



SPACE CYBERSECURITY WEEKLY WATCH

Week 40

September 30 – October 6, 2025

Timeframe: Weekly
of articles identified: 34
Est. time to read: 70 minutes

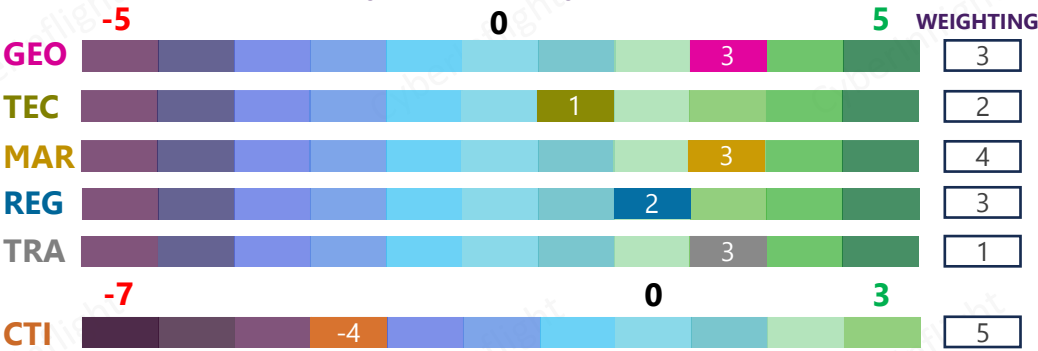
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

- 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 2025



The RISC score for this watch is 1.23, which represents a significant decrease from last week. This decline is primarily due to a notable drop in technological developments, along with less impactful news on the market and geopolitical fronts.

This week, CyberInflight was cited in an article by Relm Insurance published on Wired, discussing the growing cyber risk exposure of the global space economy. In the piece, Florent Rizzo, CEO of CyberInflight, warns that attacks targeting space infrastructure are “not a question of if, but when.” On the geopolitical front, the Netherlands took a leading role in strengthening Europe’s quantum-secure communications through the SEEWQCI project, part of the EU’s EuroQCI initiative. The country is helping to build one of Europe’s first cross-border quantum networks linking the Netherlands with Greece, Cyprus, and Bulgaria via both satellite and fiber connections. On the regulatory front, a briefing from the European Parliamentary Research Service outlines the main challenges facing the satellite sector and details the EU’s policy response. It emphasizes that the proposed EU Space Act aims to improve supply chain resilience, enhance competitiveness, and strengthen European sovereignty in the space domain. The technological section highlights the now fully operational Deloitte-1 cubesat, which has successfully withstood 6 simulated cyberattacks. Over the next 60 days, Deloitte plans to open the platform to partner organizations, enabling external teams to test and challenge its cyber defenses in orbit. In market developments, the UK Space Agency announced a new batch of 23 projects aimed at strengthening international space partnerships, developing national capabilities, and boosting economic growth, representing a £6.5m (\$8.26m) investment under the International Bilateral Fund (IBF). Additionally, the UK also features in the threat intelligence domain, with a top space general warning of Russia’s “weekly” attempts to disrupt UK military satellites through jamming activities. Lastly, the training and education section highlights a paper examining the NIST Cybersecurity Framework 2.0 and NIS2, which reveals imbalances in academic research, with certain CSF 2.0 functions remaining underrepresented.



CYBERINFLIGHT'S NEWS

Could the first billion-dollar space heist be on the horizon?

This article, written by Relm Insurance, explores the growing cyber risk exposure of the global space economy and raises the prospect of the first billion-dollar cyberattack in space and highlights insights from CyberInflight,. According to Florent Rizzo, CEO of CyberInflight, attacks targeting space infrastructure are “not a question of if, but when,” with the company’s Space Cybersecurity Report showing sharp increases in incidents since 2022 and projecting continuous growth through 2033. **#SpaceInsurance #ZeroTrust**

Source: [Wired](#)



GEOPOLITICS

Towards a secure Europe: The Netherlands at the forefront to build a pan-European quantum network

Through the EuroQCI project, the European Commission is working on a quantum-secure communication infrastructure for all of Europe. This will help to ensure that personal data, financial transactions, and confidential communications remain protected, even against future quantum-assisted cyberattacks. The Netherlands is taking a key role in the pan-European quantum cybersecurity project SEEWQCI, which will establish a quantum interconnection between the Netherlands, Greece, Cyprus and Bulgaria via satellite and fiber links. **#SEEWQCI #Quantum**

Sources: [Satnews](#), [Satcom Digital](#)



Space forces open aggressive satellite to add realism to test and training

A new satellite, the first of its kind, is being launched by the U.S. Space Force to test and train its cyber capabilities. The satellite, named the Space Force Cyber Satellite (SFCSS), is designed to simulate a real-world cyber attack on a satellite. It will be used to test the Space Force's cyber capabilities and to train its personnel. The satellite is expected to be launched in the near future.

Source: [U.S. Space Force](#)



After tighter grip on what U.S. and France plan fresh military satellite mission

The U.S. and France are planning a new joint military satellite mission. The mission is expected to be launched in the near future. It will be used to test the Space Force's cyber capabilities and to train its personnel. The satellite is expected to be launched in the near future.

Source: [U.S. Space Force](#)



Iran's Challenge space center set for historic first launch -- West Asia's largest spacecraft to challenge global powers

The Islamic Republic of Iran is planning a new satellite mission. The mission is expected to be launched in the near future. It will be used to test the Space Force's cyber capabilities and to train its personnel. The satellite is expected to be launched in the near future.

Source: [U.S. Space Force](#)



REGULATION

Satellites: State of play and challenges for the EU

This briefing from the European Parliamentary Research Service provides an overview of the satellite sector, its challenges, and the EU's policy response. The EU is strengthening its space policy with flagship programs such as Galileo (navigation), Copernicus (Earth observation), and IRIS² (secure connectivity). The proposed EU Space Act is positioned as a key step to secure supply chain resilience, competitiveness, and sovereignty in the space domain. **#EUSpaceAct #Briefing**

Sources: [European Parliament](#), [European Parliament](#)



Securing the Road to the New Legal Regime of Space Security in Space

The European Union is working on a new legal regime for space security. The new regime is expected to be adopted in the near future. It will be used to test the Space Force's cyber capabilities and to train its personnel. The satellite is expected to be launched in the near future.

Source: [U.S. Space Force](#)

REGULATION



Spanish satcom company Sateliot warns against 'overly restrictive' security measures in India's national telecom policy

Spanish satellite communication company Sateliot has cautioned the Indian government against employing overly restrictive measures on satcom companies under the National Telecom Policy 2025. "This can be seen in the goal of monitoring satellite communications to ensure cybersecurity, data integrity, and protection against unauthorized access or interference. Such a goal is laudable but can be interpreted in different ways," the company argued.

#Satcom #SecurityMeasures

Source: [Medianama](#)



TECHNOLOGY



New satellite will help cyber defenders train to stop hackers in orbit

Now fully operational, Deloitte-1, a cubesat launched into low Earth orbit to act as an on-orbit, live-fire cyber training range, has already faced six simulated cyberattacks and its Silent Shield intrusion detection system successfully detected each one. Over the next 60 days, Deloitte will open the system to partner organizations, allowing external teams to challenge its defenses. The company plans to scale this model into a nine-satellite constellation, enabling autonomous cyber-defense experimentation across space-based systems. **#Deloitte-1 #Experimentation**

Source: [Air & Space Forces Magazine](#)



European UHF & VHF is a quantum solution for satellite navigation

The United Kingdom has signed a quantum navigation satellite constellation with the European Space Agency (ESA) to develop a quantum navigation system. The system will use quantum entanglement to provide secure and accurate navigation services. The system is expected to be operational by 2030.

Source: [The Telegraph & others](#)



MARKET & COMPETITION



UK Space Agency goes global with 23 new projects

A new batch of 23 projects will strengthen international space partnerships, develop national capabilities and boost economic growth, the UK Space Agency announced. Representing a £6.5m investment under the International Bilateral Fund (IBF), these collaborations unite UK companies and universities with partners from Australia, Canada, France, Germany, India, Japan, Lithuania, and the USA and cover fields such as orbital threat detection, in-orbit servicing and deep-space radar. **#UKSA #Projects**

Source: [Gov UK](#)



Canadian Space Agency offers funding for dual-use technologies

The Canadian Space Agency (CSA) has announced a new funding program for dual-use technologies. The program will provide funding for the development of technologies that can be used in both space and terrestrial applications. The program is expected to be operational by 2025.

Source: [CBC News](#)



Belgian Aerospace awarded 10M contract to build satellite infrastructure in crowded orbit

Belgian Aerospace has been awarded a 10M contract to build satellite infrastructure in crowded orbit. The contract is for the development of a satellite constellation for the Belgian government. The constellation is expected to be operational by 2025.

Source: [The Telegraph & others](#)



French Space Agency and ESA sign contract for 10M mission to demonstrate Europe's first quantum key distribution ground-based service

The French Space Agency (CNES) and the European Space Agency (ESA) have signed a contract for a 10M mission to demonstrate Europe's first quantum key distribution ground-based service. The mission is expected to be operational by 2025.

Source: [The Telegraph & others](#)



THREAT INTELLIGENCE

7

Sources: *BBC, Tech Space 2.0*



THREAT INTELLIGENCE

US satellite reportedly down with debris of Russia over satellite system jamming

The US satellite system reportedly experienced an incident with debris in connection with jamming in connection with the satellite system. The debris is reportedly from a Russian satellite system. The debris is reportedly from a Russian satellite system. The debris is reportedly from a Russian satellite system.

USAT Satellite

Source: [Space.com](#)



Russia's Starlink jammer – How can NATO and NATO satellite systems use defense

Russia's Starlink jammer is a satellite system that is used to jam Starlink satellites. The jammer is reportedly from a Russian satellite system. The jammer is reportedly from a Russian satellite system. The jammer is reportedly from a Russian satellite system.

Source: [Space.com](#)



Why cyber attacks target the satellites and the satellites

The satellites are the most vulnerable part of the satellite system. The satellites are the most vulnerable part of the satellite system. The satellites are the most vulnerable part of the satellite system. The satellites are the most vulnerable part of the satellite system.

Source: [Space.com](#)

TRAINING & EDUCATION

Space-based information system training detection techniques and performance evaluation for the Starlink satellite system.

The paper presents a comprehensive review of satellite system training detection techniques and performance evaluation for the Starlink satellite system. The paper presents a comprehensive review of satellite system training detection techniques and performance evaluation for the Starlink satellite system.

Source: [Space.com](#)



Developing security metrics for space systems: A study considering the NIST cybersecurity framework 2.0 and the NIS2

This paper evaluates whether existing security metrics in the literature cover all NIST functions, categories, and subcategories in the Cybersecurity Framework 2.0 (CSF 2.0). This framework provides a strong foundation for industry sectors and can serve as a baseline to ensure compliance with directives like NIS2. Our analysis reveals imbalances in academic discourse, with certain CSF 2.0 functions underrepresented. **#Frameworks #Paper**

Source: [Science Direct](#)



Theoretical error analysis of GPS orbit determination by GNSS of multiple ground stations and its application to geodesy.

The paper presents a comprehensive review of GPS orbit determination by GNSS of multiple ground stations and its application to geodesy. The paper presents a comprehensive review of GPS orbit determination by GNSS of multiple ground stations and its application to geodesy.

Source: [Space.com](#)



Estimating the impact of satellite system on GPS satellite system and its application to geodesy.

The paper presents a comprehensive review of GPS satellite system and its application to geodesy. The paper presents a comprehensive review of GPS satellite system and its application to geodesy.

Source: [Space.com](#)



TRAINING & EDUCATION

SpaceForce's satellite network is critical to the nation's global communication and defense efforts. The nation's satellite network is critical to the nation's global communication and defense efforts. The nation's satellite network is critical to the nation's global communication and defense efforts. The nation's satellite network is critical to the nation's global communication and defense efforts.



Space Force is working to ensure the nation's satellite network is secure and resilient. The nation's satellite network is critical to the nation's global communication and defense efforts. The nation's satellite network is critical to the nation's global communication and defense efforts.



Space Force is working to ensure the nation's satellite network is secure and resilient. The nation's satellite network is critical to the nation's global communication and defense efforts. The nation's satellite network is critical to the nation's global communication and defense efforts.



A security satellite has been launched by Space Force. The satellite is designed to provide the nation with the ability to detect and respond to threats in space. The satellite is designed to provide the nation with the ability to detect and respond to threats in space.



Space Force is working to ensure the nation's satellite network is secure and resilient. The nation's satellite network is critical to the nation's global communication and defense efforts. The nation's satellite network is critical to the nation's global communication and defense efforts.



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