

SPACE CYBERSECURITY WEEKLY WATCH

W25

June 16 – June 22, 2026

Timeframe: Weekly

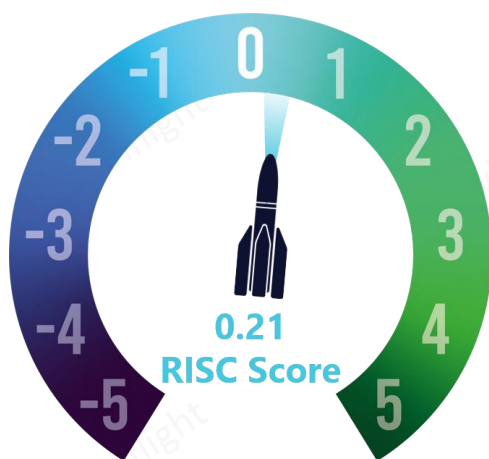
of news identified: 39

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.

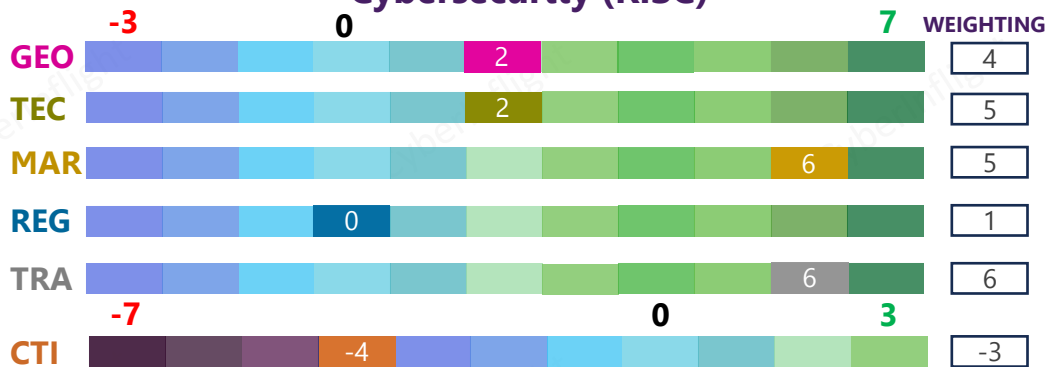
- GEOPOLITICS
- TECHNOLOGY
- MARKET & COMPETITION
- REGULATION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- ★ IMPORTANT NEWS

RISC Score Assessment

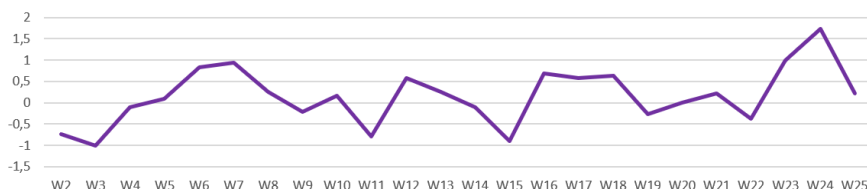


The RISC score for this watch is 0.21, down 1.52 from last week. This is especially due to fewer technological and geopolitical news, balanced by a strong market and training climate.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



This week, CyberInflight is participating in the EU Space ISAC Board and General Meetings, held at EUSPA's premises in Prague. Initially co-chaired by the European Commission's Directorate-General for Defense Industry and Space (DG DEFIS) and EUSPA, these meetings marked another important milestone, with more autonomy given to the industry to run the ISAC, and CyberInflight is willing to take a key role in the future. Moreover, on the geopolitical front, the U.S. Defense Advanced Research Projects Agency (DARPA) is soliciting **input from the space industry through a Request for Information (RFI) on how the United States could rapidly restore critical space capabilities if satellites were disabled or destroyed** during a conflict. On the market side, **Northrop Grumman advances secure, jam-resistant satellite communications with a \$398m USSF award** for the Enhanced Protected Tactical Satellite Communications Prototype (PTS-P), enabling resilient, scalable Ka-band connectivity in contested environments. On the threat front, **Russia has developed an electronic warfare (EW) system** capable of jamming the signal of the Starlink satellite communication system over an area of 20 square kilometers. 2 of them have already been destroyed in recent days. Still on the threat front, an unidentified threat actor claims to possess a **decryption tool and source code capable of compromising the Thuraya-4 satellite communication system and the GRM-1 key recovery mechanism**. On the training side, **the Space Systems Cybersecurity Workshop 2026 will be held in August in Pasadena, California, U.S.** It will focus on technologies, frameworks, and strategies for improving the cyber-resilience of space systems.

CYBERINFLIGHT'S NEWS

★ CyberInflight is participating in the EU Space ISAC Board and General Meetings, held at EUSPA's premises in Prague

Initially co-chaired by the European Commission's Directorate-General for Defence Industry and Space (DG DEFIS) and EUSPA, these meetings marked another important milestone, with more autonomy given to the industry to run the ISAC, and CyberInflight is willing to take a key role in the future. **#EUSpaceISAC #CyberInflight**

Source: [LinkedIn](#)



GEOPOLITICS

★ DARPA to explore ways to rapidly rebuild satellite networks if attacked

The Defense Advanced Research Projects Agency is soliciting input from the space industry on how the United States could rapidly restore critical space capabilities if satellites were disabled or destroyed during a conflict. **#DARPA #RFI**

Sources: [SpaceNews](#), [WPN](#)



France releases the French 2026 version of the dissemination of satellite telecommunications capabilities for the benefit of the armed forces

The French Ministry of the Armed Forces and Veterans is continuing to improve its military capabilities with satellite telecommunications to disseminate information and coordinate operations. **#DARPA #RFI**

Source: [US Intelligence](#)



The space sector under cyber risk in the US based from war

During the last week, the US has been facing a series of cyber attacks against its space sector, including the disabling of several satellites. These attacks highlight the need for the US to develop a more robust and resilient space sector, with a focus on protecting critical infrastructure and ensuring the availability of satellite services. **#DARPA #RFI**

Source: [Reuters](#)



Integrating space for cross-domain operations: Architecture challenges in modern warfare

The space sector is increasingly being used by the US, France, and other countries to support their military operations. This is leading to a growing need for a more integrated and resilient space sector, with a focus on protecting critical infrastructure and ensuring the availability of satellite services. **#DARPA #RFI**

Source: [USCIB News](#)



From orbit to desktop: Why satellite cybersecurity matters in satellite data analysis

Increasingly, the satellite data has become a key source of information for many countries. This is leading to a growing need for a more secure and resilient satellite data analysis, with a focus on protecting critical infrastructure and ensuring the availability of satellite services. **#DARPA #RFI**

Source: [USCIB News](#)

MARKET & COMPETITION

Lockheed Martin awards \$140m USMC contract for 100 M700 & 24, boosting space communications capability

Lockheed Martin announced that the US Space Force has awarded the company a 10-year contract to build and maintain a fleet of 100 M700 and 24 M700-2 satellites. This contract is a significant milestone for Lockheed Martin, as it marks the company's first contract to build and maintain a fleet of satellites. **#DARPA #RFI**

Source: [USCIB News](#)



★ Northrop Grumman to advance military's protected satellite communications

Northrop Grumman advances secure, jam-resistant satellite communications with a \$398m U.S. Space Force award for the Enhanced Protected Tactical Satellite Communications Prototype (PTS-P), enabling resilient, scalable Ka-band connectivity in contested environments. **#NorthropGrumman #USSF**

Sources: [NorthropGrumman](#), [ArabianDefence](#)



USF promotes latest space cybersecurity research in 2024

The US Space Force is increasingly being used by the US, France, and other countries to support their military operations. This is leading to a growing need for a more integrated and resilient space sector, with a focus on protecting critical infrastructure and ensuring the availability of satellite services. **#DARPA #RFI**

Source: [USCIB News](#)



MARKET & COMPETITION

USCIS Systems and MIT sign MOU to strengthen Japan's satellite cyber defense

USCIS Systems and MIT, in cooperation with Japan's Ministry of Defense, signed a Memorandum of Understanding (MOU) to conduct research on the implementation of satellite cyber defense (SCD) solutions for the Japanese government. The MOU demonstrates the intent of both organizations to work together to address satellite cyber threats, building on the cooperation of the Japan-US Strategic Cyber Partnership agreement and the respective governments' security policies. [Read More](#)



UK and Japan launch frontier tech joint briefing to space, space, and quantum

The UK and Japan have launched a new "Frontier Technology Partnership" that highlights the growing cooperation in space, AI, quantum and advanced manufacturing. [Read More](#)



Further evidence for CyberShield, the US CyberShield has now been integrated into Australia's DODged Flow, making one step closer to launch

There is still CyberShield will work as an in-orbit operations designed to strengthen the resilience of space systems against satellite cyber threats. The mission will consist of capabilities, advanced data analysis tools, and cryptographic technologies in a real operational environment. [Read More](#)



Major partners with NATO on AI security detection tool

France is working to provide the satellite defense in the military. The AI-based space security is working with the US Space Force's AI security tool, under a cooperation framework and development agreement. France is already working to do so for terrestrial-based tool with NATO, with hopes of expanding the military partnership with NATO. [Read More](#)



Poland signs bilateral cooperation agreement for satellite communications defense with Japan, India, South Korea and the UK

Poland, Japan and South Korea, India, South Korea, and the United Kingdom signed a bilateral agreement on 16 June signed in bilateral cooperation agreement to develop a comprehensive defense communication satellite technology. The four nations of defense, the protection of satellite communication systems, and the development of the defense communication systems. [Read More](#)



South Korea signs bilateral cooperation agreement for satellite communications defense with Japan, India, South Korea and the UK

South Korea, Japan, India, South Korea, and the United Kingdom signed a bilateral agreement on 16 June signed in bilateral cooperation agreement to develop a comprehensive defense communication satellite technology. The four nations of defense, the protection of satellite communication systems, and the development of the defense communication systems. [Read More](#)



USCIS Systems signs MOU with Korea for Space Quantum Computing Center, joint R&D and government projects

USCIS Systems and Korea signed an MOU to explore space-based quantum computing, including an in-orbit demonstration of a quantum processing unit (QPU) payload and collaboration in future commercial and research activities. [Read More](#)



THREAT INTELLIGENCE



Russians resumed use of stations capable of jamming operation of Starlink satellites: 2 of them have already been destroyed

Russia has developed an electronic warfare (EW) system capable of jamming the signal of the Starlink satellite communication system over an area of 20 square kilometers. Two of them have already been destroyed in recent days.

#Russia #Ukraine

Sources: [UkrainianNews](#), [X](#), [Facebook](#), [Facebook](#), [Defence Industry Europe](#), [Trench Art](#)



THREAT INTELLIGENCE

ISIRI claims 77th Russian SPY targeting satellites and defense

ISIRI claims 77th Russian SPY targeting satellites and defense. The report states that the 77th Russian SPY is targeting satellites and defense systems. The report also mentions that the 77th Russian SPY is targeting satellites and defense systems. The report also mentions that the 77th Russian SPY is targeting satellites and defense systems.

Source: [ISIRI](#)



China unveils space-based control system for high-speed rail, can it be hacked?

China unveils space-based control system for high-speed rail, can it be hacked? The report states that China has unveiled a space-based control system for high-speed rail. The report also mentions that the system can be hacked.

Source: [ISIRI](#)



The growing gap between orbital data collection and data confidence

The growing gap between orbital data collection and data confidence. The report states that there is a growing gap between orbital data collection and data confidence. The report also mentions that the gap is growing.

Source: [ISIRI](#)

How encrypted satellite channels are protected and their content stolen online

How encrypted satellite channels are protected and their content stolen online. The report states that encrypted satellite channels are protected and their content is stolen online. The report also mentions that the content is stolen online.

Source: [ISIRI](#)



An unidentified threat actor is claiming to possess a decryption tool and source code capable of compromising the Thuraya-4 satellite communication system and GRM-1 key recovery mechanism

A threat actor has surfaced on a dark web forum claiming to have successfully developed a decryption tool for the Thuraya-4 satellite communication system and its associated GRM-1 key recovery mechanism. The individual, operating under the alias 'overflow0x4', asserts that they possess both the source code for the tool and video evidence demonstrating the decryption of live communications. **#Decryption #Thuraya-4**

Source: [SOC Radar](#)



Satellite reveals increasing scale of GPS signal tampering

Satellite reveals increasing scale of GPS signal tampering. The report states that a satellite has revealed the increasing scale of GPS signal tampering. The report also mentions that the scale is increasing.

Source: [ISIRI](#)



TECHNOLOGY

ISIRI claims 77th Russian SPY targeting satellites and defense

ISIRI claims 77th Russian SPY targeting satellites and defense. The report states that the 77th Russian SPY is targeting satellites and defense systems. The report also mentions that the 77th Russian SPY is targeting satellites and defense systems.

Source: [ISIRI](#)



ISIRI claims 77th Russian SPY targeting satellites and defense

ISIRI claims 77th Russian SPY targeting satellites and defense. The report states that the 77th Russian SPY is targeting satellites and defense systems. The report also mentions that the 77th Russian SPY is targeting satellites and defense systems.

Source: [ISIRI](#)



TECHNOLOGY

Workshops revitalize the Cyber Resilience Suite

Workshops are an essential part of the Cyber Resilience Suite of Initiatives (CRSI), a portfolio for protecting critical entities and assets against cyber threats. The CRSI workshops focus on enhancing resilience, security, and trust across various sectors, including critical infrastructure, government, and the private sector.

Source: [CyberInflight](#)



Space industry is standardizing on 4G LTE

In the 4G LTE, a standard for 4G LTE, telecommunications industry, software developers, and aerospace engineers gathered to discuss the changing landscape of computing in space. 4G LTE is a key technology for the future of space.

Source: [CyberInflight](#)



TRAINING & EDUCATION



Space Systems Cybersecurity Workshop 2026

The Space Systems Cybersecurity Workshop 2026 will focus on technologies, frameworks, and strategies for improving the cyber-resilience of space systems. This includes cyber-hardening space flight software, vulnerability analysis of space systems, and implementing zero-trust cybersecurity policies into space networks. This workshop is relevant to multiple topics of interest to SMC-IT, including the following: cybersecurity, advanced modeling and digital twins for onboard systems, intelligent and autonomous systems, and software reliability for mission-critical applications.

#Workshop #SpaceSecurity

Source: [IEEE SMC-IT/SCC 2026](#)



2026 2026 Workshop

Workshops are an essential part of the 2026 2026 Workshop, which provides participants with hands-on learning opportunities. The workshops focus on enhancing resilience, security, and trust across various sectors, including critical infrastructure, government, and the private sector.

Source: [CyberInflight](#)



Space cybersecurity is a priority: Defense at Space2026 Day

During the 2026 Space2026 Day, the 2026 2026 Workshop, participants of the administration, space policy, and space security will discuss the challenges and opportunities of space cybersecurity. The workshop will focus on enhancing resilience, security, and trust across various sectors, including critical infrastructure, government, and the private sector.

Source: [CyberInflight](#)



2026 2026 Workshop 2026 2026

The 2026 2026 Workshop 2026 2026 will focus on technologies, frameworks, and strategies for improving the cyber-resilience of space systems. This includes cyber-hardening space flight software, vulnerability analysis of space systems, and implementing zero-trust cybersecurity policies into space networks.

Source: [CyberInflight](#)



From Intelligence/Engineering/IT, Space 'Integrating 4G LTE with 4G LTE Building Hybrid Terrestrial-Space Networks'

The workshop is a key event in the 2026 2026 Workshop, which provides participants with hands-on learning opportunities. The workshop focuses on enhancing resilience, security, and trust across various sectors, including critical infrastructure, government, and the private sector.

Source: [CyberInflight](#)



4G LTE supports highlight role of quantum technologies in future space and security systems

Workshops are an essential part of the 4G LTE, a portfolio for protecting critical entities and assets against cyber threats. The workshops focus on enhancing resilience, security, and trust across various sectors, including critical infrastructure, government, and the private sector.

Source: [CyberInflight](#)



TRAINING & EDUCATION



Contact us at: research@cyberinflight.com