SPACE CYBERSECURITY WEEKLY WATCH

Week 34

August 19 - 25, 2025

Timeframe: Weekly

# of articles identified: 37

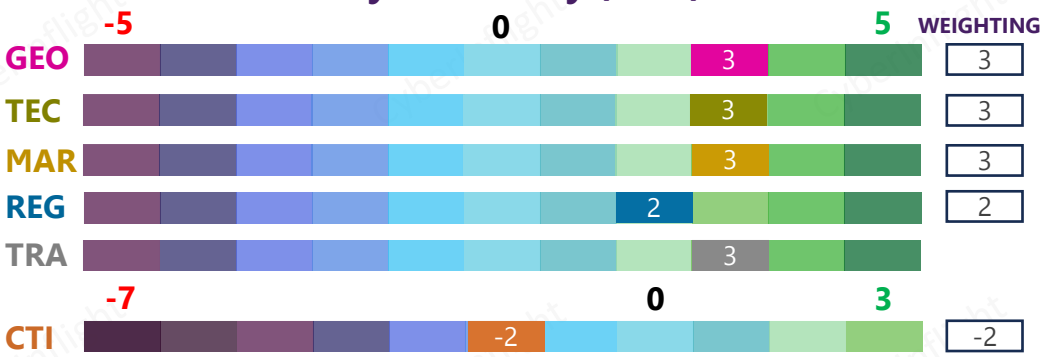
Est. time to read: 85 minutes

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)



The RISC score for this watch is 2, a slight increase from last week. This difference is due to several geopolitical, technological, and market initiatives.

RISC Score evolution in 2025

This week, the UK Space Agency announced it will cease to exist as an independent entity to cut the cost of bureaucracy. It will be absorbed by the Department for Science, Innovation and Technology (DSIT) in April 2026. On the regulation front, the EU's NIS Cooperation Group called for input to shape Europe's quantum-resistant digital infrastructure roadmap, including developing a Quantum Technology Roadmap in space with the European Space Agency and contributing to the European Armament Technological Roadmap. On the technological front, the U.S. Space Force launched X-37B, carrying quantum and comms experiments. While many of the experiments it will conduct in the coming months are classified, the Space Force has identified space-based laser communications and quantum sensing as two focus areas. Regarding the market, Mercury Systems announced a new production agreement with AeroVironment to support the U.S. Space Force's Satellite Communication Augmentation Resource (SCAR) program valued at $1.4bn. On the threat intelligence front, an article looks at the two major cuts of Elon Musk's Starlink, which have shown how vulnerable satellite internet systems can be. Cyberattacks on centralized routing systems and disruptions at ground gateways that link satellites to the global internet could all degrade or shut down service on a large scale. Lastly, a podcast discusses the Spacecraft Cybersecurity Act introduced this past summer. The regulation would require NASA contractors to submit a cybersecurity plan before receiving federal funding to build spacecraft, an effort driven by the wave of cyberattacks targeting the agency, allegedly from state-backed actors in China and Russia.

GEOPOLITICS

[redacted]

[redacted]

[redacted]

UK independent Space Agency scrapped to cut costs

The UK Space Agency will cease to exist as an independent entity to cut the cost of bureaucracy. It will be absorbed by the Department for Science, Innovation and Technology (DSIT) in April 2026. The government says this will save money, cut duplication and ensure ministerial oversight. But space scientists said the move would lead to disruption in the short term and the UK losing ground to its international competitors over the long run. **#UKSA #Reconfiguration**

Source: *BBC*

[redacted]

REGULATION

EU's NIS Cooperation Group calls for input to shape Europe's quantum-resistant digital infrastructure roadmap

The European Commission's NIS Cooperation Group has opened a public consultation to gather feedback on its recently published roadmap for building a quantum-safe European digital infrastructure. The effort includes developing a Quantum Technology Roadmap in Space with the European Space Agency and contributing to the European Armament Technological Roadmap. **#NIS #Quantum**

Source: *Industrial Cyber*

[redacted]

[redacted]

TECHNOLOGY

Space Force launches X-37B carrying quantum and comms experiments

The spacecraft flew from NASA's Kennedy Space Center in Florida on a SpaceX Falcon 9 rocket on August 21. While many of the experiments it will conduct in the coming months are classified, the Space Force has identified space-based laser communications and quantum sensing as two of its focus areas. These experiments come as part of a broader push across the US Space Force to uphold the safety and security of the space domain by enhancing the resilience and flexibility of U.S. orbital systems. **#X-37B #Quantum**

Source: *Defense News*

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

MARKET & COMPETITION

[redacted]

MARKET & COMPETITION

[redacted]

[redacted]

Mercury signs new hardware production agreement with AV to support US Space Force's SCAR program

Mercury Systems, Inc., a technology company that delivers mission-critical processing to the edge, announced a new production agreement with AeroVironment, Inc. to support the U.S. Space Force's Satellite Communication Augmentation Resource (SCAR) program valued at $1.4bn. **#SCAR #Contract**

Source: *Benzinga*

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

THREAT INTELLIGENCE

Starlink power cuts reveal vulnerabilities of space-based internet systems

Two major power cuts on Elon Musk's Starlink have shown how vulnerable satellite internet systems can be, especially when compared to the more resilient fibre and mobile networks most people rely on. Cyberattacks on centralized routing systems, disruptions at ground gateways that link satellites to the global internet, or even exploits in user terminals could all degrade or shut down service on a large scale. **#Vulnerability #Starlink**

Source: *The National*

THREAT INTELLIGENCE

The rise of space cybersecurity: Safeguarding satellites in a digital orbit

As space becomes the next frontier for innovation, exploration, and commerce, it's also becoming a new battleground for cyber threats. From satellites powering GPS and weather forecasts to missions reaching deep into the cosmos, the systems that make space operations possible are increasingly vulnerable to hacking, interference, and espionage.

#Vulnerability #SpaceOperation

Source: Global Security Mag

Why satellite cybersecurity threats matter to everyone

In this new fast security interview, Scott Lundahl, leader of Deloitte's U.S. Space practice, talks about the most pressing risks, the vulnerable points across satellite systems, and the practices that can make space operations more secure. #SatelliteSystem #Security

Source: National Cyber Security

Hijacking satellites in space: Is it possible and how big could the damage be?

Satellites rely on software systems and ground stations, both of which are vulnerable to cyber intrusions. Ground stations, responsible for satellite control, often run on outdated computer systems with weak security. Hackers can exploit these flaws to inject commands, steal data, or alter satellite orbits. Weak encryption, delayed software updates, and outdated IT hardware make satellites more susceptible to such attacks. #Hijacking #Cyberattacks

Source: Newsbreak

Суд в Калининграде отправил в СИЗО бывшего сотрудника предприятия Роскосмоса, обвиняемого в передаче США данных о спутниках *(Trad.: A court in Kaliningrad sent to a pre-trial detention center a former employee of the Roscosmos enterprise, accused of transferring satellite data to the United States)*

The Central District Court of Kaliningrad sent a 40-year-old man to a pre-trial detention center, accused of transmitting classified information about satellites to U.S. intelligence agencies. According to investigators, in the summer of 2020 he entered into a "confidential cooperation agreement" with a company that works in the interests of the US government and defense departments. #Russia #Espionage

Source: Zona Media

Russia targets NATO skies with GPS jamming and signal spoofing

European countries bordering Russia have reported a significant increase in GPS jamming and signal spoofing, raising concerns about aviation safety and military logistics, according to Institute for the Study of War (ISW). Reports from the Baltic states, Finland, Poland, and Sweden point to intensified electronic interference over recent months, coinciding with the expansion of Russian electronic warfare systems along its western border and the Baltic Sea. #GNSS #GPSJamming

Sources: Lindwall Media, ISW

TRAINING & EDUCATION

Global radio frequency interference in L-band SAR data from ALOS-1 and JERS-1 satellites

This work develops algorithms, workflow and system for operationally measuring global RFI experienced by L-band SAR data. #RFI #Paper

Source: Science Direct

Detection of GNSS spoofed signals based on the weighted moving average bias correction method

This paper proposes a Weighted Moving Average Bias Correction (WMA-BC) algorithm for metric post-processing. Comparative experiments with Moving Average (MA) and Moving Variance (MV)-based GLRT methods demonstrate that the WMA-BC algorithm achieves substantial advantages in Detection Rate enhancement and significantly improves the Area Under Curve (AUC) of the Receiver Operating Characteristic (ROC). #SpoofDetection #Paper

Source: Springer Nature

TRAINING & EDUCATION

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Legislation now calling for spacecraft manufacturers to create cybersecurity plan when working with NASA

The Spacecraft Cybersecurity Act was recently introduced in the House this past summer. The legislation would require NASA to secure a cybersecurity protection plan from manufacturers applying to use federal dollars to build NASA spacecrafts. The introduction comes after thousands of cyberattacks from malicious actors, including China and Russia, have been launched against NASA. So what can and needs to be done to make sure cyber protections are considered during the manufacturing stage? **#SpacecraftCybersecurityAct #Podcast**

Source: *Federal News Network*

[redacted]