



# SPACE CYBERSECURITY WEEKLY WATCH

Week 8

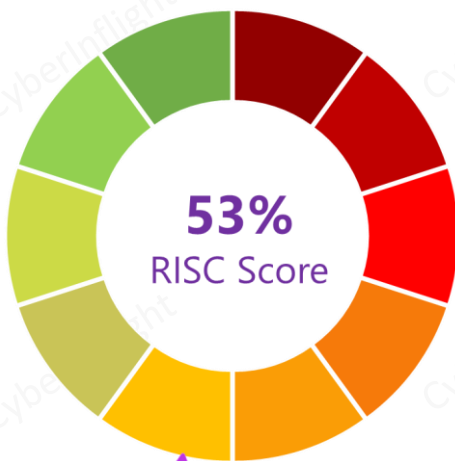
February 20 – 26, 2024

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

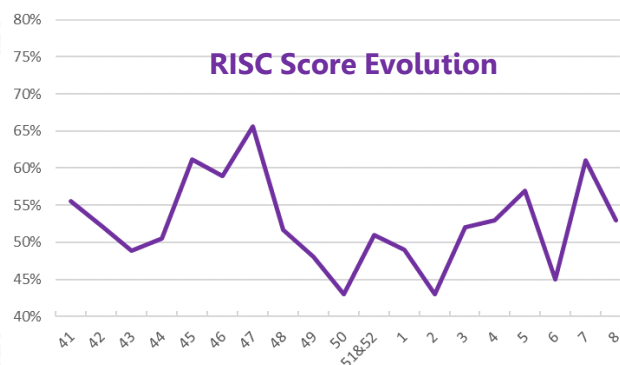
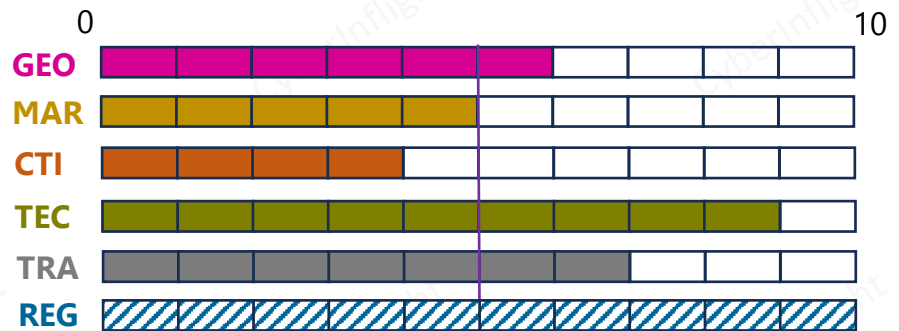
Timeframe : Weekly  
# of articles identified : 29  
Est. time to read : 50 minutes

- **GEOPOLITIC**
- **MARKET & COMPETITION**
- **THREAT INTELLIGENCE**
- **TECHNOLOGY**
- **TRAINING & EDUCATION**
- ★ **IMPORTANT NEWS**

## Overview & RISC Score



↓ *Decrease from last week (from 61% to 53%)*



*After a rising period since the start of 2024, W6 has shown a decrease, W7 has shown an increase and W8 has shown a small decrease again.*

This week's RISC Score is 53. This week, a study by the New York Times revealed the intelligence partnership between Washington and Kyiv where the US helps with tracking Russian troop movements and supporting spy networks. On the market front, the Pentagon has long pursued augmented GPS capabilities, including using allied backup systems, but is now looking for a potential partnership with a promising company to reduce GPS dependence. On the threat intelligence side, pilots flying the over Norway have been seeing a sharp spike in disturbances of navigation caused by Russian electronic warfare units located on the Kola Peninsula. Norwegian Communication Authority says it has received about disturbances to the GPS navigation 44 days in 2024. Moreover, iDirect Government's Communication Signal Interference Removal (CSIR) technology has been named a Finalist for the 2023 Satellite Technology of the Year Award organized by Via Satellite. CSIR mitigates interference and meets the specialized needs of military and government SATCOM users by delivering uninterrupted secure communications on any radio frequency. Last but not least, EU Member States, with the support of the European Commission and ENISA, the EU Agency for Cybersecurity, published a report on the cybersecurity and resiliency of Europe's communications infrastructures and networks.



# GEOPOLITIC

## Space Force, NRO Will Fly Targeting Satellites 'Shoulder to Shoulder'

The Space Force is making progress in its plan with the National Reconnaissance Office to enable space based targeting and replace legacy Air Force AC-133J multiple sensor leaders used at the QM Warfare Symposium.

**Link:** <https://www.defense.com/space-force-will-targeting-satellites/>



## China Latin America Space Cooperation - An Update

China's expanding space capabilities and cooperation for extended engagement around the globe, from initiatives to build international coalitions such as ISIS, to the search for access to ground stations and other space communication sites to support China's expanding constellation of satellites, as well as beyond earth orbits. China MultiMedia

**Link:** <https://www.defense.com/china-latin-america-space-cooperation/>



## ★ The Spy War : How the C.I.A Secretly Helps Ukraine Fight Putin

Now entering the third year of the war, the intelligence partnership between Washington and Kyiv is a linchpin of Ukraine's ability to defend itself. The C.I.A. and other American intelligence agencies provide intelligence for targeted missile strikes, track Russian troop movements and help support spy networks. #CIA #Surveillance

**Link:** <https://www.nytimes.com/2024/02/25/world/europe/cia-ukraine-intelligence-russia-war.html?searchResultPosition=1>



## 10 Lessons from Russia-Ukraine War As It Enters Third Year

Ukraine is looking to secure more help from the US and its allies as donor fatigue sets in. As the war enters its third year on February 23, here are 10 lessons & offers to countries around the world. #CyberWarfare #Russia

**Link:** <https://www.informationweek.com/10-lessons-from-russia-ukraine-war-as-it-enters-third-year-02023-02-23/>



## The Space Force is Not There Yet on Offensive Cyber, But It Will Come

The U.S. Space Force is stepping up its space based assets against cyber attacks. And although its cyber operations only include defensive cyber, the service will certainly add offensive capabilities in the future. said Lt. Zachary Wardinski, senior cyber officer, U.S. Space Force, Pentagon. #SpaceForce #OffensiveCyber

**Link:** <https://www.defense.com/space-force-will-add-offensive-cyber-operations/>



## Space Based Intelligence: The Eyes And The Ears Above

In the space age, the ability to gather information from orbit has been critical to understand our world and safeguard national security. Space based intelligence, surveillance and reconnaissance (SBIR) capabilities offer a unique and unprecedented perspective for observing the Earth and monitoring activities worldwide. #Surveillance #Intelligence

**Link:** <https://www.defense.com/space-based-intelligence-the-eyes-and-ears-above/>

## Cybersecurity for satellites is a growing challenge, as threats to space based infrastructure grow

As our dependence on space based technology increases, so too do the cyber threats. A satellite's service could be interrupted, or at least the speed of service disabled. The expansion of the digital world into space has opened new frontiers for cyber threats, posing unique and complex challenges. #SpaceInfrastructure #CyberSecurity

**Link:** <https://www.defense.com/cybersecurity-for-satellites-is-a-growing-challenge-as-threats-to-space-based-infrastructure-grow-02023/>



# MARKET & COMPETITION



## The Race to Back Up Vulnerable GPS

While the Pentagon has long pursued augmented GPS capabilities, including using allied backup systems, it is now scoping a burgeoning commercial market promising innovative options to reduce GPS dependence.

#SpaceForce #GPSAlternatives

**Link:** <https://spacenews.com/the-race-to-back-up-vulnerable-gps/>



## European Defense Summit - Investing in Tech - AI, Quantum Computing, Cyberwarfare - Need of More - Says Defense Min Rajawade Singh

India will invest heavily in technology in the defense sector, including AI, Quantum Computing, Cyberwarfare - Need of More - Says Defense Min Rajawade Singh while speaking at the European Defense Summit in New Delhi as the chief guest. The Minister said that although security is not guaranteed in the next 20-25 years, India will grow up doing that in one or two decades now. That's why we are investing in defense technology development and introducing technology development fund. **Media Headlines**

**Link:** <https://www.pib.gov.in/Press-Release-Details.aspx?prid=1924444>



## Space 2025 CEO Says India Shows Company Vision for In-Orbit Testing and Data

Space 2025 is a U.S.-based space startup working to pioneer a paradigm shift in space materials qualification to expedite the process for the space industry. Space 2025 CEO talks about adjusting company strategy with customer feedback, fundraising, and building up a company while navigating the new cyber challenges in the sector. **Space 2025 CEO Discusses In-Orbit Testing and Data**

**Link:** <https://www.spacenews.com/space-2025-ceo-discusses-in-orbit-testing-and-data/>



# THREAT INTELLIGENCE



## Electronic Warfare - Russia's GPS Jamming in Poland

Russia tests with special electronic warfare (EW) jamming in GPS infrastructure over the past month. According to a report on the website of the Media and Media Intelligence Institute (MMII), on January 23, 2024, jamming system (GPS jamming) was recorded over the eastern territory of Poland, particularly covering the Lublin region. **Media Headlines**

**Link:** <https://www.pib.gov.in/Press-Release-Details.aspx?prid=1924444>



## Russian Jamming Is Now Messing up GPS Signals for Norwegian Aviation Practically Every Day

Pilots flying the Finnmark region see a sharp spike in disturbances of navigation caused by Russian electronic warfare units located on the Kola Peninsula. In the far north, Norwegian Communication Authority says it has received about disturbances to the GPS navigation 44 days in 2024. That is practically every day. **#Russia #Jamming**

**Link:** <https://thebarentsobserver.com/en/security/2024/02/russian-jamming-now-messing-gps-signals-norwegian-aviation-practically-every-day>



## A Cyberattack Against Satellite Infrastructures in the United Arab Emirates

Anonymous cyber actors targeted the Satellite Communications Company (SCC) and Al Yah Satellite Communications, **Anonymous Cyberattacks**

**Link:** <https://www.pib.gov.in/Press-Release-Details.aspx?prid=1924444>



## A Indian Government Website Has Been Down

Anonymous cyber targets the website of North Eastern Space Applications Centre (NESAC). Anonymous cyber actors targeted the Satellite Communications Company (SCC) and Al Yah Satellite Communications, **Anonymous Cyberattacks**

**Link:** <https://www.pib.gov.in/Press-Release-Details.aspx?prid=1924444>







# TECHNOLOGY



## iDirect Government CSIR Technology Named Finalist For Via Satellite's 2023 Satellite Technology of The Year Award

iDirect Government's Communication Signal Interference Removal (CSIR™) technology has been named a Finalist for the 2023 Satellite Technology of the Year Award organized by Via Satellite. With increasing spectral usage and frequency overlap, CSIR mitigates interference and meets the specialized needs of military and government SATCOM users by delivering uninterrupted secure communications on any radio frequency. **#Contest #CSIR**

**Link:** <https://spacewatchafrica.com/idirect-government-csir-technology-named-finalist-for-via-satellites-2023-satellite-technology-of-the-year-award/>



## Breaking The Cosmic Silence: Quantum Communications Across Interstellar Space

Imagine a future where we can communicate seamlessly across the vast distances of interstellar space, bridging the gap between stars and potentially connecting with extraterrestrial civilizations. A team of physicists at the University of Edinburgh's School of Physics, led by Professor John G. Cramer, has used mathematical simulations to demonstrate that quantum communications across interstellar space could be possible. **#Quantum #Communications**

**Link:** <https://www.earth.com/news/quantum-communications-across-interstellar-space/>



## Royal Navy Works on GPS-Free Technology For Advanced Navigation At Sea

The Royal Navy has worked with scientists to progress on the next set of quantum technology experiments. The Office for the Chief Technology Officer (OCTO) supported specialists from the University of Birmingham and the Dstl to conduct quantum experiments that may pave the way for advanced positioning and navigation tools while at sea. **#Quantum #UK**

**Link:** <https://www.earth.com/news/quantum-technology-advanced-navigation-at-sea/>



## Scientific Systems Advances non-GPS Navigation Technology for Military Use in GPS-Denied Areas

Scientific Systems has announced the advancement of Inaglyph, an image-based navigation software designed for use in environments where GPS signals are compromised. With over a decade of development and funding exceeding \$40 million, Inaglyph offers an alternative to traditional GPS navigation for military operations, particularly in contested environments where electronic jamming poses a threat to GPS reliability. **#Inaglyph #ScientificSystems**

**Link:** <https://www.earth.com/news/scientific-systems-advances-non-gps-navigation-technology-for-military-use-in-gps-denied-areas/>



## Avigo and Cellfree Deliver World's First Quantum-Safe 5G Cellular Technology Products

Avigo, a leader in quantum-safe encryption, and Cellfree, a leader in 5G Radio networks, have recently announced the availability of integrated quantum-safe cellular technology products for Private 5G networks using Symmetric Key Agreement. **#Quantum #5G**

**Link:** <https://www.earth.com/news/avigo-and-cellfree-deliver-worlds-first-quantum-safe-5g-cellular-technology-products/>



## Chinese PLA Navy's Type 055 Destroyer Kiangyong Is Now Operational

According to information published by Global Times on February 16, 2024, the Chinese People's Liberation Army (PLA) Navy has successfully brought its eighth Type 055 large destroyer to operational readiness. The ship boasts advanced electronic warfare and countermeasures, including dual-band radar systems for enhanced detection and tracking capabilities, particularly against stealth targets, and for anti-satellite operations. **#PLA #ElectronicWarfare**

**Link:** <https://www.earth.com/news/chinese-pla-navys-type-055-destroyer-kiangyong-is-now-operational/>



## Space Hacks: AI Protects Aerospace Systems from Cyber Threats Part 1

Imagine a world where space missions are safe from cyberattacks. Explore the growing concern of cyber threats in the aerospace industry and how AI is revolutionizing cybersecurity, protecting rockets, satellites, and critical infrastructure from potential attacks. **#AI #Space #Cybersecurity**

**Link:** <https://www.earth.com/news/space-hacks-ai-protects-aerospace-systems-from-cyber-threats-part-1/>

## UK Signal - A Vital Link in Strategic Military Communications

Signal is the United Kingdom's military communications satellite system. Since its inception, it has been the cornerstone of the UK Armed Forces' global communications capability, providing secure and reliable strategic and tactical communications. **#Signal #UK**

**Link:** <https://www.earth.com/news/uk-signal-a-vital-link-in-strategic-military-communications/>



## Lower Communications: The Next Frontier in Secure, High-Speed Satellite Links

While traditional satellite communications rely on radio frequency (RF) signals, there is growing interest in laser communications, especially for uplink, downlink, and satellite-to-satellite links. This article will focus on uplinks and downlinks. **#LaserLinks #Communications**

**Link:** <https://www.earth.com/news/lower-communications-the-next-frontier-in-secure-and-high-speed-satellite-links/>



# TRAINING & EDUCATION

## Here is Why Robust Space Security Framework is Need of the Hour

Satellite systems are critical for communication, weather monitoring, navigation, internet access, and numerous other services. These systems, however, suffer multiple challenges that jeopardize their security and integrity. To tackle these challenges, we must establish a strong cybersecurity framework to safeguard satellite operations.

**Product Awareness**

**Link:** <https://www.capttechu.edu/degrees-and-programs/doctoral-degrees/space-cybersecurity-phd>

## Redefining Society Paradigm: Exploring The Frontiers of AI, Space Technology, and Cybersecurity with Debra Evers, VP and Chief Technology Officer at the Aerospace Corporation

Join us to hear from Debra Evers, VP and Chief Technology Officer at the Aerospace Corporation, exploring AI's impact on space exploration and the importance of cybersecurity.

**Product Awareness**

**Link:** <https://www.capttechu.edu/degrees-and-programs/doctoral-degrees/space-cybersecurity-phd>



## Report on the Cybersecurity and Resiliency of the EU Communications Infrastructures and Networks

EU Member States, with the support of the European Commission and ENISA, the EU Agency for Cybersecurity, published a report on the cybersecurity and resiliency of Europe's communications infrastructures and networks. This marked another major step in the coordinated work at EU level on the security of telecommunications, and complements the work already done on 5G cybersecurity. **#EU #Report**



**Link:** <https://www.capttechu.edu/degrees-and-programs/doctoral-degrees/space-cybersecurity-phd>

## The Download : Space Competition – Can the US Deter Its Adversaries From Launching Cyberattacks on Space Systems?

This is the fourth in a series of episodes examining cyber attacks and space systems. Laura Miller speaks with General James Space Information Sharing and Analysis Center (SISAC) Board Chair and fellow at The Aerospace Corporation National Security, an independent scholar on space policy and great power politics and co-author of the book "Scramble for the Stars" and her colleague, the head for NATO's cybersecurity operations, and Director of Cyber Policy at the US. **Product Awareness**

**Link:** <https://www.capttechu.edu/degrees-and-programs/doctoral-degrees/space-cybersecurity-phd>

## US and Allied Collaboration

With the rapid growth of the space domain, the U.S. Space Force is developing a next-generation, multi-domain system known as the Protected Air-Sea-Terrestrial Satellite Communications (PATSS) family of systems. For the program to be successful, it must address numerous challenges to promote interoperability, cybersecurity, resilience, and compatibility among the U.S. and its international partners. **Collaboration Awareness**



**Link:** <https://www.capttechu.edu/degrees-and-programs/doctoral-degrees/space-cybersecurity-phd>

## Communication – Satellite and Other Space – USMC World Geography Notes

The applications of satellite communication are widespread, encompassing civilian, public, business, internet services, and military operations. Around 2010, there are over 2000 artificial satellites orbiting the space just above us.

Each satellite serves a specific purpose and is positioned in diverse orbits. In this context, an orbit refers to the trajectory that a satellite follows as it revolves around a celestial body. Let's delve into a closer examination of the various types of orbits employed in satellite communication. **Industry Awareness**

**Link:** <https://www.capttechu.edu/degrees-and-programs/doctoral-degrees/space-cybersecurity-phd>

*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)