SPACE CYBERSECURITY WEEKLY WATCH

W27

June 30 – July 6, 2026

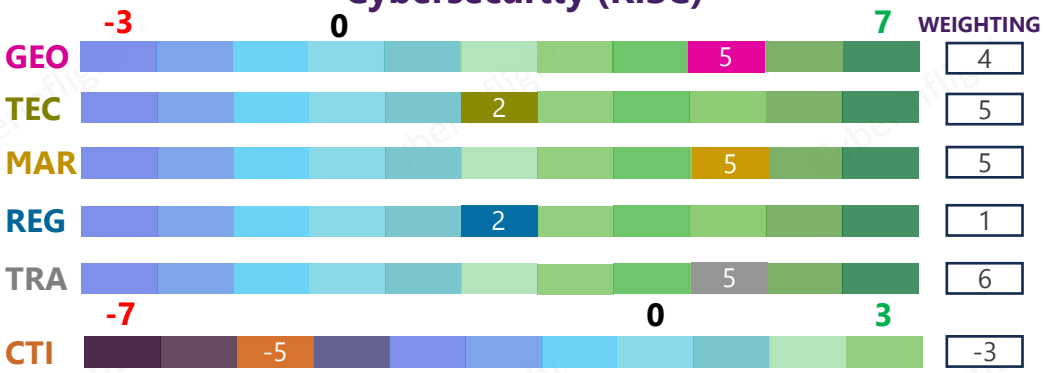
Timeframe: Weekly
# of news identified: 35
Est. time to read: 70 minutes

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

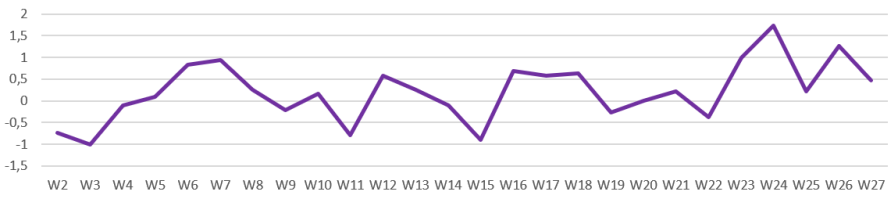
- GEOPOLITICS
- TECHNOLOGY
- MARKET & COMPETITION
- REGULATION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- IMPORTANT NEWS

RISC Score Assessment

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



The RISC score for this watch is 0.47, down 0.79 from last week. This is especially due to fewer technological and market news, and a slight depreciation of the threat intelligence environment, with a few alleged attacks reported.

This week, EUSPA and CyberInflight posted a throwback to the **recent EU Space ISAC Board and General Meetings**, held in June, in Prague, at EUSPA's premises. Participants gained access to critical peer-to-peer vulnerability insights, established real-time early warning pathways, and actively shaped the newly unveiled 2026–2027 roadmap. Meanwhile, on the geopolitical side, the **European Parliament held a discussion on July 1 on the safety of European Union satellites**, the resilience of space-based services, and crisis management. Its central question is whether the current EU framework can ensure continuity of satellite services during a crisis. On the market front, the space-surveillance Luxembourg-backed firm **NorthStar Earth & Space has been tracking the movements of Russian spy satellites for military clients** as Moscow seemed intent on intercepting data from SES and other European-owned spacecraft. On the regulation side, the **U.S. Cybersecurity Maturity Model Certification (CMMC) program is entering a new phase of enforcement**. Beginning Nov. 10, new Department of Defense contracts that include CMMC requirements may require a Level 2 third-party assessment to be on file in the Supplier Performance Risk System. On the threat intel side, **Ukraine struck a space communications center near Moscow**, according to President Volodymyr Zelensky. Zelensky, in a Telegram report, described the target as a special satellite communications facility used for reconnaissance and coordination of Russia's forces in Ukraine. Moreover, **the Gentlemen ransomware gang has listed the NATO contractor Indra Group among its alleged victims**. On the technological front, **Xiphera was selected for the ESA ARTES project to advance secure high-speed satellite communications**. Lastly, the **Greek Space Tech Forum 2026** will take place on Tuesday, July 7, and Wednesday, July 8, 2026.

CYBERINFLIGHT'S NEWS

EU Space ISAC meeting strengthens shared cyber resilience

The recent general meeting of the EU Space Information Sharing and Analysis Centre (EU Space ISAC) in Prague offered public and private stakeholders a direct answer to this challenge: a unified platform for actionable threat intelligence. Participants gained access to critical peer-to-peer vulnerability insights, established real-time early warning pathways and actively shaped the newly unveiled 2026–2027 roadmap. **#EUSpaceISAC #CyberInflight**

Sources: EUSPA, LinkedIn

Kick-off of the new EU Space ISAC Working Group on Space Launcher & Space Transportation

Mid-June marked a milestone for the EU Space ISAC: the official launch, during the General Meeting at EUSPA - EU Agency for the Space Programme's premises in Prague, of a new Working Group dedicated to Space Launcher & Space Transportation cybersecurity. **#EUSpaceISAC #CyberInflight**

Source: LinkedIn

GEOPOLITICS

Opening remarks by Commissioner Kubilius at the seminar "Securing Europe's Eyes in the Sky: the Security of EU Satellites"

The European Parliament held a discussion on July 1 on the safety of European Union satellites, the resilience of space-based services and crisis management. The event was initiated by Members of the European Parliament from the European People's Party group: Paulius Saudargas, Hélder Sousa Silva and Christophe Gomart. Its central question is whether the current EU framework can ensure continuity of satellite services during a crisis. **#Europe #SpaceSecurity**

Source: Kurzycz

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

MARKET & COMPETITION

[redacted]

[redacted]

[redacted]

Luxembourg-backed firm snoops on Russian satellite spies

The fledgling space-surveillance company NorthStar Earth & Space has been tracking the movements of Russian spy satellites for military clients as Moscow seemed intent on intercepting data from SES and other European-owned spacecraft, NorthStar said in a disclosure to investors. **#SpySatellite #NorthStar**

Source: Luxembourg Times

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

REGULATION

CMMC's November deadline forces new calculations across the Space Industrial Base

The Cybersecurity Maturity Model Certification (CMMC) program is entering a new phase of enforcement. Beginning Nov. 10, new Department of Defense contracts that include CMMC requirements may require a Level 2 third-party assessment to be on file in the Supplier Performance Risk System. **#CMMC #SpaceIndustrialBase**

Source: KratosSpace

[redacted]

[redacted]

THREAT INTELLIGENCE

Ukraine hits Moscow's space communications node for second time

Ukraine struck a space communications center near Moscow for the second time on Tuesday, June 30, according to President Volodymyr Zelensky. Zelensky, in a Telegram report, described the target as a special satellite communications facility used for reconnaissance and coordination of Russia's forces in Ukraine. He added that the facility is located more than 500 kilometers (311 miles) from Ukraine's state border. **#Russia #Ukraine**

Source: Kyiv Post

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

THREAT INTELLIGENCE

Hackers threaten to leak data from NATO contractor Indra, as company investigates

The Gentlemen ransomware gang has listed one of Europe's defense powerhouses – the Spanish multinational company and NATO contractor, the Indra Group. So far, it is unknown what kind of data is involved in the alleged data breach. The gang released a post on June 30th on its leak site on the dark web, setting the deadline for the company to start communication. According to the post, Indra Group has 9 days before the data is publicly released. Indra has confirmed a ransomware attack that affected one of its subsidiaries but has "guaranteed the security and continuity of its services. **#NATO #Indra**

Sources: Cybernews, Democrata

TECHNOLOGY

[redacted]

Xiphera selected for ESA ARTES project to advance secure high-speed satellite communications

Xiphera has been selected for a new project under the European Space Agency's (ESA) ARTES program. The project will focus on developing a high-speed security IP core for optical satellite communications, further strengthening Xiphera's position as a provider of advanced hardware-based cybersecurity solutions for the space sector. **#Xiphera #ESAARTES**

Sources: Design&Reuse, TheDefensePost

TRAINING & EDUCATION

[redacted]

TRAINING & EDUCATION

[redacted]

Greek Space Tech forum 2026

The Greek Space Tech Forum 2026 will gather public administration executives and the growing Greek business ecosystem of the space market, aiming to analyze the opportunities and challenges for the further development of the Greek presence. At the same time, it serves as a platform to strengthen collaborations and networking within the Greek space ecosystem, connecting it with critical sectors of the Greek economy as well as abroad—both within the EU and in the wider region of the Southeastern Mediterranean and the Middle East. The Greek Space Tech Forum 2026 – GSTF 2026 will take place on Tuesday, July 7 and Wednesday, July 8, 2026. **#Greece #GSTF2026**

Source: EthosEvents

[redacted]

[redacted]

[redacted]