



# SPACE CYBERSECURITY WEEKLY WATCH

Week 8

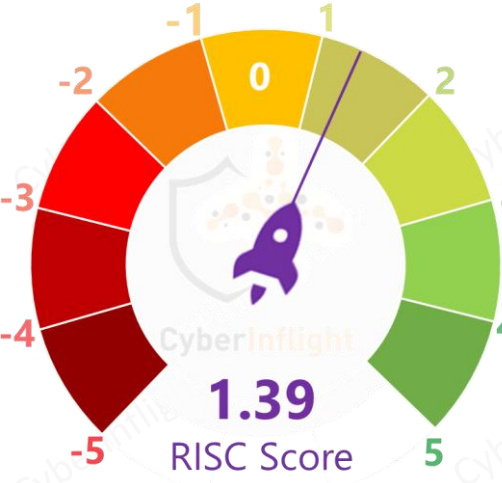
February 18 – 24, 2025

Timeframe: Weekly  
# of articles identified: 23  
Est. time to read: 30 minutes

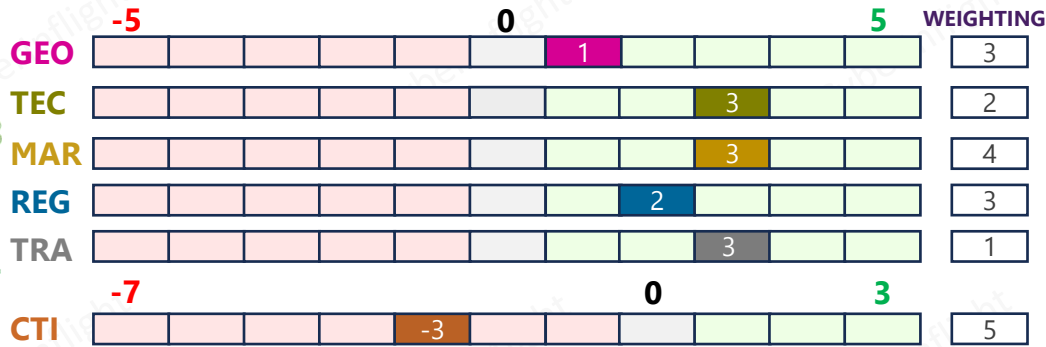
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

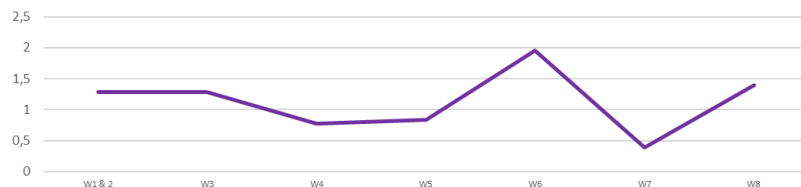
## RISC Score Assessment



## Overview & Resilience Index for Space Cybersecurity (RISC)



## RISC Score evolution in 2025



The RISC score for this watch is 1.39, a big increase from last week. This score is due to a certain homogeneity between the categories, fewer threats than in the last weeks, and more technological news.

This week, while the US government and the military are cutting its spending on scientific and technical research, an article states that China is ramping up, seeking to close the gap in technology that has underpinned US military superiority in space and other domains for two generations. On the market side, Zephr.xyz, a provider of augmented Position, Navigation, and Timing (AugPNT) technologies, has been awarded a \$1.74m Small Business Innovation Research (SBIR) Direct-to-Phase II contract from the Air Force Research Laboratory (AFRL) to develop real-time detection of GNSS jamming and spoofing in contested domains while geolocating the sources of attacks.

From a regulation side, Almenar et al. address the overarching legal challenges posed by integrating AI into outer space operations, specifically on cybersecurity, intellectual property, and data governance, which are critical for safeguarding autonomous systems in a new paper.

On the technological side, the European Space Agency (ESA) invites researchers, engineers, and innovators to propose experimental ideas for testing new technologies, methods, algorithms, protocols, and techniques in the domain of cybersecurity applied to space systems.

Lastly, some space officials at the International Defence Conference (IDC) warned about evolving threats to spacecraft. "Space has become a domain for warfighting," Mohamed Alahbabi said, adding that it is making it "subject to threats."



## GEOPOLITICS



### Space Force official warns of China outpacing US defense tech with greater investment

While the US government and the military in particular is cutting its spending on scientific and technical research, China is ramping up, seeking to close the gap in technology which has underpinned US military superiority in space and other domains for two generations, a senior Space Force official said last week. **#USSF #China**



**Link:** <https://www.satellitetoday.com/cybersecurity/2025/02/19/space-force-official-warns-of-china-outpacing-us-defense-tech-with-greater-investment/>

**Key Impact:** *Space Force's warning highlights the growing technological gap between the US and China in space defense, emphasizing the need for increased investment in scientific and technical research to maintain military superiority.*



## REGULATION



### Almenar et al. on "The protection of AI-based space systems from a data-driven governance perspective"

The paper aims to address the overarching legal challenges posed by the integration of AI into outer space operations, specifically on cybersecurity, intellectual property, and data governance, which are critical for safeguarding autonomous systems. **#AI #Paper**

**Link:** <https://ailawblawg.com/2025/02/18/almenar-et-al-on-the-protection-of-ai-based-space-systems-from-a-data-driven-governance-perspective/>

**Key Impact:** *The paper identifies legal challenges in AI integration for space operations, focusing on cybersecurity, intellectual property, and data governance, and proposes a data-driven governance perspective for autonomous systems.*



## MARKET & COMPETITION



### Zephr.xyz awarded \$1.7m Air Force Research Laboratory contract for GNSS jamming detection technology

Zephr.xyz, a provider of augmented Position, Navigation, and Timing (AugPNT) technologies, has been awarded a \$1.74m Small Business Innovation Research (SBIR) Direct-to-Phase II contract from the Air Force Research Laboratory (AFRL) to develop real-time detection of GNSS jamming and spoofing in contested domains while geolocating the sources of these attacks. **#GNSS #Jamming**



**Link:** <https://insidegnss.com/zephr-xyz-awarded-1-7m-air-force-research-laboratory-contract-for-gnss-jamming-detection-technology/>

**Key Impact:** *Zephr.xyz has secured a \$1.74m SBIR contract from AFRL to develop real-time detection of GNSS jamming and spoofing, highlighting the growing market for advanced navigation and timing technologies in contested domains.*





# MARKET & COMPETITION

## Space Force Launches Action Plan to Accelerate U.S. Program

The Space Force has unveiled a strategy with one of the top priorities: accelerating progress for its Special Operations Cyber Command (SOCC) to ensure the United States has the necessary capabilities to protect its interests in space.

**Link:** [https://www.spaceforce.mil/News/2025/02/18/space-force-launches-action-plan-to-accelerate-u-s-program](#)



## European Communications Market Research Report Information by product type by application and by region - market forecast till 2030

Global Communications Market Research Report provides an in-depth analysis of the market, covering a comprehensive overview of the market, including the current market size, growth rate, and key players. The report also includes a detailed analysis of the market by product type, application, and region.

**Link:** [https://www.researchandmarkets.com/research/communications-market-research-report](#)

## Further work in the defense sector - supply chains, cybersecurity and space

The defense sector has increasingly prioritized supply chain security, cybersecurity, and satellite. The emphasis on the latter is likely to continue, with a focus on ensuring a secure and resilient supply chain. This is particularly important for the defense sector, which relies heavily on satellite technology for a wide range of operations.

**Link:** [https://www.defenseindustry.com/2025/02/18/further-work-in-the-defense-sector-supply-chains-cybersecurity-and-space](#)

## Governmental Security Canada's next test gap (NSG) will focus on the U.S.

As the world's largest supplier of military and police equipment, Canada is looking to improve its cybersecurity and communications capabilities. The next test gap (NSG) will focus on the U.S. market, with a particular emphasis on ensuring that Canadian equipment is secure and resilient to cyber threats.

**Link:** [https://www.defenseindustry.com/2025/02/18/governmental-security-canada-s-next-test-gap-nsg-will-focus-on-the-u-s](#)



# TECHNOLOGY

## Working with AI, blockchain, and quantum resistant security to strengthen digital trust

Working to ensure digital trust in communications with quantum resistant encryption, providing confidential access to critical information with quantum resistant encryption, and quantum resistant security. AI, blockchain, and quantum resistant security are key technologies for strengthening digital trust.

**Link:** [https://www.defenseindustry.com/2025/02/18/working-with-ai-blockchain-and-quantum-resistant-security-to-strengthen-digital-trust](#)



## NSA, DHS and DOD

The technology developed by the National Association of Broadcasters (NAB) through the NSA, DHS, and DOD is designed to protect the nation's critical infrastructure and communications. The technology is a key component of the nation's cybersecurity strategy.

**Link:** [https://www.defenseindustry.com/2025/02/18/nsa-dhs-and-dod](#)

## Modernizing space communications: building stronger links for a connected future

As the world's largest supplier of military and police equipment, Canada is looking to improve its cybersecurity and communications capabilities. The next test gap (NSG) will focus on the U.S. market, with a particular emphasis on ensuring that Canadian equipment is secure and resilient to cyber threats.

**Link:** [https://www.defenseindustry.com/2025/02/18/modernizing-space-communications-building-stronger-links-for-a-connected-future](#)



## Call for ideas: cybersecurity experiments in orbit

The European Space Agency is pleased to invite researchers, engineers, and innovators to propose experimental ideas for testing new technologies, methods, algorithms, protocols, and techniques in the domain of cybersecurity applied to space systems. #CyberCUBE #ESA

**Link:** <https://security4space.esa.int/2025/cfi-cybersecurity-experiments-in-orbit/>





# THREAT INTELLIGENCE

## Cybersecurity in space and Earth and the future of security beyond earth

Space-based intelligence and other system collection from GPS satellites to global communications, satellite navigation, and weather forecasting, space assets are vital to security, the environment, global commerce, and scientific exploration. As such, protecting these resources is space security. However, the satellite and launching it has become a high-priority mission.

**Link:** [https://www.cisa.gov/cybersecurity-in-space-and-earth-and-the-future-of-security-beyond-earth](#)

## State-aligned APT groups are increasingly exploiting weaknesses in satellite systems and their land users

There are a few ways the US can improve satellite systems and their users. First, satellite systems are often used to provide intelligence and other services to the public sector. But their weaknesses in the government sector are being exploited by state-aligned APT groups. The researchers describe steps to better protect satellite systems, including: 1) improve the security of satellite systems, 2) improve the security of satellite users, and 3) improve the security of satellite systems.

**Link:** [https://www.cisa.gov/state-aligned-apt-groups-are-increasingly-exploiting-weaknesses-in-satellite-systems-and-their-land-users](#)

## ★ US satellites enabled with AI tech to make them immune to cyberattacks

China has emerged as one of the primary geopolitical and technological adversaries of the United States, a fact widely acknowledged on the global stage. In its pursuit of dominance, China continuously competes with the West, with the satellite sector being a significant area of contest. **#AI #Cyberattack**



**Link:** <https://www.cybersecurity-insiders.com/us-satellites-enabled-with-ai-tech-to-make-them-immune-to-cyber-attacks/>

## Speeding and jamming from state-sponsored jamming activity in Norway

GPS signals are affected by jamming and spoofing activity. These activities are used to disrupt and degrade GPS signals. This is a significant security concern for the public sector. The researchers describe steps to better protect GPS signals, including: 1) improve the security of GPS signals, 2) improve the security of GPS users, and 3) improve the security of GPS systems.



**APT: #APT**

**Link:** [https://www.cisa.gov/speeding-and-jamming-from-state-sponsored-jamming-activity-in-norway](#)

## Cyber threat intelligence (CTI) handbook

The world of cyber security is both an art and a science. Information is essential for understanding cyber threats and making effective decisions. This handbook provides a comprehensive overview of the field, including: 1) the importance of CTI, 2) the challenges of CTI, and 3) the future of CTI.

**Link:** [https://www.cisa.gov/cyber-threat-intelligence-handbook](#)

# TRAINING & EDUCATION

## An integrated AI communication and APT system for beyond 5G 6G

The next generation of wireless networks is beyond 5G and 6G. These networks are used for a variety of applications, including: 1) the public sector, 2) the private sector, and 3) the military. The researchers describe steps to better protect these networks, including: 1) improve the security of these networks, 2) improve the security of these users, and 3) improve the security of these systems.

**Link:** [https://www.cisa.gov/an-integrated-ai-communication-and-apt-system-for-beyond-5g-6g](#)

## Focus is expanding on military satellites

The US military satellite system is being expanded to include: 1) the public sector, 2) the private sector, and 3) the military. The researchers describe steps to better protect these satellites, including: 1) improve the security of these satellites, 2) improve the security of these users, and 3) improve the security of these systems.

**Link:** [https://www.cisa.gov/focus-is-expanding-on-military-satellites](#)



## ★ IDEX: Space leaders worry about evolving threats to spacecraft

Warns by space officials at the International Defence Conference (IDC) on Sunday: "Space has become a domain for warfighting," Mohamed Alahbabi said at the event, adding that it is making it "subject to threats". **#IDEX #IDC**



**Link:** <https://www.timesaerospace.aero/news/events/idx-space-leaders-worry-about-evolving-threats-to-spacecraft>



## TRAINING & EDUCATION

Intelligent and processing algorithms for satellite communications under limited channel state information conditions

The work has been supported by the National Natural Science Foundation of China (NSFC) under Grant 61871401, 61871402, 61871403, 61871404, 61871405, 61871406, 61871407, 61871408, 61871409, 61871410, 61871411, 61871412, 61871413, 61871414, 61871415, 61871416, 61871417, 61871418, 61871419, 61871420, 61871421, 61871422, 61871423, 61871424, 61871425, 61871426, 61871427, 61871428, 61871429, 61871430, 61871431, 61871432, 61871433, 61871434, 61871435, 61871436, 61871437, 61871438, 61871439, 61871440, 61871441, 61871442, 61871443, 61871444, 61871445, 61871446, 61871447, 61871448, 61871449, 61871450, 61871451, 61871452, 61871453, 61871454, 61871455, 61871456, 61871457, 61871458, 61871459, 61871460, 61871461, 61871462, 61871463, 61871464, 61871465, 61871466, 61871467, 61871468, 61871469, 61871470, 61871471, 61871472, 61871473, 61871474, 61871475, 61871476, 61871477, 61871478, 61871479, 61871480, 61871481, 61871482, 61871483, 61871484, 61871485, 61871486, 61871487, 61871488, 61871489, 61871490, 61871491, 61871492, 61871493, 61871494, 61871495, 61871496, 61871497, 61871498, 61871499, 61871500.



*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)