SPACE CYBERSECURITY WEEKLY WATCH

W30

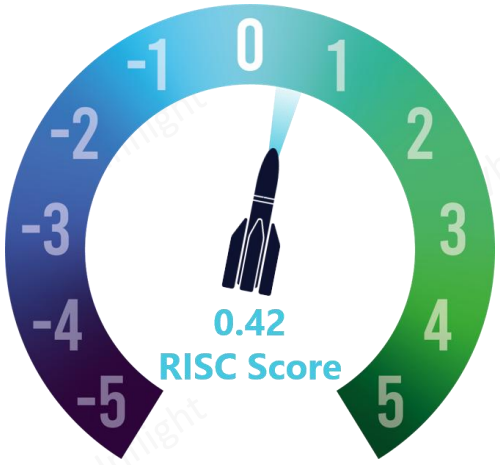
July 21 – 27, 2026

Timeframe: Weekly
# of news identified: 58
Est. time to read: 90 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.

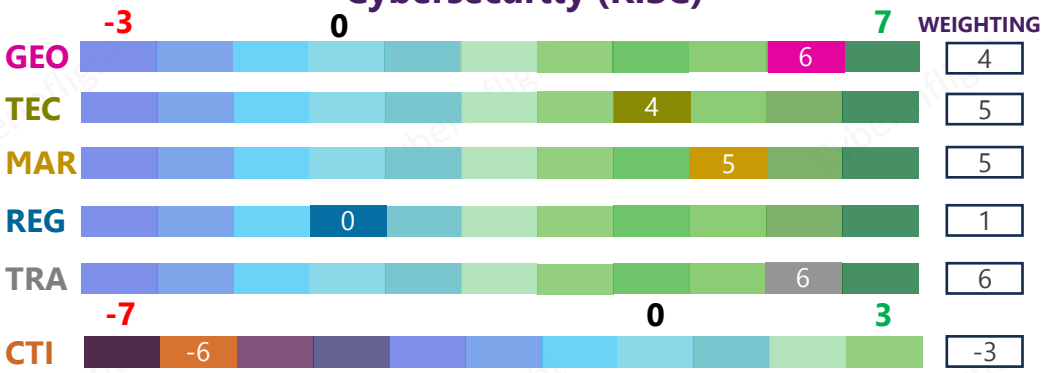
- GEOPOLITICS
- TECHNOLOGY
- MARKET & COMPETITION
- REGULATION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- IMPORTANT NEWS

RISC Score Assessment

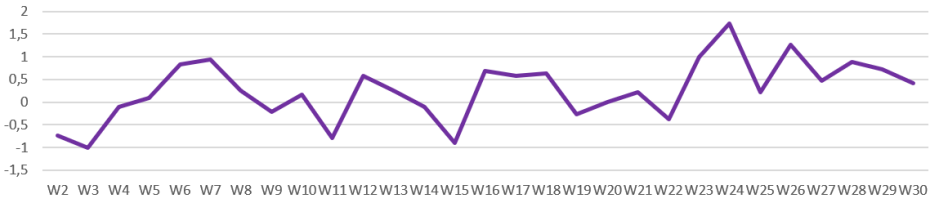


The RISC score for this watch is 0.42, a decrease from last week. This is due mainly to several news items in the Threat Intel section.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



This week, discover some insights about the **2026 General Meeting of the EU Space ISAC** that brought together institutions, authorities, and companies in the space sector, such as CyberInflight. On the geopolitical side, the **House Appropriations Committee (HAC) recommended roughly $55.6bn in discretionary funding for the USSF**. Still on the geopolitical front, an article examines the **cybersecurity challenges facing the Space Defense Industrial Base (SDIB)** as military space operations become increasingly dependent on commercial partnerships, interconnected digital infrastructure, and rapidly expanding industrial capabilities. On the market side, during Thales' first-half financial presentation, Chairman and Chief Executive Officer Patrice Caine addressed investors and confirmed that **development work on the European Union's IRIS² secure satellite communications constellation is progressing as planned**. Meanwhile, on the threat side, an actor claims to have **leaked an internal technical document from the Starshield Constellation program**, developed by SpaceX, that allegedly provides a detailed technical baseline and architecture description of the Starshield constellation, which is a secure satellite network designed for Earth observation, secure communications, and data relay. Moreover, during the U.S. Joint Readiness Training Center (JRTC) rotation 26-06, the 3rd Mobile Brigade (MB), 101st Airborne Division (Air Assault), faced **simulated adversary cyber and electronic warfare attacks – dubbed "Operation Space Jam –** that disabled commercial satellite communications (COMSATCOM). On the technological side, the **SnT and the NSPA launch an AI system to counter satellite jamming**. Lastly, CERT-In, in collaboration with SIA-India and IN-SPACe, has successfully conducted **Cy-AI-X 2026 for Space Sector**, and a **podcast by Space Cafe Radio** was released about Cyber-threats in space.

CYBERINFLIGHT'S NEWS

The EU Space ISAC strengthens European space cybersecurity. Presentation of the 2026–2027 roadmap

Cybersecurity has become one of the key issues for Europe's future in space. Against this rapidly evolving backdrop, the 2026 General Meeting of the EU Space ISAC (Information Sharing and Analysis Center) was held at EUSPA's headquarters in Prague. The meeting brought together institutions, authorities, and companies in the sector to strengthen cooperation in protecting space infrastructure and sharing information on cyber-threats, such as CyberInflight.

#EUSpaceISAC #CyberInflight

Source: Key4Biz

GEOPOLITICS

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

How Congress is pressing the U.S. Space Force to mature

The House Appropriations Committee (HAC) recommended roughly $55.6bn in discretionary funding for the U.S. Space Force. However, HAC provided more than just funds; its report reads like a maturity test for Washington's newest military service: Congress wants faster acquisition, more maneuverable spacecraft, stronger industrial competition, smarter classification standards, and evidence that America's space architecture can survive in a contested domain.

#Congress #USSF

Source: FDD

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

GEOPOLITICS

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Building mission assurance into the space Defense Industrial Base

This article examines the cybersecurity challenges facing the Space Defense Industrial Base (SDIB) as military space operations become increasingly dependent on commercial partnerships, interconnected digital infrastructure, and rapidly expanding industrial capabilities. **#SpaceDIB #MissionAssurance**

Source: The Cyber Defense Review

[redacted]

[redacted]

[redacted]

MARKET & COMPETITION

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Thales CEO confirms progression on EU's multi-billion euro IRIS² sovereign satellite constellation

Addressing investors during Thales' first-half financial presentation on Thursday, July 23, 2026, Chairman and Chief Executive Officer Patrice Caine confirmed that development work on the European Union's IRIS² secure satellite communications constellation is progressing as planned. **#Thales #IRIS2**

Source: satnews

[redacted]

THREAT INTELLIGENCE

[redacted]

THREAT INTELLIGENCE

[illegible]

[illegible]



[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]



[illegible]

[illegible]



Starshield exposed: Inside SpaceX's next-gen satellite architecture











An actor leaks an internal technical document from the Starshield Constellation program, developed by SpaceX that allegedly provides a detailed technical baseline and architecture description of the Starshield constellation, which is a secure satellite network designed for Earth observation, secure communications, and data relay. **#Starshield #DataLeak**



Source: BFD Forum



THREAT INTELLIGENCE

[redacted]



[redacted]



[redacted]



[redacted]



Resilience through redundancy



The enduring Signaleer builds resilient networks not by preventing failure, but by ensuring the formation can fight through it. During Joint Readiness Training Center (JRTC) rotation 26-06, the 3rd Mobile Brigade (MB), 101st Airborne Division (Air Assault), faced simulated adversary cyber and electronic warfare attacks – dubbed "Operation Space Jam – that disabled commercial satellite communications (COMSATCOM). **#JRTC #Exercice**

Source: Line of Departure

TECHNOLOGY

[redacted]



The SnT and the NSPA launch an AI system to counter satellite jamming



In response to the rise in attacks on satellite communications, the SnT at the University of Luxembourg and the NATO Support and Procurement Agency (NSPA) are launching an artificial intelligence-based research project. The aim is to strengthen NATO's communications resilience against new jamming techniques. **#NSPA #AI**

Source: Delano

[redacted]



TECHNOLOGY

[redacted]



[redacted]



TRAINING & EDUCATION

★

CERT-In, in collaboration with SIA-India and IN-SPACe, has successfully conducted Cy-AI-X 2026 for Space Sector

With participation from 70+ professionals representing start-ups and MSMEs across the space ecosystem, the program combined expert sessions, strategic & operational Tabletop Exercise and hands-on technical cyber drill to strengthen organizational preparedness, incident response, crisis coordination, business continuity, secure recovery and resilience against sophisticated AI-enabled cyber threats. **#CERT-In #India**

Source: Facebook



[redacted]



[redacted]



[redacted]



[redacted]



[redacted]



[redacted]

TRAINING & EDUCATION

[redacted]



[redacted]



[redacted]



[redacted]



Space Cafe Radio – Cyber-threats in space: Why the ground segment is the real target with Roger Patrick



"If someone ever claims they've finished implementing all the cyber, it's nonsense – it's a continually evolving problem." That clear-eyed honesty runs through this entire conversation, recorded live at SmallSat Europe in Amsterdam, where Torsten Kriening sits down with Roger Patrick, Director of Sales and Business Development at TERMA.

#Podcast #SmallSatEurope

Source: Space Watch Global

[redacted]



[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