SPACE CYBERSECURITY WEEKLY WATCH

W18

April 28 – May 4, 2026

Timeframe: Weekly
# of articles identified: 27
Est. time to read: 55 minutes

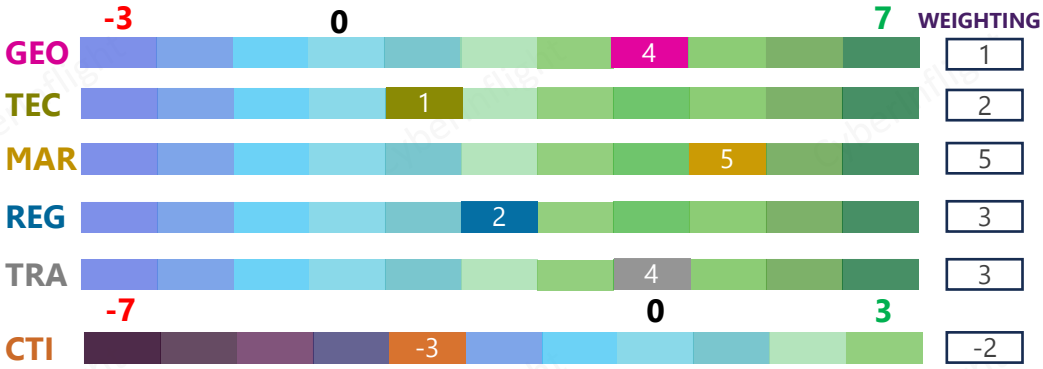
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

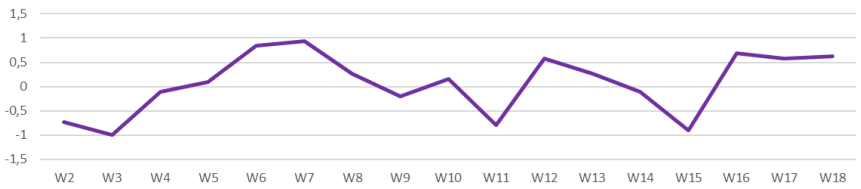
RISC Score Assessment

The RISC score for this watch is 0.63, up 0.5 from last week. This is due to several positive market, geopolitical, and training announcements.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



This week, on the geopolitical front, **the U.S. Space Force would receive an additional $2.9bn over current funding for national security space launches**. Meanwhile, on the European side, **Italian and Spanish institutional and private space stakeholders met in Madrid to foster, together, with the embassy, contacts between Italian and Spanish companies in the space sector**. On the regulation side, the **EEA EFTA States made comments on the proposed EU Space Act**, underlining that a successful Space Act should enhance Europe's competitiveness by fully utilizing the potential of the Internal Market of 30 States. On the market front, **the UK Ministry of Defence has awarded a £6m contract to QinetiQ-led Team Elaris** to develop a deployable solution concept for enhanced Long-Range Navigation, an alternative to satellite-based positioning systems that can continue to function when GPS signals are jammed or spoofed by adversaries. In the threat intel category, an **alleged data leak targeted Blue Origin**, the U.S. space company. The attackers alleged a total of 492GB of sensitive company documents have been leaked, and they are demanding a ransom of $250K. On the technological front, **Telepix and S2W, by signing a Memorandum of Understanding, are set out to build 'Multi-Domain Security AI' combining satellite and dark web**. Lastly, in the training and education side, **VisionSpace announced it will perform a Satellite Radio Analysis & Disruption (S-RAD) training at DEF CON 34.** Participants will work through how satellite links are structured, how signals can be analyzed and manipulated, and how disruptions arise from protocol design, signal-processing assumptions, and operational workflows.

GEOPOLITICS

[redacted]

[redacted]

Source: [redacted]

Budget request directs record $338.8bn to Air Force and Space Force to meet "challenges of today and tomorrow"

Another $500m will be directed to cyber warfare operations to safeguard satellites. The Space Force would also receive an additional $2.9bn over current funding for National Security Space Launches. That boost in funding will procure 22 launches. **#USSF #Budget**

Source: SpaceForce

[redacted]

Source: [redacted]

Italy-Spain institutional and industrial meetings in the space sector

Meetings took place on April 28 and 29 in Madrid, led by the head of the Space Unit at the Office of the Military Advisor to the Prime Minister, Gen. Luigi Riggio, the Director of Space and Science at the Ministry of Foreign Affairs and International Cooperation (MAECI), Minister Plenipotentiary Lamberto Moruzzi, and Lt. Col. Nicola Donati Guerrieri of the Joint Cyber Intelligence Command of the Ministry of Defense, with the aim of fostering, together with the embassy, contacts between Italian and Spanish companies in the space sector. **#Europe #Dialogue**

Source: ANSA

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

REGULATION

[redacted]

[redacted]

Source: [redacted]

REGULATION

[redacted]

EEA EFTA Comment on the EU Space Act Proposal

The EEA EFTA States welcome the EU Space Act proposal and its objective to strengthen the safety, resilience, and sustainability of space activities in the Internal Market. They underline that a successful Space Act should enhance Europe's competitiveness by fully utilizing the potential of the Internal Market of 30 States. **#EFTA #EUSpaceAct**

Source: EFTA

MARKET & COMPETITION

[redacted]

[redacted]

UK funds QinetiQ-led GPS alternative to protect from jamming

The Ministry of Defence has awarded a £6m contract to QinetiQ-led Team Elaris to develop a deployable solution concept for enhanced Long-Range Navigation, an alternative to satellite-based positioning systems that can continue to function when GPS signals are jammed or spoofed by adversaries, according to QinetiQ. **#QinetiQ #UKMoD**

Sources: Ukdj, MSN

[redacted]

[redacted]

THREAT INTELLIGENCE

[redacted]

THREAT INTELLIGENCE

The alleged hack announcement is detected for Blue Origin

A total of 492GB of sensitive company documents have allegedly been leaked, and attackers are demanding a ransom of $250K. **#DataLeak #BlueOrigin**

Source: SOCRadar

[redacted]

[redacted]

TECHNOLOGY

Telepix and S2W set out to build 'Multi-Domain Security AI' combining satellite and dark web

Cooperation in next-generation security technologies combining space data and cyber intelligence is set to begin in earnest. TelePIX, a space AI solution company, announced that it has signed a Memorandum of Understanding (MOU) with S2W, a big data AI company, to advance security intelligence. **#TelePIX #S2W**

Source: VentureSquare

[redacted]

TRAINING & EDUCATION

[redacted]

Satellite Radio Analysis & Disruption (S-RAD) training at DEF CON 34

This training is built around real satellite radio systems, not just theory. You will work through how satellite links are structured, how signals can be analyzed and manipulated, and how disruptions arise from protocol design, signal-processing assumptions, and operational workflows. **#VisionSpace #DEFCON**

Source: Linkedin

[redacted]

TRAINING & EDUCATION

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