SPACE CYBERSECURITY WEEKLY WATCH

Week 35

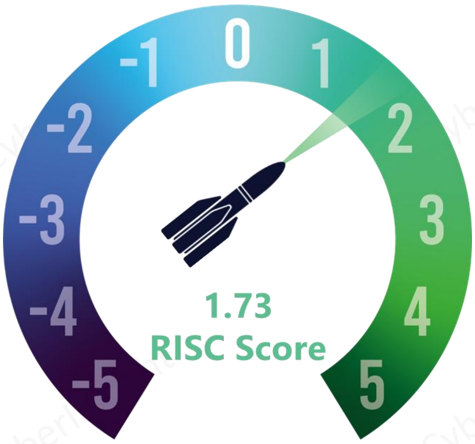
August 26 – September 1, 2025

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

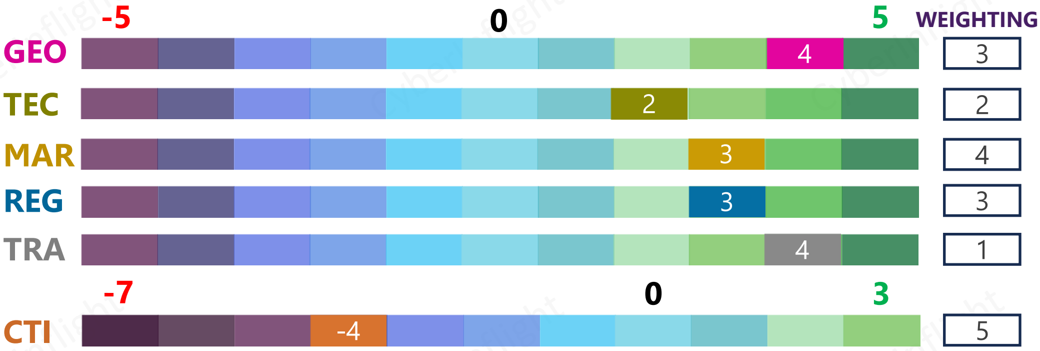
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

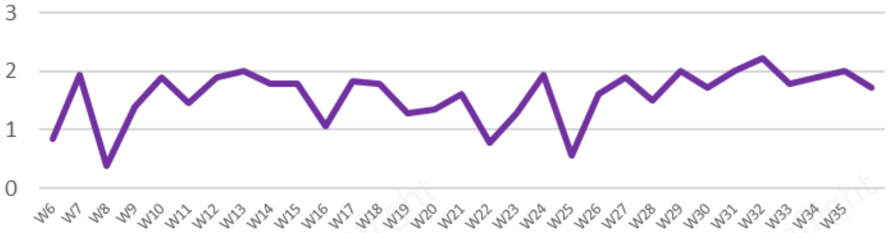
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



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.

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, Britain defence chiefs agree to boost cyber, space cooperation

[illegible]

Sources: [illegible]

India and Japan adopt Joint Declaration on security cooperation to boost defence, maritime, cyber, and space cooperation across Indo-Pacific

[illegible]

Sources: [illegible]

Hungary's media regulator prioritises AI, space and quantum tech

[illegible]

Source: [illegible]

★ 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 missile shield raises legal and cybersecurity concerns

[illegible]

Source: [illegible]

Securing EU CyberSpace: New cyber requirements in the EU Space Act

[illegible]

Source: [illegible]

REGULATION

[illegible]

[illegible]

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*

[illegible]

MARKET & COMPETITION

[illegible]

[illegible]

★ 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

[illegible]

[illegible]

[illegible]

[illegible]

THREAT INTELLIGENCE

[illegible]

[illegible]

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

[illegible]

[illegible]

TRAINING & EDUCATION

[illegible]

[illegible]

[illegible]

[illegible]

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

[redacted]

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