SPACE CYBERSECURITY WEEKLY WATCH

Week 20

May 13 - 19 , 2025

Timeframe: Weekly

# of articles identified: 42

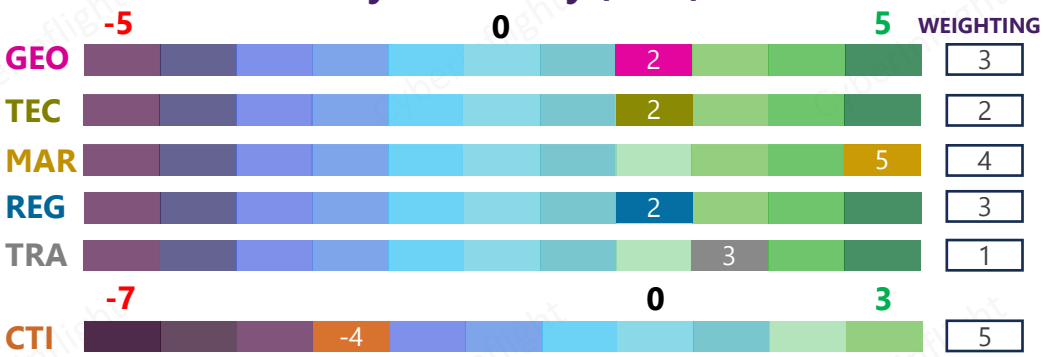
Est. time to read: 90 minutes

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

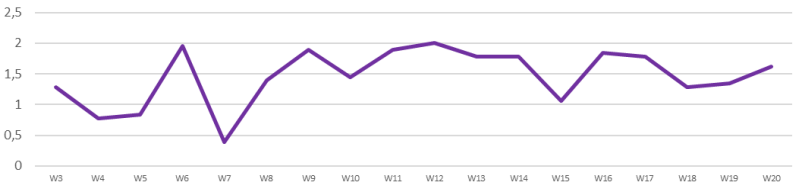
- GEOPOLITICS
- TECHNOLOGY
- MARKET & COMPETITION
- REGULATION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- IMPORTANT NEWS

RISC Score Assesment

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



The RISC score for this watch is 1.62, a slight increase from last week. This difference is due to a great market climate this week, with the highest RISC grade possible, and a slight amelioration on the threat side.

CyberInflight's team is delighted to have participated in CYSAT 2025 and met the ecosystem in Station F in Paris. We are also deeply happy and proud to have taken part in the writing of the recently released Orbital System Cybersecurity Hygiene Guide by CNES. This regulatory document does not aim to be coercive, but to ensure good practices for all players. Moreover, CyberInflight is delighted to announce its participation in the European MAKERSPACE project alongside great partners. This week's news includes Josef Aschbacher, director general of the European Space Agency (ESA), who keynoted CYSAT 2025 in Paris, underscoring a new approach toward securing space infrastructure. It is a newfound urgency toward space cybersecurity in Europe. On the technological front, experts worldwide are working urgently on post-quantum cryptography. On the market side, on the sidelines of the Aerospace Power Conference held in Rome, General Chance Saltzman, Chief of Space Operations of the U.S. Space Force (USSF), and General Luca Goretti, Chief of Staff of the Italian Air Force, signed a statement of understanding aimed at strengthening their cooperation in space security. Moreover, Resecurity and Starlink announced a strategic cybersecurity partnership at GISEC Global 2025. On the threat front, Earth Ammit disrupted drone supply chains through coordinated multi-wave attacks in Taiwan to target high-value entities downstream and amplify their reach. Lastly, a thorough analysis of the experimental data obtained during multiple communication sessions between Micius and one of the ground stations designed specifically for it was carried out. Relative time delays between all eight laser diodes on board have been found.

CYBERINFLIGHT'S NEWS

Exciting partnership announcement !

CyberInflight is thrilled to announce its participation in the MAKERSPACE project. **#Collaboration #Makerspace**

Link: https://www.linkedin.com/posts/dominant-information-solutions-canada-disc-inc_cybersecurity-satcomsystems-innovation-activity-7325977074848968704-w_pt?rcm=ACoAADea9_AB2PdJmljyibz-Zx3TxKHosCPhMgo

Face à la menace cyber, le spatial s'organise *(Trad: In the face of the cyber-threat, the space industry is getting organized)*

During CYSAT, CNES officially presented the "Guide d'hygiène cybersécurité des systèmes orbitaux" (Orbital System Cybersecurity Hygiene Guide), written with the contribution of its institutional, industrial and academic partners, including CyberInflight. **#CNES #HygieneGuide**

Link: https://cnes.fr/actualites/face-menace-cyber-spatial-sorganise

GEOPOLITICS

Da Costa (EUSPA): "L'Europa è una potenza spaziale. Non dovremmo aver paura di dirlo" *(Trad: Da Costa (EUSPA): "Europe is a space power. We shouldn't be afraid to say it")*

During the largest international event dedicated to cyber security for the space industry, CYSAT 2025, which takes place in Paris on the initiative of the Franco-Swiss cybersecurity company CYSEC, Rodrigo Da Costa, Executive Director of the European Union Agency for the space program on defense, threats to digital security and European satellite structures, was interviewed. **#EUSPA #SpacePower**

Link: https://strumentipolitici.it/da-costa-euspa-leuropa-e-una-potenza-spaziale-non-dovremmo-aver-paura-di-dirlo/

Attacco satellitare e treno deragliato: così la Difesa si esercita nel Poligono di Teulada (*Trad: Satellite attack and derailed train: this is how the Defense exercises in the Teulada Polygon)*

The organizers of Joint Stars 2025, the maxi inter-force, inter-agency and multi-domain exercise of the Italian Defense, planned and conducted by the Joint Operations Command (Covi) currently underway in the Sardinian shooting ranges, asked themselves these questions. **#JointStars #Defense**

Link: https://www.unionesarda.it/en/sardinia/satellite-attack-and-derailed-train-this-is-how-the-defense-exercises-in-the-teulada-polygon-pqm4pevr

ESA director general signals a bold new approach to European space cybersecurity

There is a newfound urgency toward space cybersecurity in Europe. Josef Aschbacher, director general of the European Space Agency (ESA), keynoted CYSAT 2025 in Paris, underlying a new approach toward securing space infrastructure. **#ESA #CYSAT**

Link: https://www.satellitetoday.com/cybersecurity/2025/05/16/esa-director-general-signals-a-bold-new-approach-to-european-space-cybersecurity/

Drones, space, cyberspace add new paradigm to military conflicts: Ex-DGMO Anil Bhatt

Operation Sindoor has brought into sharp focus the importance of drones in modern warfare, which along with space and cyberspace will write the new paradigm of future military conflicts, a former Director General of Military Operations who oversaw the Doklam crisis, has said. **#Warfare #Military**

Link: https://economictimes.indiatimes.com/news/defence/drones-space-cyberspace-add-new-paradigm-to-military-conflicts-ex-dgmo-anil-bhatt/articleshow/121202714.cms

10 reasons why America needs a Cyber Force

America's cyber force generation system is clearly broken. Fixing it demands nothing less than the establishment of an independent cyber service. Here are 10 reasons why. **#U.S. #CyberForce**

Link: https://www.fdd.org/analysis/2025/05/15/10-reasons-why-america-needs-a-cyber-force/

Cybersecurity concerns rise for Australia's infrastructure

Australian Signals Directorate says 11% of 1,100 cyber incidents in targeted critical infrastructure, with phishing & credential compromise leading threats. **#CriticalInfra #Concerns**

Link: https://cybermagazine.com/articles/australia-11-of-cyber-incidents-hit-infrastructure

No one knows who's in charge of Trump's dramatic space policy

Space industry officials and Capitol Hill staffers describe a rudderless administration when it comes to space policy, with no single person driving the big shifts. **#U.S. #SpacePower**

Link: https://www.politico.com/news/2025/05/14/trump-space-policy-leadership-void-00349131

TECHNOLOGY

Ground Station virtualization: revolutionizing satellite communication

As the demand for satellite communication grows across industries such as Earth observation, IoT, and global connectivity, the need for efficient and cost-effective ground station operations has never been greater. **#GSV #GroundStation**

Link: https://idstch.com/space/ground-station-virtualization-revolutionizing-satellite-communication/

Espace militaire : les députés veulent plus de capteurs, plus de vitesse, plus de protection *(Trad: Military space: MEPs want more sensors, more speed, more protection)*

Dazzling advances in space technology are transforming the art of warfare. According to General Philippe Steininger, military advisor to the Chairman of CNES, we are witnessing a strategic breakthrough comparable to the advent of aviation in the First World War. Satellites may not yet have a direct kinetic effect, but they will revolutionize two essential aspects: the transparency of the battlefield and the reduction in latency between detection and action. **#Satellites #CNES**

Link: https://opexnews.fr/espace-militaire-capteurs-vitesse-protection/

Les ordinateurs quantiques pourraient déchiffrer les codes de sécurité utilisés par les satellites *(Trad: Quantum computers could decipher the security codes used by satellites)*

Experts worldwide are working urgently to develop new types of digital “locks” that can't be tampered with by quantum computers - a field known as “post-quantum cryptography”. **#QuantumComputing #Locks**

Link: https://infohightech.com/les-ordinateurs-quantiques-pourraient-dechiffrer-les-codes-de-securite-utilises-par-les-satellites/

MARKET & COMPETITION

US Space Force partners with Italian Air Force to counter growing threats in space

On May 8, 2025, on the sidelines of the Aerospace Power Conference held in Rome, General Chance Saltzman, Chief of Space Operations of the U.S. Space Force (USSF), and General Luca Goretti, Chief of Staff of the Italian Air Force, signed a statement of understanding aimed at strengthening their cooperation in space security. **#USSF #Partnership**

Link: https://armyrecognition.com/news/aerospace-news/2025/us-space-force-partners-with-italian-air-force-to-counter-growing-threats-in-space

Leonardo partners with Faculty AI to serve armed forces

Leonardo has partnered with Faculty AI, one of the UK’s leading independent AI companies. The companies will look to bring AI-driven defense capabilities, such as Cognitive Intelligent Sensing (CoInS) and Electronic Warfare (EW), out of the lab and into the hands of the UK armed forces quicker. **#Partnership #FacultyAI**

Link: https://businesscloud.co.uk/news/leonardo-partners-with-faculty-ai-to-serve-armed-forces/

FCC opens door to GPS alternatives, but risks undermining its greatest strength

The move signals growing federal concern about the reliability of space-based navigation and timing infrastructure amid rising global interference and spoofing incidents. **#GPS #FCC**

Link: https://www.gpsworld.com/fcc-opens-door-to-gps-alternatives-but-risks-undermining-its-greatest-strength/

La DGA - Direction générale de l'armement a récemment publié son bilan d’activité, mettant en lumière son engagement stratégique *(Trad: DGA - Direction Générale de l'Armement - recently published its activity report, highlighting its strategic commitment)*

This report highlights the extent to which technological sovereignty depends on a strategy of continuous innovation, and the extent to which the civilian ecosystem plays a leading role alongside the armed forces. **#DGA #ActivityReport**

Link: https://www.linkedin.com/posts/dfy-partners_spatial-cyber-innovation-activity-7327994558431047680-nM7X?rcm=ACoAACVjFHoBnJXMQv4pQkVRLVCw1GWctJMWTvU

La Chine démarre l’assemblage de son superordinateur spatial *(Trad: China starts assembly of its space supercomputer)*

China's ADA Space recently marked a milestone in space exploration by launching the first 12 satellites in an ambitious network of 2,800 satellites dedicated to artificial intelligence. This initiative, announced during a mission on May 18, 2025, aims to create a network of orbital supercomputers capable of processing data directly from space. **#ADASpace #AI**

Link: https://abestit.fr/la-chine-demarre-lassemblage-de-son-superordinateur-spatial/

MARKET & COMPETITION

SEALSQ to invest $10m in WISeSat.Space to accelerate satellite constellation deployment, space-based quantum key distribution (QKD) communications, and decentralized IoT transactions

SEALSQ Corp, a company that focuses on developing and selling Semiconductors, PKI, and Post-Quantum technology hardware and software products, during its Quantum Day in France, announced the intention to invest $10m in WISeSat.Space AG ("WISeSat"), and join its parent company, WISeKey International Holding Ltd as a strategic investor in the WISeSat satellite constellation. **#Investment #SEALSQ**

Link: https://forextv.com/sealsq-to-invest-10-million-in-wisesat-space-to-accelerate-satellite-constellation-deployment-space-based-quantum-key-distribution-qkd-communications-and-decentralized-iot-transactions/

Q-KON and Rivada Space Networks partner for next-gen secure connectivity in Africa

Q-KON and Rivada Space Networks partner to deliver secure, high-speed satellite connectivity across Africa, enhancing digital transformation and network resilience. **#Contract #Africa**

Link: https://techafricanews.com/2025/05/13/q-kon-and-rivada-space-networks-partner-for-next-gen-secure-connectivity-in-africa/

The UAE's role in the next era of satellite intelligence

The impact of public-private collaborations, advancements in satellite data usage, and the UAE's drive to lead in space intelligence and sustainable development. **#SpaceIntelligence #Collaboration**

Link: https://www.broadcastprome.com/news/satellite/the-uaea%c2%92s-role-in-the-next-era-of-satellite-intelligence/

Quantum computing company IonQ to acquire Capella Space

Quantum computing company IonQ has signed an agreement to acquire Capella Space to accelerate its plans in quantum networking. **#IonQ #Acquisition**

Link: https://www.satellitetoday.com/finance/2025/05/07/quantum-computing-company-ionq-to-acquire-capella-space/

SES to demonstrate 'satellite orchestration' tech for military communications

As military operations increasingly depend on rapid and resilient communications across multiple domains, satellite operators are racing to provide not just bandwidth, but smarter ways to use it. Under a new contract with the Pentagon's Defense Innovation Unit (DIU), satellite communications provider SES Space & Defense plans to demonstrate a software platform that would make it easier for users to access and manage bandwidth from multiple satellite networks across orbits. **#SES #Military**

Link: http://spacenews.com/ses-to-demonstrate-satellite-orchestration-tech-for-military-communications/

Resecurity and Starlink announce strategic cybersecurity partnership at GISEC Global 2025

This partnership will integrate Resecurity's cutting-edge cybersecurity solutions into Starlink's extensive distribution network, enabling organizations across the META region to proactively detect, analyze, and respond to cyber-threats. **#Partnership #Resecurity**

Link: https://arab.news/c2e7b

SpaceX proposes Starlink as a GPS alternative

SpaceX is positioning its Starlink satellite constellation as a viable alternative to the Global Positioning System (GPS), proposing that its network can deliver Positioning, Navigation, and Timing (PNT) services to complement existing systems. **#GPS #Starlink**

Link: https://driveteslacanada.ca/news/spacex-proposes-starlink-as-a-gps-alternative/

THREAT INTELLIGENCE

Will satellite dogfights be the final frontier for the U.S.-China space rivalry?

Analysts warn of more intense space race as rival powers grappling with low trust and transparency seek both superiority and deterrence. **#U.S. #China**

Link: https://www.scmp.com/news/china/military/article/3310469/will-satellite-dogfights-be-final-frontier-us-china-space-rivalry

U.S. space chief warns of emerging threats from China and Russia

Surging technologies spearheaded by Chinese and Russian forces represent the greatest threat in space defense, Chief of Space Operations Gen. B. Chance Saltzman said Thursday at the POLITICO Security Summit. **#China #Russia**

Link: https://www.politico.com/news/2025/05/15/space-chief-saltzman-china-russia-threats-00351616

THREAT INTELLIGENCE

Russian military cadet reportedly arrested for selling hacking tool to FSB agent

A cadet from the Russian military space academy in St. Petersburg has reportedly been arrested for allegedly developing and attempting to sell a hacking tool capable of breaching a classified security system used by law enforcement and military personnel. **#HackingTool #FSB**

Link: https://therecord.media/russian-military-cadet-reportedly-arrested-for-selling-hacking-tool

Earth Ammit disrupts drone supply chains through coordinated multi-wave attacks in Taiwan

Victims of the TIDRONE and VENOM campaigns primarily originated from Taiwan and South Korea, affecting a range of industries including military, satellite, heavy industry, media, technology, software services, and healthcare sectors. Earth Ammit's long-term goal is to compromise trusted networks via supply chain attacks, allowing them to target high-value entities downstream and amplify their reach. **#Attacks #EarthAmmit**

Link: https://www.trendmicro.com/en_us/research/25/e/earth-ammit.html

What you need to know about firmware security in chips

The rapid advancement of semiconductor technologies has transformed industries across the globe, from data centers to consumer devices, and even critical infrastructure. With the ever-growing reliance on interconnected devices, robust security systems are paramount. **#SupplyChain #Firmware**

Link: https://www.edn.com/what-you-need-to-know-about-firmware-security-in-chips/

Pakistan-allied hackers launched 1.5m cyberattacks on India since the Pahalgam strike

Maharashtra Cyber has uncovered over 1.5m cyberattacks by seven Pakistan-allied hacking groups targeting India's critical infrastructure following the Pahalgam terror strike. Despite a ceasefire, attacks from Pakistan, Bangladesh, and Middle Eastern countries persist, with only 150 succeeding, officials said. **#APT #Pakistan**

Link: https://organiser.org/2025/05/13/291915/bharat/pakistan-allied-hackers-launched-1-5-million-cyber-attacks-on-india-since-pahalgam-strike/

Data breach claimed by Moroccan soldiers hacktivist group on Starlink

Skeptical claim by Moroccan Soldiers hacktivist group, who claim to have breached some data from SpaceX but provides no evidence. **#Morocco #Claim**

Link: https://x.com/Cyberknow20/status/1825891902618742971

MSC ANTONIA GPS jamming incident / Steve Bomgardner & Pole Star Global

It has been reported recently that an MSC container vessel, MSC ANTONIA, has run aground around 100 nautical miles (nm) off the coast of Jeddah, in Saudi Arabia due to a GPS jamming incident. **#Jamming #MSC**

Link: https://allaboutshipping.co.uk/2025/05/15/comment-msc-antonia-gps-jamming-incident-steve-bomgardner-pole-star-global/

[WID-SEC-2023-1143] Red Hat Satellite: Multiple vulnerabilities

A remote, anonymous attacker can take advantage of multiple vulnerabilities in Red Hat Satellite to run any program code, disclose information, perform a cross-site scripting attack, or cause a denial of service condition. **#RedHat #Vulnerability**

Link: https://wid.cert-bund.de/portal/wid/securityadvisory?name=WID-SEC-2023-1143

What can we learn about cybersecurity for space from existing safety procedures?

Space systems are growing in importance, raising the stakes if infrastructure is disrupted. In response to growing cyber-threats, the conversation surrounding cyber security and space is evolving rapidly, as regulations are developed to increase security baselines. **#Procedures #Report**

Link: https://www.satellitetoday.com/opinion/2025/05/16/what-can-we-learn-about-cybersecurity-for-space-from-existing-safety-procedures/

Consult the European vulnerability database to enhance your digital security!

The European Union Agency for Cybersecurity (ENISA) has developed the European Vulnerability Database - EUVD as provided for by the NIS2 Directive. The database provides aggregated, reliable, and actionable information such as mitigation measures and exploitation status on cybersecurity vulnerabilities affecting Information and Communication Technology (ICT) products and services. **#NIS2 #Database**

Link: https://www.enisa.europa.eu/news/consult-the-european-vulnerability-database-to-enhance-your-digital-security

TRAINING & EDUCATION

GNSS/GPS signal integrity in autonomous systems: Key issues and solutions

Outside of the military, interference is the most common threat to GNSS, with the dominant source being cellular transmission harmonics. It is commonly addressed with out-of-band filters. **#GNSS #Interference**

Link: https://www.gpsworld.com/gnss-gps-signal-integrity-in-autonomous-systems-key-issues-and-solutions/

Building a global quantum internet using a satellite constellation with inter-satellite links

The quantum internet is a global network to distribute entanglement and communicate quantum information with applications in cybersecurity, quantum computing, and quantum sensing. Here, we propose building a quantum internet using a constellation of low-Earth-orbit satellites equipped with inter-satellite laser links. **#Quantum #Constellation**

Link: http://arxiv.org/abs/2505.08075

Micius, the world's first quantum communication satellite, was hackable

The National University of Singapore carried out a thorough analysis of the experimental data obtained during multiple communication sessions between Micius and one of the ground stations designed specifically for it. Relative time delays between all the eight laser diodes on board have been found. **#Quantum #Micius**

Link: http://arxiv.org/abs/2505.06532

Enriched K-Tier heterogeneous satellite networks model with user association policies

In this paper, two representative user association policies (UAPs) for multi-tier heterogeneous satellite networks (HetSatNets) are investigated, namely the nearest satellite UAP and the maximum signal-to-interference-plus-noise-ratio (max-SINR) satellite UAP, where each tier is characterized by a distinct constellation configuration and transmission pattern. **#HetSatNets #UAPs**

Link: http://arxiv.org/abs/2505.09917

New frontiers in global security: Emerging technologies and outer space

On 19 May 2025, UNIDIR and United Nations University (UNU) will co-host the panel discussion "New frontiers in global security: Emerging technologies and outer space". **#Discussion #UNU**

Link: https://unidir.org/event/new-frontiers-in-global-security-emerging-technologies-and-outer-space/

Space Threat Landscape 2025, le sfide alle porte e come affrontarle *(Trad: Space Threat Landscape 2025, the challenges ahead and how to face them)*

The EU's leading cybersecurity agency has published a new detailed report outlining the threat landscape and recommending measures to mitigate the most serious risks in the space sector. **#ENISA #Report**

Link: https://www.cybersecurity360.it/outlook/space-threat-landscape-2025-le-sfide-alle-porte-e-come-affrontarle/

How do zero-day exploits relate to space cyber warfare?

This informative video dives into the critical topic of zero-day exploits within the context of space cyber warfare. As technology continues to advance, understanding the vulnerabilities in software and hardware becomes increasingly important. **#Video #Zero-Day**

Link: https://www.youtube.com/watch?v=79QlpTTfYu8