

SPACE CYBERSECURITY WEEKLY WATCH

Week 45

November 4 - 10, 2025

Timeframe: Weekly
of articles identified: 37
Est. time to read: 80 minutes

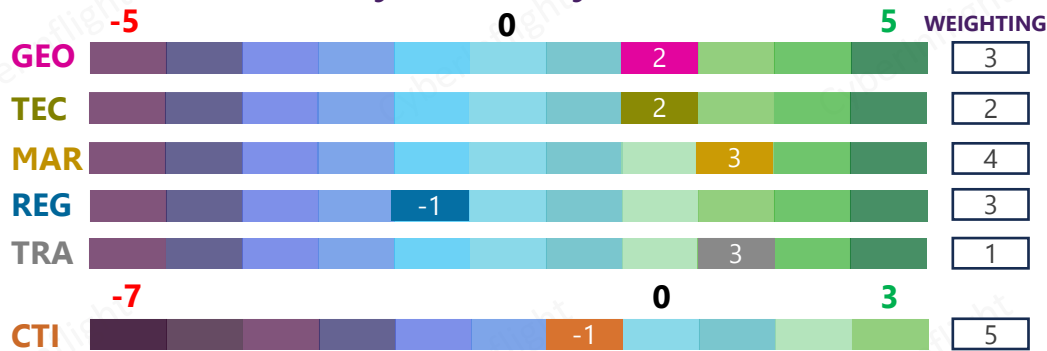
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

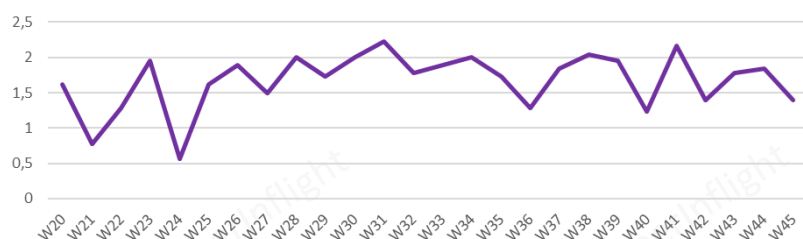
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



The RISC score for this watch is 1.39, a decrease from last week. This change is primarily due to a low score in the regulatory area, along with minimal changes in both the geopolitical and technological fronts. Slight movements in the threat intelligence section balanced these factors out.



This week, the geopolitical section focuses on the U.S. Space Force, which is preparing to deploy 2 new ground-based systems designed to jam Chinese and Russian spy satellites. This expansion enhances the Pentagon's capability to disrupt enemy surveillance in space. Meanwhile, on the regulatory section, the U.S. Department of State has provided feedback on the EU Space Act, expressing deep concern regarding certain measures that could impose "unacceptable" regulatory burdens on U.S. providers of space services to European customers. Regarding technology, the media SpaceNews featured an article about the Deloitte-1 satellite, which is designed to hunt for hackers in orbit. In market news, GMV and LuxQuanta have formed a strategic alliance to accelerate the real-world deployment of quantum key distribution (QKD) technologies, thereby strengthening Europe's sovereignty in quantum-safe communications. The threat intelligence section highlights a CNN article that revisits public declarations from Germany and the United Kingdom regarding Russia, which has been accused of systematically targeting Western satellite systems. The article further explores the threats posed by Russia and China to European space assets. Lastly, Europe successfully hosted its first in-orbit cybersecurity competition, the CTRL+Space Capture-the-Flag (CTF) challenge, the world's first live challenge involving multiple satellites, which took place in the Netherlands during the 3S Conference. CyberInflight was represented at this conference by its CEO, Florent Rizzo.



GEOPOLITICS

Space must be safeguarded for the common good, says Russian diplomat

Russian diplomat says that the international community must be the guarantor of security, ensuring the safety of space for all. He calls for a "new space law" that would be based on the principles of transparency, accountability, and non-aggression. He also calls for a "new space law" that would be based on the principles of transparency, accountability, and non-aggression.

Sources: [The Guardian](#)



Report: Pentagon can't forget about NATO for Golden Dome

The Pentagon's new Golden Dome program, designed to detect and track hypersonic missiles, must not ignore NATO allies, a report says. The report says that the program must be able to detect and track hypersonic missiles from all directions, not just from the North Atlantic.

Sources: [U.S. Space Force](#), [Pentagon](#), [NATO](#), [Space Force](#), [Golden Dome](#)



How the U.S. can stay ahead of China in space

The U.S. must stay ahead of China in space by investing in research and development, and by strengthening its space infrastructure. The report says that the U.S. must invest in research and development to stay ahead of China in space.

Sources: [The Guardian](#)



U.S. Space Force deploying ground-based jammers to counter Chinese, Russian surveillance

The U.S. Space Force is preparing to field 2 new ground-based systems designed to jam Chinese and Russian spy satellites, expanding the Pentagon's ability to disrupt enemy surveillance in space. Called Meadowlands and the Remote Modular Terminal (RMT), the systems will join the older Counter Communications System, which became operational in 2020 to "dominate the electromagnetic spectrum" during conflict. While still in early deployment phases, Space Force officials said the weapons are capable of being "operationally employed" now if needed. **#USSF #Jammers**

Sources: [The Defense Post](#), [The National Interest](#)



Space force announced? New report says guidelines in space would be an asset for future ops

The U.S. Space Force is preparing to field 2 new ground-based systems designed to jam Chinese and Russian spy satellites, expanding the Pentagon's ability to disrupt enemy surveillance in space. The report says that the U.S. must invest in research and development to stay ahead of China in space.

Sources: [The Guardian](#)



REGULATION



U.S. slams EU's proposed space law as 'unacceptable'

The U.S. has come out swinging against the draft law by the European Union that Washington claims would establish restrictive market barriers, impose costly environmental protection requirements, and create regulatory hurdles for US commercial firms — thus undermining bilateral, as well as NATO-wide, cooperation. The U.S. "expresses deep concern regarding measures in the proposed Act that would impose unacceptable regulatory burdens on U.S. providers of space services to European customers," the State Department charges in a document submitted to the EU. **#EUSpaceAct #DoS**

Sources: [Breaking Defense](#), [European Commission](#)



The threat of space terrorism is no longer science fiction, but we're ill prepared to combat it

The threat of space terrorism is no longer science fiction, but we're ill prepared to combat it. The report says that the U.S. must invest in research and development to stay ahead of China in space.

Sources: [The Guardian](#)



REGULATION

India's ISRO leads to look up Chinese satellite operations

The Indian National Space Promotion and Authorization Centre (NSIC) has reportedly plans to look satellite operators from the Chinese space agency, China National Space Administration (CNSA) and other entities in the name of national security. NSIC is also planning to look up satellite operators and launch to other satellite services in India, under the Indian Space Promotion and Authorization Centre (ISPA) satellite operators from space information from ISRO to the Indian Space Research Organisation (ISRO).



TECHNOLOGY



The race to defend satellites from cyberattacks

A small satellite named Deloitte-1 is hunting for hackers in orbit. Launched in March, it's the first of nine spacecraft the consulting firm Deloitte expects to be operating over the next 18 months to demonstrate a technology to detect cyber intrusions targeted at satellites in space. The company is building these satellites to prove that defending space networks from cyberattack requires putting defenses in orbit and not just on the ground. Deloitte's move comes amid a broader rethink of how to protect space infrastructure from cyber-threats. **#Deloitte #SilentShield**



Source: [Spacenews](#)

US offers cyber to quantum computing available for national security work

The US offers cyber to quantum computing systems, software, and services to national security agencies to help them better understand and defend against quantum computing threats. The technology has been used at a variety of national security agencies, including the NSA, and is available for government civilian agencies as well as private industry. **#Quantum #Cyber**



Reducing global dependence on GPS: Alternative PNT for critical infrastructure security

Reduction of global dependence on GPS is being explored as a critical infrastructure security measure. The technology is being used to provide precise timing and positioning, which are essential for a variety of critical infrastructure applications. The technology is being used to provide precise timing and positioning, which are essential for a variety of critical infrastructure applications. **#PNT #GPS**



SpaceX provides ground positioning for GPS satellites

SpaceX provides ground positioning for GPS satellites. The technology is being used to provide precise timing and positioning, which are essential for a variety of critical infrastructure applications. The technology is being used to provide precise timing and positioning, which are essential for a variety of critical infrastructure applications. **#GPS #SpaceX**



Germany and EU Spaceflight establish Germany-based Satellite Operations Centre to enhance Europe's coverage satellite connectivity

Germany and EU Spaceflight have selected Germany as the location for their new satellite operations centre. The centre will provide precise timing and positioning, which are essential for a variety of critical infrastructure applications. The centre will provide precise timing and positioning, which are essential for a variety of critical infrastructure applications. **#Satellite #Germany**



Scientists reveal it is possible to track up quantum signals

Scientists reveal it is possible to track up quantum signals. The technology is being used to provide precise timing and positioning, which are essential for a variety of critical infrastructure applications. The technology is being used to provide precise timing and positioning, which are essential for a variety of critical infrastructure applications. **#Quantum #Signals**





MARKET & COMPETITION

Spain to explore novel based technologies for QKD in

Spain's Defense & Security Ministry announced that it has signed a cooperation agreement to explore QKD in the defense sector. The agreement, signed with the Spanish QKD consortium, aims to explore the use of QKD in the defense sector, focusing on the development of secure communication systems for the Spanish Armed Forces. The agreement will explore the use of QKD in the defense sector, focusing on the development of secure communication systems for the Spanish Armed Forces.

Source: [Defense Ministry](#)



Polymorphic and quantum threats force strategic collaboration to accelerate quantum computing for aerospace and defense

Polymorphic and quantum threats have driven the need for collaboration of understanding efforts to accelerate the development of quantum computing applications in aerospace and defense. Building on years of strategic collaboration, the new effort will explore the use of quantum computing to address the challenges of quantum computing in the aerospace and defense sectors. The agreement will explore the use of quantum computing to address the challenges of quantum computing in the aerospace and defense sectors.

Source: [Defense Ministry](#)



Industry and Space-based Forces advance quantum secure satellite security

Industry and Space-based Forces are working together to advance quantum secure satellite security. The partnership aims to bridge the terrestrial fiber network segment with the secure space segment of quantum communication. The partnership aims to bridge the terrestrial fiber network segment with the secure space segment of quantum communication.

Source: [Space Force](#)



Full awarded Space QKD contract to deploy software for rapid system integration

The engineering for the contract will be completed in the next few weeks. The contract will explore the use of quantum computing to address the challenges of quantum computing in the aerospace and defense sectors. The agreement will explore the use of quantum computing to address the challenges of quantum computing in the aerospace and defense sectors.

Source: [Space Force](#)



Spain Aerospace sector and Defense Forces & Government to explore QKD in the use of QKD in the defense sector

Spain Aerospace sector and Defense Forces & Government to explore QKD in the use of QKD in the defense sector. The partnership aims to bridge the terrestrial fiber network segment with the secure space segment of quantum communication. The partnership aims to bridge the terrestrial fiber network segment with the secure space segment of quantum communication.

Source: [Defense Ministry](#)



★ GMV and LuxQuanta partner to integrate terrestrial and space-based quantum-safe communications

GMV, a Spanish technology group specializing in cybersecurity, space, and defense, and LuxQuanta, a company focused on Continuous-Variable Quantum Key Distribution (CV-QKD) technologies, have established a strategic alliance. This collaboration is intended to accelerate the real-world deployment of QKD technologies and strengthen Europe's sovereignty in quantum-safe communications. The partnership aims to bridge the terrestrial fiber network segment with the secure space segment of quantum communication. **#QKD #Partnership**

Source: [Quantum Computing Report](#)



Industry and Aerospace Association Group explore quantum satellite security collaboration agreement to

Industry and Aerospace Association Group explore quantum satellite security collaboration agreement to accelerate the real-world deployment of QKD technologies and strengthen Europe's sovereignty in quantum-safe communications. The partnership aims to bridge the terrestrial fiber network segment with the secure space segment of quantum communication. The partnership aims to bridge the terrestrial fiber network segment with the secure space segment of quantum communication.

Source: [Space Force](#)



Industry and Aerospace Association Group explore quantum satellite security collaboration agreement to

Industry and Aerospace Association Group explore quantum satellite security collaboration agreement to accelerate the real-world deployment of QKD technologies and strengthen Europe's sovereignty in quantum-safe communications. The partnership aims to bridge the terrestrial fiber network segment with the secure space segment of quantum communication. The partnership aims to bridge the terrestrial fiber network segment with the secure space segment of quantum communication.

Source: [Space Force](#)





THREAT INTELLIGENCE

Germany accuses Russia of jamming its satellites through the European protected frequency and with other means

Germany has accused Russia of jamming its satellites through the European protected frequency and with other means. The German Defense Minister Boris Pistorius said that two Russian Luch-Olymp reconnaissance satellites were tracking Intelsat spacecraft used by Germany's armed forces. In London, Major General Paul Tedman, head of the UK Space Command, reported that Russian forces are "shadowing" British military satellites and attempting to jam them on a weekly basis. This CNN article comes back on these declarations and decrypts Russia and China's threats to European space assets. #Jamming #CriticalInfra



Source: [CNN](#)

European countries have called for new EU strategy to counter the communication intelligence system that tracks the use of other forms of IT despite denying the vulnerability of satellite communication

European countries have called for a new EU strategy to counter the communication intelligence system that tracks the use of other forms of IT despite denying the vulnerability of satellite communication. The strategy requires the EU to develop a common approach to counter intelligence threats and to coordinate efforts to protect the use of space-based and satellite services. The EU should also consider the use of space-based intelligence. #CriticalInfra



Source: [European Parliament](#)

Space-based counterintelligence tactics

Space-based counterintelligence tactics are being used to track and intercept satellite communications. The US has been accused of using such tactics to track and intercept satellite communications. The US has been accused of using such tactics to track and intercept satellite communications. The US has been accused of using such tactics to track and intercept satellite communications. #CriticalInfra



Source: [CNN](#)

Space up satellite for space superiority

Space up satellite for space superiority. The US has been accused of using such tactics to track and intercept satellite communications. The US has been accused of using such tactics to track and intercept satellite communications. The US has been accused of using such tactics to track and intercept satellite communications. #CriticalInfra



Source: [CNN](#)



UK and Germany have accused Russia of threatening their satellites. Here's what that means

Germany and the United Kingdom have publicly accused Russia (and by extension China) of systematically targeting Western satellite systems, raising fresh concerns about the militarization of space. German Defense Minister Boris Pistorius said that two Russian Luch-Olymp reconnaissance satellites were tracking Intelsat spacecraft used by Germany's armed forces. In London, Major General Paul Tedman, head of the UK Space Command, reported that Russian forces are "shadowing" British military satellites and attempting to jam them on a weekly basis. This CNN article comes back on these declarations and decrypts Russia and China's threats to European space assets. #Jamming #CriticalInfra



Source: [CNN](#)

Australia Space Cybersecurity report challenges intelligence, and future direction

Australia Space Cybersecurity report challenges intelligence, and future direction. The report highlights the need for a common approach to counter intelligence threats and to coordinate efforts to protect the use of space-based and satellite services. The report also considers the use of space-based intelligence. #CriticalInfra



Source: [Australian Government](#)

China Space Security Strategy and Defense with new capabilities

China Space Security Strategy and Defense with new capabilities. The report highlights the need for a common approach to counter intelligence threats and to coordinate efforts to protect the use of space-based and satellite services. The report also considers the use of space-based intelligence. #CriticalInfra



Source: [CNN](#)

TRAINING & EDUCATION

Space and space-based intelligence (SBI) systems

Space and space-based intelligence (SBI) systems. The report highlights the need for a common approach to counter intelligence threats and to coordinate efforts to protect the use of space-based and satellite services. The report also considers the use of space-based intelligence. #CriticalInfra



Source: [European Parliament](#)



TRAINING & EDUCATION

★ Europe hosts first-ever multi-satellite cybersecurity challenge

Europe has completed its first in-orbit cybersecurity competition, marking a new step in space defense collaboration. The CTRL+Space Capture-the-Flag (CTF) challenge, held in the Netherlands, was also the world's first live event involving multiple satellites. Organized by D-Orbit and ethical hacking group mhackeroni, with backing from the ESA Security Cyber Centre of Excellence and ESA Security Office, the event aimed to strengthen Europe's ability to protect spacecraft from cyber threats. D-Orbit confirmed the competition's completion on 6 November. CyberInflight was represented at this conference by its CEO, Florent Rizzo. #CTF #3SConference



Sources: [Orbital Today](#), [Via Satellite](#), [CyberInflight](#)

OSINT spending detection method used on 500+ satellite systems
A new method for detecting OSINT spending on satellite systems has been developed by researchers at the University of Southampton. The method involves analyzing satellite data to identify patterns of activity that are indicative of OSINT spending. The researchers used this method to identify OSINT spending on a range of satellite systems, including those used by the UK, US, and other countries. The researchers also identified the countries that are most likely to be spending on OSINT. The researchers presented their findings at the 3S Conference in the Netherlands.



First learning-based radio frequency fingerprinting for 5G/6G spending detection
A new method for detecting OSINT spending on satellite systems has been developed by researchers at the University of Southampton. The method involves analyzing satellite data to identify patterns of activity that are indicative of OSINT spending. The researchers used this method to identify OSINT spending on a range of satellite systems, including those used by the UK, US, and other countries. The researchers also identified the countries that are most likely to be spending on OSINT. The researchers presented their findings at the 3S Conference in the Netherlands.



CyberSec 2025
The 2025 CyberSec conference is the largest event of its kind, bringing together leading experts from industry, academia, and government to discuss the latest in space security. The conference will feature a range of sessions, including keynote speeches, panel discussions, and workshops. The conference is organized by the European Space Agency (ESA) and the European Space Security Centre (ESSC). The conference is held in the Netherlands.



OSINT: How and where satellite data is used to identify satellite systems for security 2025
The new report, OSINT: How and where satellite data is used to identify satellite systems for security, provides a comprehensive overview of the OSINT landscape. The report covers a range of topics, including the use of satellite data for OSINT, the challenges of OSINT, and the future of OSINT. The report is published by CyberInflight.



EU Satellite Ground Station Cybersecurity cooperation conference
The second conference on EU Satellite Ground Station Cybersecurity cooperation will be held in Bonn, Germany, on 10-11 November 2025. The conference is organized by the European Space Agency (ESA) and the European Space Security Centre (ESSC). The conference is held in the Netherlands.



Workshop of the Space Cybersecurity Challenge at 3S 2025
The workshop of the Space Cybersecurity Challenge at 3S 2025 will be held in the Netherlands on 6 November 2025. The workshop is organized by D-Orbit and mhackeroni. The workshop is held in the Netherlands.



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

