SPACE CYBERSECURITY WEEKLY WATCH

W8

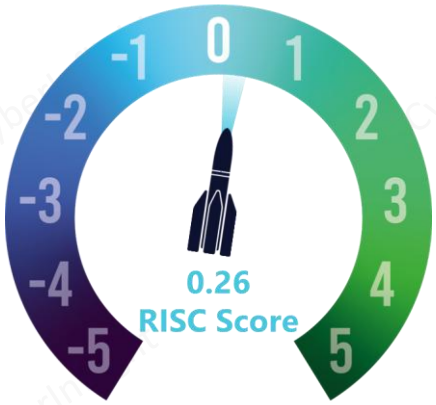
February 17 – 23, 2026

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

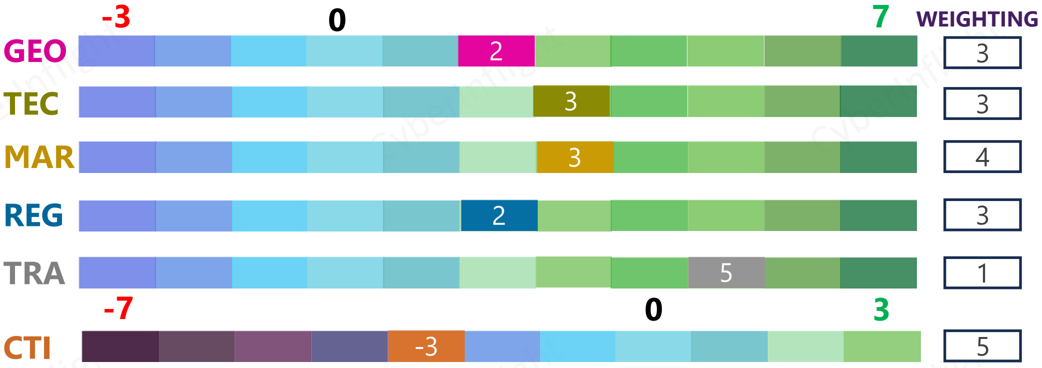
Timeframe: Weekly
# of articles identified: 20
Est. time to read: 45 minutes

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

RISC Score Assessment

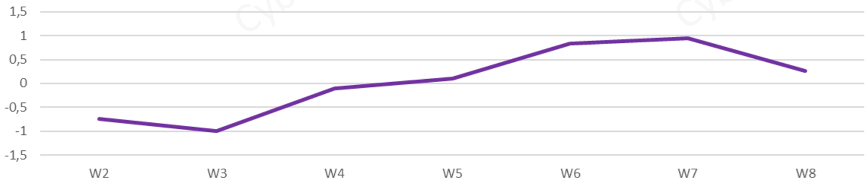


Overview & Resilience Index for Space Cybersecurity (RISC)



The RISC score for this watch is 0.26, down from last week, due to a poor Market and Geopolitical week.

RISC Score evolution in 2026



This week, the **French Space Command launched the sixth edition of its SparteX exercise** in Toulouse, aiming to demonstrate operational credibility in space as a new "conflict environment." General Vincent Chusseau emphasized the need to prepare for emerging threats in orbit, reflecting Europe's commitment to securing its space assets amid rising global tensions. On the regulatory side, **ENISA published its Cybersecurity Exercise Methodology**, providing a standardized framework for designing, conducting, and evaluating cybersecurity exercises across the EU. On the market front, Spain's **Indra signed strategic agreements with Italy's Elt Group and Leonardo** to strengthen cooperation in multi-domain defense, including space and cybersecurity. The partnerships aim to expand their joint capabilities in Europe, NATO, and high-potential markets, reinforcing Europe's sovereign defense industry. On the threat intel front, French aerospace giant **Safran suffered a significant data breach**, with a threat actor leaking over 1m internal records on a hacking forum. On the technological side, **Thales Alenia Space delivered the first Celeste navigation satellite for ESA's LEO-PNT mission.** Designed to operate alongside Galileo, Celeste will provide centimeter-level geolocation accuracy and enhanced resilience against jamming and spoofing, marking a major step forward for Europe's sovereign navigation capabilities. Lastly, the **U.S. Space Force's SWORD platform** emerged as a key tool for maintaining space superiority. This cloud-based, synthetic training environment simulates contested space operations—including electronic warfare and cyber effects—enabling realistic, decentralized training for guardians without relying on live assets.

GEOPOLITICS

[illegible]

★ In Toulouse, the French army is getting to grips with space, the new “conflict zone,” in the SparteX exercise

The French Space Command is conducting the sixth edition of its annual space exercise in Toulouse in order to “demonstrate our operational credibility” in this new “conflict environment,” General Vincent Chusseau, head of the CDE, told reporters on Wednesday. **#SparteX #ConflictEnvironment**

Source: France24

REGULATION

[illegible]

★ ENISA publishes Cybersecurity Exercise Methodology to guide and standardize EU cybersecurity exercises

The European Union Agency for Cybersecurity (ENISA) published its Cybersecurity Exercise Methodology, offering organizations comprehensive guidance in designing, conducting, and evaluating cybersecurity exercises from start to finish. The methodology presents an end-to-end theoretical framework that ensures the right stakeholders and profiles are involved at the appropriate stages. It draws on lessons learned, industry best practices, and cybersecurity expertise and has been designed to be used alongside a support toolkit that includes templates and guidance materials to help planners organize effective exercises. **#ENISA #ExerciceMethodology**

Source: Industrial Cyber

MARKET & COMPETITION

[illegible]

★ Indra signs cooperation agreements with Italian companies Elt Group and Leonardo

The Spanish company and Italy’s Elt Group have signed a collaboration agreement aimed at strengthening their industrial and technological cooperation in multi-domain defence, establishing a common framework for developing and promoting collaboration in three key areas: the land domain, the space domain and unmanned aerial vehicles. Indra Group and Leonardo have also signed a Memorandum of Understanding (MoU) to reinforce their cooperation in cyber defence, with the aim of jointly identifying and expanding their international reach within Europe, NATO and in other high-potential markets. **#Collaboration #SpaceDefense**

Sources: The Corner, Defense Arabia

[illegible]

THREAT INTELLIGENCE

[redacted]

[redacted]

★ Safran SA data breach exposes aerospace supply chain records

Safran S.A., a French multinational aerospace and defense company, has allegedly been compromised after a threat actor posted its database and internal files on a popular hacking forum. The leak purportedly impacts 1,030,031 lines of internal records. **#DataLeak #Safran**

Sources: Daily Dark Web, X

[redacted]

TECHNOLOGY

[redacted]

★ Space: Thales Alenia Space delivers the first European Celeste navigation satellite

The first in-orbit demonstration satellite (IOD-2) of the European Space Agency's (ESA) Celeste mission (formerly known as LEO-PNT) has officially begun its journey ahead of launch. This program aims to strengthen resilience and exponentially improve the performance of existing navigation services. Built on a multi-orbit approach, it will operate alongside Galileo and other satellite navigation systems to offer centimeter-level geolocation accuracy, increased robustness, and high resistance to jamming and spoofing. **#Celeste #ESA**

Sources: Inside GNSS, Report Difesa,

[redacted]

TRAINING & EDUCATION

★ SWORD training platform key to US space superiority, program head says

SWORD, the Space Force's primary synthetic training environment, is a cloud-enabled, digital simulation platform designed to replicate contested space operations, including orbital dynamics, electronic warfare, cyber effects and adversary tactics. It allows guardians to train in realistic scenarios without relying solely on live, on-orbit assets or centralized facilities. **#TrainingPlateform #Exercice**

Source: C4ISRNET

Key themes at the Munich Cyber Security Conference 2026

The Munich Cyber Security Conference 2026 centered on the recognition that cybersecurity has evolved from a technical discipline into a core pillar of geopolitical stability, economic security, and military power. Throughout the discussions, speakers repeatedly emphasized that resilience and traditional defensive measures are no longer sufficient in the face of increasingly sophisticated and politically motivated cyber threats. **#Conference #Cybersecurity**

Source: [illegible]

Cybersecurity of Quantum Key Distribution Implementations

Practical implementations of Quantum Key Distribution (QKD) often deviate from the theoretical protocols, exposing the implementations to various attacks even when the underlying (ideal) protocol is proven secure. We present new analysis tools and methodologies for quantum cybersecurity, adapting the concepts of vulnerabilities, attack surfaces, and exploits from classical cybersecurity to QKD implementation attacks. **#Paper #QKD**

Source: Cornell University

A political space: Satellites as instruments of space defense (Euronews Tech Talk)

Podcast episode of Euronews Tech Talk, about the position of the EU in space and a presentation of the program GOVSATCOM for Europe. **#Podcast #GOVSATCOM**

Source: Euronews

Le Général qui prépare la guerre spatiale (Michel Friedling) *(Trad.: The General Preparing for Space Warfare)*

Podcast episode of Charles Gaillard with Michel Friedling, a former fighter pilot who became France's first Space Commander, then a space entrepreneur, co-founding Look Up. **#Podcast #LookUp**

Source: YouTube

Space Cybersecurity Innovation Through AI and OrbitWhisperer

Embry-Riddle professor [illegible] is defining the future of space cybersecurity and AI-driven resilience with the help of undergraduate students through her recently developed satellite resilience framework, OrbitWhisperer.

#OrbitWhisperer #AI

Source: [illegible]

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