



SPACE CYBERSECURITY WEEKLY WATCH

W6

February 3 – 9, 2026

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



The RISC score for this watch is 0.84, up from last week, driven by stronger scores in the Technology and Market sections. This score is balanced by an active threat climate.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score changes in 2026

In 2026, CyberInflight updated its methodology for calculating the RISC Score to better reflect observed realities. The scoring ranges for some categories were adjusted, as these were rarely assessed negatively and more often show moderate to high positive signals. The weighting of Technology was also increased. This change enables the RISC Score to more accurately capture meaningful variations in the risk environment.

This week, **Starlink cut off Russian troops' access to its satellite internet in Ukraine**, following a direct request from Kyiv. The move disrupted Moscow's frontline communications, highlighting the growing role of commercial space infrastructure in modern conflicts and the strategic leverage of private actors like SpaceX. On the regulatory side, **the White House advanced a draft Executive Order to unify U.S. quantum policy**, establishing a whole-of-government strategy to accelerate innovation, secure supply chains, and maintain American leadership. On the technological front, **China unveiled the TPG1000Cs, the world's first compact high-power microwave weapon capable of disrupting low-Earth-orbit satellites like Starlink**. With a sustained output of 20 gigawatts, this system raises concerns about the vulnerability of satellite constellations to ground-based directed-energy attacks, potentially reshaping the future of electronic warfare in space. Regarding the threat landscape, **European security officials revealed that Russian "inspector" satellites have intercepted communications** from at least a dozen key European spacecraft. These maneuvers, targeting unencrypted command links, risk not only espionage but also potential manipulation of satellite trajectories, underscoring the need for robust space situational awareness and encrypted systems. On the market front, **Spirent partnered with ESA to launch a PNT resilience initiative** for critical national infrastructure. The project will provide UK operators with a comprehensive test framework to measure, track, and enhance the robustness of positioning, navigation, and timing systems against growing disruptions, addressing a long-standing gap in GNSS security. Lastly, a **paper explores distributed anti-jamming strategies for LEO mega-constellations** using game-theoretic beamforming.



GEO POLITICS

Iran abandons U.S. GPS for Chinese Beidou, reducing the strategic grip of Middle East electronic warfare

Iran's latest abandonment of U.S. GPS for Chinese Beidou satellite navigation system is a sign of closer military cooperation between the two nations, according to a senior Iranian official. The move is seen as a strategic decision to reduce dependence on U.S. technology and to align with China's growing influence in the Middle East.

Source: [Reuters](#)



Musk's Starlink blocks Russian troops' internet access at Ukraine's request

Russian troops fighting in Ukraine have reported losing their Starlink satellite internet, according to Russia's pro-war military bloggers, after the SpaceX tycoon Elon Musk acted on a Ukrainian request to curtail access to his network, which Russian soldiers had been using illicitly.

Source: [DNYUZ](#)



The launch of the Galileo system

The launch of the Galileo system marks a significant milestone in the development of the European satellite navigation system. It is expected to provide more accurate and reliable positioning services for both civilian and military users across Europe and beyond.

Source: [ESA](#)



REGULATION



Draft quantum order tasks many agencies with reinvigorating the tech's development

The White House is currently developing a landmark Executive Order focused on quantum information sciences and technology, which is expected to establish a whole-of-government approach to bolstering the U.S. quantum ecosystem.

Source: [NextGov](#)



Congress just killed the Department of Energy's GPS satellite

The U.S. House of Representatives has passed a bill to prevent the Department of Energy from launching a GPS satellite. This move is seen as a significant step in reducing government involvement in the GPS system.

Source: [Reuters](#)



India reveals national plan for quantum safe security

India is working to secure its digital infrastructure against future quantum threats through a national quantum safe security plan. The plan includes developing quantum-resistant cryptographic algorithms and standards.

Source: [The Hindu](#)



TECHNOLOGY

UK moves to update existing infrastructure to strengthen national resilience

The UK is undertaking a major program to update its existing infrastructure to strengthen national resilience. This includes upgrading power grids, water supply systems, and other critical services to be more secure and resilient against cyber threats.

Source: [BBC](#)



Ability to Connect to the Internet from Space is a Key Issue for the International Space Station

The ability to connect to the Internet from space is a key issue for the International Space Station. This is due to the need for reliable communication links between the station and Earth, which is essential for scientific research and crew safety.

Source: [ESA](#)





TECHNOLOGY

Researchers develop compact high-power microwave weapon capable of sustained output strong enough to disrupt low-Earth-orbit satellites, raising fresh concerns over space security

Chinese researchers say they have developed the world's first compact high-power microwave weapon capable of sustained output strong enough to disrupt low-Earth-orbit satellites, raising fresh concerns over space security. The researchers, from the Chinese Academy of Space Technology, say the device is a compact, high-power microwave weapon capable of sustained output strong enough to disrupt low-Earth-orbit satellites, raising fresh concerns over space security.

Source: [Tippr Insights](#)



Researchers develop compact high-power microwave weapon capable of sustained output strong enough to disrupt low-Earth-orbit satellites, raising fresh concerns over space security

Chinese researchers say they have developed the world's first compact high-power microwave weapon capable of sustained output strong enough to disrupt low-Earth-orbit satellites, raising fresh concerns over space security. The researchers, from the Chinese Academy of Space Technology, say the device is a compact, high-power microwave weapon capable of sustained output strong enough to disrupt low-Earth-orbit satellites, raising fresh concerns over space security.

Source: [Tippr Insights](#)



China unveils microwave weapon capable of disrupting Starlink satellites

Chinese researchers say they have developed the world's first compact high-power microwave weapon capable of sustained output strong enough to disrupt low-Earth-orbit satellites, raising fresh concerns over space security. **#Disruption #TPG1000Cs**

Source: [Tipp Insights](#)



Researchers develop compact high-power microwave weapon capable of sustained output strong enough to disrupt low-Earth-orbit satellites, raising fresh concerns over space security

Chinese researchers say they have developed the world's first compact high-power microwave weapon capable of sustained output strong enough to disrupt low-Earth-orbit satellites, raising fresh concerns over space security. The researchers, from the Chinese Academy of Space Technology, say the device is a compact, high-power microwave weapon capable of sustained output strong enough to disrupt low-Earth-orbit satellites, raising fresh concerns over space security.

Source: [Tippr Insights](#)

Researchers develop compact high-power microwave weapon capable of sustained output strong enough to disrupt low-Earth-orbit satellites, raising fresh concerns over space security

Chinese researchers say they have developed the world's first compact high-power microwave weapon capable of sustained output strong enough to disrupt low-Earth-orbit satellites, raising fresh concerns over space security. The researchers, from the Chinese Academy of Space Technology, say the device is a compact, high-power microwave weapon capable of sustained output strong enough to disrupt low-Earth-orbit satellites, raising fresh concerns over space security.

Source: [Tippr Insights](#)



THREAT INTELLIGENCE



Russian spy spacecraft have intercepted Europe's key satellites, officials believe

European security officials believe two Russian space vehicles have intercepted the communications of at least a dozen key satellites over the continent. Officials believe that the likely interceptions, which have not previously been reported, risk not only compromising sensitive information transmitted by the satellites but could also allow Moscow to manipulate their trajectories or even crash them. **#SIGINT #Russia**

Source: [FinancialTimes](#), [Kyiv Post](#)



Alleged Russian spy spacecraft have intercepted Europe's key satellites, officials believe

European security officials believe two Russian space vehicles have intercepted the communications of at least a dozen key satellites over the continent. Officials believe that the likely interceptions, which have not previously been reported, risk not only compromising sensitive information transmitted by the satellites but could also allow Moscow to manipulate their trajectories or even crash them.

Source: [FinancialTimes](#), [Kyiv Post](#)



Alleged Russian spy spacecraft have intercepted Europe's key satellites, officials believe

European security officials believe two Russian space vehicles have intercepted the communications of at least a dozen key satellites over the continent. Officials believe that the likely interceptions, which have not previously been reported, risk not only compromising sensitive information transmitted by the satellites but could also allow Moscow to manipulate their trajectories or even crash them.

Source: [FinancialTimes](#), [Kyiv Post](#)





THREAT INTELLIGENCE

Continuum group launches 'Strategic Aerospace Market 2026'

The Continuum group has launched its 'Strategic Aerospace Market 2026' report, which provides a comprehensive overview of the global aerospace market. The report highlights key trends and opportunities in the industry, including the impact of digital transformation and the growing importance of cybersecurity in aerospace operations.



[View Article](#)

US spy satellite agency launches high-speed data streaming service

The National Reconnaissance Office (NRO) has launched a new high-speed data streaming service for its spy satellites. This service will enable the agency to deliver real-time intelligence to its customers, significantly improving its operational effectiveness and response time.



[View Article](#)

European satellite, which was launched in space from European space of Russia, China

A European satellite, which was launched in space from the European Space Agency (ESA) launch complex in Russia, China, has been successfully launched. This marks a significant milestone in the agency's efforts to expand its global reach and enhance its satellite capabilities.



[View Article](#)

Major commercial launch set for 2026

A major commercial launch is set for 2026, featuring a new generation of satellites. This launch is expected to mark a significant milestone in the commercial satellite market, demonstrating the capabilities of next-generation launch vehicles and satellites.



[View Article](#)

MARKET & COMPETITION

Space 2026 to include satellite launch & satellite is generating the most growth of Middle East launch

Space 2026 is expected to include satellite launch & satellite is generating the most growth of Middle East launch. This trend is driven by the increasing demand for satellite services in the region, particularly in the areas of telecommunications and navigation.



[View Article](#)

Europe and Asia Space Systems sign MOU to develop innovative LEO-MEO solutions

Europe and Asia Space Systems have signed a Memorandum of Understanding (MOU) to develop innovative LEO-MEO solutions. This collaboration aims to leverage the strengths of both regions in satellite technology and launch services, creating a competitive and innovative market for low Earth orbit (LEO) and medium Earth orbit (MEO) satellites.



[View Article](#)

Space Force plans to create 'satellite ground' for physical layer training needs in the service

Space Force plans to create 'satellite ground' for physical layer training needs in the service. This initiative is designed to provide a realistic and immersive training environment for personnel involved in satellite operations, ensuring they are well-prepared for the challenges of the space domain.



[View Article](#)

Wallops, White Sands and Vandenberg join forces to prepare a future series of satellite constellations

Wallops, White Sands, and Vandenberg Air Force Base have joined forces to prepare a future series of satellite constellations. This collaboration focuses on space technology, satellite operations, and the development of new satellite constellations, ensuring the Air Force is ready to support the growing needs of the space program.



[View Article](#)

U.S. intelligence community launches 'Digital Living' satellite constellation program

The U.S. intelligence community has launched a 'Digital Living' satellite constellation program. This program is designed to provide a secure and resilient communication network for intelligence operations, ensuring the integrity and confidentiality of sensitive information.



[View Article](#)



MARKET & COMPETITION

ESA Awards 277 Million US Space Force contract to enhance digital engineering and support infrastructure

The European Space Agency (ESA) has awarded a 277 million US dollar contract to Lockheed Martin to enhance digital engineering and support infrastructure for the Space Force. The contract will support the development and testing of digital engineering tools and support infrastructure to support the Space Force's operations. The contract will be awarded to Lockheed Martin's Space and Missile Defense Research and Development Center (SMDC) in Huntsville, Alabama.

Source: [Space News](#)



Spirent partners with ESA to spearhead PNT resilience initiative for critical infrastructure

Spirent Communications, now part of Keysight Technologies, has partnered with the European Space Agency (ESA) to lead an initiative aimed at increasing the resilience of positioning, navigation and timing (PNT) systems used in critical national infrastructure. Under the initiative, Spirent and partners will deliver a comprehensive test framework to drive measurable resilience in PNT systems for users, operators and providers of critical infrastructure in the United Kingdom.

#Contract #NAVISP

Source: [GPS World](#)



Space cybersecurity leaders convene in Singapore to address escalating threats to integrated networks of GNSS

Space cybersecurity leaders convened in Singapore to address escalating threats to integrated networks of GNSS. The meeting was part of the Space Cybersecurity Summit, which brought together experts from the United States, Europe, and Asia. The summit focused on the challenges of securing GNSS systems and the need for international cooperation to address these threats. The summit was held at the Singapore Convention Centre and was attended by representatives from the US Space Force, ESA, and the Singapore Space Agency.

Source: [The National Space Society](#)



Space health services providers that use space signals when forces need them

Space health services providers that use space signals when forces need them. The article discusses the challenges of providing space health services and the need for providers to use space signals to ensure that they can provide services in a timely and effective manner. The article also discusses the need for providers to work closely with the military to ensure that they can provide services in a way that meets the needs of the military.

Source: [Space News](#)



Space Systems for Safety and Security (SS3) work plan for 2026

Space Systems for Safety and Security (SS3) work plan for 2026. The article discusses the SS3 work plan for 2026, which focuses on the development of space systems for safety and security. The work plan includes the development of space systems for the protection of critical infrastructure, the protection of space assets, and the protection of the space environment.

Source: [Space News](#)



TRAINING & EDUCATION

Building and New Mexico University launch satellite cybersecurity research center to boost

Building and New Mexico University launch satellite cybersecurity research center to boost. The article discusses the launch of a satellite cybersecurity research center at the University of New Mexico. The center will focus on the development of satellite cybersecurity research and the training of students in this field.

Source: [Space News](#)



Building a resilient ready force

Building a resilient ready force. The article discusses the need for a resilient ready force and the challenges of building such a force. The article also discusses the need for a resilient ready force to be able to respond to a wide range of threats and to be able to provide services in a timely and effective manner.

Source: [Space News](#)





TRAINING & EDUCATION



Distributed uplink anti-jamming in LEO mega-constellations via game-theoretic beamforming

Low-Earth-Orbit (LEO) satellite constellations have become vital in emerging commercial and defense Non-Terrestrial Networks (NTNs). However, their predictable orbital dynamics and exposed geometries make them highly susceptible to ground-based jamming. Traditional single-satellite interference mitigation techniques struggle to spatially separate desired uplink signals from nearby jammers, even with large antenna arrays. This paper explores a distributed multi-satellite anti-jamming strategy leveraging the dense connectivity and high-speed inter-satellite links of modern LEO mega-constellations. **#Paper #AntiJamming**

Source: [Cornell University](#)



*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*