

SPACE CYBERSECURITY WEEKLY WATCH

Week 41

October 7 - 13, 2025

Timeframe: Weekly

of articles identified: 37

Est. time to read: 80 minutes

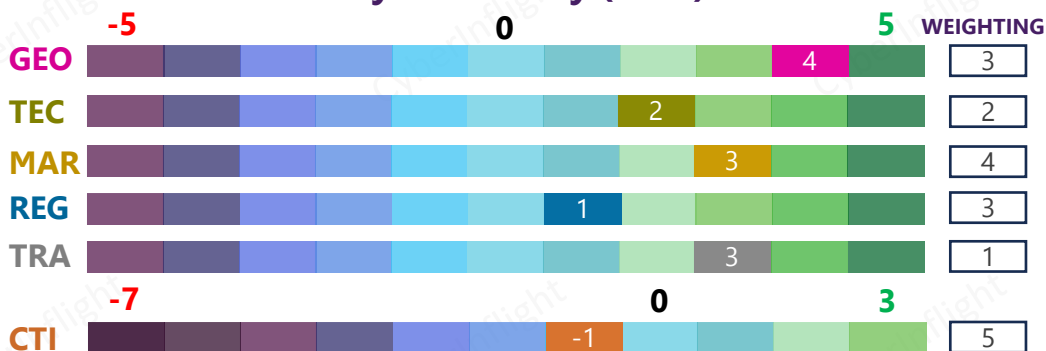
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

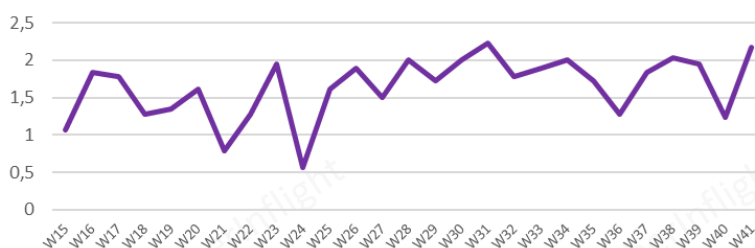
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



The RISC score for this watch is 2.17, an increase from last week. This change is attributed to an improvement on the threat intelligence side, with fewer incidents reported in the past few days.

This week, CyberInflight unveiled the Cyberdefense Monthly Watch, designed to support defense professionals and organizations engaged in defense-related activities, helping them stay informed and ahead in an increasingly complex operational environment. On the geopolitical front, the European Space Agency (ESA) took part in Jammertest 2025, which brought together 360 participants from 120 organizations across more than 20 countries. The organizers broadcast real satellite navigation interference for participants to observe how their equipment responds to it. The regulatory section focuses on India's growing ambitions in the direct-to-cell (D2C) satellite sector and the debates on how to regulate satellite-terrestrial coexistence and ensure affordable satellite communication access nationwide. On the technological side, Neuraspace has announced the launch of "Neuraspace DEF", designed to provide rapid, autonomous responses to the growing range of risks and threats facing space assets. On the market front, Lauryn Williams from the CSIS argues that protecting space systems from cyber-threats requires stronger public-private collaboration. She calls for renewed cross-sector cooperation, urging the government to declassify relevant threat data and the industry to prioritize cybersecurity in space operations. The threat intelligence section highlights an article written by Clémence Poirier on the cyberattack on Russia's Dozor-Teleport satellite network. Initially attributed to Wagner-linked hackers, the attack has now been claimed by the Ukrainian Cyber Alliance (UCA), highlighting the complex entanglement of hacktivist groups, state intelligence services, and the fragile infrastructure of the space sector. Lastly, in Training & Education, the focus is on a work that presents SpyChain, the first end-to-end design and implementation of an independent and colluding hardware supply chain threats targeting small satellites.

CYBERINFLIGHT'S NEWS



CyberInflight is proud to unveil its latest initiative: the Cyberdefense Monthly Watch

CyberInflight is leveraging its extensive experience in the space domain to provide actionable insights across the 5 warfare domains: space, air, land, sea, and cyber. The Cyberdefense Monthly Watch is designed to support defense professionals and organizations engaged in defense-related activities, helping them stay informed and ahead in an increasingly complex operational environment. **#CyberDefense #MonthlyWatch**

Source: [CyberInflight](#)



GEOPOLITICS



ESA Space Agency unveils ambitious 2025-26 plan to boost Europe's role in global space economy

The ESA Space Agency has unveiled its ambitious 2025-26 plan to boost Europe's role in the global space economy. The plan focuses on strengthening the ESA's role in the space domain, particularly in the areas of space exploration, space science, and space technology. The plan will also aim to enhance the ESA's role in the space domain, particularly in the areas of space exploration, space science, and space technology. The plan will also aim to enhance the ESA's role in the space domain, particularly in the areas of space exploration, space science, and space technology.

Source: [ESA](#)



ESA tests GNSS resilience during jamming test in the Arctic

In its pursuit of strengthening European resilience in navigation, the European Space Agency (ESA) took part in Jammertest 2025, which brought together 360 participants from 120 organizations across more than 20 countries, spanning academia, industry and governmental institutions. In a complex coordination exercise among seven Norwegian public authorities and facilitator Testnor, the organizers broadcast real satellite navigation interference for participants to observe how their equipment (on vehicles, drones, aircrafts, helicopters and vessels) responds. **#Jammertest2025 #Exercise**

Sources: [ESA](#), [GPS World](#)



Australian Space Command considers 'space control' options for its office

The Australian Space Command is considering 'space control' options for its office. The command is looking at ways to protect its own satellites and those of its allies. The command is looking at ways to protect its own satellites and those of its allies. The command is looking at ways to protect its own satellites and those of its allies.

Source: [Defence News](#)



European Space Agency sets out plan to boost Europe's role in global space economy

The European Space Agency (ESA) has set out its plan to boost Europe's role in the global space economy. The plan focuses on strengthening the ESA's role in the space domain, particularly in the areas of space exploration, space science, and space technology. The plan will also aim to enhance the ESA's role in the space domain, particularly in the areas of space exploration, space science, and space technology.

Source: [ESA](#)



Why cyber resilience in space is essential for economic security

Ensuring that space has become a critical enabler of economic security, particularly in the context of the global space economy. The space domain is becoming increasingly important for economic security, particularly in the context of the global space economy. The space domain is becoming increasingly important for economic security, particularly in the context of the global space economy.

Source: [CyberInflight](#)

In direction générale de l'Armement lance le projet Space (France): The Directorate General of Armaments launches the Space Plan

The Directorate General of Armaments (DGA) has launched the 'Space Plan' in October 2025. The plan focuses on strengthening the DGA's role in the space domain, particularly in the areas of space exploration, space science, and space technology. The plan will also aim to enhance the DGA's role in the space domain, particularly in the areas of space exploration, space science, and space technology.

Source: [CyberInflight](#)



REGULATION



India's D2C satcom race: power limitations, device ecosystem, and spectrum issues

This article discusses India's growing ambitions in the direct-to-cell (D2C) satellite sector and the regulatory challenges. Despite successful demonstrations by Viasat and BSNL, the absence of a legal framework for D2C/D2D services and spectrum coordination continues to delay commercial rollout. Policymakers are now debating how to regulate satellite-terrestrial coexistence and ensure affordable satcom access across the country. **#D2C #Opinion**

Source: [Medianama](#)



TECHNOLOGY



Neuraspace boosts defense resilience with new system to respond to threats to space assets

Neuraspace has announced its increased investment and renewed commitment to the defense and civil protection sector with the launch of "Neuraspace DEF". The new system is designed to provide rapid, autonomous responses to the growing range of risks and threats facing space assets. These risks and threats include jamming and spoofing of communications and navigation, cyberattacks on satellites and control stations, collisions with space debris, anti-satellite weapons (ASAT), orbital espionage, and potentially intrusive orbital technologies. **#NeuraspaceDEF #Resilience**

Source: [Satcom.digital](#)



ESA delivers the first EDRIS-DEF to the European Union

The European Space Agency (ESA) has delivered the first EDRIS-DEF (European Data Relay Infrastructure - Defense) to the European Union. This system is designed to provide rapid, autonomous responses to the growing range of risks and threats facing space assets. These risks and threats include jamming and spoofing of communications and navigation, cyberattacks on satellites and control stations, collisions with space debris, anti-satellite weapons (ASAT), orbital espionage, and potentially intrusive orbital technologies. **#NeuraspaceDEF #Resilience**

Source: [ESA](#)



India's satellite navigation system network plan

India's satellite navigation system network plan is a key component of the country's space strategy. The plan aims to provide a robust and resilient navigation system for the country's defense and civil protection sectors. The plan includes the development of a new generation of satellites and ground stations, as well as the integration of the system with other space-based systems. **#NeuraspaceDEF #Resilience**

Source: [ESA](#)



Poland's satellite navigation system network plan

Poland's satellite navigation system network plan is a key component of the country's space strategy. The plan aims to provide a robust and resilient navigation system for the country's defense and civil protection sectors. The plan includes the development of a new generation of satellites and ground stations, as well as the integration of the system with other space-based systems. **#NeuraspaceDEF #Resilience**

Source: [ESA](#)



US satellite navigation system network plan

The US satellite navigation system network plan is a key component of the country's space strategy. The plan aims to provide a robust and resilient navigation system for the country's defense and civil protection sectors. The plan includes the development of a new generation of satellites and ground stations, as well as the integration of the system with other space-based systems. **#NeuraspaceDEF #Resilience**

Source: [ESA](#)



MARKET & COMPETITION

ESA delivers the first EDRIS-DEF to the European Union

The European Space Agency (ESA) has delivered the first EDRIS-DEF (European Data Relay Infrastructure - Defense) to the European Union. This system is designed to provide rapid, autonomous responses to the growing range of risks and threats facing space assets. These risks and threats include jamming and spoofing of communications and navigation, cyberattacks on satellites and control stations, collisions with space debris, anti-satellite weapons (ASAT), orbital espionage, and potentially intrusive orbital technologies. **#NeuraspaceDEF #Resilience**

Source: [ESA](#)



MARKET & COMPETITION

Building Systems and Engineering Capabilities to enhance cybersecurity for aerospace and defense systems

A significant need for the aerospace and defense sector, Boeing has teamed up with Northrop Grumman, Lockheed Martin, and Raytheon to develop a multi-phase program. The program's goal is to enhance cybersecurity, software, and systems engineering, thereby enhancing aerospace systems' ability to resist cyber threats in high-risk environments like military operations and intelligence gathering. [Boeing-Boeing](#)



Spacecraft and New Age Fleet to accelerate adoption of next-gen navigation technology

Spacecraft, a leader in high-precision timing, and New Age Fleet, a leader in new high-precision clock units, will collaborate to develop a navigation system. The partnership aims to develop a navigation system that is more accurate, reliable, and secure than current systems. The company will continue to work on developing and testing the system, with the goal of providing a next-generation navigation system to the aerospace and defense sectors. [Spacecraft](#)



Early completion acquisition of Vector Space

Early completion acquisition of Vector Space, a leading space-based security company based in California, Vector Space, brings to the table 15 employees, which include senior-level executives, engineers, and operations staff. The acquisition is expected to enhance Vector Space's cybersecurity, intelligence, and defense capabilities. The company will continue to work on developing and testing the system, with the goal of providing a next-generation navigation system to the aerospace and defense sectors. [Vector Space](#)



Spanish industry aims to position itself in the GPS league of quantum leap

The consortium of Spanish companies are working to set up a new system to develop quantum navigation systems. The system is designed to be a quantum leap over current GPS systems, offering higher precision and security. The consortium is currently in the development phase, with the goal of launching the system in the near future. The system is expected to be a significant advancement in navigation technology, with the potential to revolutionize the industry. [Spanish industry](#)



Golden Space: A golden opportunity for the space industry

The current development of Golden Space, the Trump administration's initiative to develop space-based security systems, continues to attract the space industry with much media attention for the first year in the administration. The system is designed to be a quantum leap over current GPS systems, offering higher precision and security. The consortium is currently in the development phase, with the goal of launching the system in the near future. The system is expected to be a significant advancement in navigation technology, with the potential to revolutionize the industry. [Golden Space](#)



The Space Intelligence Federal Mission Cybersecurity Planning (SMICP) Level 2

The Space Intelligence Federal Mission Cybersecurity Planning (SMICP) Level 2 is a key component of the Space Intelligence Federal Mission. The mission is designed to be a quantum leap over current GPS systems, offering higher precision and security. The consortium is currently in the development phase, with the goal of launching the system in the near future. The system is expected to be a significant advancement in navigation technology, with the potential to revolutionize the industry. [SMICP Level 2](#)



First awarded contract by U.S. Space Force for Protected Tactical SATCOM-based (PTSC) system

The first awarded contract by U.S. Space Force for Protected Tactical SATCOM-based (PTSC) system is a significant milestone for the space industry. The system is designed to be a quantum leap over current GPS systems, offering higher precision and security. The consortium is currently in the development phase, with the goal of launching the system in the near future. The system is expected to be a significant advancement in navigation technology, with the potential to revolutionize the industry. [U.S. Space Force](#)



Securing the final frontier: the need for public-private collaboration on space cybersecurity

This article by Lauryn Williams (CSIS) argues that protecting space systems from cyber-threats requires stronger public-private collaboration. Despite growing risks, industry and government still operate in silos due to classification barriers and limited information sharing. She calls for renewed cross-sector cooperation, urging government to declassify relevant threat data and industry to prioritize cybersecurity in space operations. [#Policy #PublicPrivatePartnership](#)

Source: [Via Satellite](#)



THREAT INTELLIGENCE

Chinese corporations fight efforts to protect American GPS infrastructure from cyberattacks

Efforts to protect GPS infrastructure from cyberattacks are being complicated by a new wave of Chinese corporations that are actively seeking to undermine the system. According to a newly released report from the House Select Committee on Intelligence, Chinese companies are working to gain access to GPS infrastructure and to disrupt the system. The report also notes that Chinese companies are working to gain access to GPS infrastructure and to disrupt the system.

Source: [Washington Post](#)



Inside the Space Force's cyber war center keeping an eye on cyber threats

The Space Force's cyber war center is keeping an eye on cyber threats. The center is responsible for monitoring and responding to cyber threats to the space force's operations. The center is also responsible for coordinating with other agencies to respond to cyber threats.

Source: [The New York Times](#)



Self-attribution in cyberspace: the hack on Russia's Dozor-Teleport satellite network

This article written by Clémence Poirier comes back on the Ukrainian Cyber Alliance (UCA) that has claimed responsibility for the June 2023 cyberattack on Russia's Dozor-Teleport satellite network, previously attributed to Wagner-linked hackers. The case highlights the dangerous entanglement of hacktivist groups, state intelligence services, and the fragile infrastructure of the space sector. **#Dozor-Teleport #AttackAttribution**

Source: [Via Satellite](#)



China's grip on America's GPS is holding them back

China's grip on America's GPS is holding them back. The article discusses the challenges that China's control over GPS infrastructure poses for the United States. It also discusses the potential for China to use GPS infrastructure to gain access to sensitive information.

Source: [The New York Times](#)



TRAINING & EDUCATION



SpyChain: Multi-vector supply chain attacks on small satellite systems

This work presents SpyChain, the first end-to-end design and implementation of an independent and colluding hardware supply chain threats targeting small satellites. Using NASA's satellite simulation (NOS3), it demonstrates that SpyChain can evade testing, exfiltrate telemetry, disrupt operations, and launch Denial of Service (DoS) attacks through covert channels that bypass ground monitoring. **#SpyChain #Paper**

Source: [Cornell University](#)



U.S. Spacepower Must Be Secured

The article argues that the United States must take steps to secure its spacepower. It discusses the challenges that the United States faces in securing its spacepower and the potential for China to use spacepower to gain access to sensitive information.

Source: [The New York Times](#)



USDA: an added value for the European space industry

The article discusses the potential for the United States to provide added value for the European space industry. It discusses the challenges that the European space industry faces and the potential for the United States to help the industry overcome these challenges.

Source: [The New York Times](#)



Advancing GPS spoofing detection for autonomous vehicles through deep learning and hybrid architectures

The article discusses the potential for deep learning and hybrid architectures to advance GPS spoofing detection for autonomous vehicles. It discusses the challenges that autonomous vehicles face in detecting GPS spoofing and the potential for deep learning and hybrid architectures to help them overcome these challenges.

Source: [The New York Times](#)



TRAINING & EDUCATION

Overview of the system-level and processing capability and developmental challenges of the world's most advanced space systems

This is a comprehensive course covering the system-level and processing capability and developmental challenges of the world's most advanced space systems. The course covers the system-level and processing capability and developmental challenges of the world's most advanced space systems. The course covers the system-level and processing capability and developmental challenges of the world's most advanced space systems.

Source: [CyberInflight](#)



CyberInflight & Airbus Defense and Space announce strategic partnership

CyberInflight & Airbus Defense and Space announce strategic partnership. The partnership will focus on the development of space systems and the provision of space services. The partnership will focus on the development of space systems and the provision of space services. The partnership will focus on the development of space systems and the provision of space services.

Source: [CyberInflight](#)



15th annual International workshop on electromagnetic spectrum as outlined in Madrid (Spain) The 15th International workshop on electromagnetic spectrum as outlined in Madrid (Spain) will be held in Madrid (Spain) on 17 and 18 October 2025. The workshop will focus on the development of space systems and the provision of space services.

The workshop will focus on the development of space systems and the provision of space services. The workshop will focus on the development of space systems and the provision of space services. The workshop will focus on the development of space systems and the provision of space services.

Source: [CyberInflight](#)



Engaging the next generation in Europe's space future

The workshop will focus on the development of space systems and the provision of space services. The workshop will focus on the development of space systems and the provision of space services. The workshop will focus on the development of space systems and the provision of space services.

Source: [CyberInflight](#)



ESA's 15th annual workshop on electromagnetic spectrum as outlined in Madrid (Spain)

The workshop will focus on the development of space systems and the provision of space services. The workshop will focus on the development of space systems and the provision of space services. The workshop will focus on the development of space systems and the provision of space services.

Source: [CyberInflight](#)



Global detection, shared collection and intelligence gathering for commercial satellite-based systems in the upper right hand

This is a comprehensive course covering the system-level and processing capability and developmental challenges of the world's most advanced space systems. The course covers the system-level and processing capability and developmental challenges of the world's most advanced space systems. The course covers the system-level and processing capability and developmental challenges of the world's most advanced space systems.

Source: [CyberInflight](#)



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