SPACE CYBERSECURITY WEEKLY WATCH

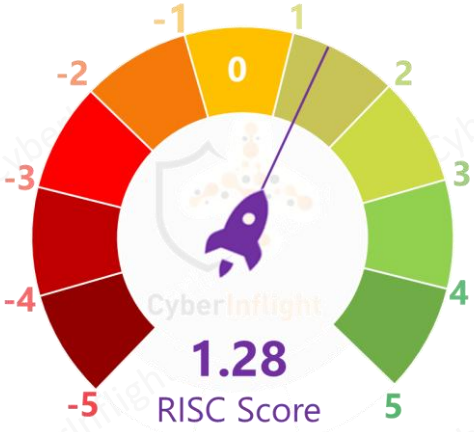
Week 1 & 2
January 1 - 13, 2025

Timeframe: Weekly
# of articles identified: 36
Est. time to read: 60 minutes

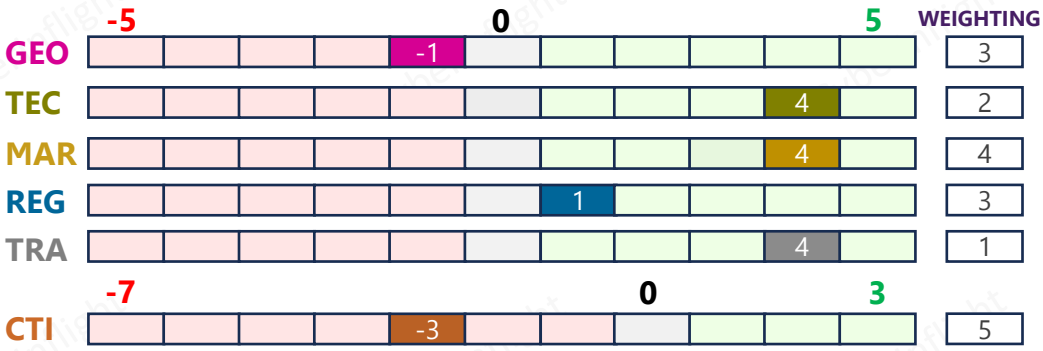
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

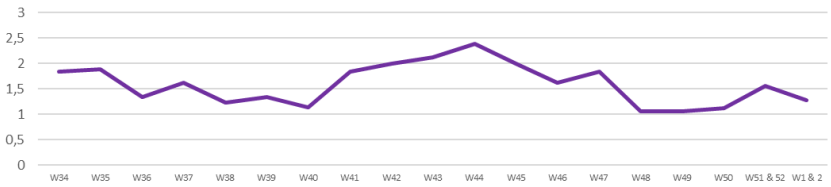
RISC Score Assesment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2024 and 2025



These weeks' RISC score is 1.28, reflecting a slight decrease compared to weeks 51 & 52. This is especially due to a few news about threat/attack events.

On the geopolitical side, these past two weeks, US Secretary of State Antony Blinken revealed that Russia is prepared to share advanced space and satellite technology with North Korea in exchange for weapons and military equipment to support its ongoing war in Ukraine. On the threat intel front, Japan linked more than 200 cyberattacks targeting the country's national security and high technology data over the past five years to a Chinese hacking group, MirrorFace, detailing their tactics and calling on government agencies and businesses to reinforce preventive measures. The attacks targeted government agencies, businesses, and individuals and aimed to steal sensitive information on defense, space, and advanced technology. Meanwhile, in the US, two competing prototype payloads, developed by Northrop Grumman and Boeing, are both set to launch in 2025, aiming to open a new era of secure, jam-resistant tactical communications. Moreover, on the market side, the eventuality for Starlink to operate in Italy has made the headlines. Parallelly, the Space Systems Command (SSC), a subordinate unit of the United States Space Force (USSF), selected Modern Technology Solutions, Inc. (MTSI) to develop and deliver Defensive Cyber Operations for Space (DCO-S) capabilities across the USSF. On the regulation front, the US DoD, GSA, and NASA are working to amend the Federal Acquisition Regulation (FAR) to incorporate the NICE Workforce Framework for Cybersecurity (NICE Framework), National Institute of Standards and Technology (NIST) Special Publication 800-181 and additional tools. Last but not least, the latest episode of Timothy De Block's podcast is out. He sits down with Tim Fowler, the creator of Tempest, a hands-on educational project focused on space cybersecurity.

GEOPOLITICS

Russia may trade space tech for North Korean arms, Blinken warns

US Secretary of State Antony Blinken revealed on Monday that Russia is prepared to share advanced space and satellite technology with North Korea in exchange for weapons and military equipment to support its ongoing war in Ukraine. **#Russia #NorthKorea**

Link: https://euromaidanpress.com/2025/01/06/russia-may-trade-space-tech-for-north-korean-arms-blinken-warns/

SpaceX launches NROL-153, expanding US spy satellite constellation

A SpaceX Falcon 9 rocket launched the National Reconnaissance Office's (NRO) NROL-153 mission on Jan. 9, marking the latest step in the agency's rapid expansion of its proliferated low Earth orbit (LEO) satellite constellation. The rocket lifted from Vandenberg Space Force Base in California, carrying classified payloads designed to bolster US intelligence and surveillance capabilities. The mission is the seventh under the NRO's proliferated architecture strategy and the first NRO launch of 2025. **#SpaceX #NROL**

Link: https://spacenews.com/spacex-launches-nrol-153-expanding-u-s-spy-satellite-constellation/

Space Force sets up first Cyber Range Squadron

The US Space Force has launched its first-ever cyber range squadron, the 33rd Range Squadron (RGS), officially adding "cyber defenders" to its roster as it prepares to battle digital threats in the space domain. For over two years, space cyber operations training and testing were managed by the 11th Delta Operations Squadron/S9. Now, the 33rd RGS steps up to take the reins, transitioning the mission to a dedicated unit designed to provide a cyber aggressor force.
#USSF #CyberRange

Link: https://www.meritalk.com/articles/space-force-sets-up-first-cyber-range-squadron/

THREAT INTELLIGENCE

GPS interference comes to Bulgaria – Putin's punishment?

Persistent GPS interference detected in and around Sofia, the capital of Bulgaria beginning on 12 December 2025. This interference may be coincidental, or part of efforts by Russia or others to destabilize Bulgaria. **#Jamming #Bulgaria**

Link: https://rntfnd.org/2025/01/02/gps-interference-comes-to-bulgaria-putins-punishment/

Atos Group denies Space Bears' ransomware attack claims

Atos Group has refuted a recent claim by ransomware group Space Bears that the firm's database had been compromised by the threat actors. **#Atos #Ransomware**

Link: https://osintcorp.net/atos-group-denies-space-bears-ransomware-attack-claims/

Japan says China-linked hackers MirrorFace targeted defence and space agencies

Japan on Wednesday linked more than 200 cyberattacks over the past five years targeting the country's national security and high technology data to a Chinese hacking group, MirrorFace, detailing their tactics and calling on government agencies and businesses to reinforce preventive measures. The attacks, which targeted government agencies, businesses, and individuals, aimed to steal sensitive information on defence, space, and advanced technology. **#Japan #MirrorFace**

Link: https://www.scmp.com/news/asia/east-asia/article/3293940/japan-says-china-linked-hackers-mirrorface-targeted-defence-and-space-agencies

RDC-M23 : l'ONU demande au Rwanda de mettre fin aux perturbations des systèmes GPS *(Trad: DRC-M23: the UN asks Rwanda to put an end to disruption of GPS systems)*

In its latest report to the Security Council, the UN Group of Experts on the DRC has called on Rwanda to put an end to the disruption of GPS systems in order to avoid any negative impact on civilian, humanitarian and UN air operations.
#Rwanda #UN

Link: https://www.mediacongo.net/article-actualite-146118_rdc_m23_l_onu_demande_au_rwanda_de_mettre_fin_aux_perturbations_des_systemes_gps.html

Comprehensive list of APT Threat groups, motives, and attack methods

Here is a list of Advanced Persistent Threat (APT) groups around the world, categorized by their country of origin, known aliases, and primary motives (cyberespionage, financial gain, political influence, etc.). APT groups are typically state-sponsored or highly organized cybercriminal groups. **#APT #TTPs**

Link: https://www.socinvestigation.com/comprehensive-list-of-apt-threat-groups-motives-and-attack-methods/

THREAT INTELLIGENCE

Russia's Starlink satellite killer

The *Economic Times* reported: "Russia has developed a new sophisticated monitoring system to detect and neutralise signals from SpaceX's Starlink satellites, called Kalinka. This new system often referred to as the 'Starlink killer' is most likely to be Elon Musk's biggest headache when it comes to establishing the Starlink system worldwide. Starlink, operated by Elon Musk's SpaceX, has been a key communication tool for Ukraine's military since the escalation of Russia's offensive in February 2022." **#Russia #Kalinka**

Link: https://constantinereport.com/russias-starlink-satellite-killer/

The United States risks starting an "electronic war" with China after the disclosure of a network of anti-satellite jammers, writes SCMP

The United States risks starting an "electronic war" with China after the disclosure of a network of anti-satellite jammers, writes SCMP. The US Space Force has revealed its plan to deploy jammers designed to disrupt satellite signals in the Indo-Pacific region. Analysts believe that this step could lead to the start of an "electronic war" with China when Donald Trump takes office as president. **#EW #USA**

Link: https://news-pravda.com/world/2025/01/11/970164.html

TECHNOLOGY

Sandboxaq publishes scientific and technical milestones for magnetic anomaly-based navigation

SandboxAQ and its MagNav partners, including the USAF, Acubed (a subsidiary of Airbus) and Boeing, have been at the forefront of scientific and engineering advancements required to commercialize the underlying quantum sensing and AI technologies that enable accurate, real-time navigation without reliance on Global Positioning Systems (GPS). **#GPS #AI**

Link: https://themalaysianreserve.com/2025/01/03/sandboxaq-publishes-scientific-and-technical-milestones-for-magnetic-anomaly-based-navigation/

UK top secret lab develops 'groundbreaking' quantum clock for military use

Developed at the Defence Science and Technology Laboratory (DSTL), the quantum clock has been dubbed a leap forward in improving intelligence, surveillance and reconnaissance by decreasing the reliance on GPS technology, which can be disrupted and blocked by adversaries. **#Quantum #GPS**

Link: https://www.ndtv.com/world-news/uk-top-secret-lab-develops-groundbreaking-atomic-clock-using-quantum-technology-7393930#publisher=newsstand

GNSS module robust against RF interference

This GNSS Module is built on the F10 dual-band GNSS technology using L1/L5 band signals, which provide solid meter-level position accuracy in urban environments. The module offers high robustness against RF interference from co-located cellular modems. **#GNSS #RF**

Link: https://www.electronicspecifier.com/products/communications/gnss-module-robust-against-rf-interference

Space Force eyes new jam-resistant tactical SATCOM options

Two competing prototype payloads, developed by Northrop Grumman and Boeing and set to launch in 2025, aim to open a new era of secure, jam-resistant tactical communications. Northrop has finished assembly and testing of its payload for the Protected Tactical SATCOM-Prototype (PTS-P) program and is now working on integrating the system onto one of its ESPAStar buses, the company said Jan. 6. Boeing is in the advanced stages of integrating its PTS-P payload with its new Wideband Global SATCOM satellite, WGS-11. **#JammingResistance #SATCOM**

Link: https://www.airandspaceforces.com/space-force-prototypes-jam-resistant-comms/

Google's Willow Quantum Chip and its potential threat to current encryption standards

Google's recent announcement of their Willow quantum processor marks a significant advancement in quantum computing technology while raising questions about the security and sustainability of current encryption methods. As quantum computers grow more powerful, cybersecurity experts grow increasingly concerned about their potential to break widely used encryption standards that protect sensitive data worldwide. **#Willow #Google**

Link: https://levelblue.com/blogs/security-essentials/googles-willow-quantum-chip-and-its-potential-threat-to-current-encryption-standards

Small satellite architectures get new boosts from SDA, NRO

The Pentagon's efforts to launch and connect hundreds of satellites in orbit got two separate boosts Jan. 9, courtesy of the Space Development Agency and National Reconnaissance Office. First came a major milestone for SDA's low-Earth orbit constellation, called the Proliferated Warfighter Space Architecture. Then, the National Reconnaissance Office successfully launched its seventh batch of satellites for a new proliferated constellation. The launch took place late Jan. 9 at Vandenberg Space Force Base, Calif., with a SpaceX Falcon 9 rocket. **#SmallSats #USA**

Link: https://www.airandspaceforces.com/sda-nro-small-satellite-architectures/

MARKET & COMPETITION

Four companies win NASA near space network contracts

NASA has selected four companies to expand its Near Space Network's commercial direct-to-Earth capabilities services. NASA says this is a mission-critical communication capability that allows spacecraft to transmit data directly to ground stations on Earth. **#NASA #Contracts**

Link: https://spaceanddefense.io/four-companies-win-nasa-near-space-network-contracts/

MTSI awarded $640m Digital Bloodhound Program

Space Systems Command (SSC), a subordinate unit of the United States Space Force (USSF), selected Modern Technology Solutions, Inc. (MTSI) to develop and deliver Defensive Cyber Operations for Space (DCO-S) capabilities across the USSF. "The Digital Bloodhound award selection is a significant step forward for MTSI in providing engineering, test, and sustainment leadership and best-value solutions in the space domain in support of the warfighter," said Kevin Robinson, MTSI President and CEO. **#MTSI #SSC**

Link: https://www.mtsi-va.com/mtsi-awarded-640m-digital-bloodhound-program/

Germany, Italy, and the UK slash ESA contributions by €430m

The European Space Agency's 2025 budget has dropped below its 2024 level after Germany, Italy, and the United Kingdom collectively cut their contributions by €430m. During his annual press briefing on 9 January, ESA Director General Josef Aschbacher revealed that the ESA budget for 2025 would be €7.68bn, down from €7.79bn in 2024. The reduction in the agency's budget could have been far worse, as all of the 'big four' countries, apart from France, significantly reduced their contributions. **#ESA #Budget**

Link: https://europeanspaceflight.com/germany-italy-and-the-uk-slash-esa-contributions-by-e430m/

Musk è pronto ad aiutare l'Italia: la cybersecurity diventa campo di battaglia *(Trad: Musk is ready to help Italy: cybersecurity becomes a battlefield)*

It is clear that cybersecurity and the efficiency of encrypted telecommunications are among the priorities of the Italian security systems, and so far the European project of a satellite network, to which the left is looking, has no guarantee of time and efficiency and the cost should be around 10bn, as if we were creating a completely autonomous and very Italian network. **#Starlink #Italy**

Link: https://www.ilriformista.it/musk-e-pronto-ad-aiutare-litalia-la-cybersecurity-diventa-campo-di-battaglia-451805/

ReOrbit and Ananth Technologies enter into strategic agreement on GEO communications satellites

ReOrbit, a leading provider of software-enabled satellites for secure communications, announced the signing of a Memorandum of Understanding (MoU) with Ananth Technologies, a leading aerospace and defence manufacturer in India. This collaboration aims to explore opportunities in designing and developing GEO communications satellites.

#MoU #ReOrbit

Link: https://news.cision.com/reorbit/r/reorbit-and-ananth-technologies-enter-into-strategic-agreement-on-geo-communications-satellites,c4088420

L3Harris Technologies to design resilient GPS satellite concepts for US Space Force

L3Harris Technologies has secured a contract from the US Space Force's Space Systems Command to develop innovative concepts for the Resilient Global Positioning System (R-GPS) programme. The initiative, currently in its initial phase, aims to enhance the resilience of GPS infrastructure through the integration of cost-effective small satellites. **#L3Harris #USSF**

Link: https://defence-industry.eu/l3harris-technologies-to-design-resilient-gps-satellite-concepts-for-u-s-space-force/

Hexagon has agreed to acquire Septentrio NV

Hexagon has agreed to acquire Septentrio NV, a market leader and OEM provider of Global Navigation Satellite System (GNSS) technologies, to drive innovation and expand the Resilient Assured Positioning market. This will ensure greater accessibility to high-accuracy and high-performance positioning technology with low SWaP (Size, Weight and Power) characteristics. The acquisition aims to accelerate the adoption of autonomous systems in existing markets and address the needs of emerging high growth segments like robotics, UAVs, autonomy and other mission-critical applications.

#Hexagon #GNSS

Link: https://www.eenewseurope.com/en/hexagon-acquires-septentrio-to-transform-the-positioning-industry/

Space Force awards BlackSky contracts for TacSRT missions

BlackSky Technology has won multiple rapid procurement contracts for analytics services supporting the US Space Force's tactical surveillance, reconnaissance and tracking, or TacSRT, missions. **#BlackSky #TacSRT**

Link: https://executivegov.com/2025/01/space-force-awards-blacksky-contracts-tacsrt-missions/

MARKET & COMPETITION

HENSOLDT to support DLR on quantum radar optimization for defense applications

HENSOLDT, in collaboration with the German Aerospace Center (DLR) and Tensor AI Solutions GmbH, is working on the QUA-SAR research project under the DLR Quantum Computing Initiative to optimize radar remote sensing scenarios using quantum computing. The project, funded by Germany's Federal Ministry for Economic Affairs and Climate Protection, addresses the challenge of distributing tasks in multi-platform, multi-sensor radar systems in highly dynamic environments. **#DLR #HENSOLDT**

Link: https://thequantuminsider.com/2025/01/10/hensoldt-to-support-dlr-on-quantum-radar-optimization-for-defense-applications/

REGULATION

DoD, GSA, NASA unite to boost cybersecurity workforce standards in FAR alignment with EO 13870

The US Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA) are working to amend the Federal Acquisition Regulation (FAR) to incorporate the NICE Workforce Framework for Cybersecurity (NICE Framework), National Institute of Standards and Technology (NIST) Special Publication 800-181 and additional tools. **#FAR #NICEFramework**

Link: https://industrialcyber.co/training-development/dod-gsa-nasa-unite-to-boost-cybersecurity-workforce-standards-in-far-alignment-with-eo-13870/

TRAINING & EDUCATION

Scotland's position to lead cyber and space

Sharon Lemac-Vincere is an academic that focuses her research on the intersection of space and cyber. She has released a report on space and cybersecurity which outlines how Scotland can lead the way in both industries.

#Podcast #SpaceCybersecurity

Link: https://space.n2k.com/podcasts/t-minus/ds78

Hacking space: cyber-securing the vulnerable space enterprise ecosystem

The space enterprise ecosystem is facing cybersecurity threats growing in both size and scope. As our industries and government become increasingly dependent on space as a mission-critical element of our communication and surveillance efforts, we need to prioritize the cybersecurity of the entire ecosystem. **#Awareness #Threat**

Link: https://www.cyberstrikebrief.com/security-strategies/hacking-space-cyber-securing-the-vulnerable-space-enterprise-ecosystem

Space-Com Expo survey highlights 2025

Space-Comm Expo, the leading UK and international event series for the space industry, has unveiled the latest results from its annual survey revealing the biggest trends and challenges for 2025. The survey reveals key insights for one of the world's most dynamic fast growth industries that underpins global economies through satellite communications and connectivity; exploring future growth, technology, innovation, government collaboration, funding, skills and regulation. **#2025Trends #SpaceCommExpo**

Link: https://memuknews.com/inmotion/space/space-com-expo-survey-highlights-2025/

Cybersecurity Specialist IRES - SSFB

The Schriever Space Force Base, Colorado Springs, is looking for a cybersecurity specialist. The Cybersecurity Specialist supports the Missile Defense Agency (MDA) on the Integrated Research and Development for Enterprise Solutions (IRES) contract. Take your shot! **#SSFB #JobApplication**

Link: https://www.amentumcareers.com/jobs/cybersecurity-specialist-ires-ssfb-colorado-springs-colorado-united-states-59881063-e16e-435b-a464-126ad703a041

Hacking space systems: inside TEMPEST with Tim Fowler

In this episode, host Timothy De Block sits down with Tim Fowler, the creator of Tempest, a hands-on educational project focused on space cybersecurity. Tim shares the story behind the development of Tempest, a 1U CubeSat designed for teaching and exploring cybersecurity in space systems. With insights from his background in space cyber, Tim explains how Tempest offers a unique, vulnerable, and modular platform for learning, hacking, and improving space security. **#Podcast #TEMPEST**

Link: https://www.exploresec.com/eis/2024/1/2/shownotes-template-y3ecp-l5yfp

TRAINING & EDUCATION

Stay tuned for the JammerTest Webinar!

We're excited to welcome Ingrid Dahl Skarstein from TESTNOR, representing the Norwegian Jammertest collaboration, as our featured speaker! Ingrid will present an in-depth overview of the Jammertest project, providing critical insights into its objectives and methodology. Whether you're involved in testing, GNSS security, or innovation, this session is a valuable opportunity to learn directly from a leading expert. Register now! **#Jammertest #GNSS**

Link: https://www.linkedin.com/posts/septentrio_jammertest-webinar-testnor-activity-7281941363292553217--AsE/

Aerospace cybersecurity wiki

To contribute to the emerging aerospace cybersecurity field, this young autodidact created a wiki that compiles knowledge with foundations, information, references, and materials from its aerospace cybersecurity research. The repository is available on GitHub, and you can find the link below. This repository is the first in a series of materials on aerospace cybersecurity that will be published so that stay tuned. **#Wiki #CourseMaterials**

Link: https://www.linkedin.com/posts/romel-marin-cordoba-812489113_over-the-past-three-years-i-have-been-studying-activity-7283271212552577024-eCOA/

Membre de la faculté d'Embry-Riddle récompensé pour sa recherche novatrice en cybersécurité aéronautique *(Trad: Embry-Riddle faculty member awarded for innovative research in aviation cybersecurity)*

For his outstanding contributions to aviation cybersecurity, Dr. Krishna Sampigethaya of Embry-Riddle Aeronautical University has been named by the American Institute of Aeronautics and Astronautics (AIAA) as the recipient of the AIAA 2025 Information Systems Award. **#AIAA #EmbryRiddle**

Link: https://lesnews.ca/tech/cybersecurite/membre-de-la-faculte-dembry-riddle-recompense-pour-sa-recherche-novatrice-en-cybersecurite-aeronautique/

ESA's budget cuts for 2025.

Listen to the latest T-minus space daily podcast, where several topics are tackled: The European Space Agency held its annual press briefing to deliver updates to their 2025 plans and provide an outlook on the agency's annual budget. The US Space Force has selected Modern Technology Solutions Inc. (MTSI) for a $640m contract for cybersecurity defense. NASA has selected Rocket Lab to provide Neutron launch services to the agency through Rocket Lab's existing Venture-Class Acquisition of Dedicated and Rideshare (VADR) contract, and more. **#Podcast #TMinus**

Link: https://www.youtube.com/watch?v=PJsN1maKxrQ

GNSS/GPS spoofing and jamming identification using machine learning and deep learning

The increasing reliance on Global Navigation Satellite Systems (GNSS), particularly the Global Positioning System (GPS), underscores the urgent need to safeguard these technologies against malicious threats such as spoofing and jamming. This paper addresses both spoofing and jamming by tackling real-world challenges through machine learning, deep learning, and computer vision techniques. **#ResearchPaper #SignalThreats**

Link:
https://www.researchgate.net/publication/387767573_GNSSGPS_Spoofing_and_Jamming_Identification_Using_Machine_Learning_and_Deep_Learning