

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.

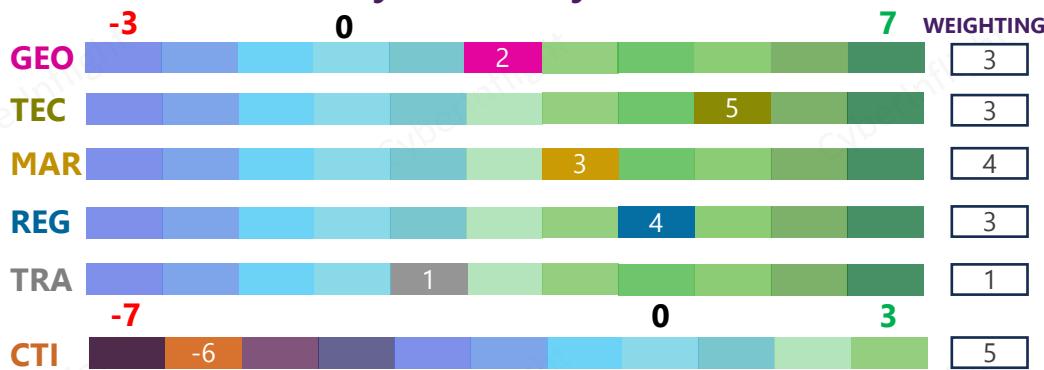
- GEOPOLITICS
- TECHNOLOGY
- MARKET & COMPETITION
- REGULATION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- IMPORTANT NEWS

RISC Score Assessment



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



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 WEForum](#)



REGULATION



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](#)

REGULATION

U.S. Space Force Issues Final Rule on Space Traffic Management

The U.S. Space Force has issued a final rule for the Space Traffic Management (STM) program, marking a significant step forward in the development of a national space traffic management system. The final rule, titled "Space Traffic Management (STM) Program: Final Rule," was published in the Federal Register on January 18, 2024. The rule aims to establish a framework for the safe and responsible operation of objects in space, including the identification, tracking, and avoidance of potential collisions.

The STM program is a key component of the Space Force's mission to ensure the safety and security of space operations. The final rule provides a clear set of guidelines for the operation of the STM system, which will be used to monitor and manage the increasing number of objects in space. The rule also establishes a process for the identification and tracking of objects in space, and provides for the avoidance of potential collisions.

The final rule is the result of a collaborative effort between the Space Force and other government agencies, including the National Aeronautics and Space Administration (NASA) and the Federal Aviation Administration (FAA). The rule is intended to provide a stable and predictable framework for the operation of the STM system, and to ensure that space operations are conducted in a safe and responsible manner.

The final rule is available for public comment until February 19, 2024. The Space Force will consider all comments before finalizing the rule. The rule is expected to take effect on March 1, 2024.



TECHNOLOGY

Advancing the Next-Generation Space-Based Space Weather Monitoring System

The National Oceanic and Atmospheric Administration (NOAA) has announced the selection of a new space-based system to monitor space weather. The new system, known as the Next-Generation Space-Based Space Weather Monitoring System (NG-SBSS), will be built by a team of scientists and engineers from the University of Colorado Boulder and the University of Colorado Denver. The system will be launched in 2026 and will provide real-time data on space weather conditions, including solar flares and geomagnetic storms.

The NG-SBSS system will be built using a combination of satellite and ground-based sensors. The satellite will be positioned in a geostationary orbit, providing a continuous stream of data on space weather conditions. The ground-based sensors will be located in the lower atmosphere, providing additional data on space weather conditions.

The NG-SBSS system is expected to provide a significant improvement in the accuracy and timeliness of space weather forecasts. The system will be able to provide real-time data on space weather conditions, allowing for more accurate forecasts and better preparedness for space weather events.

The NG-SBSS system is a key component of the National Space Weather Program, which is designed to protect the nation's critical infrastructure from the effects of space weather. The program is funded by the National Science Foundation and the National Oceanic and Atmospheric Administration.

The NG-SBSS system is expected to be operational by 2026.



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

China sending over 8000



China's cyber forces are impressive and growing



China's powerful sensors in the hands of new cyber warfare



China

China just sent Russia 'Wukong' growing power on Russia



Russia's 1000 disconnected by Russia



Russia's 1000 disconnected by Russia

Russia's 1000 disconnected by Russia creating emergency of Russia

Russia's 1000 disconnected by Russia creating emergency of Russia



THREAT INTELLIGENCE



'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



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**



TRAINING & EDUCATION



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