NOVEMBER 2024

Space Cybersecurity Monthly Watch

Source: European Space Agency - Artist's view of a Galileo satellite

Monthly RISC Score & Highlights
Weekly Observations
Expert Analysis
Monthly Articles

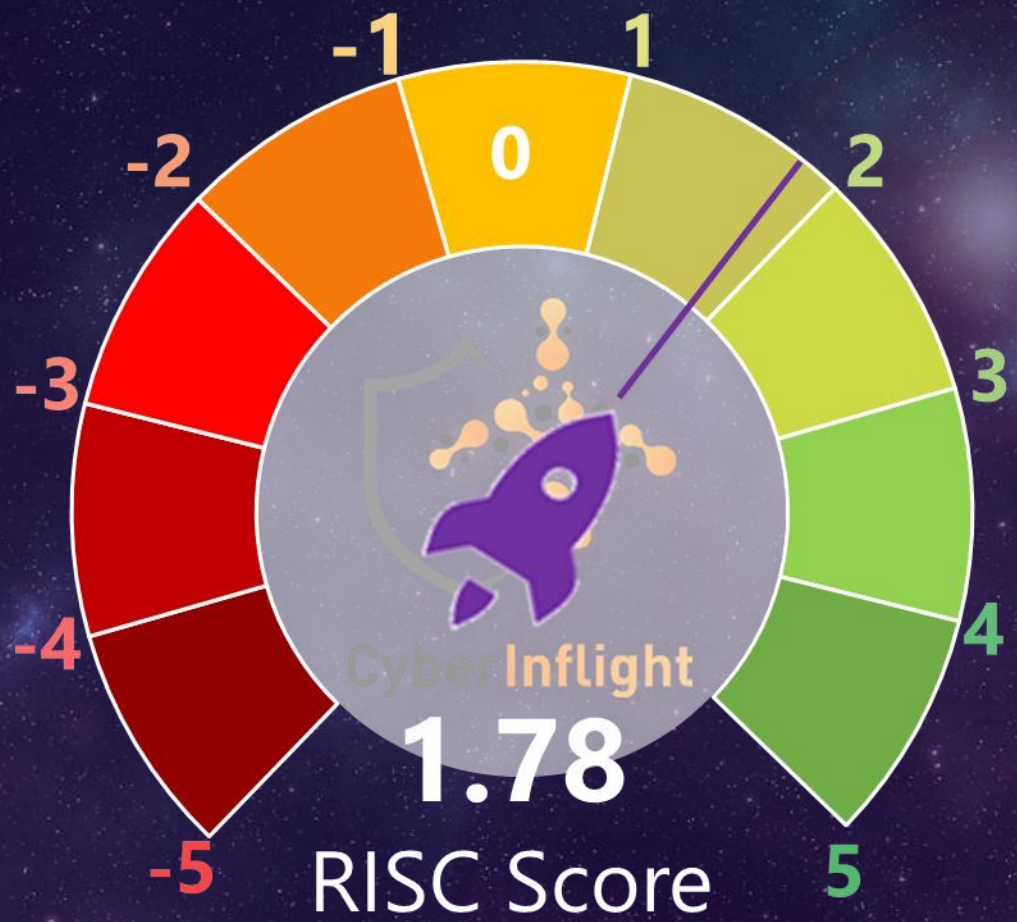
CyberInflight

NOVEMBER 2024 RISC Score

The **Resilience Index for Space Cybersecurity (RISC) Score** is a unique assessment of the space industry. It is an **indicator that provides an overview and score of the space cybersecurity resilience** for the week or month.

To perform the calculation of the final weighted average, a score from a range of -7 to 5 is assigned to each news category based on the importance of the news identified.

A weight is then assigned to each category: Market Intelligence (4), Threat Intelligence (5), Technology (2), Geopolitics (3), Regulation (3), Education & Training (1). We can see that the threat and market intelligence news have a greater impact on the score because CyberInflight has assigned them greater importance to space cybersecurity resilience.



The RISC Score was 1,9 in October, which decreased in November (0,12 points decreased). The score can fluctuate for different reasons, such as geopolitical tensions, technological advancements, and rising cybersecurity threats.

Monthly Highlights - November 2024

Geopolitically, **reinforcing priorities and cooperation has been a defining trend this month**. EU authorities are outlining priorities for the space domain, such as competitiveness and security. In the meantime, the United Kingdom is reinforcing its cooperation with the US Space Force and the Space ISAC. Moreover, the Indian military is developing its cybersecurity culture regarding space Intelligence, Surveillance, and Reconnaissance (ISR) capabilities.

Global satellite cyber protection and jamming were two of the most critical trends identified this month. During the CyberSat event, the National Reconnaissance Office (NRO) stated its will to reinforce the cyber protection of its satellites. Also, as the market grows, **many technologies related to GNSS resilience are being developed**, such as Safran's new Vision navigation system, the new generation of the GPS ground segment, and the development of more resilient SATCOM technologies in the US.

In the meantime, the US Space Force continues to develop the Meadowlands program. It is part of a new concept in electronic warfare known as **SEWOL (Space Electronic Warfare Operating Location)**, which emphasizes coordinating **different electronic warfare systems from the cloud**.

Another major trend is **the massive introduction of AI technologies within the space industry.** For instance, Thales is developing **AI-embedded technologies.**

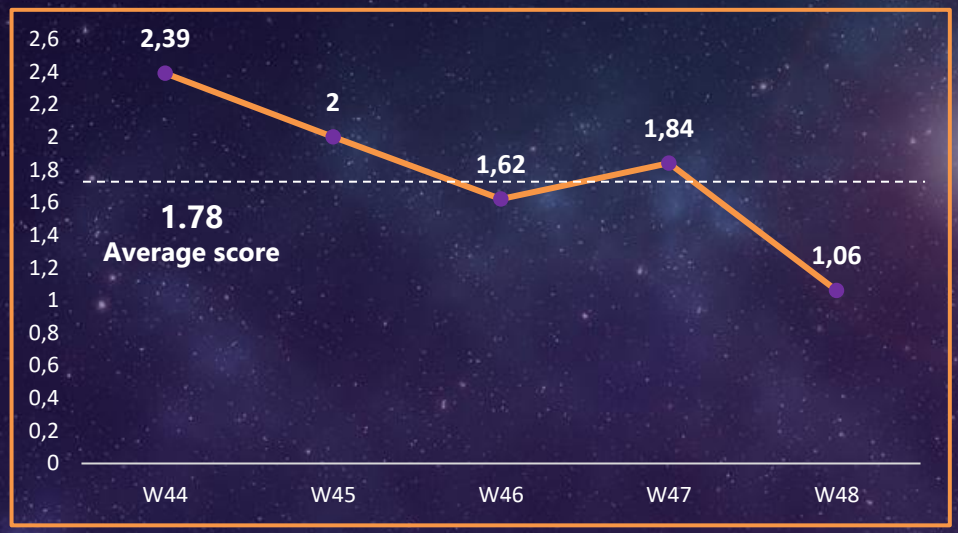
Cyberthreats have remained a persistent concern, with high-profile incidents and emerging trends shaping the threat landscape. In parallel to sabotage action in the Baltic Sea, a ransomware group called Medusa Locker targeted an Estonian telecommunication company. Also, various data leaks and thefts within high-profile industries generated uncertainties. Parallelly, jamming from North Korea is becoming more common. Thus, the **Korean peninsula joins the geographical areas frequently subject to GNSS interference**. This represents a shift as those areas were primarily in Eastern Europe and the Middle East. Last but not least, during an interview with the Commander of the French Space Force, General Philippe Adam, **several aspects of the space threat landscape were highlighted**. Among them were cyber and electronic warfare threats but also offensive space operations.

Multiple regulatory actions have also been initiated this month. In the EU, for instance, there is a will to assess the cybersecurity results of NIS implementation to set up the right metrics for the incoming NIS 2.
Meanwhile, the Vietnam Authority of Information Security (AIS) has signed a memorandum of understanding (MoU) with the Cybersecurity and Infrastructure Security Agency (CISA) under the US Department of Homeland Security (DHS). This MoU establishes a partnership focused on ensuring network security and strengthening the comprehensive strategic relationship between Vietnam and the United States. **These new guidelines emphasize the importance of resilience in interconnected systems critical to national infrastructure**.

Weekly Observations

W44
RISC Score: 2.39

Safran's new Vision navigation system has achieved a significant breakthrough by developing a jam-proof technology that promises enhanced navigation reliability. This innovation is particularly crucial for military and aerospace applications. The system's robust design ensures it can withstand jamming attempts, providing accurate and uninterrupted navigation data.



W45
RISC Score: 2.00

The UK Space Command (UKSC) and the US Space Force (USSF) are strengthening ties to enhance defense capabilities in space, targeting potential adversarial threats. This partnership covers collaborative activities, from monitoring space activities to potential joint missions, positioning both nations as leaders in space.

W46
RISC Score: 1.62

Vietnam's Authority of Information Security is collaborating with the US Cybersecurity and Infrastructure Security Agency (CISA) to enhance critical infrastructure protection. The partnership aims to strengthen cybersecurity resilience through knowledge sharing, training, and joint response strategies. Vietnam, facing rising cyberattacks on essential services, views this collaboration as pivotal in improving its cyber defenses.

W47
RISC Score: 1.84

In a lengthy interview with La Tribune, Space Commander General Philippe Adam analyzes the state of the threat in space and how France is responding, despite relatively limited resources. Considered by the United States as a leading nation in military space, France has been invited to join the permanent American operation Olympic Defender. This alliance is increasingly confronted with the militarization of space and the omnipresent threats from problematic nations such as Russia, China and Iran.

W48
RISC Score: 1.06

US Space Force is reportedly advancing its "Meadowlands" project to jam adversarial satellite signals as a countermeasure against potential threats. This jamming technology could disrupt enemy satellites, preventing adversaries from leveraging space-based communication or intelligence capabilities during conflict. Focused primarily on countering threats from nations like Russia and China, Meadowlands highlights the strategic importance of satellite jamming in modern defense, emphasizing the U.S. aim to maintain space superiority.

W44: October 29 – November 4, 2024
W45: November 5 – 11, 2024
W46: November 12 – 18, 2024
W47: November 19 – 25, 2024
W48: November 26 – December 2, 2024

Expert Analysis 1/2

At CYBERWARCON 2024, Microsoft Threat Intelligence unveiled a report that looked closely at North Korean and Chinese nation-states' cyber actors. In the report, it is stated that **Ruby Sleet, a North Korean group, has conducted supply chain attacks against the defense and aerospace sectors**. For instance, in December 2023, they replaced legitimate software with backdoored versions targeting South Korean defense contractors. Such operations are believed to **support North Korea's missile research**. Parallelly, at the end of the month, in South Korea, 5 key figures from a firm (mid-size player) active in the satellite communications sector since 2017 were arrested for having complied with the request of an overseas client that asked the supplier to provide them with tools to launch retaliatory DDoS attacks. Accepting the request, **the South Korean firm voluntarily manufactured and shipped nearly 98,000 satellite receivers overseas that bore malicious software between January 2019 and September 2024**. Those two examples highlight the **need for supply and value chain securing in the aerospace sector**.

The expansion of supply and value chains, as well as their growing digitization, increase the attack surface and the associated cyber risks.

As explained in a recently published paper from RMIT University Melbourne, Australia, **the growing complexity of space assets, reliance on Commercial-Off-The-Shelf (COTS) components, and third-party dependence**,

> The expansion of supply and value chains, as well as their growing digitization, increase the attack surface and the associated cyber risks.

among other things, open opportunities for malicious actors to introduce vulnerabilities into the supply chain, which poses security risks. In addition, as shown in the South Korean malicious software units, insider threats represent another risk that needs to be tackled when securing the supply chain. Indeed, **malicious insiders can introduce vulnerabilities or facilitate cyberattacks on space systems and infrastructure**. The result of all those stakes is a need for knowledge and control of supply and value chains in a **context of national and regional sovereignty**, to which, moreover, dual aspects are very often added (civilian/commercial and military use).

Expert Analysis 2/2

Recently, a few initiatives have been implemented to answer those stakes. In Western Europe, the UK (ADS), German (BDLI), and French (GIFAS) aerospace and defense trade associations have formalized the creation of **Aero Excellence International**, an association designed to improve operational excellence, sustainability, and cybersecurity within the aerospace, defense and space supply chain. The initiative is based on labels (bronze, silver, gold) recognizing suppliers' industrial maturity. More than 100 industrial sites have been involved in the approach in France since January 2024. Moreover, **companies like Airbus and Safran have already begun deploying Aero Excellence assessments in their supply chains in Morocco, the US, China, and India.**

Conferences and events worldwide also panel the issue through multiplied conferences, such as one at the **Cybersecurity Business Convention (CBC) in Toulouse, France**, or one at **CYBERSAT, Reston, Virginia, USA**, both attended by CyberInflight. At CBC, the conference notably discussed the **AirCyber tool (by BoostAerospace).** Meanwhile, the one at CYBERSAT was handled by Jeremy Mucha, the NRO's technical director of national communication systems, who discussed the **lack of supply chain traceability**. He added that stakeholders worldwide must treat space architecture and production like they do their ground architectures and production, where they have full traceability and **integrate cybersecurity principles from the outset.**

Those events highlighted the need for growing collaboration regarding supply and value chain-associated cyberthreats. Indeed, **collaboration seems needed to raise awareness, draft and publish standards and norms, and build new active stakeholders in the field**.

Valentine Crepineau
Market Analyst at CyberInflight

> Companies like Airbus and Safran have already begun deploying Aero Excellence assessments in their supply chains in Morocco, the US, China, and India.

Monthly Watch – Threat Intelligence Articles

Space Force stands up new mission Deltas to oversee SSA, missile tracking

US Space Force has restructured its operations with the launch of new Mission Deltas focused on improving Space Situational Awareness (SSA). These units, designated as Mission Delta 2 and Mission Delta 4, are tasked with monitoring space activity and addressing potential threats. This restructuring underscores the Space Force's commitment to maintaining a clear, real-time picture of the space domain as adversarial activities increase in orbit. **#USSF #SSA**

Link: https://executivegov.com/2024/11/space-force-new-integrated-mission-deltas/

North Korea's GPS jamming threats escalate

North Korea has conducted more than 300 GPS jamming attacks on South Korea over a single month, raising serious concerns about regional security and aviation safety. South Korean officials warn that these disruptions, primarily targeting Seoul's air and maritime traffic, may also impact critical infrastructure. Such GPS jamming incidents are considered aggressive provocations, and South Korea is working to counter these risks while monitoring its neighboring state's activities closely. **#GPSjamming #CriticalInfra**

Link: https://www.theepochtimes.com/world/north-korea-carried-out-300-gps-jamming-attacks-in-a-month-says-seoul-5757569

Ransomware group Medusa Locker allegedly hits a leading cable & satellite company with $700m revenue in Estonia

After months of silence, ransomware group Medusa Locker returns with a major claim. The group is selling over 3TB of sensitive data, including emails, customer info, and audits, allegedly from a leading cable & satellite company with $700m revenue in Estonia. Price: $800k. **#MedusaLocker #Estonia**

Link: https://x.com/ido_cohen2/status/1861524677287715040

Employee data exposed in Maxar Space Systems security breach

Maxar Space Systems, a leading satellite manufacturer in the United States, has revealed a data breach that compromised the personal information of its employees. The incident, which was discovered on October 11, 2024, involved a hacker using a Hong Kong-based IP address to infiltrate the company's network. This breach is a significant concern, given Maxar's reputation as a key player in the American aerospace industry. **#MaxarSpaceSystems #CyberVulnerability**

Link: https://izoologic.com/region/us/employee-data-exposed-in-maxar-space-systems-security-breach/

« Les Russes sont également très actifs ailleurs qu'en Ukraine » (Général Philippe Adam) *(Trad: "The Russians are also very active outside Ukraine" (French General Philippe Adam))*

Space commander General Philippe Adam analyzes the state of the threat in space and how France is responding despite relatively limited resources. Considered by the US as a leading nation in military space, France has been invited to join the permanent American operation Olympic Defender. This alliance is increasingly confronted with the militarization of space and the omnipresent threats from problematic nations such as Russia, China and Iran. **#CDE #France**

Link: https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/satellites-butineurs-nous-constatons-qu-il-y-a-un-peu-de-proliferation-general-philippe-adam-1011602.html

Monthly Watch – Geopolitics articles

New EU space commissioner outlines priorities

Andrius Kubilius formally started his tenure as the European Commissioner for Defence and Space on Dec. 1 after members of the European Parliament confirmed him among a slate of 26 commissioners Nov. 27 for five-year terms. The new European Union commissioner responsible for space says he will focus on improving European competitiveness and security in space, including passage of a long-delayed space law. **#Europe #SpaceStrategy**

Link: https://spacenews.com/new-eu-space-commissioner-outlines-priorities/

India strengthens space cybersecurity for national defense

During a recent talk at the Institute for Defence Studies and Analyses (IDSA), India's Defence Minister emphasized the critical role of space-based technologies in enhancing intelligence, surveillance, and reconnaissance (ISR) capabilities. He also underlined the importance of robust cybersecurity frameworks to safeguard national space assets from evolving cyber threats. The minister called for greater collaboration between defense agencies, ISRO, and private players to innovate and secure India's space infrastructure, vital for communication, defense, and economic resilience. **#India #IDSA**

Link: https://opengovasia.com/2024/11/13/india-leveraging-digital-technologies-for-national-security/

British and American space forces work together

In a recent strategic move, the UK Space Command (UKSC) and the US Space Force (USSF) are strengthening ties to enhance defense capabilities in space, targeting potential adversarial threats. This partnership covers collaborative activities, from monitoring space activities to potential joint missions, positioning both nations as leaders in space. The alliance reflects a shared vision to uphold security amid evolving global tensions. **#USSF #UKSC**

Link: https://ukdefencejournal.org.uk/british-and-american-space-forces-work-together/

Facing growing threats, space industry expands its cyber warding center

The Space Information Sharing and Analysis Center (Space ISAC) is bolstering its cyber threat intelligence operations with an expanded network that includes partnerships with key UK stakeholders. This collaborative effort aims to provide real-time alerts and intelligence-sharing to protect critical space infrastructure in both the US and the UK. As cyber risks to satellites and related assets grow, Space ISAC's enhanced capabilities are expected to improve communication and responsiveness across borders, fostering a cooperative defense approach in the space cybersecurity domain. **#SpaceISAC #UK**

Link: https://www.airandspaceforces.com/facing-growing-threats-space-industry-expands-its-cyber-warning-center/?utm_source=rss&utm_medium=rss&utm_campaign=facing-growing-threats-space-industry-expands-its-cyber-warning-center

Monthly Watch – Market & Competition articles

Space Force awards Raytheon $196.7m for additional work on GPS ground control system

The US Space Force awarded Raytheon a $196.7m contract extension for the Global Positioning System Next Generation Operational Control System (OCX), a critical upgrade to the GPS infrastructure that is years behind schedule. The contract, announced Nov. 27 by Space Systems Command, targets the next software upgrade to be delivered by November 2025. This latest award brings Raytheon's total OCX contract value to nearly $4.5bn since the program's inception in 2010. **#USSF #Raytheon**

Link: https://spacenews.com/space-force-awards-raytheon-196-7-million-for-additional-work-on-gps-ground-control-system/

Thales partenaire du premier projet européen pour une IA souveraine de cyberdéfense embarquée *(Trad: Thales partner of the first European project for a sovereign onboard cyberdefense AI)*

Thales announces the selection of the AIDA (Artificial Intelligence Deployable Agent) project funded by the European Commission under the European Defense Fund (EDF), involving 28 European start-ups, manufacturers and research centers to ensure the development of a sovereign cybersecurity AI agent for embedded defense systems. The aim of this 3.5-year European project is to design an AI with autonomous or semi-autonomous response capability that protects on-board systems, such as on-board computers and electromagnetic warfare systems on combat aircraft, against cyber-attacks of increasing sophistication during high-intensity conflicts. **#Thales #AI**

Link: https://www.globalsecuritymag.fr/thales-partenaire-du-premier-projet-europeen-pour-une-ia-souveraine-de.html

US Space Force explores support for WGS & DSCS Systems

US Space Force (USSF) is exploring follow-on support for its Wideband Global SATCOM (WGS) and Defense Satellite Communications System (DSCS) as part of the COSMOS Project. SpOC Delta 8, tasked with satellite operations, is leading efforts to ensure these vital communication systems remain operational and resilient. The initiative reflects the USSF's commitment to strengthening its SATCOM capabilities to meet the demands of modern military operations and counter emerging threats in the contested space domain.

#USSF #SATCOM

Link: https://www.satellitetoday.com/government-military/2024/11/11/us-space-force-examining-follow-on-support-for-wgs-and-dscs/

EUSPA's new projects achieve big results and set ambitious goal

The European Union Agency for the Space Programme (EUSPA) shared recent successes and laid out ambitious targets under the Horizon Europe initiative. These projects aim to drive innovation in Europe's space sector, with a focus on sustainable technology and market resilience. EUSPA's work exemplifies Europe's commitment to advancing space capabilities. **#EUSPA #HorizonEurope**

Link: https://www.linkedin.com/posts/euspa_big-results-even-bigger-expectations-activity-7259858494567170048-Dnxb?utm_source=share&utm_medium=member_desktop

Monthly Watch – Training & Education articles

Évènement Cyber et Spatial : « Innovation en cybersécurité spatiale : État de l'art et perspectives » ***(Trad: Space cyber event : "Innovation in space cybersecurity: state of the art and perspectives")***

The COMET CYB (by CNES) is organizing an event on 19/12 in Toulouse (at La cité, Montaudran). This COMET CYB event will be an opportunity to take stock of current R&T or research projects at the crossroads of cybersecurity and space, and to explore prospects in this field. **#COMETCYB #CNES**

Link: https://www.linkedin.com/posts/yohann-bauzil_event-cyber-et-spatial-innovation-en-activity-7269084250157584384-mR5p?utm_source=share&utm_medium=member_desktop

SSC Commander garrant talks cyber focus, integrating commercial tech

The US Space Force command leader focusing on buying and operating satellites for the US military, told the CyberSat conference last week that he, like many other government technology leaders, faces challenges recruiting and retaining personnel with the right technical skills, especially in cyber. **#CyberSatSummit #SSC**

Link: https://www.satellitetoday.com/government-military/2024/11/22/ssc-commander-garrant-talks-cyber-focus-integrating-commercial-tech/

India's first-ever space exercise "Antariksha Abhyas" begins

India has launched its first space-focused military exercise, "Antariksha Abhyas," involving ISRO, DRDO, and the Indian Armed Forces. This exercise aims to enhance space situational awareness and operational readiness in defending national assets in orbit. Participants will simulate real-world scenarios, including satellite protection and counter-space operations. The event underscores India's commitment to strengthening its space defense capabilities amid rising global militarization of space. **#SpaceDefense #India**

Link: https://www.indiatoday.in/india/story/military-army-navy-air-force-chief-of-defence-staff-cds-general-anil-chauhan-space-exercie-antariksha-abhyas-2631937-2024-11-12

Trawling hacker forums uncovers crucial information on space cyber attacks

Researchers at ETH Zurich have conducted an extensive study by trawling hacker forums, uncovering critical information about planned and past cyber attacks targeting space infrastructure. This investigation highlights how cybercriminals share techniques, vulnerabilities, and tools specific to space systems on these forums. The insights gathered are invaluable for developing more robust cybersecurity defenses **#SpaceCyberAttack #ResearchPaper**

Link: https://interactive.satellitetoday.com/via/november-2024/trawling-hacker-forums-uncovers-crucial-information-on-space-cyber-attacks

BEREC cybersecurity workshop opens for registration

The Body of European Regulators for Electronic Communications (BEREC), in collaboration with the European Union Agency for Cybersecurity (ENISA), invites participants to an upcoming workshop focused on enhancing network resilience. The event will provide hands-on cybersecurity training and foster cooperation between UK and EU stakeholders in digital security. As cyber threats increase across industries, this workshop represents a critical effort to build stronger defense strategies across national boundaries. **#CyberResilience #ENISA**

Link: https://www.berec.europa.eu/en/news/latest-news/berec-network-resilience-workshop-registration-open

Monthly Watch – Regulation articles

NIS investments 2024

This report aims at providing policy makers with evidence to assess the effectiveness of the existing EU cybersecurity framework specifically through data on how the NIS Directive has influenced cybersecurity investments and overall maturity of organisations in scope. As 2024 is the year of the transposition of NIS 2, this report also intends to capture a pre-implementation snapshot of the relevant metrics for new sectors and entities in scope of NIS 2 to help future assessments of the impact of NIS 2. **#ENISA #NIS**

Link: https://www.enisa.europa.eu/publications/nis-investments-2024

Local representative introduces bill to counter Iranian satellite threats in space

US Rep. Jimmy Panetta, who represents Paso Robles and other areas in California's 19th Congressional District, has introduced a bipartisan bill aimed at enhancing satellite security and countering space threats posed by Iran and its affiliates. The Space Technology and Regional Security Act, known as the STARS Act, would direct the Department of Defense to develop a strategy and establish a data-sharing agreement with Middle Eastern partners to address Iranian space activities. These activities could disrupt satellite communications and GPS navigation systems, officials said. **#Iran #Bill**

Link: https://pasoroblesdailynews.com/panetta-introduces-bill-to-counter-iranian-satellite-threats-in-space/205761/

Vietnam partners with CISA for critical infrastructure protection

Vietnam's Authority of Information Security is collaborating with the US Cybersecurity and Infrastructure Security Agency (CISA) to enhance critical infrastructure protection. The partnership aims to strengthen cybersecurity resilience through knowledge sharing, training, and joint response strategies. Vietnam, facing rising cyberattacks on essential services, views this collaboration as pivotal in improving its national cyber defenses. The agreement also reflects growing global cooperation in addressing shared cyber threats. **#CriticalInfra #CyberResilience**

Link: https://thecyberexpress.com/vietnam-authority-of-information-security-cisa/

NIST SP 800-161r1-upd1 document updates cybersecurity guidelines to tackle supply chain risks

The National Institute of Standards and Technology (NIST) has revised its guidelines for supply chain cybersecurity, addressing current vulnerabilities and risks. The updated guidelines provide organizations with new frameworks to secure their supply chains, particularly in response to increasing cyber-attacks. This regulatory move emphasizes the importance of resilience in interconnected systems critical to national infrastructure. **#NIST #SupplyChainSecurity**

Link: https://industrialcyber.co/threats-attacks/nist-sp-800-161r1-upd1-document-updates-cybersecurity-guidelines-to-tackle-supply-chain-risks/

Monthly Watch – Technology articles

US Space Force develops "Meadowlands" project to jam enemy satellites

US Space Force is reportedly advancing its "Meadowlands" project, designed to jam adversarial satellite signals as a countermeasure against potential threats. This jamming technology could disrupt enemy satellites, preventing adversaries from leveraging space-based communication or intelligence capabilities during conflict. Focused primarily on countering threats from nations like Russia and China, Meadowlands highlights the strategic importance of satellite jamming in modern defense, emphasizing the U.S. aim to maintain space superiority. **#USSF #SatelliteJamming**

Link: https://www.dailymail.co.uk/sciencetech/article-14001079/Secretive-American-weapon-JAMS-satellites.html?ns_mchannel=rss&ns_campaign=1490&ito=1490

NRO looks to bolster satellite cyber protection

The National Reconnaissance Office (NRO) is moving to a zero trust/defense in depth cyber protection schemata for the agency's satellites. "Whereas in the past the government was really the main tenant of air and space, that equation has flipped," Jeremy Mucha, the NRO's technical director of national communication systems, told the CyberSat conference in Reston, Virginia. "For us — the government — we're still grappling with that, to be perfectly honest, and how we manage and secure our systems. This has really caused us to evolve and think about everything as an IT system."

#NRO #CyberSatSummit

Link: https://www.satellitetoday.com/cybersecurity/2024/11/19/nro-looks-to-bolster-satellite-cyber-protection/

Safran launches GSG-8 Gen2 at ION GNSS+, displays XONA PULSAR simulation capabilities

Safran Electronics & Defense made various announcements at ION GNSS+ in Baltimore, including the launch of the GSG-8 Gen2. This simulator is the latest evolution of the company's GSG simulator series, building on the success of the GSG-8, according to the company. The upgraded simulator offers improvements in capabilities, operability and performance, providing a high-end solution for multi-antenna/vehicle and jamming/spoofing scenarios. Safran also announced the availability of Xona Space Systems' PULSAR XL on Skydel simulation software. **#Safran #IONGNSS**

Link: https://insidegnss.com/safran-launches-gsg-8-gen2-at-ion-gnss-displays-xona-pulsar-simulationcapabilities/

Unaffected by jamming, the revolutionary French navigation system VISION delivers on its promises

Safran's new Vision navigation system has achieved a significant breakthrough by developing a jam-proof technology that promises enhanced navigation reliability. This innovation is particularly crucial for military and aerospace applications, where navigation integrity is critical. The system's robust design ensures that it can withstand jamming attempts, providing accurate and uninterrupted navigation data. Safran's achievement is a major step forward in secure navigation technology. **#JamProofNavigation #Safran**

Link: https://indiandefencereview.com/french-vision-navigation-system-jam-proof-breakthrough-delivers-promises/

WiseSat prepares satellite launch for European IoT connectivity

Swiss company WiseSat, part of WiseKey, is set to launch a new generation of satellites designed to support IoT connectivity across Europe. Featuring quantum-resistant cryptographic keys, these satellites will boost Europe's satellite independence and security. The launch aligns with broader European goals of advancing IoT capabilities while prioritizing robust encryption standards**. #WiseSat #IoT**

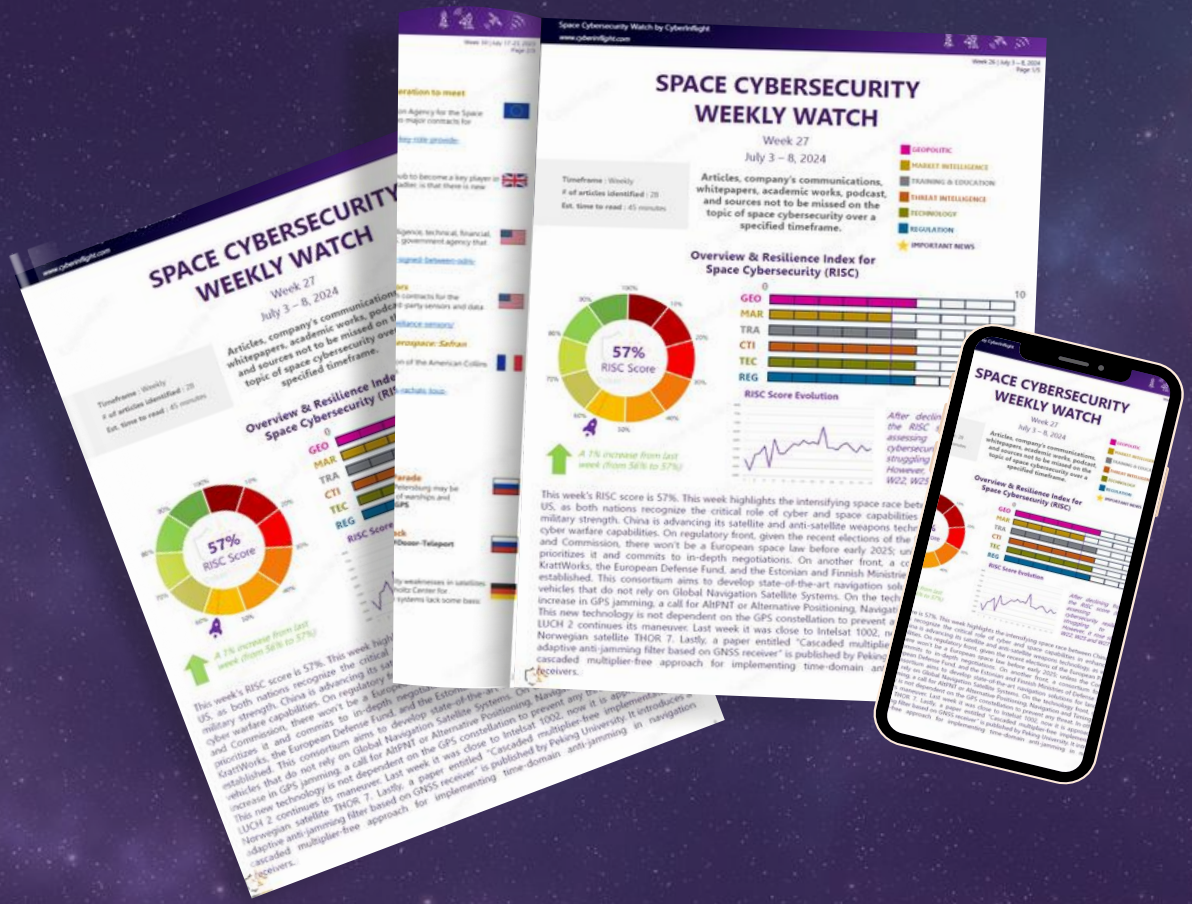
Link: https://news.satnews.com/2024/11/04/wisekey-subsidiary-wisesat-space-prepares-for-a-january-2025-launch-of-next-generation-satellite-supporting-european-satellite-independence-and-iot-connectivity/

CyberInflight is an independent company at the heart of the Space Cybersecurity ecosystem. Discover our unique products.

The only Research Report entirely dedicated to the sector

Get our latest Space Cybersecurity Market Intelligence Report, Edition 2024

Stay updated every week with the dedicated watch on Space Cybersecurity!



Get access to the full version now !

The watch can be customized to your needs, you can order yours!

To register or for more information, reach out to research@cyberinflight.com

CYBERINFLIGHT

SPACE CYBERSECURITY
MARKET INTELLIGENCE

Raise the cybersecurity awareness of the space industry

cyberinflight.com

SPACE ISAC
PROUD MEMBER