SPACE CYBERSECURITY WEEKLY WATCH

Week 10

March 5 - 11, 2024

Timeframe : Weekly

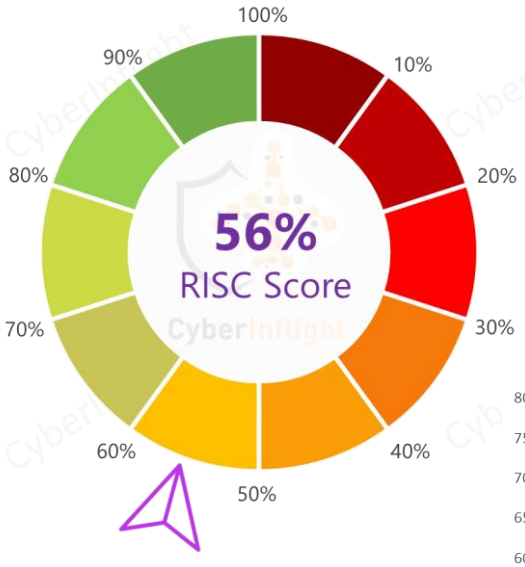
# of articles identified : 28

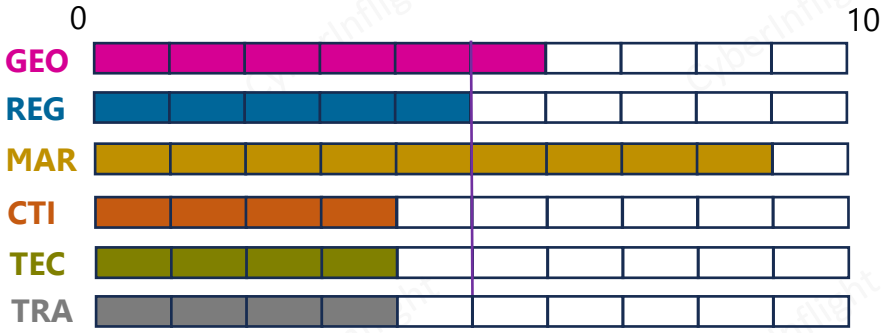
Est. time to read : 50 minutes

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

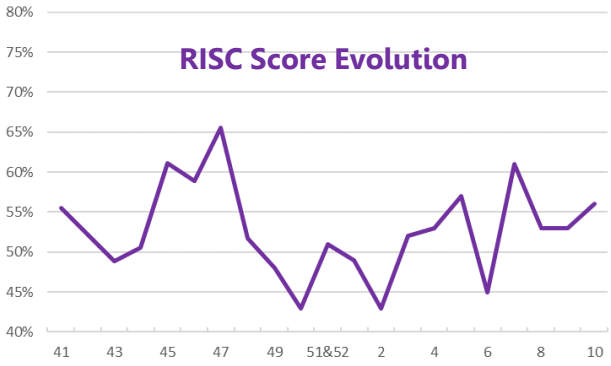
- GEOPOLITIC
- REGULATION
- MARKET INTELLIGENCE
- THREAT INTELLIGENCE
- TECHNOLOGY
- TRAINING & EDUCATION
- IMPORTANT NEWS

Overview & RISC Score





Increase from last week (from 53% to 56%)



After a rising period since the start of 2024, W6 has shown a decrease, W7 has shown an increase followed by a decrease for W8. Compared to the latest, W9 got the same result and W10 saw a small improvement.

This week's RISC score is 56%. This week, North Korea conducted artillery drills of the Korean People's Army Grand Combined Units. There is also an interpretation that they staged some sort of armed demonstration by sending out GPS jamming waves during the ROK-US joint Shield of Freedom exercise. Also this week, the U.S. Office of the National Cyber Director (ONCD) released a technical report that builds on President Joe Biden's National Cybersecurity Strategy by describing the urgent need to address undiscovered vulnerabilities that malicious actors can exploit. On the market front, Boeing was awarded a $439.6 million contract to build the 12th Wideband Global SATCOM (WGS) communications satellite for the U.S. Space Force's Space Systems Command. This week also saw the Space-Comm Expo in the UK, and on the second day, threat intelligence, cyber, and defense dominated the conversation as speakers addressed the growing threat of cyber attacks on space systems and how to counter them. In terms of new technologies, an article was released about Galileo and its groundbreaking service called Open Service - Navigation Message Authentication (OSNMA), which will allow detection of spoofing events in Galileo enabled receivers. Last but not least, the enhanced EU Space Academy learning platform has just been released! Participants can now choose from 12 learning modules and 44 lessons covering the entire EU Space Program.

GEOPOLITIC

CyberSight 360 : Is space the forgotten sector in critical infrastructure cyber security ?

Outer space has become a critical domain for daily life. From essential services and national security applications to the growing role of commercial ventures in space activities, our dependence on space assets, and in particular satellites, cannot be understated. As cyber operations are enabled by space and space operations are enabled by technology and cyber operations, space security and cyber security are closely interlinked. **#Australia #Cybersecurity**

Link: https://www.landers.com.au/legal-insights-news/is-space-the-forgotten-sector-in-cyber-security

Research institutions join forces to enhance space security of South Korea

On March 5, the Electronics and Telecommunications Research Institute (ETRI) revealed it had signed a letter of intent with the Defense Security Institute (DSI) to facilitate the exchange of research and technology in military defense. ETRI stated that this partnership aims to support research and development (R&D) efforts in space and cybersecurity for military applications. **#SouthKorea #SpaceCybersecurity**

Link: https://therecordable.co/research-institutions-join-forces-to-enhance-space-security-of-south-korea/

Space Force reimagines training, operations as conflicts intensify

After four years of growth amid a steadily rising operational tempo, Space Force leaders say it's time to improve on what they've built. But as the newest service has taken shape — pulling together soldiers, sailors, airmen, Marines and fresh recruits to form the military's smallest branch — the growing importance of space in global security has highlighted the need for a flexible, collaborative workforce for the decades to come. **#USSF #Warfare**

Link: https://www.defensenews.com/news/your-air-force/2024/03/06/space-force-reimagines-training-operations-as-conflicts-intensify/

Kim Jong-Un leads artillery training and GPS jamming signals : updates on North Korea's military activities

North Korea led artillery training of the Korean People's Army Grand Combined Units on the 7th. The US Joint Chiefs of Staff announced on the 8th, "Over the past three days from the 5th to the 7th, we have detected North Korea's GPS jamming signal several times in the area north of the NLL in the West Sea." There is an interpretation that they staged a kind of armed demonstration by sending out GPS jamming waves during the ROK-US joint exercise 'Shield of Freedom'. **#NorthKorea #CyberWarfare**

Link: https://www.archyde.com/kim-jong-un-leads-artillery-training-and-gps-jamming-signals-updates-on-north-koreas-military-activities/

France prepares for space wars in 'Aster X' European exercise

During the event called Aster X 2024, some 100 participants from France and 11 partner countries are training for everything from jammed space communications to hostile satellites maneuvering to take out friendly orbiters.

"This type of exercise is absolutely essential for our operators, but also our processes, training for what we call operational readiness, so we're ready to fight a real war," General Philippe Adam, the commander of France's space command, said during a presentation of the exercise. "It's as realistic as an exercise scenario can be, obviously – inspired by a lot of things you've probably recognized." **#GPS #Jamming**

Link: https://www.defensenews.com/battlefield-tech/space/2024/03/06/france-prepares-for-space-wars-in-asters-european-exercise/

REGULATION

ONCD report outlines path to enhanced cybersecurity through secure software and hardware practices

The U.S. Office of the National Cyber Director (ONCD) published a technical report built upon President Joe Biden's National Cybersecurity Strategy in describing the urgent need to address undiscovered vulnerabilities that malicious actors can exploit. The report aims to reduce memory security vulnerabilities at scale so that software and hardware developers can better secure the building blocks of cyberspace. **#ONCD #Strategy**

Link: https://industrialcyber.co/threat-landscape/oncd-report-outlines-path-to-enhanced-cybersecurity-through-secure-software-and-hardware-practices/

Séphora Alberti partage son dernier article sur NIS2 (Trad : Séphora Alberti shares her latest article on NIS2)

In this article, S. Alberti highlights an often overlooked aspect: Belgium's national cybersecurity authority recently published a reference framework for compliance with NIS2 regulations. Although it initially seems specific to Belgium, this framework can also be used as a dashboard to assess cyber maturity in France, and why not, increase it. **#NIS2 #Belgium**

Link: https://industrialcyber.co/threat-landscape/oncd-report-outlines-path-to-enhanced-cybersecurity-through-secure-software-and-hardware-practices/

MARKET & COMPETITION

USSF awards Boeing WGS-12 satellite production contract

Boeing received a $439.6 million contract to build the 12th Wideband Global SATCOM (WGS) communications satellite for US Space Force's Space Systems Command. The WGS constellation delivers vital high-capacity, secure, and resilient communications capabilities to the U.S. military and its allies. **#Boeing #USSF**

Link: https://news.satnews.com/2024/03/06/ussf-awards-boeing-wgs-12-satellite-production-contract/

Iridium (IRDM) to acquire Satellas for secure PNT services

Iridium Communications IRDM announced the acquisition of a leading provider of secure satellite-based time and location services — Satellas. The acquisition aligns with Iridium's strategy of investing in advanced technologies that excel within its network. **#Iridium #PNT**

Link: https://finance.yahoo.com/news/iridium-irdm-acquire-satellas-secure-031000340.html

LeoLabs raises $29 million to deliver enhanced AI-powered insights for space operations

LeoLabs, the company with the largest and most comprehensive commercial catalog of objects in low Earth orbit, today announced it raised an additional $29M in financing. This latest funding enables LeoLabs to scale up its insight delivery by further investing in advanced end-user applications and partner integrations. **#LeoLabs #Funding**

Link: https://spacewatch.global/2024/3/leolabs-raises-29-million-to-deliver-enhanced-ai-powered-insights-for-space-operations/

Spring budget 2024 : NHS AI, Space connectivity, Quantum computing

The Chancellor of the Exchequer, Jeremy Hunt, has finished presenting his Spring Budget 2024 to the House of Commons. Technology-related subjects included the use of AI in the NHS, connectivity from space, a quantum computing error correction programme, and funding for the Lawshford Spaceport, along with mentions of drones and facial recognition systems. **#UK #Budget2024**

Link: https://www.electronicsweekly.com/news/spring-budget-2024-nhs-ai-space-connectivity-quantum-computing-2024-03/

Cordero receives Yes, if award for mission security approach

Manuel Cordero, Information Technology security specialist for NASA's Independent Verification and Validation (IV&V) Program and advisor for the agency's Enterprise Protection Program (EPP), recently received a "Yes, if" coin for proactively increasing awareness about software security risks to protect NASA missions. Cordero received the "Yes, if" coin from Ryan Driscoll, NASA chief of Safety and Mission Assurance, during the Office of Safety and Mission Assurance face-to-face meeting in February. **#NASA #Cordero**

Link: https://sma.nasa.gov/news/articles/newsitem/2024/03/07/cordero-receives-yes-if-award-for-mission-security-approach

Vaxcent secures $5m seed funding to boost Quantum tech commercialization, led by corporate fuel

Vaxcent has secured $5 million in Series Seed funding led by Corporate Fuel and Caruso Ventures. The funding will accelerate the company's new product introduction, scale manufacturing, and expand its market reach. Vaxcent's products, including Frequency Combs, Lasers, and Controls, are used in quantum timing, computing, networking, and sensing. **#Vaxcent #Quantum**

Link: https://quantumintelligence.io/vaxcent-secures-5m-seed-funding-to-boost-quantum-tech-commercialization-led-by-corporate-fuel/

DQ Technology and Deutsche Telekom IoT collaborate for global satellite 5G IoT connectivity

In collaboration with DQ Technology, Deutsche Telekom IoT will offer a converged mobile satellite connectivity service, providing global IoT network coverage. This collaboration empowers businesses with reliable IoT services even in previously inaccessible areas. **#DeutscheTelekom #DQTechnology**

Link: https://spacewatch.global/2024/3/dq-technology-and-deutsche-telekom-iot-collaborate-for-global-satellite-5g-iot-connectivity/

BlackSky secures back-to-back contracts with US Air Force

BlackSky won a $11 million contract from the Air Force Research Laboratory to provide satellite imagery and analysis to support of global moving target engagement, the Air Force announced March 8. This contract is the first task of a contract worth up to $23 million over four years, an AFRL spokesperson said in a statement. BlackSky was selected for a Space Technology Advanced Research (STAR) contract used by AFRL for rapid acquisitions in support of space technology research. **#BlackSky #AirForce**

Link: https://executivebiz.com/2024/03/blacksky-secures-back-to-back-contracts-with-us-air-force/

THREAT INTELLIGENCE

[redacted]

[redacted]

Mystery GPS jamming on NATO borders fomenting 'atmosphere of threat'

A rise in daily GPS interference—often concentrated around sensitive strategic locations—has raised alarm among Western governments, transport authorities and militaries over the past two years, as Moscow presses its war on Ukraine and slides deeper into confrontation with NATO. **#NATO #Jamming**

Link: https://www.newsweek.com/gps-jamming-nato-borders-russia-threat-gnss-1876403

[redacted]

[redacted]

[redacted]

TECHNOLOGY

SPEAR OSNMA SKD : GNSS anti-spoofing solution White Paper

Given the advent of the increasing number of GNSS spoofing events being reported, applications relying on satellite navigation are in need of protection against this sophisticated kind of interference. The European GNSS constellation, Galileo, will soon provide a pioneering service that will allow the detection of these spoofing events in Galileo capable receivers. This service, which is called Open Service – Navigation Message Authentication (OSNMA), provides the necessary cryptographic means to authenticate the navigation message broadcasted by Galileo satellites. **#OSNMA #Rokubun**

Link: https://www.rokubun.cat/white-paper/

India pioneering Quantum communication

In a development that marks a significant leap forward in quantum communication, the Centre for Development of Telematics (C-DOT) and the Physical Research Laboratory (PRL) have achieved a milestone by integrating indigenous quantum key distribution (QKD) systems. **#India #Quantum**

Link: https://spacegoveia.com/2024/03/07/india-pioneering-quantum-communications/

HORACIO ED satellite equipped with its own state-of-the-art high-resolution optical system, successfully launched

SATLANTIS launched HORACIO, currently its sixth Earth Observation mission and third full-solution satellite, equipped with its own state-of-the-art high-resolution optical system, with visible, infrared, and agility capabilities, designed for a multitude of Earth Observation applications. **#Satlantis #HORACIO**

Link: https://spacewatch.global/2024/03/horacio-ed-satellite-equipped-with-its-own-state-of-the-art-high-resolution-optical-system-successfully-launched/

TRAINING & EDUCATION

Image-based intrusion detection system for GPS spoofing cyberattacks in unmanned aerial vehicles

The operations of unmanned aerial vehicles (UAVs) are susceptible to cybersecurity risks, especially because of their strong reliance on the Global Positioning System (GPS) and radio frequency (RF) sensors. GPS and RF sensors are vulnerable to potential threats such as spoofing attacks that can cause the UAVs to behave erratically. It is imperative to develop effective intrusion detection systems. In this paper, we present a deep learning-based methodology for detecting GPS spoofing cyberattacks. **#Aerospace #Spoofing**

Link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4747855

Empower your EU Space journey with the enhanced EU Space Academy Learning Platform

The enhanced EU Space Academy Learning Platform provides the business and technical skills you need to build ground-breaking new apps and disruptive business solutions. The platform covers the entire EU Space Programme, including EGNOS, Galileo, Copernicus, GOVSATCOM and Space Situational Awareness (SSA). Participants can now choose from 12 learning modules and 44 lessons. **#EUSPA #EUSpaceAcademy**

Link: https://www.euspa.europa.eu/newsroom/news/empower-journey-eu-space-academy-learning-platform

UK Space leaders talk countering cyber threats

On the second day of Space Comm Expo in the United Kingdom, cyber and defense dominated the conversations as speakers addressed the growing threat of cyber attacks on space systems and how to counter them. **#UK #CyberWarfare**

Link: https://www.satellitetoday.com/cybersecurity/2024/03/06/uk-space-leaders-talk-countering-cyber-threats/

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