-based assets. This is a critical area of research and development for many nations, as space-based assets are becoming increasingly vulnerable to cyber attacks.



[https://breakingdefense.com/2024/10/space-based-surveillance-capabilities-for-space-based-cyber-defense/](#)

## Canada Space Agency and Italian Space Agency enhance collaboration

The Canadian Space Agency (CSA) and the Italian Space Agency (ASI) are enhancing their collaboration in space-based operations. This includes joint efforts to improve space-based surveillance capabilities and enhance coordination in space-based operations. The partnership is seen as a significant step towards a more secure and stable global environment.



[https://breakingdefense.com/2024/10/canada-space-agency-and-italian-space-agency-enhance-collaboration/](#)



# 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/>



# TECHNOLOGY

## **US Army sets industry for satellite technologies in competition within DARPA's to control orbital capabilities**

The US Army set the industry to develop new satellite technologies for competition within DARPA's. These technologies are aimed at controlling satellite communications capabilities in contested environments. The Army's goal highlights the growing need for advanced systems to ensure the reliability and security of military communication systems. **#DARPA #Army**



## **New satellites are pushing security innovation at Boeing**

Boeing's satellite program is set to boost the company's security innovation efforts by adding satellite services. Boeing aims to provide secure data communications while enhancing cybersecurity protection. The program emphasizes the growing importance of space technologies and advanced security strategies, setting new standards for satellite communication services. **#Boeing #Space**



## **Space Administration launches System (SIS) system performance qualification with service**

The Space Administration launched System (SIS) system performance qualification with service. This program will test a ground-based communication system for demonstration of system performance in enhancing satellite communication capabilities. The qualification results will be used to certify the system's ability to support critical operations in space. **#Space #SIS**



## **China's "groundbreaking" satellite launch 1.22 month system using 60000 satellite signals**

China's satellite launch system is set to boost the country's satellite communication capabilities. The system will use 60,000 satellite signals to provide secure data communications while enhancing cybersecurity protection. The program emphasizes the growing importance of space technologies and advanced security strategies, setting new standards for satellite communication services. **#China #Space**



## ★ **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/>



## ★ 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/>





# THREAT INTELLIGENCE



## 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>



## OTI launching in Myanmar

Myanmar's OTI (Operational Threat Intelligence) program is launching, focusing on cyber threats and critical infrastructure protection. The program aims to enhance the country's ability to detect and respond to cyber threats, particularly those targeting critical infrastructure. **#OTI #Myanmar**

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



## Network access of 48 states cyber threats and consequences

Network access of 48 states cyber threats and consequences. The report highlights the increasing number of cyber threats targeting critical infrastructure and the potential consequences of such attacks. **#CyberThreats #Infrastructure**

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



## US Dept. Justice releases Southern Baptist Convention cyber threat report

The Department of Justice has released a report detailing the cyber threats faced by the Southern Baptist Convention. The report highlights the increasing number of cyber threats targeting religious organizations and the potential consequences of such attacks. **#CyberThreats #Religion**

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



## China says US spy satellites in US espionage and disinformation campaign

China has accused the US of using spy satellites for espionage and disinformation campaigns. The report highlights the increasing number of cyber threats targeting critical infrastructure and the potential consequences of such attacks. **#CyberThreats #Espionage**

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



## 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>



## Networks in Egypt: Security concerns in a red sea

Networks in Egypt: Security concerns in a red sea. The report highlights the increasing number of cyber threats targeting critical infrastructure and the potential consequences of such attacks. **#CyberThreats #Egypt**

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

## Cyber threats by Russian State: surge beyond control

Cyber threats by Russian State: surge beyond control. The report highlights the increasing number of cyber threats targeting critical infrastructure and the potential consequences of such attacks. **#CyberThreats #Russia**

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



# TRAINING & EDUCATION

**2024 NATO Cyber Defence and Resilience Conference will be held in Istanbul**  
The 2024 NATO Cyber Defence and Resilience Conference will take place in Istanbul, Turkey, from 15 to 19 October 2024. The conference will focus on the latest developments in cyber defence and resilience, including the role of artificial intelligence, quantum computing, and space-based cyber operations. The event will feature keynote speeches, panel discussions, and a range of workshops and training opportunities. For more information, visit [https://www.nato.int/cyberdefence](#).



## 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>

**2024 International Union of Pure and Applied Chemistry (IUPAC) 118th General Assembly**  
The 118th General Assembly of the International Union of Pure and Applied Chemistry (IUPAC) will be held in Beijing, China, from 28 August to 7 September 2024. The assembly will focus on the discovery and naming of the 118th element, Oganesson (Og), and will also discuss the future of chemistry and the role of IUPAC in the global scientific community. For more information, visit [https://www.iupac-union.org](#).

**India to host Space Cyber Days in 2025**  
India will host the Space Cyber Days 2025, a two-day event that will bring together experts from the space industry, academia, and government to discuss the latest developments in space cyber security. The event will feature keynote speeches, panel discussions, and a range of workshops and training opportunities. For more information, visit [https://www.isro.gov.in](#).



**2024 Cyber Defence Conference 2024: Empowering Canada's Defence Industry and Innovation**  
The 2024 Cyber Defence Conference 2024 will be held in Ottawa, Canada, from 15 to 17 October 2024. The conference will focus on the latest developments in cyber defence and resilience, including the role of artificial intelligence, quantum computing, and space-based cyber operations. The event will feature keynote speeches, panel discussions, and a range of workshops and training opportunities. For more information, visit [https://www.cdc2024.ca](#).



*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](mailto:research@cyberinflight.com)*