



# SPACE CYBERSECURITY WEEKLY WATCH

Week 35

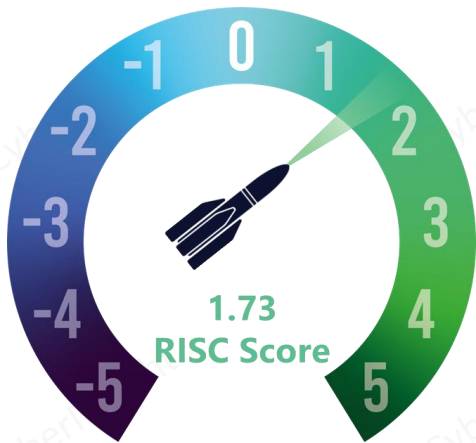
August 26 – September 1, 2025

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

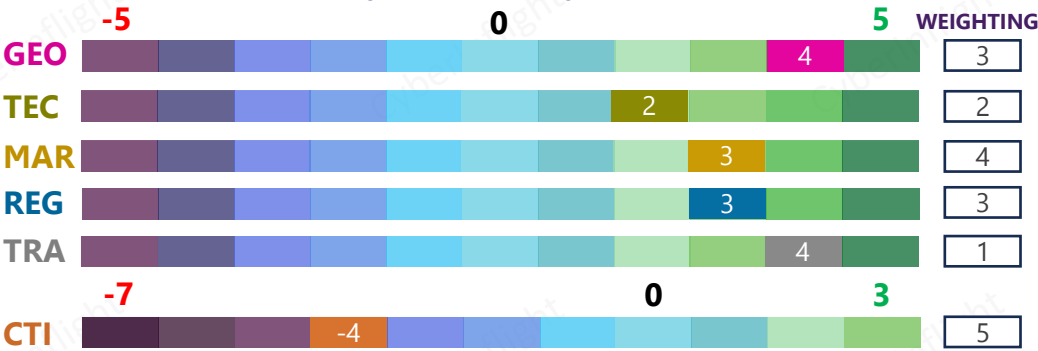
Timeframe: Weekly  
# of articles identified: 35  
Est. time to read: 70 minutes

## RISC Score Assessment

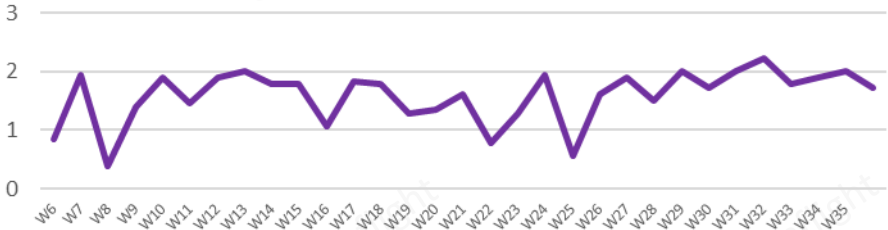


The RISC score for this watch is 1.73, a slight decrease due to more threat intelligence reports than in previous weeks, despite positive developments on the geopolitics, regulation and training fronts.

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



## RISC Score evolution in 2025



This week, Norway announced the establishment of the Norwegian Communications Authority (Nkom) in Tromsø, a new office to answer the growing problem of GPS disruptions in northern Norway, especially in East Finnmark, Svalbard, and the Barents Sea. On the regulation front, China will promote the high-quality development of the satellite communication industry by optimizing business access, according to new guidelines released by the Ministry of Industry and Information Technology (MIIT) this week. Regarding the technological sector, the Australian Defence Force (ADF) has formally stood up a Joint Positioning, Navigation and Timing (PNT) Directorate to ensure operational effectiveness in environments where GPS is degraded or unavailable, as threats from jamming, spoofing, and anti-satellite weapons grow. On the market front, the European Space Agency (ESA) presented its Moonlight program, a joint initiative between ESA’s Directorate of Connectivity and Secure Communications, the Directorate of Navigation, and the Directorate of Human and Robotic Exploration. It aims to lead Europe in enabling connectivity from the lunar surface to the Earth. On the threat intelligence front, it has been announced that the hacking group Lab Dookhtegan allegedly disrupted the communications of 60 Iranian ships. Hackers breached the satellite communications company Fannava, disabling the Falcon communications system and wiping core data. They also published screenshots demonstrating they achieved root access on Linux terminals running iDirect satellite software. The training and education section focuses on a paper that presents HoneySat, the first high-interaction satellite honeypot framework, fully capable of convincingly simulating a real-world CubeSat, a type of Small Satellite (SmallSat).

## GEOPOLITICS

### Japan, British defense chiefs agree to boost cyber, space cooperation

The defense chiefs of Japan and the United Kingdom agreed on August 15 to the UK-Japan defense cooperation to cyber and space security, including cooperation on intelligence, cyber defense, and the critical importance of space capabilities and their resulting defense to collective security, prosperity and well-being. They affirmed their willingness to enhance cooperation in the space domain through exchange of opinions on satellite communications and space threat management. [Ministerial Statement](#)

**Sources:** [Asahi Shimbun](#), [BBC](#)



### India and Japan adopt joint Declaration on security cooperation in space defense, maritime, cyber, and space cooperation across Indo-Pacific

India and Japan issued a joint declaration to their special relationship, which have been in space cooperation, cyber defense, maritime security, and cyber and space security. The declaration states that the two nations will enhance their cooperation in space defense, maritime security, cyber defense, and space security. The declaration also states that the two nations will enhance their cooperation in space defense, maritime security, cyber defense, and space security. The declaration also states that the two nations will enhance their cooperation in space defense, maritime security, cyber defense, and space security. [Ministerial Statement](#)

**Sources:** [Asahi Shimbun](#), [The New York Times](#)



### Hungary's media regulator prioritizes AI, space and quantum tech

Hungary's media regulator, the Media Council, has announced that it will prioritize AI, space and quantum technology in its future work. The Council stated that these technologies are crucial for the future of the country and that it will focus on ensuring their security and integrity. The Council also stated that it will work to ensure that these technologies are used in a responsible and ethical manner. [Media Council Statement](#)

**Sources:** [Asahi Shimbun](#)



### Regjeringen tar grep etter økt GPS-jamming i nord (Trad.: Norwegian government takes action after increased GPS jamming in the north)

A new office of the Norwegian Communications Authority (Nkom) will be established in Tromsø. The news was announced by Minister of Digitalisation and Public Administration Karianne Tung during a visit to the satellite company KSAT in Tromsø. She highlighted that the increased presence in the north, and in Tromsø, is important to strengthen Norway's security. The reason for this move is the growing problem of GPS disruptions in northern Norway, especially in East Finnmark, Svalbard, and the Barents Sea. [#GPSJamming](#) [#Nkom](#)

**Sources:** [Adresseavisen](#), [NRK](#)



## REGULATION



### New satellite rules to drive China's trillion-yuan industry growth

China will promote the high-quality development of the satellite communication industry by optimizing business access, according to new guidelines released by the Ministry of Industry and Information Technology (MIIT) on August 27. The guidelines aim to promote the launch of satellite communication services and stimulate innovation in the commercial space sector. They also seek to foster new drivers of productivity, supporting China's transformation into a manufacturing and cyber power. [#MIIT](#) [#Guidelines](#)

**Source:** [CGTN](#)



### America's satellite data rules legal and cybersecurity concerns

The new satellite data rules of the United States, which were announced on August 27, have raised concerns about the legal and cybersecurity implications of the rules. The rules require satellite operators to provide access to their data to the US government, which has raised concerns about the potential for data breaches and the impact on the satellite industry. [Ministerial Statement](#)

**Sources:** [Asahi Shimbun](#)



### Securing EU cyberintelligence: New cyber requirements in the EU Space Act

A security review of the European Union Space Act, which was adopted in the European Council, has been completed. The review found that the Act contains provisions that are necessary to ensure the security of the EU's space infrastructure. The review also found that the Act contains provisions that are necessary to ensure the security of the EU's space infrastructure. The review also found that the Act contains provisions that are necessary to ensure the security of the EU's space infrastructure. [Ministerial Statement](#)

**Sources:** [Asahi Shimbun](#)



## REGULATION

### Regulation in the U.S. & NATO on GPS

In March 2025, the United States and NATO announced a joint effort to enhance the resilience of GPS signals in the event of a cyber or physical attack. The initiative focuses on developing common standards for GPS receivers and ensuring that critical infrastructure can continue to operate even if GPS signals are degraded or denied. The U.S. and NATO are working to create a framework for GPS receivers that can detect and respond to threats, such as jamming and spoofing. This framework will be used to develop common standards for GPS receivers that can detect and respond to threats, such as jamming and spoofing. This framework will be used to develop common standards for GPS receivers that can detect and respond to threats, such as jamming and spoofing.



### Source: [CyberInflight](#)

### U.S. and NATO announce joint effort to enhance GPS resilience

The United States and NATO have announced a joint effort to enhance the resilience of GPS signals in the event of a cyber or physical attack. The initiative focuses on developing common standards for GPS receivers and ensuring that critical infrastructure can continue to operate even if GPS signals are degraded or denied. The U.S. and NATO are working to create a framework for GPS receivers that can detect and respond to threats, such as jamming and spoofing. This framework will be used to develop common standards for GPS receivers that can detect and respond to threats, such as jamming and spoofing.



### Source: [CyberInflight](#)

## TECHNOLOGY

### ★ Australia stands up joint PNT directorate to counter GPS threats

The Australian Defence Force (ADF) has formally stood up a Joint Positioning, Navigation and Timing (PNT) Directorate, a 17-member unit that has reached initial operating capability and is tasked with ensuring forces can operate effectively when GPS is degraded or denied. As threats from jamming, spoofing, and anti-satellite weapons grow, Defence leaders are moving to reduce reliance on GPS alone. **#ADF #PNT**

**Sources:** [Inside GNSS](#), [Air Land & Sea](#)



### Indonesian Government Announces Joint PNT Directorate to Counter GPS Threats

The Indonesian Government has announced a joint effort to enhance the resilience of GPS signals in the event of a cyber or physical attack. The initiative focuses on developing common standards for GPS receivers and ensuring that critical infrastructure can continue to operate even if GPS signals are degraded or denied. The U.S. and NATO are working to create a framework for GPS receivers that can detect and respond to threats, such as jamming and spoofing. This framework will be used to develop common standards for GPS receivers that can detect and respond to threats, such as jamming and spoofing.



### Source: [CyberInflight](#)

## MARKET & COMPETITION

### U.S. and NATO announce joint effort to enhance GPS resilience

The United States and NATO have announced a joint effort to enhance the resilience of GPS signals in the event of a cyber or physical attack. The initiative focuses on developing common standards for GPS receivers and ensuring that critical infrastructure can continue to operate even if GPS signals are degraded or denied. The U.S. and NATO are working to create a framework for GPS receivers that can detect and respond to threats, such as jamming and spoofing. This framework will be used to develop common standards for GPS receivers that can detect and respond to threats, such as jamming and spoofing.



### Source: [CyberInflight](#)

### U.S. and NATO announce joint effort to enhance GPS resilience

The United States and NATO have announced a joint effort to enhance the resilience of GPS signals in the event of a cyber or physical attack. The initiative focuses on developing common standards for GPS receivers and ensuring that critical infrastructure can continue to operate even if GPS signals are degraded or denied. The U.S. and NATO are working to create a framework for GPS receivers that can detect and respond to threats, such as jamming and spoofing. This framework will be used to develop common standards for GPS receivers that can detect and respond to threats, such as jamming and spoofing.



### Source: [CyberInflight](#)

### ★ Moonlight program aims to lead Europe in enabling connectivity from the lunar surface and to the Earth

The Moonlight program is a joint initiative between ESA's Directorate of Connectivity and Secure Communications, the Directorate of Navigation and the Directorate of Human and Robotic Exploration. Working across Directorates enables ESA to develop the program into a powerful asset for international cooperation among its trusted partners, such as the U.S. and Japan. **#Moonlight #ESA**

**Source:** [ESA](#)



## MARKET & COMPETITION

### USAF launches 'Cyberguard' - A strategic initiative utilizing AI, quantum, and next-generation technologies

The US Air Force announced on August 26 the launch of 'Cyberguard', a strategic initiative designed to enhance the Air Force's cyber defense capabilities. This initiative will leverage AI, quantum computing, and next-generation technologies to protect the Air Force's critical systems and data. The program will focus on developing and deploying advanced cyber defense technologies, including AI-powered threat detection and response systems, quantum-resistant encryption, and next-generation network security solutions. The program is expected to be completed by 2030.



### Italy launches a deep value defense strategy with expanding cyber security and aerospace exposure

Italy has announced a new deep value defense strategy, focusing on expanding its cyber security and aerospace capabilities. The strategy is designed to protect Italy's critical infrastructure and data from cyber threats, while also enhancing its aerospace capabilities. The program will involve the development and deployment of advanced cyber defense technologies, including AI-powered threat detection and response systems, quantum-resistant encryption, and next-generation network security solutions. The program is expected to be completed by 2030.



### Willing to withdraw voluntary export to ground segment network in Switzerland

Switzerland has announced its willingness to withdraw its voluntary export to ground segment network in Switzerland. The network is designed to protect Switzerland's critical infrastructure and data from cyber threats, while also enhancing its aerospace capabilities. The program will involve the development and deployment of advanced cyber defense technologies, including AI-powered threat detection and response systems, quantum-resistant encryption, and next-generation network security solutions. The program is expected to be completed by 2030.



### UK's Gateway One and two space innovations are supporting British defense

The UK's Gateway One and two space innovations are supporting British defense. The program is designed to enhance the UK's cyber defense capabilities, while also enhancing its aerospace capabilities. The program will involve the development and deployment of advanced cyber defense technologies, including AI-powered threat detection and response systems, quantum-resistant encryption, and next-generation network security solutions. The program is expected to be completed by 2030.



## THREAT INTELLIGENCE

### Aviation Researchers allegedly breach Canadian aerospace and defense contractor NDC

Aviation Researchers allegedly breached Canadian aerospace and defense contractor NDC. The breach is believed to have resulted in the theft of sensitive information, including design data and technical specifications. The breach is being investigated by Canadian authorities.



### Lab Dookhtegan struggles to make of cyber incident

Lab Dookhtegan is struggling to make sense of a cyber incident. The incident is believed to have resulted in the theft of sensitive information, including design data and technical specifications. The incident is being investigated by Iranian authorities.



### Lab Dookhtegan hacking group allegedly disrupted communications of 60 Iranian ships run by sanctioned firms NITC and IRISL

The hacking group Lab Dookhtegan allegedly disrupted the communications of 60 Iranian ships. Hackers breached the satellite communications company Fannava, disabling the Falcon communications system and wiping core data. The group published screenshots demonstrating they achieved root access on Linux terminals running iDirect satellite software (version 2.6.35). The software is considered ancient and not compliant with basic cybersecurity standards.



#LabDookhtegan #VSAT

Source: [Security Affairs](#), [Cyber Security News](#)



## THREAT INTELLIGENCE

### Space domain awareness following anomalous behavior detection in orbit

An open domain awareness framework, designed to collect and analyze data, reports, and intelligence, and identify potential threats to space assets, is being developed by the U.S. and other space powers. This system would enable monitoring of space assets in orbit, including those in the vicinity of the United States, and would be used to identify potential threats to space assets. The system would also be used to identify potential threats to space assets, such as identifying potential threats to space assets in orbit.

Source: [Department of Defense, Security & Technology](#)

### Real space war? NATO and Space Force backed with defending against outer space threats

The U.S. Space Force is looking for a way to defend against threats to its assets, including those from China and Russia. The Space Force is looking for a way to defend against threats to its assets, including those from China and Russia. The Space Force is looking for a way to defend against threats to its assets, including those from China and Russia. The Space Force is looking for a way to defend against threats to its assets, including those from China and Russia.

Source: [Yahoo News](#)



## TRAINING & EDUCATION

Space is already militarized. Space forces are looking for ways to defend against threats to their assets, including those from China and Russia. The Space Force is looking for a way to defend against threats to its assets, including those from China and Russia. The Space Force is looking for a way to defend against threats to its assets, including those from China and Russia.

Source: [Yahoo](#)



Space is already militarized. Space forces are looking for ways to defend against threats to their assets, including those from China and Russia. The Space Force is looking for a way to defend against threats to its assets, including those from China and Russia. The Space Force is looking for a way to defend against threats to its assets, including those from China and Russia.

Source: [Yahoo](#)



### Research principal analysis and mitigation of space cyber risks

The research principal analysis and mitigation of space cyber risks. The research principal analysis and mitigation of space cyber risks. The research principal analysis and mitigation of space cyber risks. The research principal analysis and mitigation of space cyber risks. The research principal analysis and mitigation of space cyber risks.

Source: [CyberInflight](#)



### The impact of signal interference on radio-based communications

The impact of signal interference on radio-based communications. The impact of signal interference on radio-based communications. The impact of signal interference on radio-based communications. The impact of signal interference on radio-based communications. The impact of signal interference on radio-based communications.

Source: [CyberInflight](#)



### HoneySat: A network-based satellite honeypot framework

This paper presents HoneySat, the first high-interaction satellite honeypot framework, fully capable of convincingly simulating a real-world CubeSat, a type of Small Satellite (SmallSat). The evidence of HoneySat's effectiveness was provided by surveyed experienced SmallSat operators in charge of in-orbit satellites and deployed HoneySat over the Internet to entice adversaries. The results show that 90% of satellite operators agreed that HoneySat provides a realistic and engaging simulation of a SmallSat mission. **#HoneySat #Paper**

Source: [Cornell University](#)



## TRAINING & EDUCATION

### Space cybersecurity and digital mobility

This report explores the challenges and opportunities of a space-based digital mobility system, focusing on the impact of space-based digital mobility on the security of space-based digital mobility systems. [Read More](#)



### Space-based digital mobility for secure digital mobility systems

This report explores the challenges and opportunities of a space-based digital mobility system, focusing on the impact of space-based digital mobility on the security of space-based digital mobility systems. [Read More](#)



### Space-based digital mobility and digital mobility for secure digital mobility systems

This report explores the challenges and opportunities of a space-based digital mobility system, focusing on the impact of space-based digital mobility on the security of space-based digital mobility systems. [Read More](#)



[Read More](#)

### Space-based digital mobility for secure digital mobility systems

This report explores the challenges and opportunities of a space-based digital mobility system, focusing on the impact of space-based digital mobility on the security of space-based digital mobility systems. [Read More](#)



[Read More](#)

### Building a secure digital mobility system for secure digital mobility systems

This report explores the challenges and opportunities of a space-based digital mobility system, focusing on the impact of space-based digital mobility on the security of space-based digital mobility systems. [Read More](#)



[Read More](#)

### Space-based digital mobility for secure digital mobility systems

This report explores the challenges and opportunities of a space-based digital mobility system, focusing on the impact of space-based digital mobility on the security of space-based digital mobility systems. [Read More](#)



[Read More](#)

### Building a secure digital mobility system for secure digital mobility systems

This report explores the challenges and opportunities of a space-based digital mobility system, focusing on the impact of space-based digital mobility on the security of space-based digital mobility systems. [Read More](#)



[Read More](#)

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)