SPACE CYBERSECURITY WEEKLY WATCH
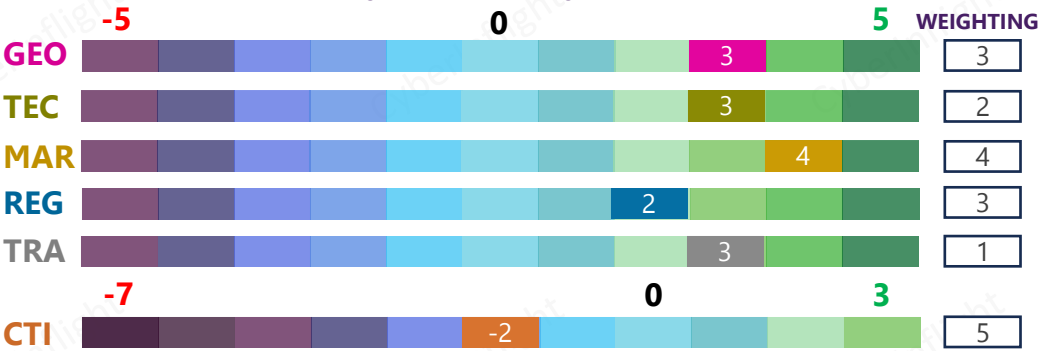
Week 31

July 29 – August 4, 2025

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

Timeframe: Weekly

# of articles identified: 34

Est. time to read: 75 minutes

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

RISC Score Assessment

2.23
RISC Score

Overview & Resilience Index for Space Cybersecurity (RISC)

	-5	0	5	WEIGHTING
GEO			3	3
TEC			3	2
MAR			4	4
REG		2		3
TRA			3	1

	-7	0	3	
CTI		-2		5

RISC Score evolution in 2025
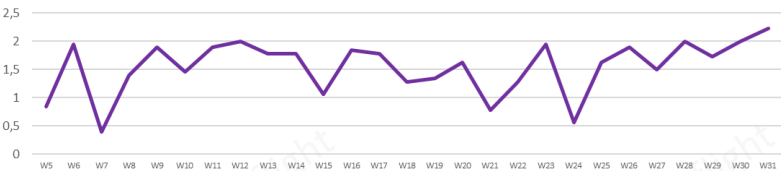
The RISC score for this watch is 2.23, an increase from last week. This difference is due to improvements on the geopolitical and market fronts.

This week, Lt. Gen. Philip A. Garrant, in charge of the USSF Orbital Watch initiative, announced that eventually Orbital Watch will be able to brief companies on specific threats they face, even when the need to protect intelligence sources and methods means the warnings must remain classified. The Orbital Watch is currently sharing unclassified threat information from U.S. intelligence agencies. Reinforcing the focus on supply chain security, NIST released the second public draft of Internal Report 8536, Supply Chain Traceability: Manufacturing Meta-Framework. This effort aims to help U.S. manufacturers securely exchange component traceability data across distributed ecosystems. Public comments are open until September 1, 2025. On the technology front, HawkEye 360 Inc. announced powerful enhancements to its GNSS Interference (GNSS-I) Detection product suite. These upgrades, designed with defense, intelligence, and national security operations in mind, offer unprecedented accuracy, coverage, and insight into global GPS jamming and spoofing threats. On the market front, Deloitte announced Silent Shield, explaining it is an out-of-band defensive cyber operations (DCO) payload designed to provide cyber analytics and anomaly detection. On the threat intel front, Estonian authorities reported that Russian GNSS jamming caused over €500,000 in damages over the past three months and included attempts to hijack Estonian border surveillance drones. Finally, wolfSSL presented a webinar on July 30 about 'Cybersecurity Solutions for the Satellite Industry'.

CyberInflight

GEOPOLITICS

Hacktivists, nation-state hackers target global maritime infrastructure as cyberattacks, GPS spoofing surge

New research from Cydle has uncovered more than a hundred cyberattacks targeting the maritime and shipping industry, linked to advanced persistent threat (APT) groups, ransomware operators, financially motivated actors, and hacktivists. Vulnerabilities including CVE-2022-32751, CVE-2019-11013, and CVE-2016-10012, affect COMNAV SAILOR 900 VSAT systems, compromising satellite communications at sea. **#GPSSpoofing #CriticalInfra**

Link: https://industrialcyber.co/ransomware/hacktivists-nation-state-hackers-target-global-maritime-infrastructure-as-cyberattacks-gps-spoofing-surge/

Kuwait to launch youth academy for AI, space, cybersecurity

Kuwait is set to launch a national youth academy focused on training young Kuwaitis in artificial intelligence, space sciences, robotics, and cybersecurity, the Public Authority for Youth announced. The initiative follows a new memorandum of understanding between the Authority and the Kuwait Space Company to establish the academy, which will serve as a hub for empowering youth with cutting edge skills. **#Academy #NationalStrategy**

Link: https://www.kuwaittimes.com/article/31494/kuwait/other-news/kuwait-to-launch-youth-academy-for-ai-space-cybersecurity/

How Air Force, Space Force secure 'ubiquitous communications'

Air Force players have to be able to communicate and share data with one another and back to their bases from any environment in the world, including degraded or denied spaces. But that's just one of the many challenges Aaron Bishop, chief information security officer of the Department of the Air Force, has to plan to provide secure communications across the Air Force and the Space Force every day. He also has to ensure safe and secure communications to and from satellites in space, as well as hardened IT for more than 100 bases — essentially small cities with housing, hospitals and other critical infrastructure — around the world. **#USSF #Communications**

Link: https://federalnewsnetwork.com/ask-the-cio/2025/07/how-air-force-space-force-secure-ubiquitous-communications/

China says Japan's space defense guidelines 'threaten security and stability'

Japan unveiled the space defense guidelines in Tokyo. Its defense ministry cited Chinese and Russian development of military capabilities in space as a reason it was seeking to boost defence in space and cooperation with the United States and other allies in response. China's foreign ministry said that in space, Japan, the US and other Western countries continued responding military cooperation and used 'defence' as a pretext to develop and deploy space weapons. **#Japan #SpaceWeapons**

Link: https://www.scmp.com/news/china/military/article/3320820/china-says-japans-space-defence-guidelines-threaten-security-and-stability

⭐ **Space Force aims to share classified threat info with industry**

The Space Force's neighborhood watch-style initiative to share information with the private sector about threats to space assets will eventually grow to include classified intelligence. **#OrbitalWatch #USSF**

Link: https://www.airandspaceforces.com/space-force-classified-threat-info-industry/

Japan joins multinational space defence drill

Japan's Air Self-Defense Force has taken part in a multinational tabletop space defence exercise in Australia aimed at enhancing cooperation among like-minded countries. Participants worked on procedures for dealing with and detecting satellite jamming signals and on how to avoid collisions with space debris. **#TabletopExercise #Exercice**

Link: https://www.japantimes.co.jp/news/2025/08/01/japan/japan-joins-multinational-space-defence-drill/

REGULATION

⭐ **New NIST Meta-Framework aims to bolster supply chain integrity across US manufacturing, improve traceability gaps**

The U.S. National Institute of Standards and Technology (NIST), through its National Cybersecurity Center of Excellence (NCCoE), has released the second public draft of NIST Internal Report 8536, Supply Chain Traceability: Manufacturing Meta-Framework. The effort supports U.S. manufacturers in securing their supply chains by developing a reference implementation that demonstrates how to exchange component traceability data securely across distributed ecosystems. **#SupplyChain #NIST**

Link: https://industrialcyber.co/manufacturing/new-nist-meta-framework-aims-to-bolster-supply-chain-integrity-across-us-manufacturing-improve-traceability-gaps/

TECHNOLOGY

US Space Force scheduled to launch eighth X-37B mission to carry quantum sensor, laser link experiments

The Defense Department's secretive X-37B Orbital Test Vehicle will lift off again in late August, carrying a quantum sensor that could enable navigation when GPS is unavailable as well as a laser communication system, the Space Force announced. The Aug. 21 mission will be the eighth for the mysterious space plane, which is operated by the Space Force in partnership with the Air Force Rapid Capabilities Office. **#X-37B #Quantum**

Link: https://www.airandspaceforces.com/x-37-eighth-mission-laser-comms-gps-alternative/

★ Hawkeye 360 launches advanced GNSS interference detection capabilities to enhance defense and intelligence operations

HawkEye 360 Inc., the global leader in signals intelligence data and analytics, announced powerful enhancements to its GNSS Interference (GNSS-I) Detection product suite. These upgrades—designed with defense, intelligence, and national security operations in mind—offer unprecedented accuracy, coverage, and insight into global GPS jamming and spoofing threats. **#AntiJamming #GNSS-I**

Link: https://www.prnewswire.com/news-releases/hawkeye-360-launches-advanced-gnss-interference-detection-capabilities-to-enhance-defense-and-intelligence-operations-302515592.html

Atomus achieves CMMC Level 2 certification to strengthen defense compliance readiness

Atomus, a cybersecurity solutions provider specializing in the aerospace and defense sector, announced it has successfully achieved Cybersecurity Maturity Model Certification (CMMC) Level 2 status with a perfect 110 out of 110 score. The certification was awarded following a formal third-party assessment completed in April 2025, reinforcing Atomus' position as a leader in defense-grade cybersecurity and compliance enablement. **#CMMC #Cybersecurity**

Link: https://atomus.com/atomus-achieves-cmmc-level-2-certification-to-strengthen-defense-compliance-readiness/

Quantum Key Distribution from Space: How SpeQtral is securing the future

What does it take to launch a quantum-secure global network from orbit? In this interview, we go to space with SpeQtral, a pioneering startup building quantum communication infrastructure via satellite. Join Chune Yang Lum and Robert Bedington at Asia Share SpeQtral's origin story, the physics behind satellite-based quantum key distribution (QKD), and how partnerships with companies like Thales and SES are helping scale the quantum internet. **#QKD #SpeQtral**

Link: https://www.youtube.com/watch?v=1Hegd7YU4a1

UK trials stratospheric balloons for ISR and comms missions

The Ministry of Defence has confirmed the successful trial of high-altitude balloons capable of conducting intelligence, surveillance and reconnaissance (ISR) missions from the stratosphere. The tests, conducted earlier this year in South Dakota under Project AETHER, mark a milestone in the development of low-cost, long-endurance surveillance and communications platforms for UK Defence. **#ISR #AETHER**

Link: https://ukdefencejournal.org.uk/uk-trials-stratospheric-balloons-for-isr-and-comms-missions/

A quantum gravimeter for GPS backup

A novel quantum sensor that measures gravity changes by detecting variations in the travel time of falling atoms has been tested in a first of its kind experiment aboard an Australian naval ship. The sensor—a dual gravimeter—has been developed by Australian company Q-CTRL and could reach the market in late 2026. During the tests onboard the Royal Australian Navy's aviation training vessel MV Sycamore, the crew was able to navigate for 144 hours without GPS access using the autonomous prototype system. **#Quantum #Australia**

Link: https://spectrum.ieee.org/quantum-gravity-sensor

MARKET & COMPETITION

Gilat awarded over $9m from Israel's Ministry of Defense for strategic defense communication solutions

Gilat Satellite Networks Ltd, a worldwide leader in satellite networking technology, solutions and services, announced that its defense division, Gilat Defense, has been awarded a contract valued at over $9m by Israel's Ministry of Defense for the delivery and integration of satellite communication systems and services. Deliveries are expected in the next 12 months. **#Contract #Defense**

Link: https://www.intelligentcio.com/apac/gilat-awarded-over-9-million-from-israels-ministry-of-defense-for-strategic-defense-communications-solutions/

MARKET & COMPETITION

WISeKey's strategic investment in WISeSat propels satellite constellation growth and accelerates commercialization of post-quantum space technology

WISeKey Corp, a company that focuses on developing and selling semiconductors, PKI, and Post-Quantum technology hardware and software products, announced a strategic investment in WISeSat.Space, the nano satellite technology venture of its parent company WISeKey International Holding Ltd, a leading global cybersecurity, blockchain, and IoT company. The investment aims to fuel the expansion of WISeSat's Low Earth Orbit (LEO) satellite constellation and fast-track the commercialization of its groundbreaking post-quantum ready space technology. The announcement follows the signing of a strategic partnership between WISeSat.Space and OrbitsEdge, the leading Bulgarian space technology firm, further expanding WISeKey's global collaboration network. **#Investment #PostQuantum**

Link: https://finance.yahoo.com/news/wisekey-strategic-investment-wisesat-propels-satellite-constellation-growth-and-accelerates-commercialization-of-post-quantum-space-technology

Deloitte launches cyber defense payload for satellites

Deloitte announced Silent Shield on July 30, explaining it is an out-of-band defensive cyber operations (DCO) payload designed to provide cyber analytics and anomaly detection. It can be deployed as a software-only payload, or as a hardware payload with dedicated compute, memory storage, and communications. Deloitte explained Silent Shield uses a one-way diode to gain visibility across the space vehicle, without being visible to adversaries or introducing additional risks to the spacecraft. **#SilentShield #Cybersecurity**

Link: https://www.satellitetoday.com/cybersecurity/2025/07/30/deloitte-launches-cyber-defense-payload-for-satellites/

Space Force picks 3 firms to develop anti-jam satellite communications

Months after cancelling a major satellite communications program, the Space Force announced contracts July 29 with three companies to showcase how their commercial designs could meet military requirements in the Protected Tactical Service Global program. PTS-G is envisioned as a constellation of small satellites in geosynchronous orbit that possess anti-jamming capabilities and offer a secure communications link worldwide. Space Systems Command, the Space Force's main acquisition arm, awarded contracts totaling $77.5m to Viasat, Northrop Grumman, Astranis, Intelsat, and Boeing. **#Contract #GEO**

Link: https://www.airandspaceforces.com/space-force-commercial-designs-satcom-pts-g/

BlackSky wins next phase of U.S. Navy Optical inter-satellite link research contract to advance Gen-3 comms for military ops

BlackSky Technology Inc. (NYSE: BKSY) has won the next phase of a competitive U.S. Navy research contract to further develop optical inter-satellite link (OISL) terminal apps for its Gen-3 constellation. Laser-based OISLs create high-bandwidth, direct communications links between satellites, reducing the time it takes to transmit and process data. In addition to reduced latency and decision-making, OISLs can provide a more secure and resilient data transmission path, making them less susceptible to interference and jamming. **#Contract #OISL**

Link: https://news.satnews.com/2025/07/blacksky-wins-next-phase-of-u-s-navy-optical-inter-satellite-link-research-contract-to-advance-gen-3-comms-for-military-ops/

Syrlinx and Kongsberg NanoAvionics to Collaborate on Next-Gen SAR Satellites for NATO and Allied Defence Applications

Syrlinx, an emerging developer of compact synthetic aperture radar (SAR) payloads, and small satellite manufacturer Kongsberg NanoAvionics (NanoAvionics) announced an agreement to place Syrlinx's inaugural SAR demonstrator into orbit. The flight will test Syrlinx's X-band radar on NanoAvionics' flight proven MP42 microsatellite bus. It will lay the groundwork for an all-European, military-grade SAR solution that provides rapid sovereign access to sub-meter, day, night, all-weather imagery for governments as well as NATO and allied defence applications. The launch aboard a SpaceX Falcon-9 Transporter rideshare mission is scheduled for the first quarter of 2026. **#Contract #NATO**

Link: https://www.satnews.com/digital-resources/syrlinx-and-kongsberg-nanoavionics-to-collaborate-on-next-gen-sar-satellites-for-nato-and-allied-defence-applications/

Viasat selected to deliver next generation encryption for US government cloud data centers

As a key provider to cloud data centers today, Viasat will develop a new generation high-assurance, high-speed Ethernet Data Encryptor (EDE) for protecting classified data across government cloud data centers and transport networks. **#Contract #CloudData**

Link: https://www.viasat.com/about/newsroom/press-releases/viasat-selected-to-deliver-next-generation-encryption-for-us-government-cloud-data-centers/

THREAT INTELLIGENCE

Damage from Russia's GPS jamming amounts to over €500k Estonia says

Satellite navigation jamming by Russia has caused more than half a million euros worth of damage in the last three months, Estonian authorities said on July 31. Russia also tries to take over the Estonian border guard's surveillance drones flying on the border. Officials from the Ministry of the Interior, the Police and Border Guard Board (PPA), and Consumer Protection and Technical Regulatory Authority (TTJA) gave an overview of the signal disruptions and Estonia's countermeasures. **#GPSJamming #Damage**

Link: https://news.err.ee/1609759581/damage-from-russia-s-gps-jamming-amounts-to-over-500-000-estonia-says

TRAINING & EDUCATION

TRAINING & EDUCATION

Live webinar: Cybersecurity solutions for the satellite industry

Join us on July 30th at 9 AM PT for the 'Cybersecurity Solutions for the Satellite Industry' webinar. As the industry leader in space-grade cybersecurity, wolfSSL products are deployed across satellites, delivery / rocket systems, and ground stations. Our software provides lightweight cryptographic and (D)TLS solutions optimized for satellite and aerospace systems. wolfSSL solutions also feature robust quantum-resistant cryptography, FIPS 140-3 certification, and CNSA 2.0 compliance.

#Webinar #Cybersecurity

Link: https://www.wolfssl.com/live-webinar-cybersecurity-solutions-for-the-satellite-industry/

TRAINING & EDUCATION

Interference analysis of BeiDou short message on GPS L1 receiver and mitigation based on cascaded hybrid blanking algorithm

The BeiDou Short Message Service (BDS-SMS) user equipment transmits signals in the frequency range of 1610-1626.5 MHz, which is adjacent to the Global Positioning System (GPS) L1 operating frequency band. Currently, reports from general aviation aircraft indicate that GPS positioning is interrupted when BDS-SMS is in use. BDS-SMS interference exhibits broadband characteristics, making it challenging to mitigate. To ensure the robustness of GPS L1 under BDS-SMS interference, it is essential to quantitatively analyze its impact on GPS L1 and develop targeted mitigation methods.

#Paper #BeiDou

Link: https://ieeexplore.ieee.org/document/11087135

Podcast Why Are Cybersecurity Risks Rising for Aerospace and Defense?

As competition between the United States and adversary nations intensifies, cybersecurity risks for aerospace and defense are rising. Listen in to this sponsored podcast as Josh Lospinoso, CEO and Co-Founder of Shift5, and David Forbes, who leads Cyber Physical Defense at Booz Allen Hamilton, explain the nature of the cybersecurity threat, the stakes involved and how to mitigate it. **#Podcast #Aerospace**

Link: https://aviationweek.com/defense/podcast-why-are-cybersecurity-risks-rising-aerospace-defense

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