OCTOBER 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

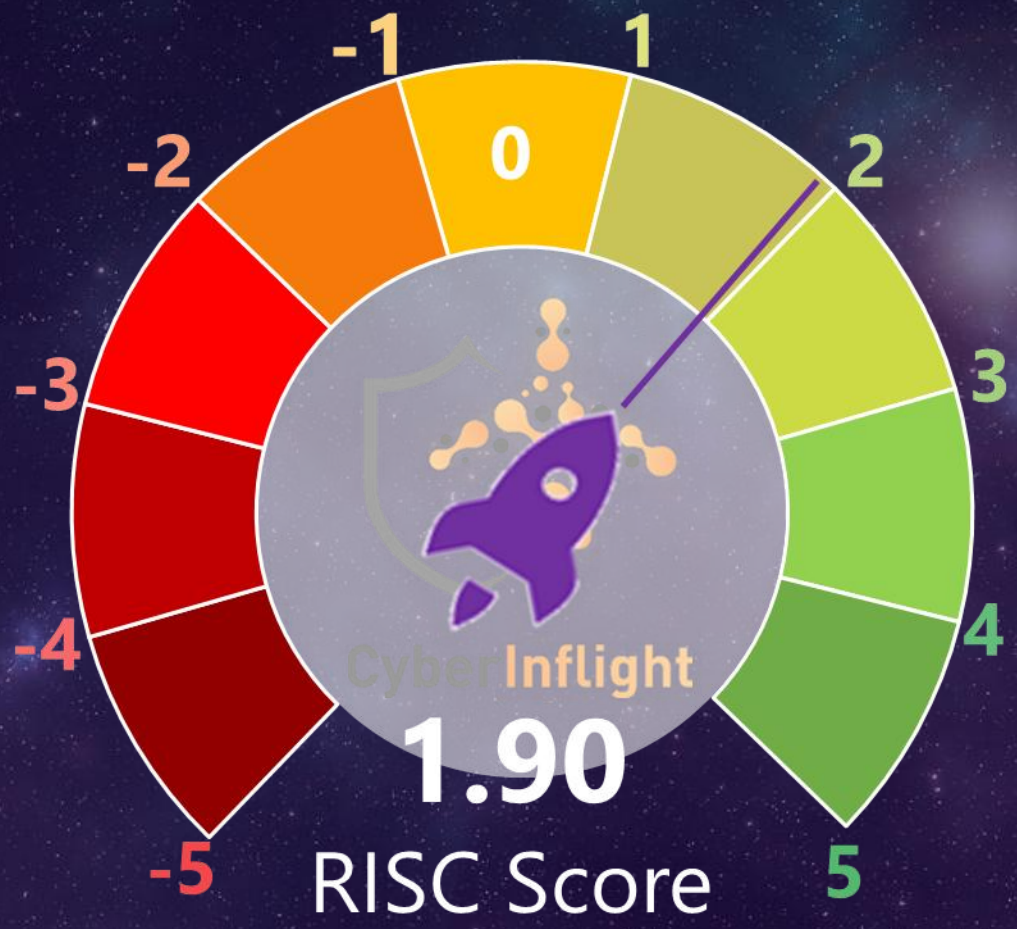
CyberInflight

OCTOBER 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 1.52 in September, which increased in October (0,38 points increased). The score can fluctuate for different reasons, such as geopolitical tensions, technological advancements, and rising cybersecurity threats.

Monthly Highlights - October 2024

Geopolitically, **collaboration has been a defining trend this month**. The Czech Republic and India held their inaugural Space Industry Day, emphasizing innovation and market growth. At the same time, Italy and the US deepened their partnership through plans for joint satellite launches and intelligence-sharing to strengthen space defense capabilities. Meanwhile, the European Space Agency (ESA) focused on securing funding for projects amid speculation of a potential merger between Airbus Defence & Space and Thales Alenia Space, signaling potential shifts in European space industry dynamics. The US and UK also expanded their collaboration through the Space ISAC, creating a robust real-time cyber-threat intelligence sharing framework to safeguard critical space infrastructure.

Quantum and jamming were two of the most critical technology trends identified this month. This focus on quantum, like the discoveries made by Chinese scientists in quantum computing, poses the question of the threat to traditional encryption standards, highlighting the urgency for solutions like NIST's post-quantum cryptography standards. Advanced defense technologies also emerged, including the US Space Force's "Meadowlands" project to jam adversarial satellite signals and Safran's development of a jam-proof navigation system to ensure reliable and secure navigation for military and aerospace applications.

Substantial investments and strategic initiatives have fueled market growth. All Space secured $44m to improve orbital connectivity through its first terminal, while Xage Security entered into a $1.5m contract with the US Navy to implement Zero Trust cybersecurity solutions. In France, the Occitanie region was selected to host a Maison du Quantique, an ambitious project to develop quantum internet via satellites, positioning the region as a leader in this emerging field.

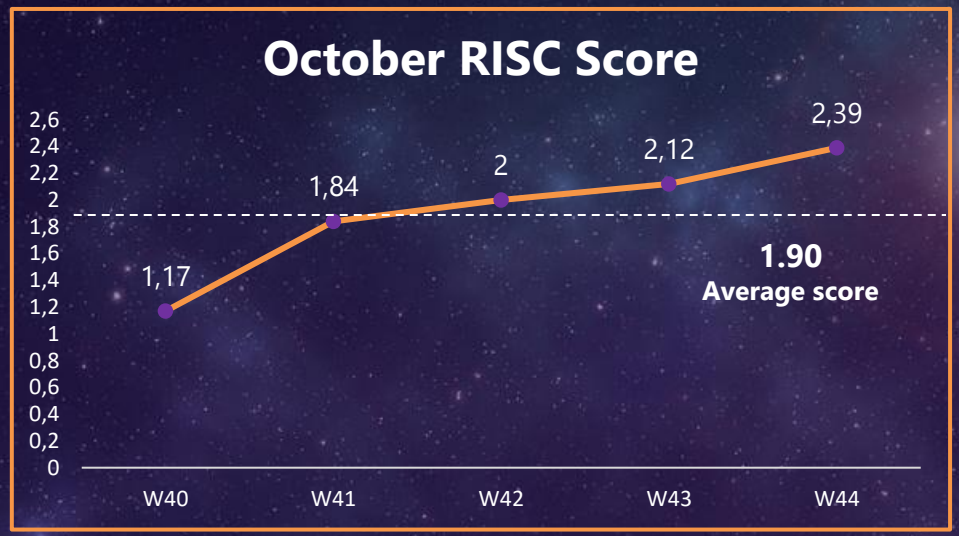
Cyber-threats have remained a persistent concern, with **high-profile incidents and emerging trends shaping the threat landscape**. NASA faced a ransomware attack by Stormous, highlighting vulnerabilities even in well-established agencies, while Ukraine demonstrated advanced cyber warfare capabilities by targeting Russian satellite communications. Simultaneously, the Ukrainian military is exploring the establishment of a dedicated cyber army, reflecting the growing significance of cyber defense in modern conflict. Insights from ETH Zurich's analysis of hacker forums uncovered critical details about planned cyberattacks on space infrastructure, reinforcing the urgency of cybersecurity measures.

On the regulatory front, **significant strides have been made to strengthen resilience across critical infrastructure**. The EU adopted the Cyber Resilience Act and implemented the NIS2 directive, which focuses on addressing vulnerabilities and enhancing cybersecurity coherence across sectors. Japan has also proposed a cybersecurity bill that mandates stricter standards for essential services, reflecting a proactive response to increasing cyber threats.

Weekly Observations

W40
RISC Score: 1.17

NASA has reportedly fallen victim to the Stormous ransomware, highlighting the escalating risks posed by cyber-threats to space agencies. The attack emphasizes the vulnerabilities in NASA's cybersecurity infrastructure, prompting a reassessment of protective measures to safeguard sensitive information and operational integrity.



W41
RISC Score: 1.84

The European Union adopted a new law on cybersecurity for digital products to ensure their safety before market entry. The Cyber Resilience Act addresses gaps, clarifies connections, and enhances coherence in the cybersecurity legislative framework. As the first regulation globally to set security requirements for product market entry, it mandates that from 2027, products with digital components must meet these standards to be available in the EU.

W42
RISC Score: 2.0

The European Union has established a new framework for implementing restrictive measures in response to Russia's ongoing destabilizing activities, particularly concerning hybrid warfare threats. The sanctions framework is designed to address Russia's influence operations and cyberattacks, highlighting the EU's commitment to counteracting hybrid threats and protecting its member states.

W43
RISC Score: 2.12

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 US aim to maintain space superiority.

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, 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.

W40: October 1 – 7, 2024
W41: October 8 – 14, 2024
W42: October 15 – 21, 2024
W43: October 22 – 28, 2024
W44: October 29 – November 4, 2024

Expert Analysis 1/2

At the 75th International Astronautical Congress (IAC), held in Milan from 14 to 18 October, experts in space cybersecurity convened to discuss pressing issues in 2 technical sessions: one on the **Legal and Institutional Frameworks** and the other on **Risks and countermeasures in space cybersecurity.**

The first one centered on the **growing necessity for comprehensive governance and tailored legal frameworks to address the unique cybersecurity challenges in space**. The opening presentation discussed the establishment of cyber operations for outer space and global governance in space cyber-operations, referencing the establishment of cyber commands among spacefaring nations. **France's ANSII, DIRSI, and COMCYBER, Germany's CIR, the UK's NCF, and the US Space Delta were highlighted as examples of expanding defense capabilities in space.**

A presentation on space resilience frameworks highlighted current EU cyber regulations. The presenter advocated for a **EU Space Law, citing that current EU regulations (NIS2, CER) do not fully cover space needs**. This law could unify EU satellite communications, providing a standardized framework across EU markets. Another presenter outlined a first-principle approach to cybersecurity, focusing on simplifying mission security through foundational methods. This approach would prioritize core, simplified cybersecurity measures, potentially through the Space Domain Cybersecurity (SpaDoCs) framework.

> The session stressed the urgent need for space-specific regulations, collaborative governance, and technological advancements to ensure cybersecurity resilience in space operations.

Subsequent presentations emphasized the importance of recognizing space-related cyber interference as a criminal activity and the environmental impacts of cyberattacks on satellites, highlighting the increasing role of artificial intelligence in space, which presents its own regulatory challenges. The **dual-use nature of satellites** sparked discussions on international humanitarian law, particularly regarding the distinction between civilian and military targets. A comprehensive security monitoring across space missions was analyzed, covering everything from ground IT systems to space-specific infrastructures**. The European Space Agency's (ESA) tools, such as AISecMon and SANM, are setting standards in this regard.** Additionally, the interplanetary defense was discussed, focusing on delay-tolerant networks (e.g. LunaNet)

Expert Analysis 2/2

The Risk and Countermeasures in Space Cybersecurity session delved into **innovative solutions for enhancing security across satellite and space communications**.

The session opened with a project on a **secure method for satellite conjunction analysis** using homomorphic encryption, which enables confidential collision probability calculations through a politically neutral server. Another presentation on **cyber insurance** emphasized the challenges in risk assessment due to limited historical data, calling for more transparent data-sharing and regulatory frameworks.

A research focused on **quantum-era cybersecurity** for satellite communications was also presented, 3 missions were highlighted: **SALSAT, RACCOON, and CyBEEsat.** RACCOON, a project on quantum-resilient communications using machine learning and software-defined radio (SDR) for critical infrastructure. This project's OS design offers a minimal update framework and adheres to space-specific standards, such as CCSDS, through a lightweight, rust-based architecture ensuring secure and adaptive data exchanges.

Innovations such as **OPS-SAT's verified secure data link measurements in orbit** and **Game theory applications for multi-spacecraft systems** have proposed solutions to counter stealth attacks by simulating zero-sum scenarios and leveraging Monte Carlo search strategies. **Cyber Range and Digital Twin technologies were also discussed as practical tools for simulating cyber threats** and enhancing resilience efforts.

The session concluded with **the use of AI for detecting cyber intrusions in orbital systems**, indicating growing support for real-time threat detection through AI-enhanced simulation as a part of the **Cyber Space Simulation (CCS) project**.

Pawan Dokhe
Market Analyst at CyberInflight

> The session highlighted the need for advanced encryption, quantum resistant solutions, resilient operating systems, and emerging technologies like AI and digital twins in managing cybersecurity risks for space missions.

Monthly Watch – Threat Intelligence Articles

Stormous ransomware claims NASA as a victim

NASA has reportedly fallen victim to the Stormous ransomware, highlighting the escalating risks posed by cyber threats to space agencies. The attack emphasizes the vulnerabilities in NASA's cybersecurity infrastructure, prompting a reassessment of protective measures to safeguard sensitive information and operational integrity. **#Ransomware #NASA**

Link: https://darkwebinformer.com/stormous-ransomware-claims-nasa-as-a-victim/

War Game: China will attack Taiwan's comms tech, GPS

Like most advanced nations, Taiwan has not widely adopted alternatives to GPS and other satnav. Denying GPS could help bring the nation to its knees. China's terrestrial complement to satnav, eLoran, is very difficult to disrupt and reaches far beyond Taiwan. Even if the US were to disable BeiDou, as envisioned in the war game, China would still have PNT at home and in the theater of conflict. **#PNT #China**

Link: https://rntfnd.org/2024/10/07/war-game-china-will-attack-taiwans-comms-tech-gps-spacenews/

Iranian cyber actors' brute force and credential access activity compromises critical infrastructure organizations

CISA has issued a warning about Iranian cyber actors using brute force and credential access tactics to compromise critical infrastructure in the US. The attackers are focusing on energy, transportation, and healthcare systems, underscoring the urgent need for stronger cybersecurity defenses to mitigate these persistent threats. **#CISA #Iran**

Link: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-290a

Ukraine eyes formation of a new cyber army branch

Amid rising cyber challenges, the Ukrainian military is exploring the creation of a dedicated cyber army branch. This new initiative is part of Ukraine's response to cyber threats posed by regional adversaries and aims to enhance the country's defensive cyber capabilities. If established, this branch would strengthen Ukraine's resilience against cyber warfare, reflecting an increasing global trend toward prioritizing cybersecurity in national defense strategies.

#Ukraine #CyberDefense

Link: https://www.msn.com/en-us/news/world/ukrainian-military-considering-creation-of-new-cyber-army-branch/ar-AA1sRcjd

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/

Monthly Watch – Geopolitics articles

Successful conclusion of the first Czech-Indian Space Industry Day

The first-ever Czech-Indian Space Industry Day focused on strengthening ties between the two nations in the space sector. Optokon Group and ARCON led discussions on market growth, innovation, and the potential for future partnerships. As the global space market evolves, collaborations like these are paving the way for new opportunities in both established and emerging space economies. **#SpaceCollaboration #GlobalMarkets**

Link: https://spacewatchafrica.com/successful-conclusion-of-the-first-czech-indian-space-industry-day/

Italy, US space cooperation plan includes launch, domain awareness

Italy and US are enhancing their collaboration in space with plans that include joint satellite launches and improved domain awareness. The partnership aims to bolster both nations' space defense capabilities while fostering cooperation in emerging technologies and intelligence sharing. This marks a significant step in strengthening transatlantic space ties in an increasingly competitive environment. **#Cooperation #Italy**

Link: https://breakingdefense.com/2024/10/italy-us-space-cooperation-plan-includes-launch-domain-awareness/

ESA's stance on Airbus and Thales Alenia Space merger talks

The European Space Agency (ESA) has stated it will not comment on the ongoing merger discussions between Airbus Defence & Space and Thales Alenia Space, opting to focus on securing funding for existing and new projects. With potential changes in European space industry dynamics, ESA's role in negotiating increased contract down payments is seen as essential for advancing its programs amid an evolving landscape of private partnerships. **#ESA #EU**

Link: https://www.spaceintelreport.com/esa-we-wont-weigh-in-on-merger-talks-beween-airbus-a-proposed-increase-in-contract-downpayments/

Facing growing threats, space industry expands its cyber warning 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

All Space raises $44m for first space terminal launch

All Space has secured $44m in funding to launch its first terminal, aimed at improving orbit connectivity. This terminal is expected to play a pivotal role in enhancing space communication and establishing stronger, more reliable connections in space networks. **#TechInnovation #OrbitConnectivity**

Link: https://www.satellitetoday.com/finance/2024/10/03/all-space-raises-44m-to-launch-its-first-terminal/

Xage Security secures $1.5m contract by US Navy to advance Zero Trust initiatives

Xage Security Government, vendor of Zero Trust access and protection solutions, announced on Wednesday a $1.5 million Sequential Phase II Small Business Innovation Research (SBIR) contract with the United States Navy to prove out Xage's Zero Trust Access and Protection and Federated Identity Management capabilities in support of multiple strategic initiatives. This initiative supports compliance with the US Department of Defense Chief Information Officer (DOD CIO) Zero Trust Target Strategy to enhance the protection of data, systems, and services with a Zero Trust model/architecture by 2027. **#XageSecurity #ZeroTrust**

Link: https://industrialcyber.co/news/xage-security-secures-1-5-million-contract-by-us-navy-to-advance-zero-trust-initiatives/

CYSEC wins European Space Agency contract to protect satellite operations

CYSEC has been awarded a major contract by the European Space Agency (ESA) to protect satellite operations under its General Support Technology Programme (GSTP). The Swiss cybersecurity firm will focus on enhancing the security of satellite communications, addressing the growing need for secure operations in the increasingly competitive space domain. **#CYSEC #ESA**

Link: https://www.cysec.com/gstp/

ESA contracts GMV for CyberCUBE space cybersecurity mission

The European Space Agency (ESA) has selected GMV for the CyberCUBE mission, which aims to tackle cybersecurity threats in space. GMV will work on developing cybersecurity protocols and technologies to protect satellite infrastructure from cyber risks. CyberCUBE will assess vulnerabilities and propose innovative strategies to enhance satellite system resilience, ensuring secure data flow and system integrity in the growing space economy. **#ESA #Cybersecurity**

Link: https://www.spacewar.com/reports/GMV_wins_ESA_contract_for_CyberCUBE_space_cybersecurity_mission_999.html

L'Occitanie, tête de pont de l'internet quantique par satellite *(Trad: Occitanie Region in France leads quantum internet by satellite initiative)*

The Occitanie region in France is spearheading an ambitious project to establish quantum internet via satellite, positioning itself as a leader in this cutting-edge field. This initiative aims to develop a secure, high-speed quantum communication network that leverages satellite technology. By focusing on quantum internet, Occitanie is set to drive significant advancements in cybersecurity and data transmission, ensuring the region remains at the forefront of technological innovation. **#QuantumInternet #Occitanie**

Link: https://toulouse.latribune.fr/entreprises/business/2024-10-28/l-occitanie-tete-de-pont-de-l-internet-quantique-par-satellite-1009661.html

Monthly Watch – Training & Education articles

NASA's orbit cybersecurity training program

A podcast discussing how NASA has implemented an extensive orbit cybersecurity training program aimed at enhancing the agency's preparedness against cyber threats. This initiative focuses on educating personnel about potential vulnerabilities and best practices for maintaining cybersecurity in space operations.

#CybersecurityTraining #SpaceOperations

Link: https://www.buzzsprout.com/2004238/episodes/15820343

How do we ensure the security of space applications ?

In this blog, Dr Basel Halak, Associate Professor of Secure Electronics and Director of the Cyber Security Academy at the University of Southampton writes about the challenge of keeping the sector safe from current and emerging threats.

#Awareness #SpaceApplications

Link: https://www.port.ac.uk/news-events-and-blogs/how-do-we-ensure-the-security-of-space-applications

Cyber resilience limitations in space systems design process: insights from space designers

Designers of space systems are facing increasing challenges in embedding cyber resilience into their processes. Insights from recent studies reveal limitations in current design frameworks that make space assets vulnerable to cyberattacks. The findings suggest a growing need for more robust and adaptable cybersecurity measures to safeguard critical space infrastructure. **#Design #Resilience**

Link: https://www.mdpi.com/2079-8954/12/10/434

ESA's 4S program invests in space system safety training

The European Space Agency's 4S Program is enhancing space safety through targeted training initiatives. Focused on supporting secure satellite operations and protecting European space assets, the program includes simulations and hands on modules to equip engineers and analysts with advanced skills in space system safety. ESA's commitment to workforce development in this field underlines its goal to strengthen Europe's strategic space infrastructure.

#SpaceSafety #ESA

Link: https://www.linkedin.com/posts/laurence-duquerroy-34183040_esa-europeanspaceagency-funding-activity-7252713221487308802-yV1u?utm_source=share&utm_medium=member_ios

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

Monthly Watch – Regulation articles

Will Japan's cybersecurity bill become a reality?

Japan is proposing a new cybersecurity bill aimed at fortifying its critical infrastructure against increasing cyber threats, particularly from state actors. The legislation would empower the government to set mandatory cybersecurity standards and regulations for industries, particularly those managing essential services such as utilities and telecommunications. This regulatory push reflects Japan's growing concern about digital vulnerabilities, especially with upcoming international events that could attract cyber adversaries. If passed, the bill would be a landmark shift in Japan's approach to cybersecurity and infrastructure resilience. **#CyberSecurityBill #CriticalInfra**

Link: https://osintcorp.net/will-japans-cybersecurity-bill-become-a-reality/

EU adopts Cyber Resilience Act, bolsters security requirements of connected devices and infrastructure

The European Union adopted a new law on cybersecurity for digital products to ensure their safety before market entry. The Cyber Resilience Act addresses gaps, clarifies connections, and enhances coherence in the cybersecurity legislative framework. As the first regulation globally to set security requirements for product market entry, it mandates that from 2027, products with digital components must meet these standards to be available in the EU. **#CyberResilienceAct #EU**

Link: https://industrialcyber.co/regulation-standards-and-compliance/eu-adopts-cyber-resilience-act-bolsters-security-requirements-of-connected-devices-and-infrastructure/

CSAC approves draft reports to strengthen national cyber resilience, address critical infrastructure vulnerabilities

The Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Advisory Committee (CSAC) has approved draft reports aimed at strengthening national cyber resilience. These reports address vulnerabilities in critical infrastructure sectors and propose measures to enhance their defense against cyberattacks. The initiative underscores the urgency of protecting essential services from emerging threats in a rapidly evolving cyber landscape. **#CSAC #CriticalInfra**

Link: https://industrialcyber.co/reports/csac-approves-draft-reports-to-strengthen-national-cyber-resilience-address-critical-infrastructure-vulnerabilities/

NIST advances standards for post-quantum cryptography, securing digital future

NIST is pushing forward with developing post-quantum cryptography standards, which are crucial for securing digital data in a future where quantum computing could easily break traditional encryption methods. These standards are designed to ensure long-term cybersecurity resilience and trust in digital systems as quantum technology advances. This milestone is expected to play a critical role in protecting data across government, finance, and other sensitive sectors.
#PostQuantum #NIST

Link: https://decentcybersecurity.eu/nist-advances-post-quantum-cryptography-standards-astrategic-milestone-for-digital-security/

Monthly Watch – Technology articles

BAE Systems unveils RAD510 software for next-gen space missions

BAE Systems has rolled out its RAD510 software development unit, a highly advanced platform tailored for critical space missions. Designed to operate in the harshest space environments, this software will enhance satellite processing power, ensuring operational resilience and the ability to support missions in areas such as planetary defense and space exploration. **#SpaceMissions #Innovation**

Link: https://news.satnews.com/2024/10/06/bae-systems-rad510-software-development-unit-available-to-support-critical-space-missions/

NASA's laser communication breaks distance record

NASA has achieved a groundbreaking milestone by setting a new distance record for laser communications in space through its Deep Space Optical Communications (DSOC) project. This achievement was made possible by successfully transmitting data over a distance of 1.2 million kilometers (about 746,000 miles) from a spacecraft in deep space back to Earth. The DSOC technology significantly enhances data transmission capabilities, allowing for much larger amounts of information to be sent back from deep space missions compared to traditional radio frequency systems.

#NASA #LaserCommunication

Link: https://scienceblog.com/548345/nasas-laser-communication-breaks-distance-record-paving-way-for-future-space-exploration/

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/

Quantum technologies for Air and Space (Part 3 of 3)

In this final installment of the series, Dr. Michal Krelina and Lieutenant Colonel Denis Dubravcik explore the practical military applications of quantum technologies in Intelligence, Surveillance, and Reconnaissance (ISR) and Positioning, Navigation, and Timing (PNT). They discuss cutting-edge quantum imaging systems, sensors such as gravimeters and magnetometers, and how these tools can revolutionize battlefield awareness and navigation in GPS-denied environments. With NATO recently adopting a Quantum Technology Strategy, the authors outline timelines for implementation and the significant operational advantages these advancements promise for the Alliance. **#Quantum #EW**

Link: https://www.japcc.org/articles/quantum-technologies-for-air-and-space-part-3-of-3/

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

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**

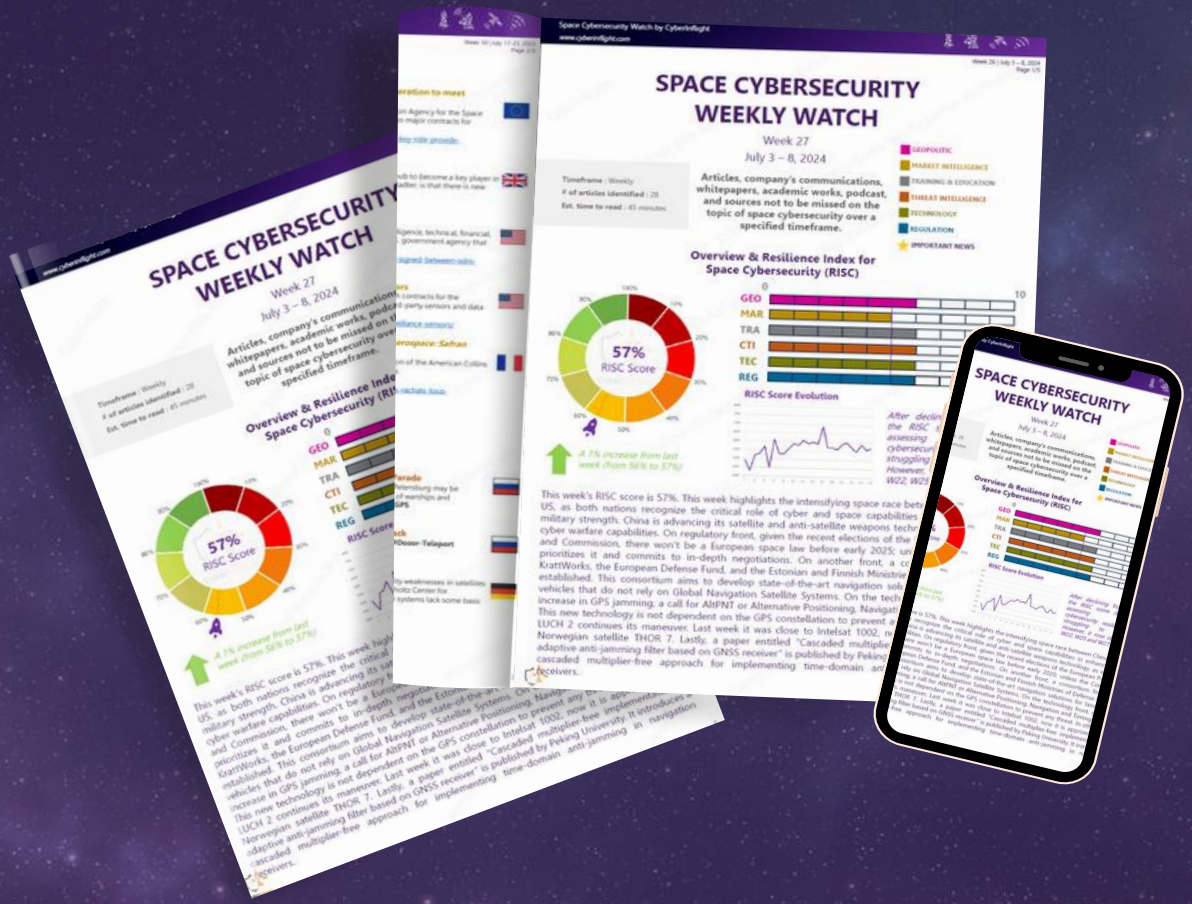
Link: https://indiandefencereview.com/french-vision-navigation-system-jam-proof-breakthrough-delivers-promises/

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