SPACE CYBERSECURITY WEEKLY WATCH

W38

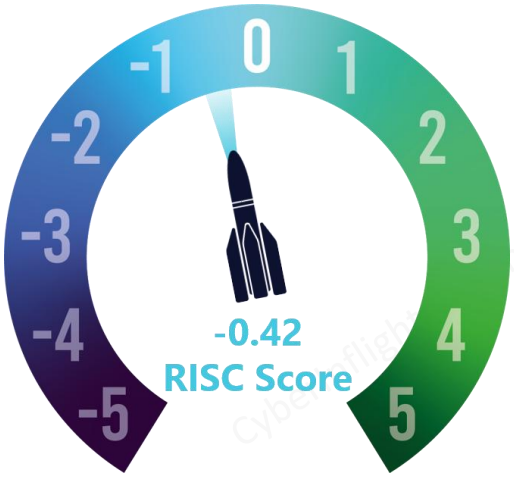
September 15 – September 21, 2026

Timeframe: Weekly
# of news identified: 21
Est. time to read: 40 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.

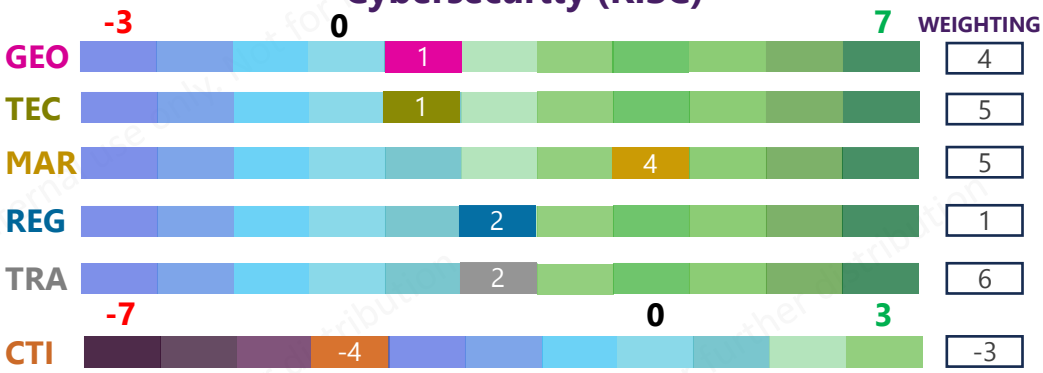
GEOPOLITICS
TECHNOLOGY
MARKET & COMPETITION
REGULATION
TRAINING & EDUCATION
THREAT INTELLIGENCE
IMPORTANT NEWS

RISC Score Assessment

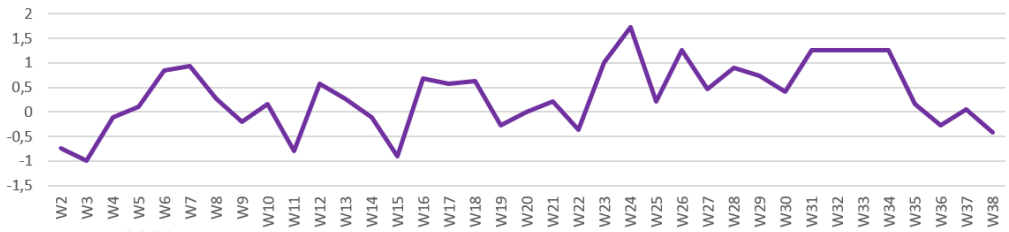


The RISC score for this watch is -0.42, a decrease of 0.47 since last week. This decrease is particularly due to a few news items in geopolitics and technology.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



This week, **the U.S. Space Force emphasized the need for speed, scale, and a more dynamic culture in space warfare**. This discussion came less than 2 months after U.S. Space Command released The Space Warfighting Environment 2040, a warfighter-centered look at how the Joint Force may have to operate in an increasingly crowded and contested space domain. In parallel, **the Air Force confirmed the deployment of on-orbit weapons for space control**, a major announcement made by Secretary of the Air Force Troy Meink.

On the market front, **KAIperShield and Cyber in Space formed a partnership** to expand NASA JPL-developed cyber resilience and mission assurance capabilities across Australia, New Zealand, and the wider Indo-Pacific region.

In Europe, frameworks such as the EU Space Act and NIS2 are shaping the governance of space cybersecurity. An article addresses the **contested boundaries of sectoral oversight in an increasingly commercialized and contested orbital environment**.

On the technological side, L3Harris Technologies announced its **RASOR hybrid satellite communications system is on track to receive NSA Type 1 certification** in early 2027, designed to maintain connectivity amid jamming and cyber disruptions.

Lastly, **Brazil's space cybersecurity initiative AuroraWatch-1**, a fictional educational assessment for a simulated LEO Earth-observation mission that offers a hands-on training approach for the region, has been announced.

GEOPOLITICS

Bythewood: Space warfare demands speed, scale, and a dynamic culture

Speed, scale and a dynamic culture: that's what it will take for the U.S. Space Force to keep pace with a rapidly evolving space fight, Lt. Gen. Dennis O. Bythewood said Sept. 14. The discussion came less than 2 months after U.S. Space Command released The Space Warfighting Environment 2040, a warfighter-centered look at how the Joint Force may have to operate in an increasingly crowded and contested space domain. It builds on Space Force efforts to define the future operating environment and the force needed to succeed in it. **#SpaceWarfare #AirSpace&Cyber**

Source: U.S. Space Forces

EXPERT OPINION – Space: The new battleground for cyber conflicts

Satellite infrastructure now plays a critical role in telecommunications, logistics, geolocation, and system synchronization. Michael Freeman, Head of Threat Intelligence at Armis, explains why its growing integration into digital ecosystems is also expanding the scope of cyber threats. **#CyberWarfare #SpaceInfra**

Source: Solutions numériques & cybersécurité

MARKET & COMPETITION

KAIperShield and Cyber in space form Indo-Pacific partnership on mission-focused cyber resilience

KAIperShield and Cyber in Space have signed a business development and customer engagement agreement to expand access to cyber resilience and mission assurance capabilities developed at NASA's Jet Propulsion Laboratory across Australia, New Zealand, and the wider Indo-Pacific. **#KAIperShield #IndoPacific**

Source: Australian Cybersecurity Magazine

Could secure satellite launch change the bull case for MDA Space stock?

The AURORA BLACK announcement is the clearest operational link to current demand from defense and government. It directly targets sovereign secure communications, which already fall within MDA Space's core offerings in broadband, direct-to-device, and defense command and control. The move aligns the satellite systems segment more closely with rising security-focused spending that has been flowing into the sector. **#MDASpace #AURORABLACK**

Source: Simply WallSt

Unseenlabs and Airbus develop military satellites

France's Minister for the Armed Forces and Veterans' Affairs announced that the Directorate-General for Armament (DGA) had awarded the CASSIOPÉE contract to Airbus Defence and Space as the lêd contractor and its co-contractor Unseenlabs, thereby initiating the renewal of France's space-based SIgnal INTelligence (SIGINT) capability. **#ADS #Contract**

Source: AeroMorning, Democrata

QSE advances European space security strategy through ESA engagement

During the mission, the company attended the delegation's meetings at ESA focused on Earth Observation programs to better understand emerging security requirements and potential applications of post-quantum cybersecurity for future satellite and space infrastructure. QSE also participated in sessions at the Canadian Embassy in The Hague and in Delft with organizations such as QDNL, House of Quantum, and TNO, discussing potential forms of cooperation in quantum communications, secure technologies, and satellite applications as part of its broader international growth strategy.

#PQC #QSE

Source: Stock Titan

Europe to test secure satellite communications against disruption and cyberattacks

Cybersecurity company CybExer is leading a ten-company European consortium developing an end-to-end capability to test and validate protected satellite communications linked to IRIS², the EU's future secure satellite connectivity system. **#CybExer #SATCOM**

Source: The Baltic Times

REGULATION

'Space technology should improve life on Earth' – Barbara Frei-Spreiter on the Swiss space program, caught between the global market and security policy

Since April 2026, Dr. Barbara Frei-Spreiter has been at the helm of Beyond Gravity, the largest Swiss aerospace supplier operating internationally, with 12 sites across six countries. Within this interview, she mentions the fact that Beyond Gravity is currently complying with its cybersecurity level to the U.S. CMMC Cybersecurity standard. **#CRA #CyberReporting**

Source: satw

CyberInflight

REGULATION

Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2026

The Federal Information Security Modernization Act requires the Office of Inspector General to conduct an annual evaluation of NASA's information security program. For fiscal year 2026, we rated NASA's information security program at a Level 3—meaning policies, procedures, and strategies were consistently implemented, but quantitative and qualitative effectiveness measures were lacking—a rating that falls short of being considered effective. **#NASA #OIG**

Source: NASA

Governing the cybersecurity of the European space ecosystem: the EU space act, NIS2, and the contested boundaries of sectoral specialty

The "Space 4.0" transition—a crowded, commercialized, and contested orbital environment populated by new spacefaring nations and private operators—has made the cybersecurity of space infrastructure a governance problem rather than a technical one. **#EUSpaceAct #NIS2**

Source: frontiers

THREAT INTELLIGENCE

U.S. admits it has weapons in orbit

Secretary of the Air Force Troy Meink made a bombshell admission this morning, disclosing that there are on-orbit weapons deployed right now to protect America's interests in space. Those weapons support a Space Control mission set, and the U.S. Space Force has now also shared additional details about that directly with TWZ. **#USSF #SpaceWeapons**

Sources: TWZ, TV5 Monde Info

CVE-2026-38058

A high-severity vulnerability, CVE-2026-38058, affects ST Engineering iDirect Evolution iQ-Series terminals. The flaw resides within a configuration endpoint that exports device settings in JSON format. **#CVE #STEngineering**

Source: LinkedIn

International Meteor Organization says cyberattack dealt 'critical blow' to website

A cyberattack has shut down the website of the premier international organization responsible for tracking meteors. The International Meteor Organization (IMO) has continued to track asteroids and meteors via its Facebook page, but its website now displays a static page notifying visitors of the cyberattack. **#IMO #Cyberattack**

Source: The Record

Space systems may become targets and tools for cyberattacks, Kaspersky warns

Kaspersky researchers audited internet-exposed GNSS hardware in collaboration with 70 global equipment vendors. They discovered that more than 3,000 GNSS receivers are directly vulnerable to attacks over the internet, posing severe risks to maritime, aviation, and land logistics. **#Kaspersky #GNSSdevices**

Sources: Kaspersky, Gulf Business

New details on how Space Force has waged Electronic Warfare against Iran

U.S. Space Force's top officer has shared new details about his service's use of electronic warfare capabilities during Operation Epic Fury against Iran earlier this year. This underscores how space is steadily becoming an arena where conflict actually occurs, and the implications this has for forces operating inside and outside of the Earth's atmosphere. **#EW #USSF**

Source: TWZ

Critical SSRF vulnerability discovered in Zenith satellite tracker 1.0

A critical security flaw has been identified in the Zenith Satellite Tracker 1.0 software, posing a significant risk to organizations utilizing the platform. The vulnerability, officially tracked as CVE-2025-56563, is a Server-Side Request Forgery (SSRF) that could allow unauthenticated remote attackers to perform unauthorized actions on behalf of the server. **#CVE #SSRF**

Source: SOCRadar

CyberInflight. For internal use only. Not for further distribution

THREAT INTELLIGENCE

How two web vulnerabilities can compromise control of satellite missions

At DEF CON, the host of the video met Milenko and Andrzej, the authors of the Spacecraft Hackers Handbook, to explore cybersecurity in spacecraft. They explained the infrastructure underlying satellite operations, the actual target of the "Via Sat" attack, and why protecting spacecraft requires expertise in both security and space engineering. Andrzej then demonstrated vulnerabilities that had previously been patched in an older version of the mission control software. Using Burp Suite, he showed how directory traversal exposes configuration files and how cross-site scripting can trigger a command to the spacecraft via an operator's browser. **#CVE #SSRF**

Source: David Bombal

TECHNOLOGY

L3Harris says RASOR hybrid SATCOM reroutes U.S. military data around jamming and cyberattacks, targets NSA approval in early 2027

L3Harris Technologies expects its RASOR hybrid satellite communications system to receive NSA Type 1 certification in early 2027. The company is developing the system to keep command centers, aircraft, and deployed forces connected when individual satellite links are disrupted. **#L3Harris #RASOR**

Source: Defence Industry Europe

TRAINING & EDUCATION

Space Cybersecurity learning project: AuroraWatch-1

AuroraWatch-1 is a fictional and educational cybersecurity assessment for a simulated Low Earth Orbit Earth-observation mission. The project focuses on the mission's Ground Segment and Mission Operations Center. **#EO #AuroraWatch1**

Source: LinkedIn

NDSS Symposium 2027

The Network and Distributed System Security (NDSS) Symposium is a top venue that fosters information exchange among researchers and practitioners of network and distributed system security. The NDSS Symposium 2027 and co-located workshops will take place in Seoul, Republic of Korea, from 22 to 26 March 2027. **#NDSS #SpaceSec2027**

Source: NDSS Symposium

Full Speech: The State of the Space Force | Air, Space & Cyber 2026 Conference

General Doug Schiess, Chief of Space Operations, delivered the opening address at the 2026 AFA Conference on Air, Space, and Cyberspace, held in National Harbor, Maryland, on September 15, 2026. **#USSF #Conference**

Source: Air & Space Forces Association

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 research, and cybersecurity awareness training.
Contact us at: research@cyberinflight.com