SPACE CYBERSECURITY WEEKLY WATCH

W36

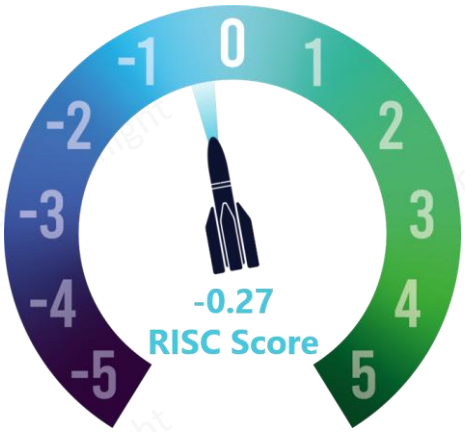
September 1 – September 7, 2026

Timeframe: Weekly
# of news identified: 20
Est. time to read: 35 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

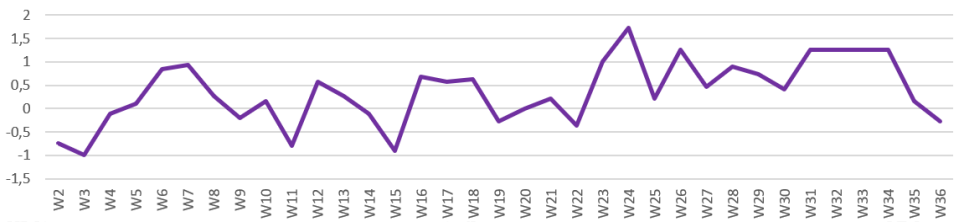


The RISC score for this watch is -0.27, a decrease from last week, largely due to a relatively small amount of news across most categories, which brought the score down slightly and highlighted a relatively calm ecosystem this week.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



This week, a geopolitical article explains how **the German Bundeswehr is massively expanding its capabilities in orbit**. With billions in investments, its own security strategy, and new military capabilities, the Bundeswehr aims to become Europe's leading space military power—right behind the U.S. and China. On the market front, SpaceWERX, working with Cyberspace Warfare professionals in the U.S. Space Force, is **seeking solutions to defend space systems from adversarial attacks through the cyber domain**. On the regulation side, the U.S. Justice Department announced that **Honeywell Aerospace Inc. has agreed to pay $2m to resolve allegations that it is liable under the False Claims Act for failing to comply with cybersecurity requirements** in a contract with the U.S. Department of Defense. On the threat front, in a post on its social media account, Darknavy, an independent cybersecurity research institute headquartered in Singapore and Shanghai, said it had used **sophisticated hardware attacks to gain full administrative control over the Starlink terminals**, allowing it to run any custom code on the devices. On the technological side, Arqit Quantum Es'hailSat, the Qatar Satellite Company, and Advanced International Electronic Equipment Company (AIEE), announced the **successful demonstration of quantum-safe security across operational satellite communications infrastructure**. Lastly, on the training and education side, SpaceCyber Inc. will hold an **online workshop in October** on the opportunities, risks, and emerging security considerations shaping the future of secure satellite communications.

GEOPOLITICS

The German Bundeswehr on its way to becoming a space power

The German Bundeswehr is massively expanding its capabilities in orbit. With billions in investments, its own security strategy, and new military capabilities, the Bundeswehr aims to become Europe's leading space power—right behind the U.S. and China. The reason is as simple as it is troubling: Without satellites, neither modern warfare nor everyday civilian life can function. **#SpacePower #Bundeswehr**

Source: militaraktuell

[redacted]

MARKET & COMPETITION

DAF SBIR DAF26BX06-DV512: Cyberspace warfare for space

DAF26BX06-DV512 is a Department of the Air Force SBIR Direct to Phase II topic under the DAF 2026 SBIR Commercial Solutions Opening, Release 6. SpaceWERX, working with Cyberspace Warfare professionals in the U.S. Space Force, is seeking solutions to defend space systems from adversarial attacks through the cyber domain.

#SpaceWERX #CyberspaceWarfare

Source: bwcoconsulting

[redacted]

REGULATION

Honeywell Aerospace Inc. agrees to pay over $2m to settle False Claims Act allegations of failing to comply with cybersecurity requirements in a U.S. Department of Defense contract

The Justice Department announced that Honeywell Aerospace Inc. has agreed to pay $2m to resolve allegations that it is liable under the False Claims Act for failing to comply with cybersecurity requirements in a contract with the U.S. Department of Defense. **#DoD #NIST**

Sources: Justice.GOV, The Washington Times

THREAT INTELLIGENCE

[redacted]

THREAT INTELLIGENCE

[redacted]

[redacted]

[redacted]

China-Singapore security team claims breakthrough in hacking Starlink terminals

In a post on its social media account, Darknavy, an independent cybersecurity research institute headquartered in Singapore and Shanghai, said it had used sophisticated hardware attacks to gain full administrative control over the Starlink terminals, allowing it to run any custom code on the devices. **#StarlinkTerminals #APAC**

Sources: SCMP, Chin@Strategy, X

[redacted]

TECHNOLOGY

[redacted]

Arqit, Es'hailSat, and AIEE demonstrate the first quantum-safe satellite communication in the Middle East

Arqit Quantum Inc, a global leader in quantum-safe encryption, Es'hailSat — the Qatar Satellite Company — a world-class satellite operator and service provider with coverage spanning the MENA region, and Advanced International Electronic Equipment Company (AIEE), a specialist systems integrator for secure communications infrastructure, announced the successful demonstration of quantum-safe security across operational satellite communications infrastructure.

#Demo #Quantum

Source: KuwaitTimes

[redacted]

[redacted]

TRAINING & EDUCATION

[redacted]



[redacted]



[redacted]

Summer technical workshop - Multi-Orbital Architecture & Cyber Security

Join SpaceCyber Inc. and industry experts for a live discussion on the opportunities, risks and emerging security considerations shaping the future of secure satellite communications. **#Webinar #Workshop**



Source: SpaceCyber Inc

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