SPACE CYBERSECURITY WEEKLY WATCH

W45

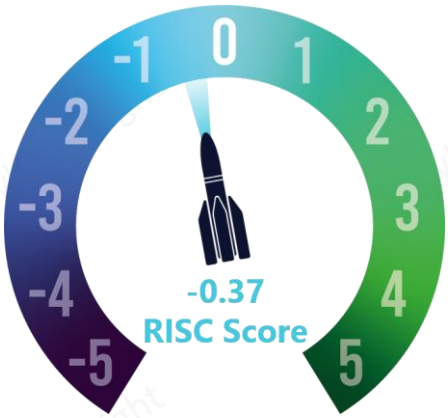
November 3 – November 9, 2026

Timeframe: Weekly
# of news items identified: 41
Est. time to read: 60 minutes

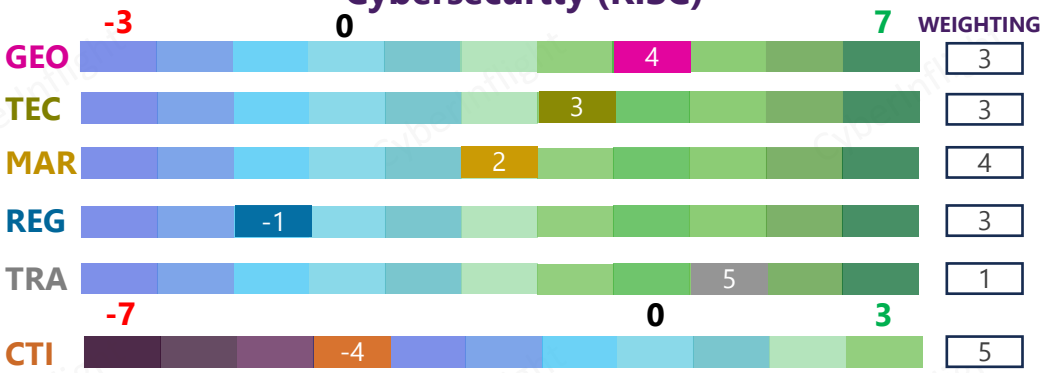
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

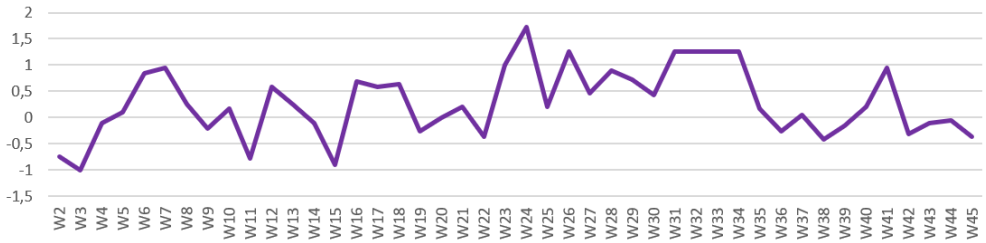
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



The RISC score for this watch is -0.37, a decrease of 0.31 since last week. This decrease is due to a more dynamic threat environment.

CyberInflight's **Market Analyst Valentine Crepineau took part in a panel at the Software Defined Space Conference 2026 in Tallinn**, exploring the evolving landscape of space cybersecurity frameworks in Europe from perspectives spanning space law and mission practice. On the geopolitical front, the **U.S. Space Force declared that it sees space as a "digital domain where cyber reigns supreme"**, with victory in space depending as much on digital combat as on physical operations, while a **DoD CIO official stated the Pentagon must fully embrace autonomous on-orbit cyber defenses** to keep space-based capabilities functioning against AI-powered hacking in the age of autonomous attacks. On the market side, **Space Systems Command officials stressed that commercial space partnerships must account for underlying realities,** signaling that innovation alone is no longer sufficient for defense procurement. Accountability also tightened, as defense and aerospace firm **ILC Dover settled for $13m over allegedly failing to meet cybersecurity contract requirements**. In threat intelligence, a **threat actor offered for sale alleged infrastructure data of the Himawari satellite network** on a dark web forum, exposing sensitive technical details of the satellite's communication and server ecosystem. Lastly, in training and education, researchers published an **empirical security analysis of open-source software used in onboard satellite systems**, auditing 126 public repositories through a pipeline combining software bills of materials, software composition analysis, static security testing, infrastructure-as-code analysis, and secret scanning, reinforcing that software supply chain integrity is now a first-order space security concern.

CYBERINFLIGHT'S NEWS

CyberInflight is on a panel at the Software Defined Space Conference 2026!

At SDSC2026, our Market Analyst Valentine Crepineau joined a panel exploring the evolving landscape of Space Cybersecurity frameworks in Europe, from perspectives spanning space law, market intelligence, cyber consulting, and mission practice. **#CyberInflight #SDSC**

Source: LinkedIn

GEOPOLITICS

[redacted]



US Military sees space as a 'digital domain' where cyber reigns supreme, Deputy CSO for cyber and data says

The U.S. Space Force sees space not just as a physical domain, governed by thermodynamic laws and orbital mechanics, but also as a digital domain. Indeed, victory in space depends as much, maybe more, on victory in digital combat as it does on prevailing at the physical level, the service's head of Data and Cyber told CyberSat Monday. **#USSF #CSO**

Source: Via Satellite



[redacted]



[redacted]



[redacted]



[redacted]



[redacted]



MARKET & COMPETITION

[redacted]



[redacted]

Space Systems Command officials focus on commercial space industry partnership and acquisition transformation at space industry days

The Space Force and industry want to bring innovative capability to the table, but industry needs to think about all the things under the surface: cybersecurity, software delivery guidelines, how to integrate with existing Space Force systems, government environments and access, operational testing and user support, licensing, and sustainment and support. **#SpaceCommand #USSF**

Source: Space Force



[redacted]



[redacted]

REGULATION

Defense and aerospace firm settles with government over allegedly failing to meet cybersecurity contract requirements

ILC settled for $13m, and its parent company said it resolved the issues before settling, without an admission of liability. **#Aerospace #Cybersecurityrequirements**

Source: Cyberscoop



THREAT INTELLIGENCE

[redacted]



[redacted]



[redacted]



[redacted]

THREAT INTELLIGENCE

[redacted]



[redacted]



[redacted]



[redacted]



Alleged Himawari satellite infrastructure data offered for sale on hacker forum

A threat actor is allegedly selling a database containing infrastructure data related to the Himawari satellite network on a dark web forum. The breach claim involves sensitive technical details regarding the satellite's communication and server ecosystem. **#Himawari #DataLeak**

Source: Dark Forums



TECHNOLOGY

[redacted]



[redacted]



TECHNOLOGY

[illegible]



[illegible]



[illegible]



[illegible]





DoD must embrace autonomous on-orbit cyber defense, DoD CIO official says

In the age of AI-powered hacking, keeping the U.S. military's vital space-based capabilities functioning through enemy cyberattacks will require the Pentagon and its contractors to fully embrace autonomous on-orbit cyber defenses, a senior defense official told CyberSat this week. **#DoD #On-OrbitCyberDefense**

Source: Via Satellite



[illegible]

TRAINING & EDUCATION

[illegible]



[illegible]



[illegible]



CyberInflight

TRAINING & EDUCATION

AFRL to cybersecurity and AI advancing resilient, AI-enabled capabilities for space warfare

AFRL Priorities in Cybersecurity and Artificial Intelligence Advancing Resilient, AI-Enabled Capabilities for Space Warfare and Strategic Deterrence. Moderated by Dr. Mark Adelson and Dr. Prakash Ranganathan, this discussion with Andrew G. "Andy" Williams, Acting Director of AFRL's Space Warfare Directorate (AFRL/RV), will examine how the Air Force Research Laboratory's priorities in cybersecurity, artificial intelligence, autonomy, and resilient space systems.



Source: [redacted]

Towards a unified research community for the cybersecurity of space systems

Space systems are critical infrastructures as their proliferation continues and they expand further into commercial and civilian use, academic contributions remain sporadic because of high barriers to entry and limited visibility into operational systems. This is a missed opportunity, as academic expertise has historically played a pivotal role in advancing the security and resilience of critical infrastructure. #Workshop #ResearchCommunity

Source: [redacted]

Workshop on the security of space and satellite systems (SpaceSec) 2027

SpaceSec 2027 is the 5th Workshop on the Security of Space and Satellite Systems. The event is co-located with the NDSS Symposium, positioning it within one of the established venues for network and distributed systems security research. The workshop format emphasizes paper presentations and structured discussion rather than commercial exhibition. #Workshop #SpaceSec



Source: [redacted]

Cyber and electromagnetic threats to space systems: Protecting the services societies rely on

UNIDIR, in partnership with the Permanent Missions of Switzerland and Singapore to the UN in Geneva, is organizing a side event to the Open-ended Working Group (OEWG) on the Prevention of an Arms Race in Outer Space (PAROS). #UNIDIR #Conference

Source: [redacted]

Cybersecurity in space missions and astronomy

Satellites are now critical infrastructure, and with the rise of New Space and mega-constellations, they have also become targets of cyberattacks. The conference has three main objectives: To review the history of cyberattacks on the space sector, from the NOAA satellite (1998) to the attack on Viasat's KA-SAT network in 2022 and the interference suffered by Starlink. To explain in simple terms the main types of attacks against the space, ground, and link segments (jamming, spoofing, command injection, ransomware, supply chain attacks, etc.). To present the frameworks used by agencies such as NASA and ESA, the role of artificial intelligence, and the challenges posed by the quantum era.



#Cybersecurity #[redacted]

Source: [redacted]

Can we trust data centers in space? | Filip Rezabek | TALK (CYBER #47)

Satellites are evolving into powerful computing platforms capable of running AI, processing sensitive data, and providing shared computing services in orbit. But how do we know which software actually ran? Can we verify that the hardware was not compromised? And how can we prove where a computation took place? In this edition of the TALK | CYBER lecture series, Filip Rezabek introduces Space Cabins, an architecture designed to make orbital computing secure, trustworthy, and verifiable. #SpaceComputer #TALK | CYBER

Source: [redacted]

1st IEEE Conference on Resilience and Integrated Security for Space and Critical Systems (RISC 2026)

The 1st IEEE Conference on Resilience and Integrated Security for Space and Critical Systems (RISC 2026) is the inaugural IEEE conference dedicated entirely to the security and resilience of space systems and the critical infrastructure that depends — or is impacted by — space applications. The event takes place from 3–5 November 2026 in San Jose, California, USA, and will be co-located with three sister IEEE conferences: TPS 2026 (CNS), Privacy and Security in Intelligent Systems, CII 2026 (Collaboration and Internet Computing), and CogML 2026 (Cognitive Machine Intelligence).



#IEEE #RISC 2026

Source: [redacted]

Bahrain space agency organizes "a safer digital life" workshop

In observance of Cybersecurity Awareness Month and in conjunction with the global "Make it a Little Harder for Them" campaign for October 2026, the Bahrain Space Agency (BSA) organized an internal workshop for its employees titled "A Safer Digital Life." The workshop was delivered by Mr. Isa Thani and highlighted key cybersecurity trends and practices, ways to strengthen digital awareness and measures to foster a secure working environment. #BSA #Workshop



Source: [redacted]

TRAINING & EDUCATION

An empirical security analysis of open-source software used in onboard satellite systems

This paper presents an empirical security study of OSS used in onboard satellite systems. Researchers analyze 126 public repositories using a pipeline that combines software bill-of-materials generation, software composition analysis, static application security testing, infrastructure-as-code analysis, and secret scanning. **#OSS #SecurityAnalysis**

Source: Science Direct

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