

SPACE CYBERSECURITY WEEKLY WATCH

W4

January 20 – 26, 2026

Timeframe: Weekly

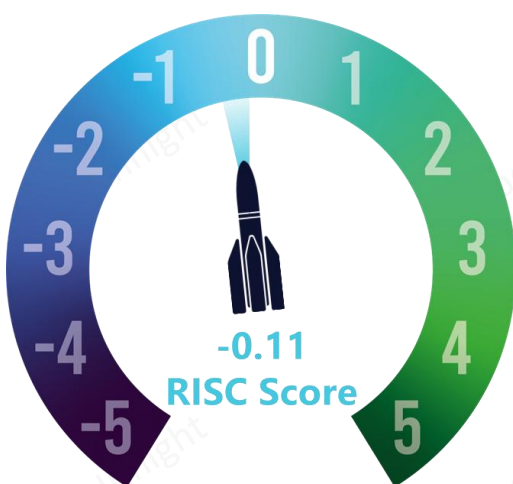
of articles identified: 36

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 & COMPETITION
- REGULATION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- ★ IMPORTANT NEWS

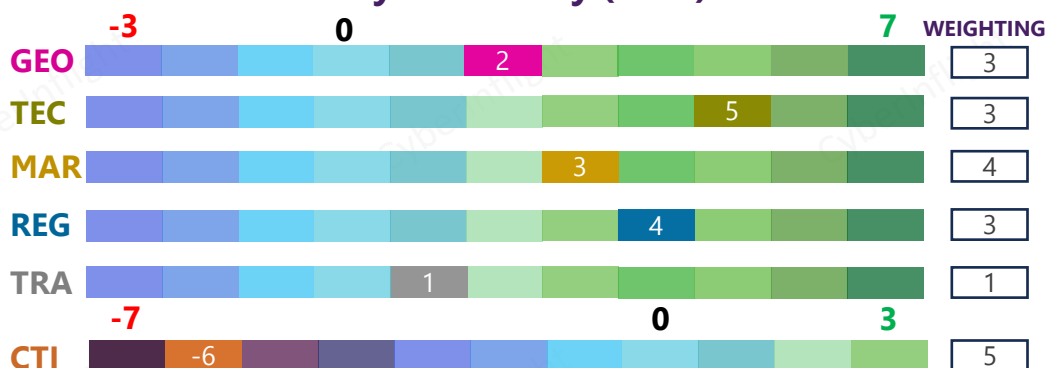
RISC Score Assessment



-0.11
RISC Score

The RISC score for this watch is -0.11, up from last week, notably because of a better score in Technology and Regulation. Overall, however, it remains low because of a disturbed threat climate.

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 some categories were adjusted, as these were rarely assessed negatively and more often show moderate to high positive signals. The weighting of Technology was also increased. This change enables the RISC Score to more accurately capture meaningful variations in the risk environment.

On the geopolitical front, this week, the **21st edition of the Global Risks Report 2026**, published annually by the World Economic Forum, is out. The report analyses global risks, including cyber risks, through 3 timeframes to support decision-makers in balancing current crises and longer-term priorities. On the regulatory side, **the European Commission has proposed a new cybersecurity package to further strengthen the EU's cybersecurity resilience and capabilities. The Proposal for a revised Cybersecurity Act is part of this package.** It aims to increase cybersecurity capabilities and resilience and prevent fragmentation across the EU digital single market. It also seeks to enhance the security of the EU's Information and Communication Technologies (ICT) supply chains, facilitate compliance with existing EU cybersecurity rules, and reinforce the EU Agency for Cybersecurity (ENISA) in its support for Member States and the EU in managing cybersecurity threats. On the technological front, the U.S. Space Force's Space Systems Command (SSC) and Combat Forces Command (CFC) confirmed the **upcoming launch of the ninth Global Positioning System (GPS) III satellite.** Meanwhile, in the threat intel category, Gen. B. Chance Saltzman, chief of Space Force operations, sounds an **alarm over Chinese and Russian space assets in an interview tackling threats in orbit.** On the market front, **Decent Cybersecurity s.r.o. has formally launched a new research and development project** focused on secure communications for space applications, with a total project volume exceeding €4m. The project is funded under the Program Slovensko 2021–2027 and co-financed by the European Regional Development Fund. Lastly, a **roundtable on the cybersecurity and resilience of satellite systems** was hosted by the Embassy of the Czech Republic.

GEOPOLITICS



10 defining moments in Space and Cybersecurity in 2025

The year 2025 has been a defining moment in space and cybersecurity for 2025. [CyberInflight Report Cybersecurity](#)

[Source: CyberInflight](#)

Geopolitical conflict is increasing the risk of cyber disruption

Geopolitical conflict is increasing the risk of cyber disruption. Cyber attacks from governments to disrupt their rivals' efforts to achieve their goals are becoming more frequent. The risk of cyber disruption is increasing as the world becomes more interconnected. The risk of cyber disruption is increasing as the world becomes more interconnected. The risk of cyber disruption is increasing as the world becomes more interconnected.

[Source: CyberInflight](#)

Global Risks Report 2026

The Global Risks Report 2026, the 21st edition of this annual report, marks the second half of a turbulent decade. The report analyses global risks, including cyber risks, through 3 timeframes to support decision-makers in balancing current crises and longer-term priorities. [#WEF #CyberRisks](#)

Sources: [World Economic Forum](#), [Report WEFForum](#)

How space could become the next battlefield

Space is becoming a new arena for conflict. The risk of space conflict is increasing as the world becomes more interconnected. The risk of space conflict is increasing as the world becomes more interconnected. The risk of space conflict is increasing as the world becomes more interconnected.

[Source: CyberInflight](#)

US Space Force is coming to Arizona. Here's what it'll do

The US Space Force is coming to Arizona. Here's what it'll do. The US Space Force is coming to Arizona. Here's what it'll do. The US Space Force is coming to Arizona. Here's what it'll do.

[Source: CyberInflight](#)



Space warfare in 2026: A preview year for US readiness

Space warfare in 2026: A preview year for US readiness. Space warfare in 2026: A preview year for US readiness. Space warfare in 2026: A preview year for US readiness.

[Source: CyberInflight](#)



Space is the fourth battlefield, says former USIA chief

Space is the fourth battlefield, says former USIA chief. Space is the fourth battlefield, says former USIA chief. Space is the fourth battlefield, says former USIA chief.

[Source: CyberInflight](#)



REGULATION



ENISA and National Cyber Security Agency

ENISA and National Cyber Security Agency. ENISA and National Cyber Security Agency. ENISA and National Cyber Security Agency.

[Source: CyberInflight](#)



Proposal for a regulation for the EU Cybersecurity Act

The European Commission has proposed a new cybersecurity package to further strengthen the EU's cybersecurity resilience and capabilities. The Proposal for a revised Cybersecurity Act is part of this package. It aims to increase cybersecurity capabilities and resilience and prevent fragmentation across the EU digital single market. It also seeks to enhance the security of the EU's Information and Communication Technologies (ICT) supply chains, facilitate compliance with existing EU cybersecurity rules, and reinforce the EU Agency for Cybersecurity (ENISA) in supporting Member States and the EU in managing cybersecurity threats. [#EUCybersecurityAct #SupplyChainSecurity](#)

Sources: [The Cyber Express](#), [European Commission](#), [European Commission](#), [Covington](#)



NSA releases Zero Trust Implementation Guidelines

The NSA's Zero Trust Implementation Guidelines (ZTIG) is a framework for implementing Zero Trust (ZT) across the entire organization. It is designed to help organizations understand the principles and practices of ZT, and to provide a roadmap for implementation. The ZTIG is a living document that will be updated as the NSA's understanding of ZT evolves.

NSA releases Zero Trust Implementation Guidelines

The NSA's Zero Trust Implementation Guidelines (ZTIG) is a framework for implementing Zero Trust (ZT) across the entire organization. It is designed to help organizations understand the principles and practices of ZT, and to provide a roadmap for implementation. The ZTIG is a living document that will be updated as the NSA's understanding of ZT evolves.

NSA publishes initial list of hardware and software categories requiring post-quantum cryptography to guide adoption

The NSA's Office of Information Security (OIS) has published an initial list of hardware and software categories that currently require post-quantum cryptography (PQC) standards. The list is intended to help organizations understand the scope of the PQC migration effort, and to provide a roadmap for adoption. The list includes categories such as hardware security modules (HSMs), cryptographic modules, and cryptographic algorithms. The list is a starting point for organizations to begin their PQC migration efforts, and it will be updated as the NSA's understanding of PQC requirements evolves.

NSA releases ZTIG

The NSA's Zero Trust Implementation Guidelines (ZTIG) is a framework for implementing Zero Trust (ZT) across the entire organization. It is designed to help organizations understand the principles and practices of ZT, and to provide a roadmap for implementation. The ZTIG is a living document that will be updated as the NSA's understanding of ZT evolves.

NSA begins work on SP 800-82 to strengthen IT cybersecurity guidance, align with updated NIST framework

The NSA's Office of Information Security (OIS) has begun work on Special Publication (SP) 800-82, a framework for implementing Zero Trust (ZT) across the entire organization. The SP 800-82 is designed to help organizations understand the principles and practices of ZT, and to provide a roadmap for implementation. The SP 800-82 is a living document that will be updated as the NSA's understanding of ZT evolves.

NSA releases ZTIG

The NSA's Zero Trust Implementation Guidelines (ZTIG) is a framework for implementing Zero Trust (ZT) across the entire organization. It is designed to help organizations understand the principles and practices of ZT, and to provide a roadmap for implementation. The ZTIG is a living document that will be updated as the NSA's understanding of ZT evolves.

[illegible]

TECHNOLOGY



U.S. Space Force Field Commands prepare upcoming GPS III launch to enhance warfighter capabilities

In an announcement from El Segundo and Colorado Springs, the U.S. Space Force's Space Systems Command (SSC) and Combat Forces Command (CFC) confirmed the upcoming launch of the ninth Global Positioning System (GPS) III satellite.

#GPSIII #USSF

Source: [satnews](#)



THREAT INTELLIGENCE

Russia spending more on GPS

Russian military spending activity in the satellite domain has increased the role of various GPS-related capabilities.

Source: [satnews](#)



China's space forces are improving and growing

China's military modernization since the start of the twenty-first century has been nothing short of astounding. In the past three decades, it has built thousands of modern combat aircraft, created a growing arsenal of missiles, and fielded the world's largest navy, rapidly changing Australia's strategic environment. But what is the discussion of its space, satellite, and maritime assets. There is a more stark but nonetheless critical element of its modernization: China's space-based capabilities. [Wahneema Lubiano](#)

Source: [The Atlantic](#)



Cyber forces combine internet, a powerful weapon in the hands of new state actors

In spring 2015, the United States and its allies saw a dramatic change in the cyber threat landscape. Since then, cyber forces have been working in a series of coordinated efforts to the point of a conflict with the United States. But what would happen if a state actor were to use its cyber forces to destabilize states in cyber space beyond the traditional realm of cyber operations? [Wahneema Lubiano](#)

Source: [The Atlantic](#)

Did Iran just use Russia's "Volcano" jamming system on Israel?

Iran's military forces in 2015, during the conflict in Syria, used a Russian-made jamming system to disrupt Israeli military operations. [Wahneema Lubiano](#)

Source: [The National Interest](#)



Iranian TV disrupted by hack

Iranian state television's satellite transmission was disrupted in an outage, according to the country's state media outlet, and calling on security forces to investigate the disruption. The outage was reported by the state media outlet, the Islamic Republic of Iran's state television, which has been disrupted several times in the past. The incident was widely reported by state television media outlets as a "hack" of the satellite system. [Wahneema Lubiano](#)

Source: [The National Interest](#)



Space-based supply chain vulnerabilities create emerging operational risks

As commercial space systems grow and governments expand their satellite constellations, the space economy could be hit by 2030, making satellite a key part of global operations, increasing reliance on satellite for supply, communication, and navigation. [Wahneema Lubiano](#)

Source: [satnews](#)

Russian Group conducted 2018 attack on American satellite

A Russian group conducted a 2018 attack on an American satellite, a group of satellite communication, navigation, and surveillance. [Wahneema Lubiano](#)

Source: [satnews](#)



THREAT INTELLIGENCE



There are threats orbiting French commercial satellites

French commercial satellites are being targeted by cyberattacks, according to a report from the French Space Agency (CNES). The report states that these attacks are becoming more frequent and sophisticated, posing a significant threat to the security of French commercial satellites. The attacks are attributed to both state and non-state actors, with the latter being particularly concerning.



'There are threats in orbit': Space Force chief sounds alarm over Chinese, Russian space assets

The head of the U.S. Space Force says his job is to "think about worst-case scenarios" when it comes to potential threats in space, whether they are Russian "nesting doll" satellites or Chinese "grappling arm" tactics that could suddenly become weaponized. "We used to say there are emerging threats. I don't say that anymore. There are threats in orbit," Gen. B. Chance Saltzman, chief of Space Force operations, said in an exclusive video interview with Threat Status at The Washington Times. **#USSF #SpaceThreats**



Source: [The Washington Times](#)

MARKET & COMPETITION

Space Force leads Russian DPA satellite program

The U.S. Space Force has unveiled the Russian DPA (Data Processing and Analysis) satellite program. The program aims to track and analyze satellite data, providing critical intelligence on Russian satellite activities. This program is part of a broader effort to enhance the Space Force's capabilities in monitoring and understanding the Russian space threat.



EU launches EUSpace for AI, Quantum tech to boost digital sovereignty

The European Union has launched EUSpace for AI and Quantum technologies. This initiative aims to foster innovation and digital sovereignty by supporting research and development in these cutting-edge fields. The program will provide funding and resources to European companies and researchers working on AI and Quantum technologies.



Initiative to develop a secure space communication infrastructure

The objective of the initiative is to develop and deploy an advanced secure space communication infrastructure based on a new concept of secure and resilient communication. This infrastructure will ensure the integrity and confidentiality of space communications, protecting against cyber threats and ensuring reliable communication for critical applications.



UK defense tech startup Shield Space raises £10m in funding to protect satellites from jamming and attacks

Shield Space, a UK defense technology startup, has raised £10 million in funding to develop and deploy satellite protection systems. The company's technology is designed to protect satellites from jamming and cyberattacks, ensuring the reliability and security of space-based communication and navigation services.



EU launches new space communication and data in space

The European Union has launched a new initiative to enhance space communication and data in space. This initiative focuses on developing advanced communication systems and data processing capabilities for space applications. The goal is to improve the efficiency and security of space-based communication and data transmission.



Decent Cybersecurity secures over €4m EU-funded project for secure space communications research

Decent Cybersecurity s.r.o. has formally launched a new research and development project focused on secure communications for space applications, with a total project volume exceeding €4m. The project is funded under Program Slovensko 2021–2027 and co-financed by the European Regional Development Fund. **#EU #DecentCybersecurity**

Source: [Decent Cybersecurity](#)



TRAINING & EDUCATION

Dr. Scott Pace invited to a strategic roundtable on cybersecurity and resilience of satellite systems, hosted by the Czech Embassy



Dr. Scott Pace invited to a strategic roundtable on cybersecurity and resilience of satellite systems, hosted by the Czech Embassy

On January 12, 2026, Dr.Scott Pace joined a roundtable focused on the cybersecurity and resilience of satellite systems – a critical issue at the intersection of space, security, and international cooperation. The event was hosted by the Embassy of the Czech Republic. **#StrategicRoundtable #CzechEmbassy**



Source: [Space Policy Institute](#)

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