SPACE CYBERSECURITY WEEKLY WATCH

W2

January 6 – 12, 2026

Timeframe: Weekly

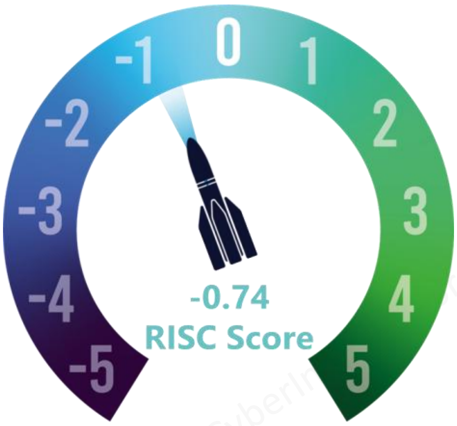
# of articles identified: 15

Est. time to read: 30 minutes

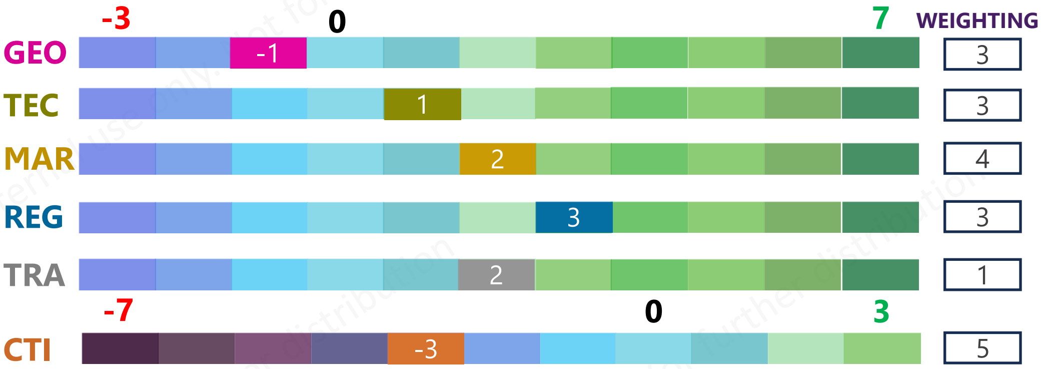
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

- 🟥 GEOPOLITICS
- 🟩 TECHNOLOGY
- 🟨 MARKET & COMPETITION
- 🟦 REGULATION
- ⬜ TRAINING & EDUCATION
- 🟧 THREAT INTELLIGENCE
- ★ IMPORTANT NEWS

RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score changes in 2026

In 2026, CyberInflight updated its methodology for calculating the RISC Score to better reflect observed realities. The scoring ranges for the Geopolitics, Market & Competition, Technology, Regulation, and Training & Education categories were adjusted. As these categories are rarely assessed as negative and more frequently show moderate to high positive signals, a wider positive range was introduced. The weighting of the Technology category was also increased, highlighting the growing importance of technology-related topics in the overall risk assessment. This change enables the RISC Score to more accurately capture meaningful variations in the risk environment while maintaining a neutral baseline and overall consistency of the score.

As the year gets underway, this week's watch reflects a typically quieter early-January news cycle, with fewer updates but several developments of strategic relevance. On the community front, CyberInflight contributed to the launch of the EU Space ISAC Survey 2026, inviting industry stakeholders to share practical insights on legal and cybersecurity compliance challenges in the space sector. This week, **reporting highlights the deepening technological alignment between Russia and China**, with increasing coordination across cyber, space, and hybrid warfare capabilities. This convergence is assessed as a growing strategic challenge for Western countries and NATO. On the regulatory front, **Germany formally transposed the NIS 2 Directive into national law**, significantly raising cybersecurity requirements for a broad range of entities and reinforcing information security governance within the federal administration. On the technological front, the **U.S. DIU announced funding for unjammable magnetic navigation** (magnav) systems, reflecting rising concern over GPS jamming and the need for resilient positioning, navigation, and timing capabilities in contested environments. On the threat intelligence front, **Iran reportedly deployed military jammers to disrupt Starlink connectivity** for the first time, marking an escalation in efforts to counter satellite-based alternative internet access and highlighting the exposure of commercial space services in politically sensitive contexts. On the market front, **Sweden announced major investments** in air defense and space-based ISR, reinforcing the central role of space capabilities in national security strategies amid growing regional tensions. Lastly, **NATO funded an international research initiative** to enhance the cybersecurity of intelligent multi-drone systems, highlighting continued focus on securing emerging autonomous and networked capabilities.

🎉 CYBERINFLIGHT'S NEWS 🎉

★ The EU Space ISAC - Survey 2026 is LIVE! 🚀

CyberInflight is proud to have contributed to the development of this survey within the EU Space ISAC. We invite the industry stakeholders to share their experience and insights on the practical challenges of meeting legal and cybersecurity compliance requirements in the space sector. Help us shape future policies and strengthen the EU's space resilience together. **#EUSpaceISAC #CyberInflight**

Source: LinkedIn

GEOPOLITICS

★ The technological alliance between Moscow and Beijing is taking hybrid warfare to a new level

Russia and China are systematically combining their efforts, creating a unified front of technological threats that endanger the security of Western countries and force NATO to completely rethink its defense strategies, as reported by Jamestown. **#Russia #China**

Source: Odessa Journey

REGULATION

Lawmakers Introduce National Quantum Initiative Reauthorization Act After Lapse

Lawmakers are introducing the National Quantum Initiative Reauthorization Act, seeking to restore a lapsed federal framework for coordinating U.S. quantum research and policy. The legislation aims to provide continued funding and direction for agencies such as NIST and NSF as quantum technology shifts from long-term research toward early deployment. **#Quantum #Act**

Source: Quantum Insider

★ Germany Transposes NIS 2 Directive – Increased Cybersecurity Requirements for Businesses

On 5 December 2025, the Act Transposing the NIS 2 Directive and Regulating Key Aspects of Information Security Management in the Federal Administration (Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung ("NIS2UmsG") became binding in Germany. **#NIS2 #Germany**

Source: Inside Privacy

Japan Prioritizes Cyber Resilience in Latest National Security Push

During the years 2026, Japan positioned economic strategy and security readiness as deeply intertwined priorities, emphasizing national resilience as a core priority. This package of comprehensive economic measures was approved by the Japanese government in November 2025, at a cost of 21.3tn yen, one of the most expansive economic policy responses in recent years. Prime Minister Sanae Takaichi has designated cybersecurity as a strategic investment domain within the second pillar of the government, aligned with other national-critical sectors, such as semiconductors, quantum computing technology, shipbuilding, space exploration, critical communications infrastructure, vital minerals, and the development of advanced information and communication technologies. **#NationalStrategy #CyberResilience**

Source: CySecurity News

TECHNOLOGY

DIU to fund 'unjammable' magnetic navigation tech

To circumvent ever-more pervasive jamming of GPS satellite signals, the Pentagon's Defense Innovation Unit (DUI) is launching a program to mature magnetic navigation (magnav) systems. **#Jamming #Magnav**

Source: Breaking Defense

THREAT INTELLIGENCE

Venezuela strike marks a turning point for U.S. cyber warfare

Trump's comments, made hours after the large-scale military operation, mark one of the first times a U.S. president has so publicly alluded to U.S. cyber efforts against other nations, as these operations are typically highly classified. **#Cyberwarfare #Venezuela**

Source: Politico

THREAT INTELLIGENCE

Ransomware Group interlock Hits: Aero Fabrications

In the latest cybersecurity news, Aero Fabrications — a company operating in the US — has fallen victim to a ransomware attack conducted by the group interlock. This data breach, discovered on 2026-01-06, underscores the increasing need for proactive cybersecurity defenses. **#DataBreach #Ransomware**

Source: HookPhish

ESA calls cops as crims lift off 500 GB of files, say security black hole still open

The European Space Agency confirmed on Wednesday yet another massive security breach and informed The Register that the data thieves responsible will be subject to a criminal investigation. **#ESA #DataBreach**

Source: TheRegister

CVE-2026-22026: CWE-789: Memory Allocation with Excessive Size Value in NASA CryptoLib

For European organizations, particularly those involved in aerospace, satellite communications, and space research, this vulnerability poses a significant risk of denial of service. Exploitation could disrupt critical communication links between spacecraft and ground stations, potentially impacting mission operations, data integrity, and command/control capabilities. **#CryptoLib #CVE**

Sources: Threat Radar, Enisa, CVE

★ 'Kill Switch'—Iran Shuts Down Starlink Internet For First Time

Iran's digital blackout has now deployed military jammers, reportedly supplied by Russia, to shut down access to Starlink Internet. This is a game-changer for the Plan-B connectivity frequently used by protesters and anti-regime activists when ordinary access to the internet is stopped. **#Jamming #Starlink**

Source: Forbes

MARKET & COMPETITION

WISeKey, together with its Subsidiaries, WISeSat and SEALSQ, to partner with Kaynes Technology's satellite subsidiary KSTPL, to manufacture post-quantum secure WISeSats satellites in India and establish India as a strategic launch hub

WISeKey International Holding Ltd, announces that its subsidiary, WISeSat.Space, signed a strategic cooperation agreement with Kaynes Technology India Limited satellite subsidiary Kaynes Space Technology Private Limited ("KSTPL"), to manufacture post-quantum-secure WISeSat satellites in India and establish India as one of its official satellite launch locations, in addition to its current launch operations in the United States. This collaboration, which brings together two of WISeKey's subsidiaries, WISeSat and SEALSQ Corp which focuses on semiconductors, PKI, and post-quantum technology products, along with KSTPL aims to create a new generation of quantum-resilient satellite infrastructure designed to protect global IoT connectivity against the emerging threats of quantum computing. **#Quantum #Satellite**

Source: Wisekey

★ Sweden allocates $1.6bn to build territorial air defense capability, $140m for space

Openly acknowledging gaps in protecting its population, Sweden has announced plans to invest 15bn Swedish kronor (about $1.6bn) in new homeland air defense units. Additionally, Stockholm is bolstering its space-based intelligence capabilities with new investments. In addition to the air defense investments, Sweden has announced a commitment of 1.3bn kroner ($140m) to "expanding" its space capabilities with new intelligence, surveillance, and reconnaissance (ISR) satellites. **#NationalDefense #ICEYE**

Sources: Breaking Defense, Artic Today

TRAINING & EDUCATION

#37 - Satellites, cyberattaques et IA : les nouveaux défis du cyberespace - Avec Anna Barraqué

Recorded at the Cybersecurity Business Convention, this episode offers an in-depth look at cybersecurity issues in cyberspace with Anna Barraqué. As satellites and space infrastructure become increasingly essential to our daily lives, they are now exposed to threats comparable to those encountered on Earth. Cyberattacks, securing ground-satellite communications, the impact of artificial intelligence, and evolving regulatory frameworks: a discussion about a sector long perceived as untouchable, but now fully affected by digital risks. **#Cyberattacks #CBC**

Source: Les Causeries Data de Data Ring

TRAINING & EDUCATION

NATO funds international research to protect drones against cyber attacks

Researchers at the University of Wollongong (UOW) in Australia have secured a North Atlantic Treaty Organization (NATO) research grant to strengthen the security of intelligent multi-drone systems operating in high-risk environments. The multi-year project, ‘Robustness against Adversarial Attacks for Intelligent Multi Drone Agents (RAID) is funded through NATO’s Science for Peace and Security Programme and brings together leading cryptography, cybersecurity, robotics, autonomous systems and artificial intelligence experts. **#NATO #Cyber**

Source: Unmanned Airspace

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