SPACE CYBERSECURITY WEEKLY WATCH

Week 49

December 2 - 8, 2025

Timeframe: Weekly

# of articles identified: 30

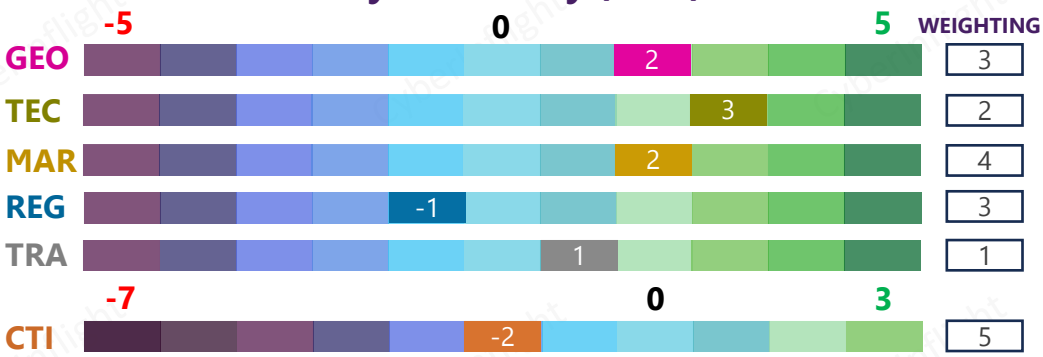
Est. time to read: 60 minutes

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

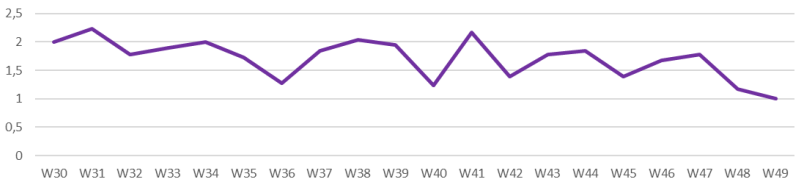
- GEOPOLITICS
- TECHNOLOGY
- MARKET & COMPETITION
- REGULATION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- IMPORTANT NEWS

RISC Score Assessment

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



The RISC score for this watch is 1.0, a decrease from last week. This difference is due to a drop in geopolitical and regulatory news, balanced by a slight improvement in technological and threat intelligence fronts.

As developments across the space and cybersecurity domains continue to reshape strategic postures, CyberInflight has updated its website to reflect better how our consulting activities complement our research and intelligence products across both traditional space stakeholders and the New Space ecosystem. This week, on the geopolitical side, Poland has formally secured access to the U.S. global military satellite communications network, gaining immediate entry into a system designed to operate under jamming and electronic attack. On the regulatory front, Russian forces in Ukraine continue to use black market Starlink terminals on drones such as the Molniya, extending operational range and lethality despite SpaceX geofencing measures and ongoing U.S. enforcement efforts. On the technological side, the US Space Force's Project Kronos aims to consolidate and modernize legacy systems into a unified software suite offering satellite operators enhanced intelligence and command and control capabilities. On the market side, GomSpace has signed the SECUSAT contract with the European Space Agency for the development of a security-enhanced generation of its NanoCom product line. On the threat side, international space cooperation has taken a new hit as a veteran Russian cosmonaut was abruptly removed from an upcoming SpaceX astronaut mission amid espionage allegations. Lastly, in the training and education section, a recent paper examines how real-world cyberattacks against space infrastructures can be characterized.

CYBERINFLIGHT'S NEWS

Discover our consulting services!

At CyberInflight, we complement our research and intelligence products with tailored consulting services designed to support both traditional space stakeholders and the New Space ecosystem. Discover our approach.

#ConsultingServices #CyberInflight

Source: *CyberInflight*

GEOPOLITICS

[redacted]

Poland enters U.S.-led global military satellite network

Poland has formally secured access to the United States' global military satellite communications network, gaining immediate entry into a system designed to operate under jamming and electronic attack. A Memorandum of Understanding was signed on December 4 at the Agency for Geospatial Reconnaissance and Satellite Services in Warsaw by Brigadier General Marcin Górka, Director of the Department of Innovation. The agreement links the Polish Armed Forces to the Wideband Global SATCOM program, a U.S.-led military satellite network providing secure broadband communications worldwide. **#SATCOM #MoU**

Source: *Defense Mirror*

[redacted]

REGULATION

Russia evades Starlink bans with black market drone terminals in Ukraine

Russian forces in Ukraine persist in using black market Starlink terminals on drones like the Molniya, enhancing range and lethality despite SpaceX's geofencing and U.S. crackdowns. Illicit supply chains through regions like Sudan evade controls, highlighting challenges in regulating dual-use tech in modern warfare. This raises ethical and geopolitical concerns. **#Crackdowns #BlackMarket**

Source: *WPN*

TECHNOLOGY

[redacted]

TECHNOLOGY

[redacted]

[redacted]

[redacted]

[redacted]

Space Force wants artificial intelligence (AI) and cybersecurity for space command and control

U.S. Space Force battle-management experts are reaching out to industry for enabling technologies that range from cloud computing infrastructure to software applications, artificial intelligence (AI), and software development services. The Space Force's Project Kronos seeks to consolidate and upgrade legacy systems into a unified software suite that provides satellite operators with intelligence tools and command-and-control capabilities. The project aims to enhance decision-making, accelerate planning and deconfliction, and provide shared situational awareness. **#USSF #KronosProject**

Source: *Military Aerospace Corporation*

[redacted]

[redacted]

[redacted]

MARKET & COMPETITION

[redacted]

[redacted]

MARKET & COMPETITION

[redacted]

[redacted]

Source: [redacted]

GomSpace signs €1.2m contract with ESA for SECUSAT: A major step forward in secure space communications for a safer world

GomSpace signs SECUSAT contract with the European Space Agency (ESA) for the development of an advanced, security-enhanced generation of its NanoCom product line. The agreement, valued at €1.2m, confirms ESA's confidence in GomSpace's technological leadership and marks a significant milestone in the evolution of secure satellite communications. **#SECUSAT #Contract**

Source: *GOMSpace*

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

THREAT INTELLIGENCE

[redacted]

[redacted]

Source: [redacted]

[redacted]

[redacted]

Source: [redacted]

Explosion & Espionage! China's bold rocket test ends in fireball, Russian cosmonaut removed from SpaceX

International space cooperation has hit a new low, with a veteran Russian cosmonaut abruptly removed from SpaceX's upcoming astronaut mission amid allegations of espionage. **#SpaceX #Espionage**

Source: *The Eurasian Times*

THREAT INTELLIGENCE

[redacted]

TRAINING & EDUCATION

[redacted]

Characterizing cyberattacks against space infrastructures with missing data: framework and case study

How can we characterize real-world cyberattacks against space infrastructures? This paper addresses the problem by proposing a framework, including metrics, while also addressing the missing-data problem by leveraging methodologies such as the Space Attack Research and Tactic Analysis (SPARTA) and the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) to “extrapolate” the missing data in a principled fashion. **#Framework #Paper**

Source: *Cornell University*

[redacted]