



SPACE CYBERSECURITY WEEKLY WATCH

W7

February 10 – 16, 2026

Timeframe: Weekly
of articles identified: 25
Est. time to read: 55 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 0.94, up from last week, driven by stronger scores in the Technology and a less active threat climate.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



This week, **Russia and Iran condemned Elon Musk's Starlink at a United Nations meeting**, accusing the satellite constellation of violating international law. Both countries criticized its use in conflicts, signaling a growing pushback against the militarization of commercial space infrastructure and the influence of private actors in global security dynamics. On the regulatory side, the **European Union Agency for Cybersecurity (ENISA) updated its international strategy** to strengthen the EU's cybersecurity cooperation beyond Europe. The revised approach aligns with the EU's long-term objectives, emphasizing partnerships with global actors to address cross-border cyber threats and enhance collective resilience. On the market front, **Japan announced plans to subsidize the development of anti-jamming technology for satellite signals**, aiming for commercialization by 2033. The initiative, funded through JAXA's Space Strategy Fund with subsidies of up to 2.5 billion yen (\$16 million), underscores Tokyo's commitment to securing its satellite communications against growing electronic threats. On the threat landscape, a **report revealed how Chinese PLA satellites enabled Iran's hybrid kill chain during the 2025 Twelve-Day War with Israel**. Beijing's orbital surveillance fused with Tehran's strike capabilities, demonstrating a new model of cross-regional military cooperation that reshapes power dynamics in the Middle East and beyond. On the technological side, the **UK launched the TOUCAN project** to test an alternative to GNSS timing signals. This two-way satellite time and frequency transfer (TWSTFT) system, linking the UK's official timekeeping authority with its eLoran navigation system, aims to reduce dependency on vulnerable satellite-based timing infrastructure. Lastly, **new research explored adversarial attacks on satellite fingerprinting systems**.



GEOPOLITICS

How space rules to mitigate cyber risk, promote secure satellite communications

The National Communications Authority (NCA) of Canada and the Information, Communications and Cybersecurity Directorate (ICCD) of the United States have signed a Memorandum of Understanding (MOU) aimed at strengthening space cooperation in the area of cybersecurity. The MOU outlines a framework for collaboration to enhance the security of space-based communications systems, including satellite navigation, satellite communications, and satellite-based data services. The MOU also addresses the protection of space-based infrastructure and the promotion of secure satellite communications.

Source: [The Hill](#)



Russia, Iran blast Musk's Starlink during UN space meeting

Officials from Russia and Iran blasted Elon Musk's Starlink at a Monday United Nations meeting held by the Committee on the Peaceful Uses of Outer Space. Both countries alleged that Musk's satellite internet constellation service program was operating in violation of international law. **#UN #SpaceX**

Source: [The Hill](#)



How is France preparing for war in space?

The emergence of cyber threats in and from space presents a new frontier for France's national security. In a recent report, the French government outlined its strategy to protect its space-based infrastructure and ensure the continuity of its operations. The report also highlights the need for international cooperation to address the growing threat of space-based cyberattacks.

Source: [The Hill](#)



REGULATION



ENISA updates its international strategy to strengthen EU's cybersecurity cooperation

The European Union Agency for Cybersecurity has released an updated international strategy to reinforce the EU's cybersecurity ecosystem and strengthen cooperation beyond Europe's borders. The revised ENISA International Strategy refreshes the agency's approach to working with global partners while ensuring stronger alignment with the European Union's international cybersecurity policies, core values, and long-term objectives. **#ENISA #EUCooperation**

Source: [The Cyber Express](#)



MARKET & COMPETITION

USA and Turkey sign MOU to enhance cooperation in electronic communications

The National Communications Authority (NCA) of Canada and the Information, Communications and Cybersecurity Directorate (ICCD) of the United States have signed a Memorandum of Understanding (MOU) aimed at strengthening space cooperation in the area of cybersecurity. The MOU outlines a framework for collaboration to enhance the security of space-based communications systems, including satellite navigation, satellite communications, and satellite-based data services. The MOU also addresses the protection of space-based infrastructure and the promotion of secure satellite communications.

Source: [The Hill](#)



ENISA leads the EU's international strategy to strengthen European Union security in satellite communications

The European Union Agency for Cybersecurity has released an updated international strategy to reinforce the EU's cybersecurity ecosystem and strengthen cooperation beyond Europe's borders. The revised ENISA International Strategy refreshes the agency's approach to working with global partners while ensuring stronger alignment with the European Union's international cybersecurity policies, core values, and long-term objectives.

Source: [The Hill](#)



France signs space cooperation MOU with cooperation of Germany, Italy

The National Communications Authority (NCA) of Canada and the Information, Communications and Cybersecurity Directorate (ICCD) of the United States have signed a Memorandum of Understanding (MOU) aimed at strengthening space cooperation in the area of cybersecurity. The MOU outlines a framework for collaboration to enhance the security of space-based communications systems, including satellite navigation, satellite communications, and satellite-based data services. The MOU also addresses the protection of space-based infrastructure and the promotion of secure satellite communications.

Source: [The Hill](#)





MARKET & COMPETITION

Germany - a German company awarded contract to develop first satellite ground station for German Armed Forces

Germany's first satellite ground station is set to be built by a German company, awarded a contract by the German Ministry of Defense. The contract is for the development and construction of a satellite ground station for the German Armed Forces. The station will be used to receive and process data from German satellites. The contract is worth approximately 100 million euros. The company is expected to start work in early 2026 and complete the project by late 2027.

Source: [Defense Security Asia](#)



Japan to subsidize anti-jamming tech that protects satellite signals

The Japanese government plans to support the development of technology that prevents satellite telecommunication signals from jamming attacks, looking to commercialize the devices around 2033, Nikkei has learned. Financial support will be provided through the Space Strategy Fund, operated by the Japan Aerospace Exploration Agency. The maximum amount for each subsidy will be 2.5 billion yen (\$16 million). #SpaceStrategyFund #AntiJamming



Source: [Nikkei Asia](#)

THREAT INTELLIGENCE

As space gets crowded, cyber threats from jamming to spoofing satellites have surged

Space-based satellite attacks, including jamming and spoofing, are on the rise, according to a report from a leading space security firm. The report states that the number of satellite attacks has increased significantly in recent years, and is expected to continue to grow. The report also notes that the attacks are becoming more sophisticated, and are now targeting critical infrastructure. The report is a call to action for governments and industry to take steps to protect their satellites from cyber threats.

Source: [Defense Security Asia](#)

USCIS warns of rising espionage and supply chain cyber threats targeting defense sector

The United States Citizenship and Immigration Services (USCIS) has issued a warning about rising espionage and supply chain cyber threats targeting the defense sector. The agency states that these threats are becoming more frequent and sophisticated, and are a significant concern for national security. The agency is urging defense contractors and other stakeholders to take steps to protect their information and systems from these threats.

Source: [Defense Security Asia](#)



USDA - Department of Defense Launches Program

The United States Department of Defense (DoD) has launched a new program to support the development and deployment of satellite-based defense systems. The program is part of the DoD's broader strategy to modernize its space capabilities. The program will focus on developing and testing new satellite-based defense systems, including those that can detect and track threats in space. The program is expected to be completed by late 2026.

Source: [Defense Security Asia](#)



Cyber Threat Intelligence Framework

The Cyber Threat Intelligence Framework (CTIF) is a new framework for sharing and analyzing cyber threat intelligence. The framework is designed to help organizations better understand and respond to cyber threats. The framework includes a set of principles and best practices for sharing and analyzing cyber threat intelligence. The framework is expected to be widely adopted by organizations in the cybersecurity industry.

Source: [Defense Security Asia](#)



Chinese eyes, Iranian fists: how PLA satellites powered Iran's kill chain against Israel in the 2025 Twelve-Day War

The 2025 Twelve-Day War between Israel and Iran did not merely exchange ballistic missiles and drones across contested skies, but instead crystallised a structural transformation in the architecture of modern warfare, as Beijing's orbital surveillance networks fused with Tehran's strike forces to create a hybridised kill chain that has permanently altered the balance of power in the Middle East. #Iran #China

Source: [Defense Security Asia](#)





TRAINING & EDUCATION



SATversary: Adversarial Attacks and Defenses for Satellite Fingerprinting

In this paper, we evaluate a range of attacks against satellite fingerprinting, building on previous works by looking at attacks optimized to target the fingerprinting system for maximal impact. We design optimized jamming, dataset poisoning, and spoofing attacks, evaluating them in the real world against the SatIQ fingerprinting system designed to authenticate Iridium transmitters, and using a wireless channel emulator to achieve realistic channel conditions. We show that an optimized jamming signal can cause a 50% error rate with attacker-to-victim ratios as low as -30dB (far less power than traditional jamming techniques), and demonstrate successful spoofing attacks, with an attacker successfully removing their own transmitter's fingerprint from messages. **#Paper #Fingerprinting**



Source: [Cornell University](#)

2025 Research: The Economic and Security Implications of Modern Satellites by Prof. David Goldberg et al.
This article discusses satellite fingerprinting, which is the process of identifying satellites by their unique signals. It explores the challenges of satellite fingerprinting, such as the need for accurate data and the potential for spoofing attacks. The authors also discuss the importance of satellite fingerprinting for national security and the need for improved detection and mitigation techniques. **#Paper #Fingerprinting**



*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*