



SPACE CYBERSECURITY WEEKLY WATCH

Week 9

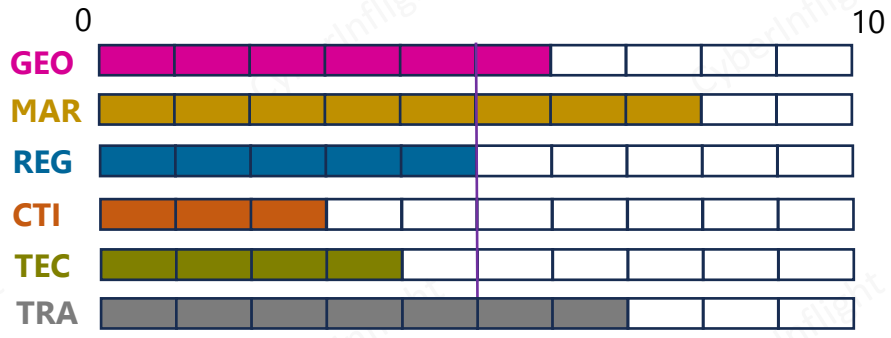
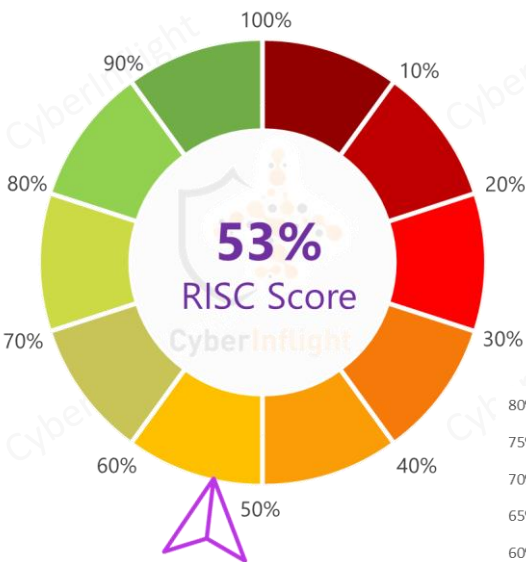
February 27 – March 4, 2024

Timeframe : Weekly
of articles identified : 30
Est. time to read : 45 minutes

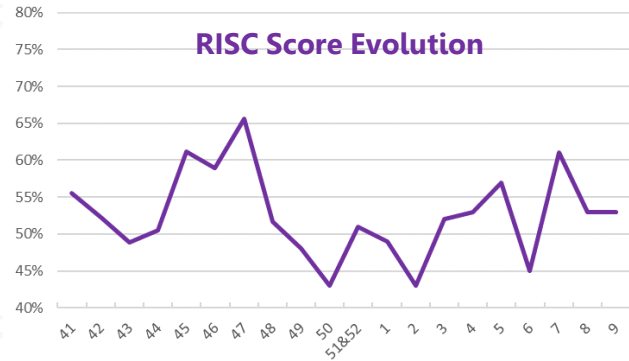
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

- **GEOPOLITIC**
- **MARKET & COMPETITION**
- **REGULATION**
- **THREAT INTELLIGENCE**
- **TECHNOLOGY**
- **TRAINING & EDUCATION**
- ★ **IMPORTANT NEWS**

Overview & RISC Score



➔ Same than last week



After a rising period since the start of 2024, W6 has shown a decrease, and W7 has shown an increase followed by a decrease for W8. W9 got the same result as W8, showing a stabilization in the ecosystem.

This week's RISC score is 53%. This week, the CYSAT 2024 Agenda was published, for which Florent Rizzo, CEO of CyberInflight will speak about the main highlights of 2023 in the space cybersecurity market as well as in a panel dedicated to ISACS: mark your calendars for April 25 ! In addition, this week, North Korea's first spy satellite, called Malligyong-1, has carried out space maneuvers, according to a space expert, and is well controlled by North Korea. On the market front, Indra and Thales have signed an agreement to collaborate in the defense sector in order to accelerate the development of advanced European technologies. In terms of regulations released this week, the main event is the released of NIST 2.0, which is the first major update since the framework was created a decade ago. On the threat intelligence side, the Philippine Navy confirmed that China has been deliberately intercepting the communication signal of Philippine ships in the West Philippine Sea (WPS), and has been doing so for several years. In addition, the establishment of space businesses by MetCom and the Japan Aerospace Exploration Agency (JAXA) will allow to conduct of research and development in order to realize a highly accurate and secure terrestrial positioning system. Last but not least, France inaugurated the AsterX 2024 Military Space Exercise, which aims to solve fictional geopolitical space war scenarios.

CYBERINFLIGHT'S NEWS



CYSAT 2024

Florent Rizzo, from CyberInflight, will speak and highlight the 2023 main moments on the space cybersecurity market, at the CYSAT event, in Paris, on 25 April 2024 ! Meet him there ! **#CYSAT2024 #CyberInflight**
Link: <https://cysat.eu/agenda/>



GEOPOLITIC

A New Frontier : Space Warfare Analysis

Satellites in space provide a range of capabilities for combat systems on Earth like GPS guidance for munitions and real-time surveillance of adversary movements, command, and control. Destroying or disabling them can have multiple effects on ground operations. **#SpaceWarfare**

Link: <https://www.cyberinflight.com/2024/02/27/a-new-frontier-space-warfare-analysis/>

Cobra Gold War Exercise Practice Response to Cyber and Space Threats

The annual focus of Thailand and the United States kicked off this year's Cobra Gold military exercise at U-Tapao International Airport in Rayong province. With the participation of 5,500 military and humanitarian personnel from several countries, Cobra Gold 2024 is deemed the largest military exercise in Southeast Asia. **#CobraGold #Military**

Link: <https://www.cyberinflight.com/2024/02/27/cobra-gold-war-exercise-practice-response-to-cyber-and-space-threats/>



In the Age of Intercepts: The C.I.A Makes the Case For Spies

Intelligence gathering today relies on electronic eavesdropping on cell and text messages as well as high-resolution satellite images. But the C.I.A. argues that even in the age of artificial intelligence and algorithmic intercepts, human sources are more important than ever. **#CIA #Espionage**

Link: <https://www.nytimes.com/2024/02/27/us/politics/in-the-age-of-intercepts-the-c-i-a-makes-the-case-for-spies/>



North Korea's First Spy Satellite 'Alive' and Working, Space Expert Says

North Korea's inaugural spy satellite, called Malligyong-1, is definitely "alive" and conducting space manoeuvres, a space expert has said, with Pyongyang successfully controlling the spacecraft. The satellite was put into orbit on 21 November after two failed attempts. **#NorthKorea #SpySatellite**

Link: <https://www.independent.co.uk/asia/east-asia/north-korea-spy-satellite-successful-b2504496.html>



GPS Independence: A Key Satcom Feature For All Critical Communications

In today's world where states and groups of nations use persistent jamming, the requirements for emergency communications equipment have never been higher. Dependability, interoperability, usability and internet speed are all key factors. We now must add jamming proof to the list. **#GPSJamming**

Link: <https://www.cyberinflight.com/2024/02/27/gps-independence-a-key-satcom-feature-for-all-critical-communications/>

US Air Force and Space Force Unite To Fortify Air, Space Operations Against Cyber Threats

The US Air Force and the U.S. Space Force have embarked on a strategic partnership to fortify air and space operations by weaving space capabilities into their overall warfighting. This collaboration underscores the critical role of cyber technology in modern military planning and operations, with a special focus on enhancing the resilience of space architecture and strengthening defenses against cyber operations. **#SpaceForce #Military**

Link: <https://www.defenselink.mil/2024/02/27/us-air-force-and-space-force-unite-to-fortify-air-space-operations-against-cyber-threats/>



South Korean Spy Satellite Transmitting High-Quality Images of Pyongyang, Says Sources

South Korea's first domestically developed spy satellite successfully sending high-quality images of Pyongyang back home during a test transmission, according to military sources Sunday. The electro-optical and infrared satellite is the first of the South Korean plans to launch by 2025 to conduct regular reconnaissance on the North. The satellite was launched on a SpaceX Falcon 9 rocket from Vandenberg Space Force Base in California on December 27. **#SouthKorea #Espionage**

Link: <https://www.defenselink.mil/2024/02/27/south-korean-spy-satellite-transmitting-high-quality-images-of-pyongyang-says-sources/>



Eyes In The Sky : Unveiling The Legacy of CORONA Satellites in Modern Surveillance

The CORONA satellite program, initiated by the CIA and the U.S. Air Force between 1959 and 1972, laid the groundwork for modern surveillance and global security through pioneering satellite imagery. These pioneering satellites were tasked with photographing key regions of the Soviet Union, China, and other strategic locations, significantly enhancing American intelligence capabilities during the Cold War. Today, the legacy of these historic endeavors is more pertinent than ever, shedding light on the evolution of global surveillance and espionage. **#CORONA #Espionage**

Link: <https://www.cyberinflight.com/2024/02/27/eyes-in-the-sky-unveiling-the-legacy-of-corona-satellites-in-modern-surveillance/>



MARKET & COMPETITION



Indra And Thales Forge Strategic Alliance For Cyber Defense And Communications Solutions

Indra, a leading global technology company, and Thales, a leading technology multinational in the defense, cybersecurity, digital security and aerospace markets, have signed an agreement to collaborate in the area of defense, intending to accelerate the development of cutting-edge European technologies and leverage synergies to compete in Spain and international markets. #Thales #Indra



Link: https://www.armyrecognition.com/defense_news_february_2024_global_security_army_industry/indra_and_thales_for_ge_strategic_alliance_for_cyber_defense_and_communications_solutions.html

Space Systems Command seeks proposals for Space And Cyber Tech Shared Agency Announcement

Space Systems Command (SSC) has begun seeking concept papers for a combined two-year, \$50 million shared agency announcement to develop, design, test, and certify cyber technologies designed to defend space assets from emerging threats. The two-step RFP will open for 30 days to solicit proposals across the SSC areas: military technologies and techniques, space domain awareness improvements, defense and offensive counter-space abilities, battle management command control and communications, and services, tools and training. #SSC #RFP



Link: <https://www.armyrecognition.com/2024/02/27/ssc-seeks-proposals-for-space-and-cyber-tech-shared-agency-announcement/>

Pacific Defense To Develop Electromagnetic, Electronic And Cyber Warfare Technologies

The Office of Naval Research in Arlington, VA, announced a \$17.4 million contract to Pacific Defense on Friday for the Pacific Defense Sensor Platform for Strategic and Distributed Autonomous Cyber Detection Warfare (SDAC) project. Pacific Defense will develop an artificial intelligence (AI) and machine learning system to process the sensor effluents for target detection, machine learning, cyber warfare, and AI at the tactical edge. #PacificDefense #Contract



Link: <https://www.military.com/defense-technology/2024/02/27/pacific-defense-sensor-platform-for-strategic-and-distributed-autonomous-cyber-detection-warfare-ai/>

Space Force Approaches Industry For Cybersecurity, Space Domain Awareness And Satellite Servicing

Officials of the Space Force's Space Domain Awareness and Combat Power branch in St. Ingeborg, CA, released a broad agency announcement (BAA) to solicit proposals for the \$50 million two-year project. Project features space cyber management, space data analysis for large networks, artificial intelligence (AI), and other satellite tasks. #SpaceForce #BAA



Link: <https://www.military.com/defense-technology/2024/02/27/space-force-approaches-industry-for-cybersecurity-space-domain-awareness-and-satellite-servicing/>

Edge Fabric Reaches IEC 62443-4-2 Certification - Advancing Critical Infrastructure Protection

The newly accredited firm SecureWorks has awarded Edge Security's Edge Fabric product the IEC 62443-4-2 certification of security level 4. The International Electrotechnical Commission (IEC) 62443 series are a set of standards for safeguarding industrial automation and control systems (IACS) against existing cyber threats. #Edge #Certification



Link: <https://www.secureworks.com/news/edge-fabric-iec-62443-4-2-certification>

REGULATION



NIST Cybersecurity Framework 2.0 Officially Released

NIST announced the official release of version 2.0 of its Cybersecurity Framework (CSF), the first major update since its creation a decade ago. The cybersecurity framework was originally aimed at critical infrastructure organizations, but it has been widely used and widely recommended and NIST highlighted that CSF 2.0 is designed to help all organizations reduce risks, regardless of sector, size, or level of security sophistication. #NIST #Framework



Link: <https://finabel.org/initiatives-an-eu-space-law-on-the-horizon-decoding-legal-foundations-and-navigating-policy-frontiers/>

THREAT INTELLIGENCE



Navy Confirms China's Jamming of Philippine's Ships Signal in West PH Sea

The Philippine Navy (PN) confirmed that China has been intentionally intercepting the communications signal of Philippine ships in the West Philippine Sea (WPS) and it has actually been ongoing for several years already. Commodore Roy Vincent Trinidad, PN spokesperson for West Philippine Sea, said there has been an increase in the incidents of electronic interference or jamming by China not only for the equipment of the Philippine ships but also for their land-based communications equipment. **#China #Jamming**



Link: <https://mb.com.ph/2024/2/27/navy-confirms-china-s-jamming-of-philippine-ships-signal-in-west-ph-sea>

South Korea Navy Confirms Investigating Hacked & Breach of WPSO (WPSO)

The South Korean Navy confirmed that it is investigating a cyber attack on the WPSO (WPSO) system, which is used for the management of the WPSO (WPSO) system. The attack is believed to have been carried out by a group of hackers who managed to gain access to the WPSO (WPSO) system and steal sensitive information. The South Korean Navy is currently investigating the attack and has issued a warning to other WPSO (WPSO) systems to be vigilant against such attacks.



Link: https://www.koreatimes.co.kr/www/east/2024/02/20240227_191234.html

Global Positioning System (GPS) Jamming On The Rise

Incidents of GPS jamming and spoofing appear to be on the rise and continue to threaten the safety of global air operations, a report from the International Civil Aviation Organization (ICAO) has revealed.

Link: <https://www.icao.int/pressroom/Pages/2024-02-27-01.aspx>

Reported on-line Cyber Espionage Campaign Targets Public and Aerospace Defense Industries

A report from the U.S. Department of Defense (DoD) has revealed that a cyber espionage campaign is targeting public and aerospace defense industries. The campaign is believed to be carried out by a group of hackers who have managed to gain access to sensitive information from these industries. The DoD is currently investigating the campaign and has issued a warning to these industries to be vigilant against such attacks.



Link: <https://www.defense.gov/Newsroom/Record/2024022701>

Space Force General Warns of 'Windows of Vulnerability' in Satellite Defense

A warning issued by the Space Force general commander, Gen. Michael Smith, highlights a critical gap in satellite defense. He stated that the current state of satellite defense is "not good" and that the Space Force is working to address these vulnerabilities. He emphasized that the Space Force is committed to protecting the nation's satellite assets and ensuring the continuity of satellite services.



Link: <https://www.spaceforce.mil/Newsroom/Record/2024022701>

The Pentagon Said That North Korea's Electronic Warfare Facilities Can Affect US Space Systems

The Pentagon has said that North Korea's electronic warfare facilities can affect US space systems. The Pentagon is currently investigating the threat and has issued a warning to US space systems to be vigilant against such attacks. The Pentagon is committed to protecting the nation's space assets and ensuring the continuity of space services.



Link: <https://www.defense.gov/Newsroom/Record/2024022701>

'GPS Have Been Reported For Months': The Baltic Incident and The Shadow of the Russians - What's Happening

The Baltic incident and the shadow of the Russians have raised concerns about the security of GPS systems. The incident involved a GPS jamming attack on a Russian ship in the Baltic Sea. The attack is believed to have been carried out by a group of hackers who managed to gain access to the GPS system and jam the signal. The incident has raised concerns about the security of GPS systems and the potential for such attacks to be used against other countries.



Link: <https://www.defense.gov/Newsroom/Record/2024022701>

LeakBot Ransomware Group Has Added 8 New Victims to Their Darkweb Portal

LeakBot ransomware group has reported that the Aerospace Corporation (AC) has been targeted by a ransomware coming from a Russian group called LeakBot. The group is currently investigating the attack and has issued a warning to the AC to be vigilant against such attacks. The group is committed to protecting the nation's space assets and ensuring the continuity of space services.



Link: <https://www.defense.gov/Newsroom/Record/2024022701>

TECHNOLOGY



JAXA And MetCom Begin Co-Creation Activities Related To “Terrestrial Positioning System”

MetCom and the Japan Aerospace Exploration Agency (JAXA) are creating space-related businesses with new ideas. Through this co-creation, in the first 1-2 years, MetCom and JAXA will each conduct research and development, creating a feedback loop for incorporating it into a MBS 3D positioning system. As a result, they aim to realize a highly accurate and safe terrestrial positioning system that incorporates new technologies. #JAXA #MetCom



Link: <https://spacewatchafrica.com/jaxa-and-metcom-begin-co-creation-activities-related-to-terrestrial-positioning-system/>

Ferret Communications Launches New Cyber Hardened Core (CHC) Redundant System

Ferret Communications has announced the launch of its new Cyber Hardened Core (CHC) Redundant System. The system is designed to provide a secure and resilient communication channel for critical operations, even in the face of cyber threats and disruptions.



Link: <https://www.ferretcommunications.com/press-releases/ferret-launches-new-cyber-hardened-core-2024-02-27>

TRAINING & EDUCATION

The Cybersecurity Defenders Podcast: Cybersecurity in Space with Tim Fowler

In this episode of The Cybersecurity Defenders Podcast, Tim Fowler, Chief Security Analyst at Black Hills Information Security, talks about cybersecurity issues as they relate to the space industry. As a frequent speaker on topics ranging from information security to open source software, Tim's mission is clear: to empower others to take control of their journey and make a positive impact in the world of cybersecurity. #SpaceCybersecurity #InfoSec

Link: <https://www.podcastaddict.com/podcast/1488842>

ISIRI's Online™ Replays Geopolitical Issues of GPS AIS Spoofing and Jamming

Recent world events have raised public awareness of the importance of satellite-based systems. However, it is rarely mentioned as a vital disruption to our lives. This timely guide from our experts, whether you use GPS or AIS directly, which you and your organization should not be aware that you know. Both GPS and AIS are subject to attacks spoofing or jamming their signals. The ISIRI's Online™ 2024 will discuss recent and future attacks and the geopolitical implications. #AISJamming

Link: <https://www.isiri.com/online-2024-ais-jamming-attacks-also-apply-to-critical-systems-2024-02-27>



AsterX 2024 : A New Edition of the French Space Military Exercise

France opens the AsterX 2024 Military Space Exercise in Toulouse today. The annual gathering is meant to encourage coordination among attendees to solve fictional geopolitical space warfare scenarios, such as attacks on communications satellites, to build capacity and understanding for possible future threats. #AsterX #Exercise



Link: <https://air.defense.gouv.fr/cde/actualite/asterx-2024-une-nouvelle-edition-de-lexercice-spatial-militaire-francais>

Space CTF : Space Grand Challenge

Welcome to Space Cyber Challenge (SC3) on the Space Grand Challenge with 400 members. The Space Grand Challenge is an international competition open to middle and high school students from across the globe. Teams from all over the world will compete in a simulated satellite operations scenario to help solve Mission Extension 2 (ME2).

#SpaceGrandChallenge #CTF

Link: <https://www.podcastaddict.com/podcast/1488842>

Post Quantum Cryptography: Securing Our Digital Life

In this video, the author and experts talk about what has happened in the Quantum and Post Quantum Cryptography (PQC) world. #PQC #InfoSec

Link: <https://www.podcastaddict.com/podcast/1488842>

CyberInflight is a Market Intelligence company dedicated to the topic of Space Cybersecurity. The company provides strategic market and research reports, bespoke consulting, market watch & OSINT researches and cybersecurity awareness training.

Contact us at: research@cyberinflight.com