



SPACE CYBERSECURITY WEEKLY WATCH

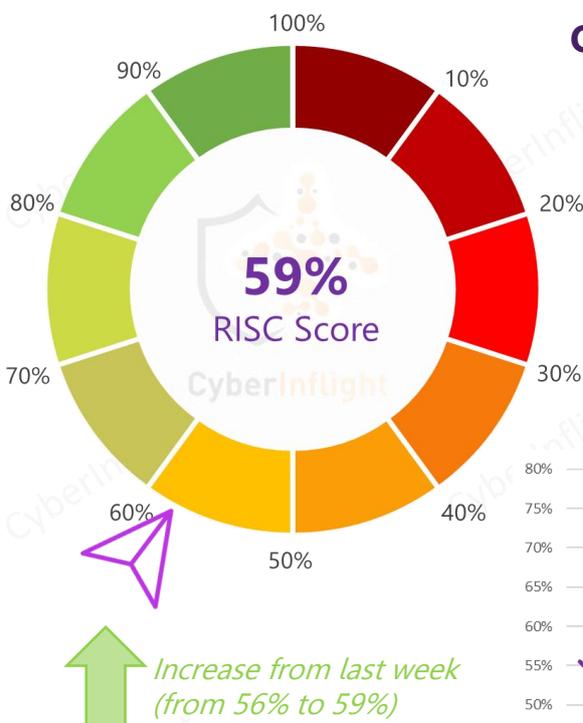
Week 11

March 12 - 18, 2024

Timeframe : Weekly
of articles identified : 45
Est. time to read : 90 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.

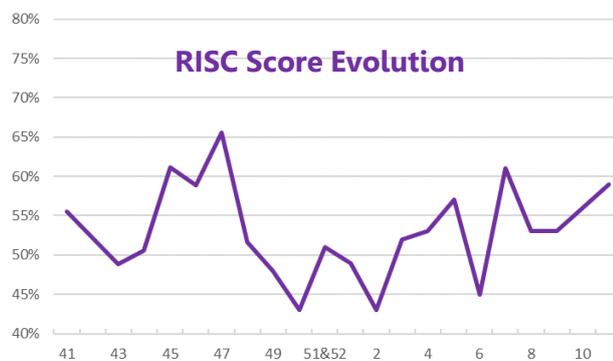
- GEOPOLITIC
- REGULATION
- MARKET INTELLIGENCE
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- TECHNOLOGY
- ★ IMPORTANT NEWS



Overview & RISC Score



RISC Score Evolution



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. Since W9 there has been an increase every week.

This week's RISC score is 59%. This week, an article was published about the US Space Force focusing on defensive cyber operations. In fact, earlier this year, 12 Guardians from the Peterson SFB moved away from base IT support to focus on defensive cyber operations. In addition, Australia's Cyber and Infrastructure Security Centre (CISC) released updated guidance to strengthen cybersecurity measures for Systems of National Significance (SoNS). On the market front, Science Applications International Corp. (SAIC) reported winning a \$444 million contract to modernize launch instrumentation and information systems at U.S. Space Force launch sites in Florida and California. In addition, the EU conducted the Space Threat Response Architecture (STRA-X-24) exercise at the European External Action Service headquarters in Brussels from March 4-13. This week, Russia is also believed to have jammed the satellite signal of an RAF aircraft carrying British Defense Secretary Grant Shapps. Defense sources called it a "wildly irresponsible" act of electronic warfare. Finally, Fleet Space Technologies, a leading Australian space company, announced the successful demonstration of satellite-based push-to-talk (PTT) capabilities for the Australian Defence Force - Joint Capabilities Group as part of their ASCEND2LEO program. This achievement represents a significant leap forward in tactical communications capabilities.



GEOPOLITIC

Jamming : How Electronic Warfare is Reshaping Ukraine's Battlefield?

Electronic warfare operations are becoming one of the Russian military's primary weapons after years of being less capable. Electronic warfare means a battle based on much of the war, and the Ukraine's disadvantage in troop numbers and ammunition supplies. Ukraine suffers in this area as well in comparison to Russia. Russia has more jamming equipment capable of overpowering Ukrainian signals by broadcasting on the same frequencies at higher power.

#Russia #EW

[Link: https://www.peterschriever.com/2024/03/07/jamming-how-electronic-warfare-is-reshaping-ukraines-battlefield/](#)



Guardians Of The Digital Frontier : USSF Focusing On Defensive Cyber Operations

Earlier this year, 12 Guardians from Peterson SFB shifted away from base IT support to focus on defensive cyber operations. All 12 Guardians were reassigned from working with the Defense Red Switch Network. "This was driven by the Chief of Space Operations' vision to get all Cyber Guardians and operations into defensive cyber operations roles, instead of the base operations support IT role," said U.S. Space Force Master Sgt. Matthew Crafton, 21st Communications Squadron test control flight chief. #SpaceForce #CyberWarfare



[Link: https://www.peterschriever.spaceforce.mil/Newsroom/News/Display/Article/3705037/guardians-of-the-digital-frontier-ussf-focusing-on-defensive-cyber-operations/](https://www.peterschriever.spaceforce.mil/Newsroom/News/Display/Article/3705037/guardians-of-the-digital-frontier-ussf-focusing-on-defensive-cyber-operations/)

Every War Is A Space War Now

Every international war is now simultaneously a space and cyber war requiring identification and active monitoring of threats from space assets and threats to space assets from dual states. In the US Department of Defense assessment, China and Russia in particular pose significant risks to space assets through various means such as cyber warfare, electronic attack and ground to orbit threats. This has prompted the United States to adopt substantial measures to better its space force. #SpaceForce #EW



[Link: https://www.peterschriever.com/2024/03/07/every-war-is-a-space-war-now/](https://www.peterschriever.com/2024/03/07/every-war-is-a-space-war-now/)

US, China Wrestling For Thailand's Cyber Soul

Washington has reported into Bangkok's satellite and cyberactivity with the US training Thailand's military in "Space Operational Awareness" for the first time during the recently completed cyber joint exercises. China, however, reportedly has partnered with Thailand's National Cyber Security Agency (NSA), which is responsible for conducting "cyber threats" to the Southeast Asian nation's critical infrastructure and other vulnerable targets. #CyberWarfare #EW



[Link: https://www.peterschriever.com/2024/03/07/us-china-wrestling-for-thailands-cyber-soul/](https://www.peterschriever.com/2024/03/07/us-china-wrestling-for-thailands-cyber-soul/)

US, UK, Australia Teaming Up To Deter China In Orbit

When Australia, the United Kingdom and the United States announced the AUKUS security partnership in September 2021, they did not include space capabilities on the initial list of emerging technologies the three countries would jointly develop as part of the trilateral alliance. However, the AUKUS partners are now embarking on a new initiative to track objects in deep space they hope will improve interoperability between the three nations and deter Chinese aggression. #AUKUS #EW



[Link: https://www.defensetrends.com/news/2024/03/07/us-uk-australia-teaming-up-to-deter-china-in-orbit/](https://www.defensetrends.com/news/2024/03/07/us-uk-australia-teaming-up-to-deter-china-in-orbit/)

SpySat Accused E GPS Fuel Use : Is Russia Is Preparing Alla Guerra Elettronica (Trad - Blinded Satellites And GPS Out Of Action) : Russia Prepares For Electronic Warfare

There is a new wild card at Russia's disposal: the world of a new constellation of services with the West. This is an electronic warfare campaign (EW) by blinding the enemy GPS, with more or less serious consequences for any device dependent on the use of the satellite positioning and navigation system. #Russia #EW



[Link: https://www.peterschriever.com/2024/03/07/spysat-accused-e-gps-fuel-use-is-russia-is-preparing-alla-guerra-elettronica-trad-blinded-satellites-and-gps-out-of-action-russia-prepares-for-electronic-warfare/](https://www.peterschriever.com/2024/03/07/spysat-accused-e-gps-fuel-use-is-russia-is-preparing-alla-guerra-elettronica-trad-blinded-satellites-and-gps-out-of-action-russia-prepares-for-electronic-warfare/)

REGULATION



Australia's CISC Releases Updated Cybersecurity Guidance For Systems of National Significance

Australia's Cyber and Infrastructure Security Centre (CISC) released on Monday updated guidance materials aimed at bolstering cyber security measures for Systems of National Significance (SoNS), which represent the country's most critical infrastructure assets. The comprehensive guidance includes specific instructions for SoNS on fulfilling the Incident Response Planning obligation and detailed guidelines for meeting the Cyber Security Exercise obligation.



#Australia #CriticalInfrastructure

[Link: https://industrialcyber.co/threats-attacks/australias-cisc-releases-updated-cybersecurity-guidance-for-systems-of-national-significance/](https://industrialcyber.co/threats-attacks/australias-cisc-releases-updated-cybersecurity-guidance-for-systems-of-national-significance/)

TRAINING & EDUCATION

US, Canadian, and French Space Command Officials Push The Importance Of Space Cybersecurity
According to the head of US Space Command, space is essential for the US, and by extension, its values and interests. The increasingly dangerous and volatile nature of space warfare needs to play a significant part in US space strategy. The Commander and Head of French Space Command also said that "we need to prepare for a high-stakes long conflict in the near future." #Research #M232



Link: <https://www.cyberinflight.com/press-releases/2024/03/12/us-canadian-and-french-space-command-officials-push-the-importance-of-space-strategy>

LED Satellite Download Distributed Jamming Optimization Method Using A Non-Dominated Sorting Genetic Algorithm

This paper has been submitted where military jamming used LED satellite communication equipment to disrupt enemy in the electromagnetic spectrum of military operations in satellite military areas. To combat jamming abnormal and illegal communications activities using LED satellites, this study proposes a LED satellite download distributed jamming optimization method using a non-dominated sorting genetic algorithm. #Research #M232

Link: <https://www.cyberinflight.com/press-releases/2024/03/12/led-satellite-download-distributed-jamming-optimization-method-using-a-non-dominated-sorting-genetic-algorithm>

Webinar - Protecting GNSS From Spoofing And Jamming

Learn more about how the industry is addressing the interference challenges in this upcoming webinar "Enhanced GNSS Jamming & Spoofing Resilience" which is slated for March 26 at 12 pm. Experts, experts from managers, Advisory & Consulting Services and the Norwegian Communications Authority will present a wide range of topics. Register now to attend live or to view the webinar on demand. #Webinar #M232

Link: <https://www.cyberinflight.com/webinars/2024/03/26/enhanced-gnss-jamming-and-spoofing-resilience>

An Aviator's Journey - Jamming and Spoofing

This talk discusses the author's experience in getting through jamming and spoofing interferences, but what are they and is there a difference between the two. #Management #Planning

Link: <https://www.cyberinflight.com/press-releases/2024/03/12/aviators-journey-jamming-and-spoofing>

GNSS Spoofing And Jamming In London

This research provides a thorough examination of GNSS interference, with a focus on multi-path effects and interference events. Field trials in London, a global analysis of interference incidents, and a specific application of the Chinese context were conducted to gather a diverse dataset. #GNSS #Research



Link: <https://www.cyberinflight.com/press-releases/2024/03/12/gnss-spoofing-and-jamming-in-london>

Lessons For Outer Space Security Now Available In All UN Official Languages

UNISPACE and the Secure World Foundation have jointly developed a Lessons for Outer Space Security to enhance common understandings around frequently used terminology. The lessons, originally prepared in English, is now also available in Arabic, Chinese, French, Russian, and Spanish. #UNISPACE #Planning

Link: <https://www.cyberinflight.com/press-releases/2024/03/12/lessons-for-outer-space-security-now-available-in-all-un-official-languages>

NIST Cybersecurity Framework 2.0: What Tech Professionals Need To Know

After two years of work, the US National Institute of Standards and Technology (NIST) released the updated Cybersecurity Framework 2.0 (CSF 2.0) with new best practices and recommendations for tech and security pros. This new version is intended to work for nearly any organization regardless of size or market sector. #NIST #Framework



Link: <https://www.cyberinflight.com/press-releases/2024/03/12/nist-cybersecurity-framework-2-0-what-tech-professionals-need-to-know>



Space : EU Carries Out Space Threat Response Architecture 2024 Exercise (STRA-X-24)

From 4 to 13 March, the EU carried out the Space Threat Response Architecture (STRA-X-24) exercise in the European External Action Service Headquarters in Brussels. The exercise tested the EU's response capacity to a situation in which EU space assets are subject of an attack targeting space services which are essential for governments, businesses, and citizens.



#EU #Exercise

Link: <https://www.eeas.europa.eu/eeas/space-eu-carries-out-space-threat-response-architecture-2024-exercise-stra-x-24-en>

Expert Warns Of Major Cyberthreat Posed By Satellite Hacking

Spies can check a professor at the Department of Computer Science & Computer Engineering at Chungnam National University delivered a speech at the 5th annual Cyber National Security Forum in Seoul. During his talk, Spies explored various hacking techniques capable of jeopardizing satellite operations. He highlighted that, in the most severe cases, these tactics have the potential to enable attackers to gain full control of satellites and, according to him, South Korea must increase its vigilance against potential hacking attempts on satellites. #Satellite #Warning



Link: <https://www.cyberinflight.com/press-releases/2024/03/12/expert-warns-of-major-cyberthreat-posed-by-satellite-hacking>



THREAT INTELLIGENCE

Global Communications Are Under Attack - Optical Satellite Networks Can Bolster Them

In recent weeks, fighters from Russia's missile movement have reportedly destroyed not four of the first years' optical communication cables between South Africa and Colombia. The cables, which are thought to belong to the AEGIS, Security, US and TSB systems, are among those that connect Europe and Asia. The cable damage proves that undersea and land cables are now considered infrastructure worthy of attack during times of conflict, and that alternative means of connectivity are increasingly vital. **#Russia #Communications**

Link: <https://www.cyberinflight.com/global-communications-under-attack-optical-satellite-networks-bolster-them>



GPS Jamming By Russia Was Already A Concern, For The NATO Countries, It May Only Get Worse

The Russian Navy's GPS disruption in NATO countries now that NATO operates as a defense report said GPS jamming continues using a frequency jamming device to block satellite communications that regulate everything from phone calls to air ambulance operations and GPS. In recent months, local news in Nordic countries have reported jamming signals in aviation when they suspect is coming from Russia. **#Russia #Jamming**

Link: <https://www.cyberinflight.com/russia-gps-jamming-by-russia-was-already-a-concern-for-the-nato-countries-it-may-only-get-worse>



Russia Suspected of Jamming GPS Signal On Aircraft Carrying Grant Shapps

Russia is believed to have jammed the satellite signal on an RAF aircraft carrying Grant Shapps, UK Secretary of State for Defence, according to government sources. Shapps was travelling from Poland to the UK when jamming interferences happened. It is understood that the GPS signal was interfered with for about 30 minutes while the plane flew close to Russia's Baltic exclave of Kaliningrad. Mobile phones could no longer connect to the internet and the aircraft was forced to use alternative methods to determine its location, the source said. Defence sources called it a "wildly irresponsible" act of electronic warfare. **#UK #Jamming**

Link: <https://www.theguardian.com/politics/2024/mar/14/russia-suspected-of-jamming-gps-signal-on-aircraft-carrying-grant-shapps>



US Agency Probes Role Of Foreign Satellite Use By Handheld Devices

The Federal Communications Commission (FCC) said Thursday it is investigating if the use of Russian and Chinese foreign satellite systems by U.S. mobile phones and other devices poses security threats. The FCC has concerns U.S. handheld devices are receiving and processing Chinese navigation satellite system (CHNS) signals from satellites controlled by foreign governments in violation of communication rules. **#US #FCC**

Link: <https://www.fcc.gov/news-releases/2024/03/fcc-probes-role-of-foreign-satellite-use-by-handheld-devices>



'Star Line' Tries To Jam The Broadcast Of Supplies Via Satellite

On March 13, the signal of the Ukrainian broadcast star Line was tried to be disrupted. The source of the interference was located on the territory of the Star Line Radio Advertising Station, located in the Moscow region. The target of the attack was the Astra satellite through which the broadcast was going on. **#Russia #Jamming**

Link: <https://www.starline.com/ua/en/news/2024/03/13/star-line-tries-to-jam-the-broadcast-of-supplies-via-satellite>



Cyberattack On Aerospace Research Firm Under NIA Lens

A cyberattack on government national aerospace laboratories that targets aerospace research company on November 15 last year has come under the scanner of the National Investigation Agency (NIA), which has started investigating the incident as a cyber-terrorist attack. **#NIA #Cyberattack**

Link: <https://www.nia.gov/news-releases/2024/03/15/cyberattack-on-aerospace-research-firm-under-nia-lens>



GPS Jamming Of UK Defense Secretary's Jet Highlights Russia's Regional EW Activities

While the precise origin of the attack, or attacks, can't be identified with complete certainty, a spokesperson for the UK Prime Minister Boris Johnson said that it is "not unusual for aircraft to experience GPS jamming near Kaliningrad, which is of course Russian territory". Kaliningrad is heavily militarized and, according to reports, hosts multiple bases and military supported test electronic warfare systems, which have been increasingly interfering with GPS signals in the Baltic states and Europe more widely. **#Russia #EW**

Link: <https://www.bbc.com/news/technology-68444444>





TECHNOLOGY



Fleet Space's Centauri Becomes Earth's Smallest Voice-Capable Satellite After In-Orbit Software Update

Fleet Space Technologies, a leading Australian space exploration company, announced the successful demonstration of satellite-enabled Push-to-Talk (PTT) capabilities for the Australian Defence Force - Joint Capabilities Group as part of their ASCEND2LEO program. This achievement signifies a major leap forward in tactical communications capabilities.



#Australia #PTT

Link: <https://fleetspace.com/news/fleet-spaces-centauri-becomes-earths-smallest-voice-capable-satellite-after-in-orbit-software-update>

ISRAELI ADAS - GNSS Anti-Jamming System

The ADAS - GNSS Anti-Jamming System, developed by the AD Company, enhances military operations against GNSS jamming by ensuring GNSS availability and reliability. GNSS-based navigation, communications, and timing systems, used in the field of attack from GPS jammers or other methods of interference. ADAS provides high levels of immunity, even in severe and dynamic multi-jammer scenarios. The system is operational, was rigorously tested and validated both in laboratory tests and in the field, and is in use in a range of operational systems. **#ISRAELI**



Link: <https://www.adcompany.co.il/en/adas/>

CTSEC - Qualification Of The ARCA SATCOM Solution

CTSEC qualified its ARCA SATCOM solution on different satellite links in August and November 2023. On 15th, the solution was tested on Starlink and Inmarsat systems and on 15th, the solution was tested on Arca Fibra, Thorpaq and Global Connect links. **#CTSEC #Israel**



Link: <https://www.ctsec.com/en/satcom-qualification>

AI, MDSAs, And The Future Of Secure Unmanned Warfare

Artificial intelligence (AI) enabled autonomous systems have revolutionized military operations and modern warfare. These unmanned systems are well suited for dangerous and repetitive tasks, enhancing situational awareness and logistical capabilities while reducing risks to human personnel. However, their growing role raises significant security concerns. Unmanned vehicles rely heavily on machine learning (ML) and can be vulnerable to cyberattacks that could jeopardize missions, troops, and critical technologies. **#AI #Warfare**



Link: <https://www.mdsas.com/en/ai-ml-secure-unmanned-warfare>

Galileo To Demonstrate 'Space To Edge' Assured Data Solutions At Satellite 2024

Galileo, a recognized industry leader in providing satellite communications (SATCOM) and edge compute and networking platforms, will showcase its portfolio of mission-critical technologies at the 2024 Satellite Conference & Exhibition from March 19-21 at the Waldorf Astoria Washington Convention Center, Washington, DC. **#Galileo #Satellite**



Link: <https://www.satellite2024.com/en/galileo-space-to-edge-assured-data-solutions-at-satellite-2024>

Satellites For Quantum Communications - Encryption By Means Of Physical Laws

Through steady advances in the development of quantum computers and their ever-improving performance, it will be possible in the future to crack our current encryption processes. To address this challenge, researchers at the Technical University of Munich (TUM) are participating in an international research consortium to develop encryption methods that will apply physical laws to prevent information of messages. To safeguard communications over long distances, the TUM's space mission will deploy satellites. **#Quantum #Encryption**



Link: <https://www.tum.de/en/quantum-communications-encryption-physicists/>

Port 17 Combines LEOs Comm Service With Cybersecurity

Port 17, a leading provider of maritime cyber security & IT solutions, announces the introduction of an all-in-one port and secure maritime connectivity solution. The service combines high-speed internet access with robust cybersecurity measures, offering vessel owners and operators a comprehensive and secure connectivity solution, all from one partner. **#Port17 #Cybersecurity**



Link: <https://www.port17.com/en/secure-maritime-connectivity-solution-with-robust-cybersecurity-and-1-combine-in-one>

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