SPACE CYBERSECURITY WEEKLY WATCH

W46

November 10 – November 16, 2026

Timeframe: Weekly
# of news items identified: 31
Est. time to read: 50 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

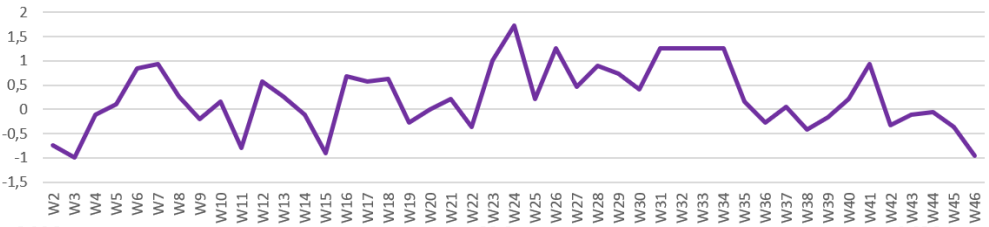
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



The RISC score for this watch is -0.95, a decrease of 0.58 since last week. This decrease is due to a more dynamic threat environment.

At the Software Defined Space Conference 2026 in Tallinn, **CyberInflight's Market Analyst Valentine Crepineau participated in a panel exploring Europe's evolving regulatory frameworks for space cybersecurity**, bringing together perspectives from space law, market intelligence, and mission practice. Discover the recording!

Moreover, this week, **geopolitical concerns intensified as an Israeli cyber official warned that rising satellite attacks threaten global communications, aviation, and shipping as space networks expand rapidly**. Technological innovation continues with **AstroCode Minds launched from Angola** as a dedicated division for aerospace software engineering and mission-critical AI systems designed for deep space resilience. On the regulation front, accountability measures tightened significantly as **defense contractor ILC Dover settled for $13m over allegations of cybersecurity noncompliance** spanning nearly 7 years, demonstrating that suspending CMMC Phase 2 does not eliminate False Claims Act liability for contractors. Threat intelligence revealed serious vulnerabilities, including an **alleged offer by Shinycorp 2 (ShinyHunters) to sell 2 terabytes of exfiltrated European Space Agency data on clandestine channels**. Additionally, on the training side, **Nightwing's Joe Mazur discussed in a podcast how space systems remain exposed** to machine-speed attacks, emphasizing that defending against AI-powered threats requires equally advanced, autonomous defensive capabilities.

CYBERINFLIGHT'S NEWS

The evolving regulatory landscape of space cybersecurity | Panel | SDSC 2026 - PART 4

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. Discover the recording! **#CyberInflight #SDSC**

Source: EIS

GEOPOLITICS

Satellite hacking poses growing global threat as cyber defenses weaken, Israeli official warns

An Israeli cyber official warns that rising satellite attacks could disrupt global communications, aviation, and shipping as space networks expand rapidly. **#Israel #Satellite**

Source: The Jerusalem Post

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

MARKET & COMPETITION

From self-healing materials to cyber defence: Protecting the next generation of satellites

Chris Range and Theo Worsley explore the materials and cyber defences helping protect satellites, and the challenges of securing intellectual property in space. **#Withers&Rogers #Patent**

Source: Aerospace Global News

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

MARKET & COMPETITION

[redacted]

REGULATION

A $13m warning for defense contractors

DoD suspended CMMC Phase 2, but defense contractors are still responsible for the cybersecurity requirements in their contracts. ILC Dover just agreed to a $13m False Claims Act settlement involving nearly 7 years of alleged cybersecurity noncompliance, missing SSPs, unsupported assessments, and a whistleblower who was the company's former Director of Cybersecurity. Speaker dives into DOJ's allegations, the consequences for contractors with inaccurate or unsupported SPRS scores, and why CMMC's suspension does not suspend contractual obligations or FCA liability.

#CMMCv2 #CybersecurityRequirements

Sources: Summit 7, Washington Technology

THREAT INTELLIGENCE

[redacted]

THREAT INTELLIGENCE

[redacted]



[redacted]



[redacted]

Alleged exfiltration and sale of 2 TB of data from the European Space Agency (Actor: Shinycorp 2 / Shinyhunters)

Centralized cyber-intelligence systems have intercepted a commercial offer posted on clandestine messaging channels by the group SHINYCORP 2 (associated with the ShinyHunters group). The report claims a compromise of the systems of the European Space Agency (ESA)—an international organization with 23 member states dedicated to space exploration—asserting the successful exfiltration of over 2 terabytes of files and confidential information. **#ESA #DataLeak**

Source: VECERT Analyzer



[redacted]



TECHNOLOGY

[redacted]



Introducing AstroCode Minds — engineering resilience for deep space and mission-critical systems

Born in Luanda, Angola, as the dedicated aerospace software engineering, space telemetry, and mission-critical AI division of The Code Minds, AstroCode Minds exists to solve high-stakes operational challenges where system failure is not an option. **#Angola #AstroCodeMinds**

Source: AstroCode Minds



TRAINING & EDUCATION

Cyber's Final Frontier with Joe Mazur (VP, Nightwing)

Joe Mazur of Nightwing joins Valley of Depth to talk about where space systems are actually exposed and what defending them looks like when attacks move at machine speed. **#Podcast #Nightwing**

Source: Tectonic



[redacted]



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