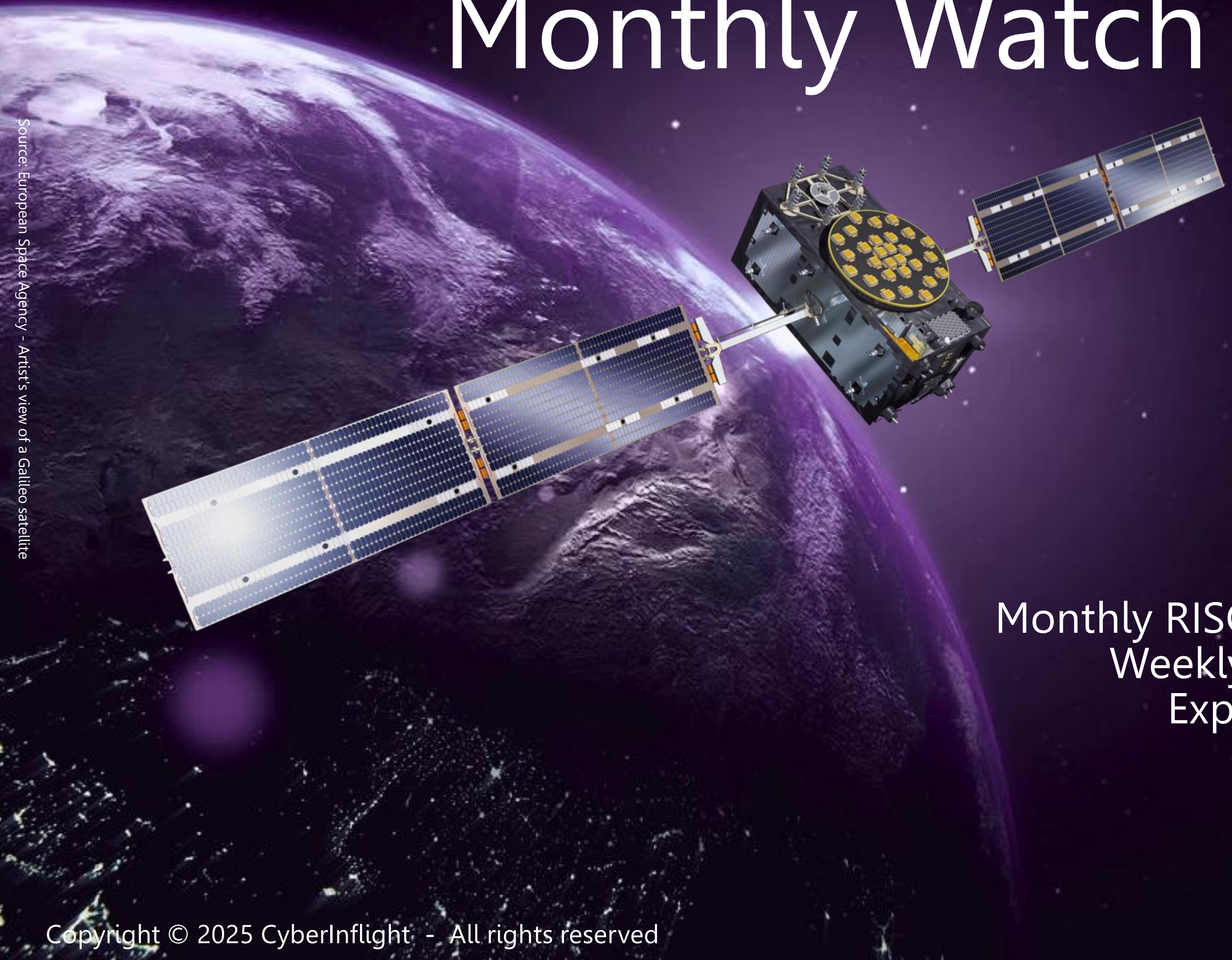
DECEMBER 2024

Space Cybersecurity Monthly Watch



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

Monthly RISC Score & Highlights
Weekly Observations
Expert Analysis

CyberInflight

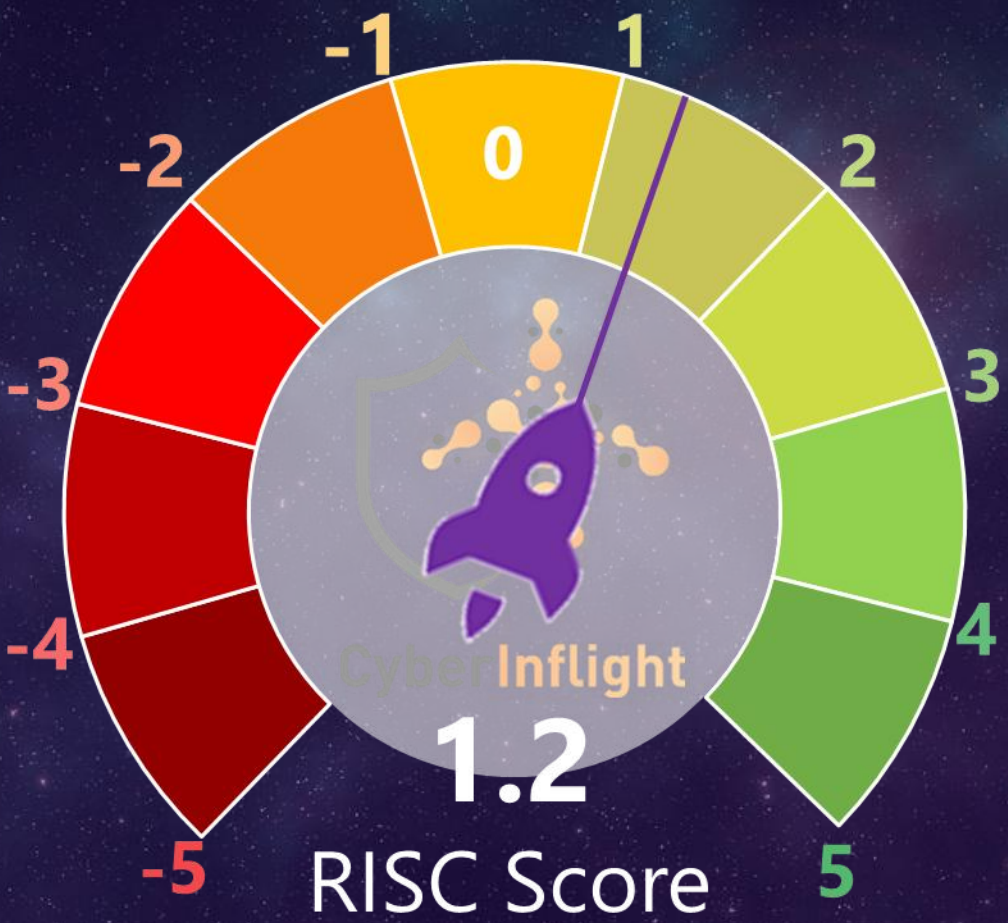
Copyright © 2025 CyberInflight - All rights reserved

DECEMBER 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 1.78 in November, which decreased in December (-0.58 points). The score can fluctuate for different reasons, such as geopolitical tensions, technological advancements, and rising cybersecurity threats.

Monthly Highlights - December 2024

The unstable American political climate shapes this month's news. With Trump taking office in January, US policy remains uncertain, leading to **few regulations worldwide** and **investment in building stronger partnerships and alliances** in the West and other parts of the world. The unstable climate also led to an **increase in cyber-threats and cyberattacks** this month.

Geopolitically**, reinforcing alliances and cooperation has been a defining trend this month**. Anticipating significant changes in the USA and considering their position in space, alliances such as NATO, the Combined Space Operations Initiative (CSpO) comprising Australia, Canada, France, Germany, Italy, Japan, New Zealand, Norway, the UK, and the USA, or the new entente of powers between China, Russia, Iran, and North Korea remain strong. **Defining priorities in cyber, space, and space cybersecurity** is also a main trend for the end of the year. The US Space Force (USSF) is celebrating its fifth anniversary and, to celebrate, gathered at the second annual Spacepower Conference in Orlando. Chief of Space Operations Gen. Chance Saltzman, in a keynote, outlined the service's achievements and challenges that lie ahead.

Also, as the market grows, the Pentagon renewed its technological and strategic ambition for space cybersecurity, notably with the development of **technologies increasing GPS resilience**, such as M-Code, a signal designed to improve anti-jamming and anti-spoofing that is now used for all GPS III space vehicles. Our expert dives into this topic in the Expert Analysis.

Investments in space and cyber technologies are also taking place in developing countries, such as India. Indeed, this month, India is set to join an elite group of countries with quantum satellite capabilities, securing communication networks against hacking and cyberattacks. Moreover, Israel launched an innovation acceleration program for startups in India that will focus on 10 technological areas, including Big Data, Quantum, Edge computing and Advanced Navigation.

Cyberthreats have remained a persistent concern, with high-profile incidents and emerging trends shaping the threat landscape, especially against the USA and India. The hybrid tensions between Russia and NATO persists, notably with strong jamming attacks in the Baltic States accredited to Russia.

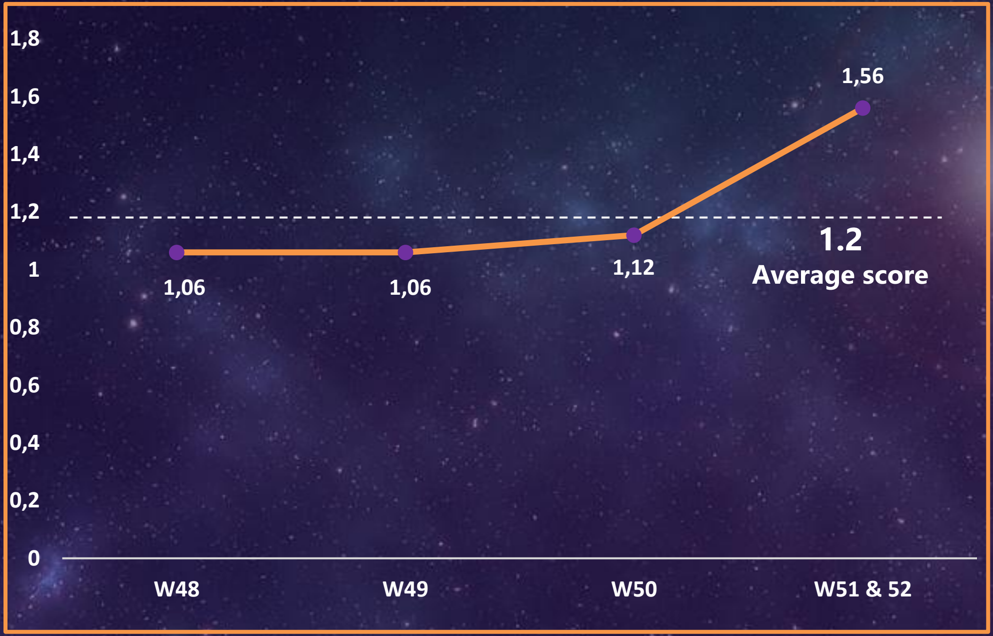
On the regulation side, only four European members met the deadline to transpose the **NIS2 Directive in their national law.** "Infringement procedures" against 23 states have been opened by the European Commission.

Last but not least, **Toulouse (France) and its surrounding areas appear to be a dynamic place when it comes to space cybersecurity**, with a few interesting events being held, such as the COMETCYB, organized by the French Space Agency (CNES). The CyberInflight team was proud to take part in this event.

Weekly Observations

W48
RISC Score: 1.06

The COMETCYB (by CNES) is organizing an event on 19/12 in Toulouse (at La Cité, Montaudran). This COMETCYB 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.



W49
RISC Score: 1.06

Since the mid-1950s, the number of space actors has proliferated, with more countries now actively participating in space activities. This interest highlights the critical role of satellites and space technologies in both the military and commercial sectors. Nations are investing heavily in advanced space capabilities to strengthen military power and protect strategic assets, making space a contested and competitive domain.

W50
RISC Score: 1.12

India is set to join an elite group of countries with quantum satellite capabilities, securing communication networks against hacking and cyberattacks. The satellite will play a key role in the larger quantum communications network under the National Quantum Mission (NQM).

W52
RISC Score: 1.56

Russia has reportedly developed an advanced system designed to detect and disrupt signals from Elon Musk-owned SpaceX's Starlink satellites, which have played a key role in Ukraine's war strategy. The system, named Kalinka, is being hailed as a 'Starlink killer' and could significantly impact Ukraine's reliance on Starlink technology.

W51
RISC Score: 1.56

The European Commission takes next step to deploy the IRIS² secure satellite system. The Commission has signed the concession contract for the IRIS², a multi-orbital constellation of 290 satellite, with the SpaceRISE consortium. This partnership will develop, deploy, and operate the European Union's new system. It is a significant step towards Europe's sovereignty and secure connectivity.

W48: November 26 – December 2, 2024
W49: December 3 – 9, 2024
W50: December 10 – 16, 2024
W51: December 17 – 23, 2024
W52: December 24 – 30, 2024

Expert Analysis 1/2

Global Navigation Satellite System (GNSS) describes **any constellation of satellites that autonomously provides positioning, navigation, and timing (PNT) services with global coverage**. GNSS has become a globally widely used tool for navigation, transport, and military purposes. However, **GNSS faces cyber and signal threats daily, such as Radio Frequency (RF) interference that can disrupt its services.** Among those is **GNSS jamming and spoofing.** Those have become a daily phenomenon, mainly due to electronic warfare (EW) actions in contested zones. Indeed, since September 2023, spoofing incidents have been especially seen in Eastern Europe and the Middle East. The **military is particularly affected when on the field**. Such incidents have challenged air and land military exercises and readiness, and the industry and Nation-states are all trying to address GNSS resilience. For the purpose of this article, we will focus on the **American GNSS: GPS**.

GPS was the **first operational satellite navigation system**, developed by the US Department of Defense in the 1970s. Today, it consists of 31 operational satellites in orbit, and is a **critical technology** used by all sectors of the economy, with an **important duality** (civilian and military use). However, the GPS system uses technologies that were conceived in the 1970s, which may not meet modern safety requirements and that may be complex to update. These legacy and obsolescence issues can lead to more vulnerability to cyberattacks. Furthermore, malicious actors also noted the growing dependency on GPS, which makes it a choice target, and consequently leads to a need for more security.

> The GPS system uses technologies that were conceived in the 1970s, which may not meet modern safety requirements and that may be complex to update.

For all these reasons, the US continuously works on different ways to enhance resilience, such as the **GPS modernization program, launched in May 2000 that is still ongoing**. The purpose is to upgrade and secure the features of the GPS. This program involves **several upgrades on the space segment** (with new satellite acquisitions such as GPS III, and GPS III Follow-On), **and on the control segment** (such as the Next Generation Operational Control System), and new capabilities to **limit vulnerabilities to cyber and electronic threats** (such as the Military Code Early Use).

Expert Analysis 2/2

The control segment upgrade is a big part of the GPS modernization program. This future version, the Next Generation Operational Control System (OCX), will command all GPS satellites, manage navigation signals, and **provide improved cybersecurity and resilience.** OCX development follows an approach in 4 blocks. First, **Block 0** is the **Launch and Control System (LCS)**. It is a subset of OCX Block 1 since it aims to provide **the hardware, software, and cybersecurity base for Block 1**. It was delivered in 2017 by Raytheon. Then, **Block 1** fields the operational capability to control all signals. It **also aims to meet cyber defense requirements. Block 2** fields the advanced operational capability to control the advanced features of the modernized military signals. Lastly, **Block 3F** aims to launch and operationally command and control GPS IIIF space vehicles.

This month, **the US Space Force's Space Systems Command (SSC) has awarded Raytheon a $196.7m contract extension for the GPS OCX program**. This latest award brings the **total OCX contract value to nearly $4.5bn** since its inception in 2010. However, according to the US Government Accountability Office (GAO), the total amount is approaching $8bn. OCX has faced multiple delays since the initial completion date was early 2016, but the USSF hopes that the OCX will become **operational in December 2025**. Those delays result from the **several cybersecurity upgrades on OCX during its development**. The Secretary of Air Force Frank Kendall explained in 2023 that cybersecurity in OCX has become more stringent over time, adding layers of complexity in designing and developing the system.

On the space segment side, this month, Lockheed Martin has challenged the narrative that military GPS users are vulnerable to service disruptions and emphasized the advanced security features set to debut with the upcoming GPS IIIF satellites. Indeed, Lockheed Martin has been mainly working on the space segment. In 2018, the company won a **$7.2bn contract to produce up to 22 GPS IIIF satellites, the first of which is scheduled for launch in 2027**.

Valentine Crepineau
Market Analyst at CyberInflight

> OCX has faced multiple delays [...] Those delays result from the **several cybersecurity upgrades on OCX during its development.**

Monthly Watch – Threat Intelligence articles

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

Orbit under siege: The cybersecurity challenges of space missions

In recent years, spacecraft, satellites, and space-based systems have increasingly become targets for malicious actors, including nation-sponsored hacker groups, raising serious concerns about mission safety and national security. According to a 2024 Deloitte report, the number of active satellites in orbit is approaching 10,000 and is expected to double every 18 months. **#Awareness #SpaceMissions**

Link: https://www.cysecurity.news/2024/12/orbit-under-siege-cybersecurity.html

Korean firm busted for Selling DDoS-enabled satellite receivers

In July 2024 Interpol tipped off South Korean authorities about a suspicious shipment of satellite receivers from a Korean firm to an overseas company known for illegal broadcasting. Subsequent analysis confirmed that the receivers either came preloaded with malicious software enabling DDoS attacks or were configured to install it during firmware updates. Nearly 98,000 units were already infected at the time of sale. **#SouthKorea #DDoS**

Link: https://cyberinsider.com/korean-firm-busted-for-selling-ddos-enabled-satellite-receivers/

Frequent freeloader part II: Russian actor Secret Blizzard using tools of other groups to attack Ukraine

After co-opting the tools and infrastructure of another nation-state threat actor to facilitate espionage activities, Russian nation-state actor Secret Blizzard used those tools and infrastructure to compromise targets in Ukraine. Microsoft Threat Intelligence has observed that these campaigns consistently led to the download of Secret Blizzard's custom malware, with the Tavdig backdoor creating the foothold to install their KazuarV2 backdoor.

#Russia #SecretBlizzard

Link: https://www.microsoft.com/en-us/security/blog/2024/12/11/frequent-freeloader-part-ii-russian-actor-secret-blizzard-using-tools-of-other-groups-to-attack-ukraine/

Chinese citizen charged with flying drone over key US military, NASA rocket launch base, taking photos

A Chinese citizen living in L.A. allegedly flew a drone and took aerial images of Vandenberg Space Force Base last month, federal prosecutors said Monday. Yinpiao Zhou, 39, was arrested this week at the San Francisco Airport prior to boarding a China-bound flight, the Justice Department said. He is charged with failure to register an aircraft not providing transportation and violation of national defense airspace. **#USSF #Drone**

Link: https://www.foxnews.com/us/chinese-citizen-charged-flying-drone-over-us-military-nasa-rocket-launch-base-taking-photos

Russia develops 'Starlink killer' Kalinka to counter Elon Musk's satellite network in Ukraine: Report

Russia has reportedly developed an advanced system designed to detect and disrupt signals from Elon Musk-owned SpaceX's Starlink satellites, which have played a key role in Ukraine's war strategy. The system, named Kalinka, is being hailed as a 'Starlink killer' and could significantly impact Ukraine's reliance on Starlink technology. **#Starlink #Russia**

Link: https://in.mashable.com/science/86786/russia-develops-starlink-killer-kalinka-to-counter-elon-musks-satellite-network-in-ukraine-report

Monthly Watch – Geopolitics articles

CyberInflight

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/

The evolving strategic importance of space in modern military operations

Since the mid-1950s, the number of space actors has proliferated, with more countries now actively participating in space activities. This interest highlights the critical role of satellites and space technologies in both the military and commercial sectors. Nations are investing heavily in advanced space capabilities to strengthen military power and protect strategic assets, making space a contested and competitive domain. **#Awareness #Military**

Link: https://iari.site/2024/12/07/the-evolving-strategic-importance-of-space-in-modern-military-operations/

Malaysian national space defence system plan being formulated

The Malaysian Armed Forces (MAF) is formulating a long-term plan to strengthen the country's space defence system capabilities, said Deputy Defence Minister Adly Zahari. He said the plan, which will start from 2030 until 2044, includes the launch of National Military Satellites to support the Space Defence System. **#Malaysia #DefencePlan**

Link: https://www.nst.com.my/news/nation/2024/12/1146817/adly-national-space-defence-system-plan-being-formulated

Pentagon report highlights China's space advancements and AI-driven 'precision warfare'

The Pentagon's annual "Military and Security Developments Involving the People's Republic of China" report, released Dec. 18, underscores the accelerating pace of China's military modernization, with increasing focus on space and artificial intelligence technologies. **#China #Warfare**

Link: https://spacenews.com/pentagon-report-highlights-chinas-space-advancements-and-ai-driven-precision-warfare/

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/

Navy asks RTX Raytheon for 13 airborne electronic warfare (EW) jammers for US and Australian combat jets

RTX Raytheon will build 13 Next Generation Jammer Mid-Band (NGJ-MB) airborne EW systems for US Navy and Australian EA-18 Growler combat jets under terms of a $591m contract announced in late November. The NGJ midband is an advanced electronic attack system that denies, disrupts, and degrades enemy communications and air-defense radar systems. **#EW #Raytheon**

Link: https://www.militaryaerospace.com/sensors/article/55247123/raytheon-technologies-corp-airborne-electronic-warfare-ew-jammers

Viasat awarded up to $568m contract from GSA to support C5ISR capabilities for DoD

Viasat has received a new five-year contract worth up to $568m from the US General Services Administration (GSA) to support US DoD technology modernization. The award supports tactical networking, ground system, satellite communication, and cybersecurity solutions. The sole-source, Indefinite Delivery/Indefinite Quantity (IDIQ) contract is a follow-on from a similar award in 2019. **#Viasat #DoD**

Link: https://www.satellitetoday.com/government-military/2024/12/11/viasat-awarded-up-to-568-million-contract-from-gsa-to-support-c5isr-capabilities-for-dod/

Commission takes next step to deploy the IRIS² secure satellite system

The Commission has signed the concession contract for the Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²), a multi-orbital constellation of 290 satellite, with the SpaceRISE consortium. This partnership will develop, deploy, and operate the European Union's new system. It is a significant step towards Europe's sovereignty and secure connectivity. **#Iris2 #EU**

Link: https://defence-industry-space.ec.europa.eu/commission-takes-next-step-deploy-iris2-secure-satellite-system-2024-12-16_en

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

What cybersecurity on the ISS teaches us about defending critical systems

🇷🇴

400 kilometers above the Earth, on board the International Space Station and inside the European Columbus module, DropCoal—a complex scientific experiment developed by the Romanian InSpace Engineering (RISE)—is performing its daily tasks, relying on real-time operations from the ground. However, real-time operations require real-time protection that adheres to rigorous cybersecurity standards set by both the European Space Agency (ESA) and the National Space Administration (NASA). **#ISS #DropCoal**

Link: https://www.bitdefender.com/en-us/blog/businessinsights/what-cybersecurity-on-the-iss-teaches-us-about-defending-critical-systems

At five years, Space Force reflects on growth, challenges and the road ahead

🇺🇸

As the US Space Force marks its fifth anniversary, senior leaders and rank-and-file members, known as guardians, gathered at the second annual Spacepower Conference in Orlando this week. Against the backdrop of an increasingly contested space domain, Chief of Space Operations Gen. Chance Saltzman in a keynote speech Dec. 10 outlined the service's achievements and challenges that lie ahead. **#USSF #Throwback**

Link: https://spacenews.com/at-five-years-space-force-reflects-on-growth-challenges-and-the-road-ahead/

Qryptonic launches $1m quantum penetration challenge to test cybersecurity resilience against future quantum computing threats

🇺🇸

Quantum computing will soon challenge today's encryption, bringing us closer to "Q-Day" when traditional security measures may no longer hold. Qryptonic is offering a high-stakes test: Engage us for a quantum-focused penetration test. If we cannot uncover any vulnerabilities, you walk away with $1m ! If we do find weaknesses, you gain valuable insights to strengthen your defenses before quantum attackers emerge. **#Quantum #Challenge**

Link: https://www.qryptonic.com/quantum-challenge

Spatial-domain wireless jamming with reconfigurable intelligent surfaces

Wireless communication infrastructure is a cornerstone of modern digital society, yet it remains vulnerable to the persistent threat of wireless jamming. Attackers can easily create radio interference to overshadow legitimate signals, leading to denial of service. The broadcast nature of radio signal propagation makes such attacks possible in the first place, but at the same time poses a challenge for the attacker: The jamming signal does not only reach the victim device but also other neighboring devices, preventing precise attack targeting. **#Paper #Jammming**

Link: https://arxiv.org/abs/2402.13773

Monthly Watch – Regulation articles

CyberInflight

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

Technology articles

Lockheed Martin challenges narrative on GPS vulnerability

Lockheed Martin is challenging the prevailing narrative that military users of the Global Positioning System (GPS) are dangerously vulnerable to service disruptions and is emphasizing the advanced security features set to debut with the upcoming GPS IIIF satellites. While GPS is widely viewed as an indispensable backbone of the global economy, it is simultaneously seen as a fragile technological system vulnerable to sophisticated electronic warfare techniques and signal disruption. Jesse Morehouse, Lockheed Martin's director of business development and strategy for positioning navigation and timing, said this narrative overlooks security upgrades and technological innovations being developed to enhance GPS. **#LockheedMartin #GPS**

Link: https://spacenews.com/lockheed-martin-challenges-narrative-on-gps-vulnerability/

India to join elite nations with quantum satellite for secure communication

India is set to join an elite group of countries with quantum satellite capabilities, securing communication networks against hacking and cyberattacks. The satellite will play a key role in the larger quantum communications network under the National Quantum Mission (NQM). **#Quantum #India**

Link: https://www.communicationstoday.co.in/india-to-join-elite-nations-with-quantum-satellite-for-secure-communication/

New US Space Force jammers aim to disrupt China's SATCOM signals

The US Space Force is on track to field its first batch of a new ground-based satellite communications jammer in the coming months — designed to disrupt signals from enemy spacecraft. **#Jamming #USSF**

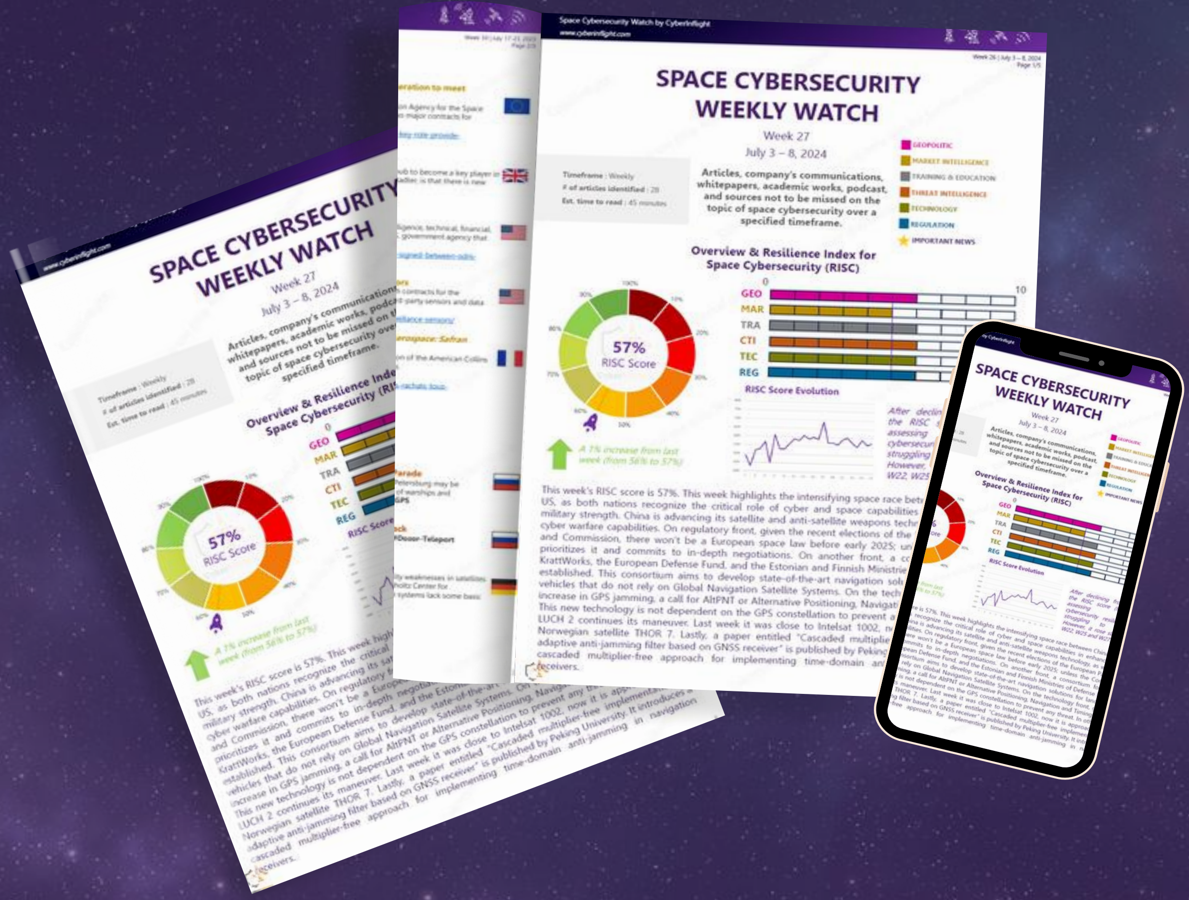
Link: https://www.defensenews.com/space/2024/12/19/new-us-space-force-jammers-aim-to-disrupt-chinas-satcom-signals/

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!


SPACE CYBERSECURITY WEEKLY WATCH
Week 27
July 3 – 8, 2024
Overview & Resilience Index for Space Cybersecurity (RISC)
57%
RISC Score
GEO
MAR
TRA
CTI
TEC
REG
RISC Score Evolution

Get access to the full version now !

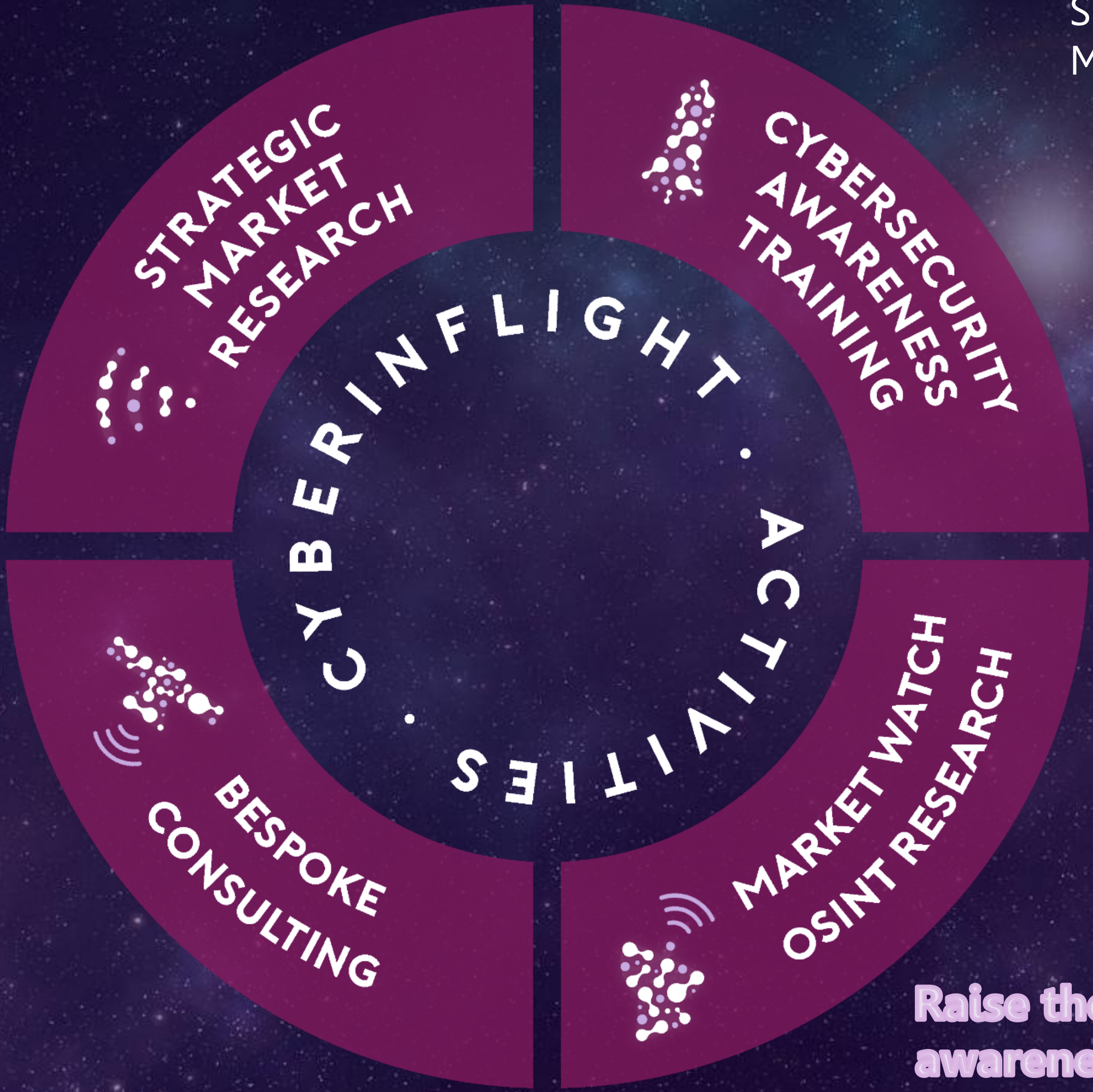
The watch can be customized to your needs, you can order yours!

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

CYBERINFLIGHT

CyberInflight

SPACE CYBERSECURITY
MARKET INTELLIGENCE


CYBERINFLIGHT · ACTIVITIES ·
STRATEGIC MARKET RESEARCH
CYBERSECURITY AWARENESS TRAINING
MARKET WATCH OSINT RESEARCH
BESPOKE CONSULTING

SPACE ISAC
PROUD MEMBER

Raise the cybersecurity awareness of the space industry

cyberinflight.com