



SPACE CYBERSECURITY WEEKLY WATCH

Week 48

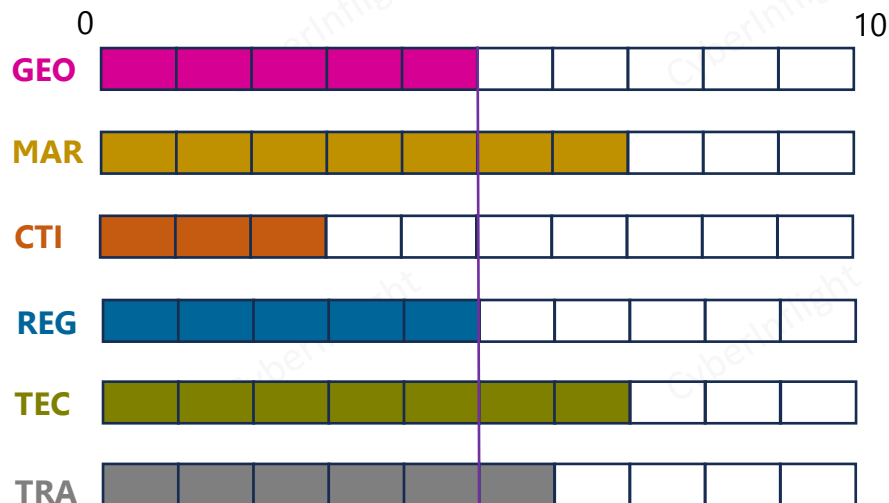
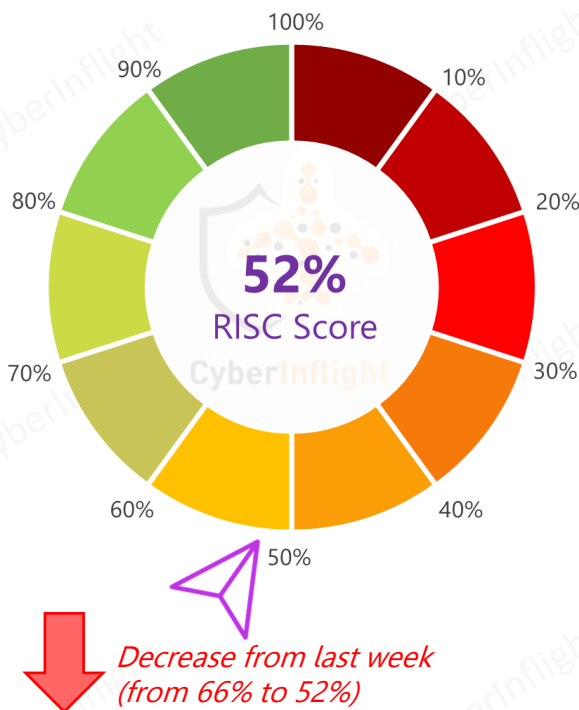
November 21 – 27, 2023

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

Timeframe : Weekly
of articles identified : 34
Est. time to read : 1h20min

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

Overview & RISC Score



This week's RISC Score is 52%. This week, a lot of information on intel. threat was reported. Numerous jamming-related news items were published, such as Finland's suspicion that Russia is jamming GPS signals crucial for weather balloons, or the fact that jamming zones in Ukraine and the Middle East are affecting commercial airlines. Also this week, a group called GARNESIA TEAM has allegedly leaked the database of ISRO. On the market front, the University of New South Wales Canberra has secured \$1.8 million in funding to improve the tracking of space debris and to develop AI capabilities for managing satellite constellations and bolstering their cybersecurity. This week, the DGCA published an advisory circular on GNSS interference in airspace, highlighting emerging threats of GNSS jamming and spoofing. On the technology front, SpaceGPT, the first Space Cybersecurity Operations and Resilience (SCOR) AI co-pilot, was created. Finally, ISRO has introduced a free online certification program focusing on cybersecurity.



GEOPOLITIC

China's Vision for Space

In recent years, China has rapidly built its capabilities and ambitions in space which encompasses a combination of scientific, military, scientific, and political interests. #China #Missions

Link: [https://www.cnas.org/public-affairs/china-vision-for-space](#)



U.S. Korea suspends military accord with South after satellite launch

North Korea said Thursday it was suspending a five-year old accord reached with South Korea to reduce military tensions — the latest retaliatory fallout over Pyongyang's spy satellite launch. #NorthKorea #Missions

Link: [https://www.bbc.com/news/world-asia-64968263](#)



MARKET & COMPETITION



UNSW Canberra Space secures \$1.8 million in funding to improve space object surveillance and satellite cybersecurity.

The University of New South Wales (UNSW) Canberra has secured \$1.8 million in funding to improve the tracking of space debris and to develop artificial intelligence (AI) capabilities for managing satellite constellations and bolster their cybersecurity #Australia #Funding

Link: <https://www.unsw.edu.au/news/2023/11/unsw-canberra-space-secures--1-8-million-in-funding-to-improve-s>



Research in Quantum Secured PNT Data Steps Up

Quantum Labs has secured \$750,000 funding for a research project aimed at modernizing a secured position, navigation, and timing (PNT) capability for defense applications. The project titled "Quantum Secured Time Transfer for Resilient PNT" will receive support from Department of Defense paving the way for cutting edge advancements in PNT security. #Australia #Funding

Link: [https://www.unsw.edu.au/news/2023/11/quantum-secured-pnt-data-steps-up](#)



Orbit Integrates Northrop's Cyber Solution into OpenSky PNT Systems for Enhanced Maritime MTCOM Security

Orbit Communications Systems, a leading global provider of maritime and defense MTCOM terminals, tracking and control station solutions and mission critical airborne public management systems, recently a major advancement in maritime MTCOM cybersecurity — the integration of the Northrop's system, with its comprehensive array of advanced cyber security features, into the company's OpenSky PNT systems. #MTCOM #Cybersecurity

Link: [https://www.orbitsystems.com/news/2023/11/orbit-integrates-northrop-cyber-solution-into-opensky-pnt-systems-for-enhanced-maritime-mtcom-security](#)

Army looking for industry input on low Earth orbit capabilities for next-gen blue force tracker

The Army is soliciting proposals from industry to examine what capability needs for current and future low Earth orbit satellite constellations as part of next-generation efforts related to its blue force tracker system. The Army wants industry when it comes to position, navigation, and timing (PNT) capabilities. #US #Army

Link: [https://www.army.mil/press/2023/11/army-looking-for-industry-input-on-low-earth-orbit-capabilities-for-next-gen-blue-force-tracker](#)



Space Force extends Kratos' contract for satellite ground systems

The new eight-year contract, worth up to \$175 million, is for maintenance and development of ground control systems for military communications satellites. #Space #Missions

Link: [https://www.spaceforce.mil/News/2023/11/space-force-extends-kratos-contract-for-satellite-ground-systems](#)



The case for LEO satellite connectivity in \$10 billion DOD contract

It is a contracting vehicle designed to enable federal agencies to procure mission-critical telecommunications infrastructure and technology services. It's the path to modernizing the government's IT infrastructure, implementing advanced cybersecurity and improving service to the public. #DOD #Missions

Link: [https://www.defenselink.com/2023/11/the-case-for-leo-satellite-connectivity-in-10-billion-dod-contract](#)





THREAT INTELLIGENCE

Electronic Warfare Combats Civilian Pilots, Far from Any Battlefield

Electronic warfare in the Middle East and Ukraine is affecting an increasing number of civilian pilots, undermining civilian air operations and representing an unintended consequence of a tactic that experts say will become more common. #Jamming #EW

Link: <https://www.cyberinflight.com/2023/11/21/electronic-warfare-combats-civilian-pilots-far-from-any-battlefield/>

Briefing 16: The Rise and Impact of Hacktivism Amidst Conflicts in Ukraine, Israel

The ongoing war between Israel and Hamas has spurred a surge in cyber activity, with a myriad of threat actors looking to contribute to the chaos through a slew of phishing, ransom attacks. Multiple threat groups have targeted infrastructure sectors that include global navigation satellite systems (GNSS) systems, Israeli cyber systems, healthcare, education, water systems and IT. Read comparison that operates in Israel. #Briefing #Hijacking

Link: <https://www.cyberinflight.com/briefing-16-the-rise-and-impact-of-hacktivism-amidst-conflicts-in-ukraine-israel/>

Utopia and Veritas 2: Russia's secretive surveillance satellites (part 1)

In March of this year, a Proton-M rocket blasted off from the Baikonur Cosmodrome in Kazakhstan, punching its way through a dense layer of fog that only thickened the veil of secrecy surrounding the launch. #Utopia #Veritas #Satellite

Link: <https://www.cyberinflight.com/utopia-and-veritas-2-russias-secretive-surveillance-satellites-part-1/>

Crewed ships up modded switch to secure Ukraine grid against Russian cyberattacks

Russian jamming activity is primarily centered to interfere with missile guidance systems, but a break in effects is expected to get operators. #Jamming #Ukraine

Link: <https://www.cyberinflight.com/crewed-ships-up-modded-switch-to-secure-ukraine-grid-against-russian-cyberattacks/>

Why Securing Supply Chain Security in the Space Sector is Critical

The space sector is facing a growing threat from nation-state cyberattacks, making it critical for organizations to know who has built every component that makes up a spacecraft. #SupplyChain #Space #Cyber

Link: <https://www.cyberinflight.com/why-securing-supply-chain-security-in-the-space-sector-is-critical/>



Finland suspects Russia jams GPS signals vital for weather balloons

Tracking data for balloons released by the Finnish Meteorological Institute in Sodankylä have been lost several times, jeopardizing weather forecasts for northern regions. #Jamming #Finland

Link: <https://thebarentsobserver.com/en/life-and-public/2023/11/finland-suspects-russia-jams-gps-signals-essential-weather-balloons>

Securing the Stars: The Crucial Role of Cybersecurity in Satellite Signal Logging

This article explores the vital role of cybersecurity in logging signals from satellites, ensuring that it safeguards communication, protects sensitive data, and ensures the uninterrupted flow of information from the vast reaches of space. #Satellite #Cybersecurity

Link: <https://www.cyberinflight.com/securing-the-stars-the-crucial-role-of-cybersecurity-in-satellite-signal-logging/>

New GPS Attacks Targeting Commercial Flight Navigation Systems

Since September 2023, a string of new GPS spoofing attacks has been detected through the Middle East, leaving commercial air routes grappling with an unprecedented threat. #Spoofing #GPS

Link: <https://www.cyberinflight.com/new-gps-attacks-targeting-commercial-flight-navigation-systems/>

Unknown Russian complex near Sevastopol creates strong interference

Recent satellite images shared on the social network, Twitter, appear to reveal an unidentified complex along the Crimean coast, specifically within the Sevastopol region. #Russia #Jamming

Link: <https://www.cyberinflight.com/unknown-russian-complex-near-sevastopol-creates-strong-interference/>



Allegedly leaked the Database of ISRO

A group called GARNESIA TEAM has allegedly leaked the database of the Indian Space Research Organisation (ISRO). The leak was claimed on a Telegram network, and the published URL provides more information. The incident is categorized as a data breach, with ISRO being the targeted organization. The leak potentially affects the defense and space industry in India. #ISRO #DataBreach

Link: <https://t.me/garnesiateam/2517>

Prover Proof claims to target the website of NASA Blogs

The post claims that a threat actor named Prover Proof targeted the website of NASA Blogs. It provides proof of successful through a link to a report on their front end. The post was published on Telegram and includes a link to the source. The authors of the attack is identified as a threat actor. The actions mentioned are the United States, NASA Blogs, and the Website Blogs manager. The industry affected is Aviation & Aerospace. #Prover #Proof

Link: <https://www.cyberinflight.com/prover-proof-claims-to-target-the-website-of-nasa-blogs/>





THREAT INTELLIGENCE

THE ANONYMOUS 80 targets NASA Space website

The post states that a threat actor known as THE ANONYMOUS 80 has targeted the NASA Space website, causing it to experience downtime. The proof of this downtime is provided through a link to a check host report. The post was published on a Telegram channel and belongs to the category of a threat attack. The victims of this attack include the United States as a country, NASA Space as an organization, and the website Space magazine. The industry affected by this attack is Aviation & Aerospace. #InfoSec #Hacking

Link: [https://www.linkedin.com/feed/update/urn:li:activity:7134316507991306241/](#)



REGULATION



DGCA issues circular on jamming and spoofing of satellite system, airlines directed to follow SOP

The Directorate General of Civil Aviation (DGCA) on Friday released an advisory circular on Global Navigation Satellite System (GNSS) interference in airspace. The circular highlights emerging threats of GNSS jamming and spoofing.

#DGCA #Jamming

Link: <https://www.cnbcvt18.com/aviation/dgca-circular-deal-with-gnss-interference-in-airspace-aai-18405131.htm>



TECHNOLOGY



Space GPT

The first Space Cybersecurity Operations and Resilience (SCOR) AI co-pilot. This innovative solution is focused on transforming the mission to close the space cybersecurity professional workforce gap as the primary companion to the ethicallyHackingspace (eHs) ® learning orbits. #SpaceGPT #AI

Link: <https://www.linkedin.com/feed/update/urn:li:activity:7134316507991306241/>

10 Tech Trends That Will Impact the Satellite Industry in 2024

From generative AI to quantum manufacturing techniques to AI for cost efforts, here are the technology trends that will drive the satellite industry over the next year. #Tech #SpaceTrend

Link: [https://www.satellite.com/technology/2023/11/21/10-tech-trends-that-will-impact-the-satellite-industry-in-2024](#)

Exploring New Frontiers in Satellite Communications Security in Space

The focus is on exploring the way in which satellite communications security in space through an innovative project at the Institute for Data Science and Computing (IDSC) at the University of Miami. This project aims to enhance the security of traditional satellites by integrating quantum-resistant satellite constellations to address various objectives, from communications and weather prediction to scientific research and Earth and data collection. #Space #Blockchain

Link: [https://www.linkedin.com/feed/update/urn:li:activity:7134316507991306241/](#)



GDMA: the latest in GNSS anti-spoofing security

To further improve transmission reliability, the European GNSS system, Galileo, has developed the GDMA anti-spoofing service, which allows secure and its transmission from Galileo satellites to GDMA-enabled GNSS receivers.

#Galileo #AntiSpoofing

Link: [https://www.satellite.com/news/galileo-gdma-anti-spoofing-service](#)



Quantum in the Stars: China's Space-Based Communication Network Initiative

A particularly notable achievement over the last decade is China's rapid progress in developing and launching quantum communication satellites. #China #Quantum

Link: [https://www.satellite.com/news/china-quantum-communication-satellites](#)



The official start of the Cygnus GOVSATCOM Study (GSS) project

The aim of the project is to form a definition study that will assist the efficient integration of Cygnus into GOVSATCOM European Union Governmental Satellite Communications and GNSS infrastructure for Resilience, Interconnectivity and Security by Satellite programmes. #Quantum #Cygnus

Link: [https://www.satellite.com/news/cygnus-go-satcom-study](#)





TRAINING & EDUCATION

Mapping Cyber-related Risks and Satellite Incidents and Confidence-Building Measures

This paper builds on IIRS work to map cyber-related incidents and satellite incidents, as well as confidence-building and multilateral efforts to provide intelligence meant to foster greater predictability and stability in cyberspace.

#Paper #IIRS

Link: <https://www.uscgspaceforce.com/2023/11/mapping-cyber-related-risks-and-satellite-incidents-and-confidence-building-measures/>

Hacking Satellites & CTF and Security Challenge

Explore the top 10 CTF challenges and a satellite CTF that will challenge your skills that offer much more than just entertainment. Today, we're starting off the season with a bit, ready to explore an intriguing variety of CTF hacking activities. **#CTF #Space #Cybersecurity**

Link: <https://medium.com/@cyberinflight/2023-hacking-satellites-a-ctf-and-security-challenge-61320440>

Space Governance Lab conducts 'Frontier' in policy and security

In recognition of the 'Frontier' in the field, the Defense Working Group established the Space Governance Lab. The goal is to explore the complex mix of challenges — political, legal, technical, social — that result from so many new players, including governments and private corporations, entering into the once largely empty space beyond the Earth's atmosphere. **#Space #Cybersecurity #Defense**

Link: <https://www.uscgspaceforce.com/2023/11/space-governance-lab-conducts-frontier/>

Satellite Hacking Demystified

Another risk to control and track satellites is hacking. Carried out by foreign governments, non-state entities, or even individual actors, cyberattacks are relatively inexpensive endeavors. On top of that, hackers often attack back to its source often prove difficult, if not impossible. **#Satellite #Hacking**

Link: <https://www.uscgspaceforce.com/2023/11/satellite-hacking-demystified/>



Opportunity to Learn: ISRO offers free course on 'Geo-data Sharing and Cyber Security'

As a part of the IIRS outreach initiative, the Indian Space Research Organisation (ISRO) has introduced a free online certification program focusing on cybersecurity. This program, titled 'Geo-data sharing and Cybersecurity,' has been specifically designed for individuals employed in the Central and State Governments. **#ISRO #Courses**

Link: <https://jagzpathshala.blogspot.com/2023/11/opportunity-to-learn-isro-offers-free.html?spref=tw>

Ep. 26: Meet Taha with Tom Cross

Special episode of the Security Center News Podcast, with Tom Cross about this year's Black Hat conference, including details on the headline-grabbing satellite hacking challenge. **#Podcast #Blackhat**

Link: <https://www.uscgspaceforce.com/2023/11/ep-26-meet-taha-with-tom-cross/>

Brown Bag seminar: Space threats and cyberattacks - how to defend against risks to satellites and satellite-dependent services?

Speaker at the University of Utah on December 14th, 2023, about how we can prepare for and defend against these space risks. **#Seminar #Space #Cybersecurity**

Link: <https://www.uscgspaceforce.com/2023/11/brown-bag-seminar-space-threats-and-cyberattacks-how-to-prepare-for-and-defend-against-these-space-risks-and-satellite-dependent-services/>

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

