SPACE CYBERSECURITY WEEKLY WATCH

Week 48

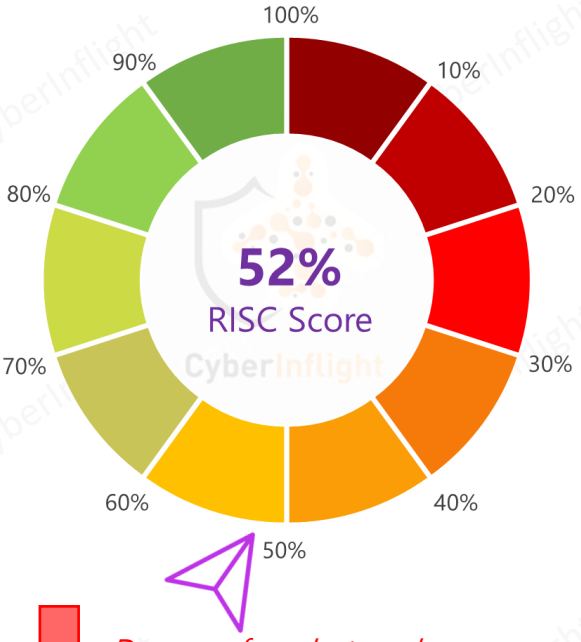
November 21 – 27, 2023

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

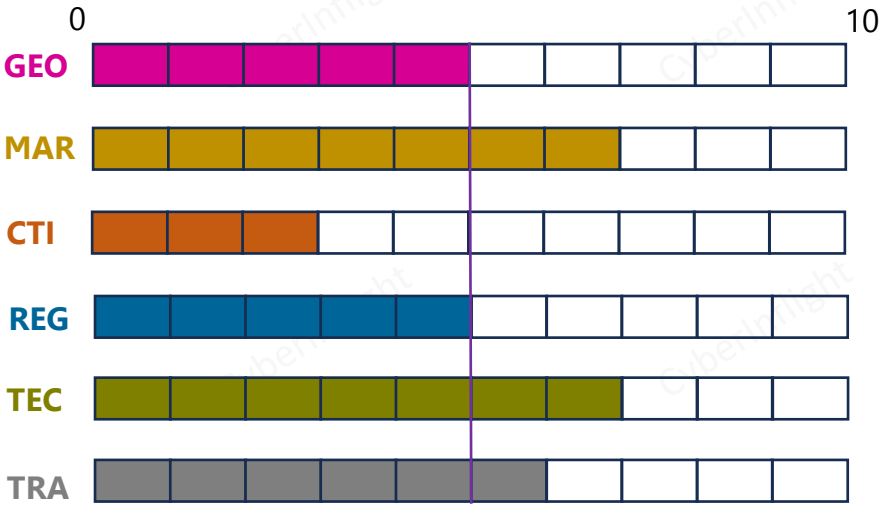
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

Overview & RISC Score



Decrease from last week (from 66% to 52%)



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 expanded its capabilities and ambitions in space, which encompass a combination of economic, military, scientific, and political interests. #China #Interview

Link: https://www.rdv.org/publications/chinas-vision-for-space/

N.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 #SouthKorea

Link: https://www.breitbart.com/news/n-korea-suspends-military-accord-with-south-after-satellite-launch/

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

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

Link: https://australiancybersecuritymagazine.com.au/research-in-quantum-secured-pnt-data-steps-up/

Orbit Integrates NetShroud+ Cyber Solution into OceanTRx MIL Systems for Enhance Maritime SATCOM Security

Orbit Communications Systems, a leading global provider of maritime and airborne SATCOM terminals, tracking ground station solutions and mission-critical airborne audio management systems, unveils a major advancement in maritime SATCOM cybersecurity – the integration of the NetShroud+ system, with its comprehensive array of advanced cyber security features, into the company's OceanTRx MIL systems. #SATCOM #Cybersecurity

Link: https://spacewatch.global/2023/11/orbit-integrates-netshroud-cyber-solution-into-oceantrx-mil-systems-for-enhance-maritime-satcom-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 exists for current and future low Earth orbit satellite constellations as part of modernization efforts related to its blue force tracker system. The Army wants resiliency when it comes to position, navigation, and timing (PNT) capabilities. #GEO #PNT

Link: https://defensescoop.com/2023/11/22/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 $170 million, is for maintenance and development of ground control systems for military communications satellites. #Kratos #USSF

Link: https://spacenews.com/space-force-extends-kratos-contract-for-satellite-ground-systems/

The case for LEO satellite connectivity in $50 billion EIS contract

EIS 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. #EIS #LEO

Link: https://www.c4isrnet.com/opinion/2023/11/24/the-case-for-leo-satellite-connectivity-in-50-billion-eis-contracts/

THREAT INTELLIGENCE

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

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

THREAT INTELLIGENCE

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.cnbctv18.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/

TRAINING & EDUCATION

Mapping Cyber-related Missile and Satellite Incidents and Confidence-building Measures
This paper builds on SIPRI work to map cyber-related missile and satellite incidents, as well as unilateral, bilateral and multilateral CBMs to provide takeaways meant to foster greater predictability and stability in cyberspace.
#Paper #SIPRI
Link: https://www.sipri.org/publications/2023/sipri-insights-peace-and-security/mapping-cyber-related-missile-and-satellite-incidents-and-confidence-building-measures

Hacking Satellites: A CTF and Security Challenge
Capture the Flag (CTF) challenges are a roller coaster ride filled with intellectual thrills and spills that offer much more than just entertainment. However, today, we're veering off the beaten path a bit, ready to explore an intriguing variety of CTF - hacking satellites. **#CTF #SpaceCybersecurity**
Link: https://medium.com/@Wisdom_Ctrl/hacking-satellites-a-ctf-and-security-challenge-d213b2904d80

Space Governance Lab confronts 'final frontier' in policy and security
In recognition of this 'final frontier' in the field, the Ostrom Workshop recently 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, rushing into the once largely empty space beyond the Earth's atmosphere. **#Course #KelleySchoolofBusiness**
Link: https://news.iu.edu/live/news/33782-space-governance-lab-confronts-final-frontier-in

Satellite Hacking Demystified
Another risk to current and future satellites is hacking. Carried out by foreign governments, non-state entities, or even individual actors, cyberattacks are relatively inexpensive endeavours. On top of that, tracing a cyber attack back to its source often proves difficult, if not impossible. **#Satellite #Hacking**
Link: https://www.linkedin.com/feed/update/urn:li:activity:7134671736251957760/

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://jagzzpathshala.blogspot.com/2023/11/opportunity-to-learn-isro-offers-free.html?spref=tw

Ep. 20: Mai Tais with Tom Cross
Newest episode of the Security Cocktail Hour 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.youtube.com/watch?v=-bEuQNaEYpg

Brown Bag seminar: Space threats and cyberattacks - how to defend against risks to satellites and satellite-dependent services?
Speaker at the University of Oulu, on December 14th, 2023, about how can we prepare for and defend against these space threats. **#Seminar #SpaceCybersecurity**
Link: https://www.oulu.fi/en/events/brown-bag-seminar-space-threats-and-cyberattacks-how-defend-against-risks-satellites-and-satellite