



SPACE CYBERSECURITY WEEKLY WATCH

Week 32

August 1 – 7, 2023

Timeframe : Weekly
of articles identified : 28
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
- TECHNOLOGY
- THREAT INTELLIGENCE
- TRAINING & EDUCATION
- ★ IMPORTANT NEWS

Overview

This week was marked by the publication of BSI's technical guidelines, "TR-03184 Information Security for Space Systems - Part 1: Space segment". Another major development this week was the introduction in the US of a bill to designate space as a critical infrastructure sector. The Senate Appropriations Committee also approved a \$831 billion defense spending bill for fiscal year 2024. There are still two ESA call for proposals open this week, one being the Space Systems for Safety and Security (4S) Call for Proposals, and the second concerning the Cyber-range testbed for Satellite Communications Physical and Data Link Layers within the ARTES program. Xona Space System was also awarded a contract with the AFRL and the US Space Force. This week, Russia made advances in jamming, targeting Starlink satellites. A paper on satellite security was widely reported this week, including an interview with one of the researchers, who pointed out that "Satellites easier to hack than a Windows device". On the technology front, Orbit Communications Systems launched a new NetShroud+ solution, designed to enhance cybersecurity within ground stations.

GEOPOLITIC

CNES joins WISSO to provide data and information from Copernicus Services and the European Sentinel satellites

The signing of an agreement between the French Space Agency (CNES) and WISSO (World Information Systems) means that CNES is now part of the WISSO network, which provides a platform that provides data and information from Copernicus Services and the European Sentinel satellites network. [WISSO Website](#)

[https://www.wisso.com/en/press-releases/cnes-joins-wisso-to-provide-data-and-information-from-copernicus-services-and-the-european-sentinel-satellites](#)

Space Force programs get trimmed in Senate appropriations bill

The Senate Appropriations Committee last week approved an \$831 billion defense spending bill for fiscal year 2024 that recommends about \$1 billion in cuts from the U.S. Space Force's \$40 billion request. [WISSO BudgetWatch](#)

[https://www.wisso.com/en/press-releases/senate-appropriations-bill-trims-space-force-programs](#)

Bipartisan bill designates space as critical infrastructure sector

A bipartisan group of House members introduced a bill to designate space as a critical infrastructure sector, a move aimed at ensuring the rapidly evolving industry gets adequate resources and future security protections.

#US #Space

[Link: https://thehill.com/homenews/space/4123413-bipartisan-bill-designates-space-as-critical-infrastructure-sector/](https://thehill.com/homenews/space/4123413-bipartisan-bill-designates-space-as-critical-infrastructure-sector/)

Enhancing ' lethality': First Space Force 'operations' doctrine comments role within Joint Force

The Space Force's new 'operations' doctrine for the first time lays out how the newest military service will work within the joint force structure and how it will be able to protect and defend the space assets that also defend terrestrial assets and enhance ' lethality' to global ' combat power' in any fight. [WISSO](#)

[https://www.wisso.com/en/press-releases/space-force-operations-doctrine-sets-out-how-it-will-work-within-the-joint-force-structure](#)





MARKET & COMPETITION



Thales to Protect Satellite Navigation System Against Cyber Threat

The European Space Agency (ESA) has awarded two contracts to Thales to ensure the security of the Galileo II satellite navigation system. #Thales #Galileo

Link: <https://www.msspalert.com/cybersecurity-news/thales-to-protect-satellite-navigation-system-against-cyber-threats/>



REGULATION



Publication of BSI Technical Guideline "TR-03184 Information Security for Space Systems - Part 1: Space segment"

with this Technical Guideline, the BSI would like to provide the user of the guideline with security measures that help to achieve an appropriate level of security for the space segment. Within the framework of the expert group "Information Security for Space Systems" between the BSI and representatives of the German space industry, analyses were carried out in numerous workshops, risks identified and best practices collected, resulting in a comprehensive table that assigns security measures to identified threats for various processes. #BSI

Link: https://www.linkedin.com/posts/manuel-hoffmann-607b4b1a3_bsi-space-spacesecurity-activity-7092479779752275968-2fo?utm_source=share&utm_medium=member_desktop





TECHNOLOGY

Resilience Assessment of GNSS GPS Receivers Against Spoofing Attacks

As GNSS spoofing becomes more of a concern, it's important to have a better understanding of the phenomena that happens during real world attacks. This article compares various spoofing signal simulators and generators available today, and looks at how various commercial off the shelf receivers behave in several real world spoofing scenarios. #spoofing #GNSS

[https://www.cyberinflight.com/2023/08/01/resilience-assessment-of-gnss-gps-receivers-against-spoofing-attacks/](#)

A Look at the Stars: Navigation with Multi-Constellation LEO Satellite Signals of Opportunity

Experimental and simulation results from Starlink, OneWeb, Iridium and other LEO satellite constellations are presented, demonstrating the efficacy and performance promise of the proposed LEO signals based opportunistic navigation framework. #satellite

[https://www.cyberinflight.com/2023/08/01/a-look-at-the-stars-navigation-with-multi-constellation-leo-satellite-signals-of-opportunity/](#)

La China dispone de BlackHole en orbita? (Trad: China dispone BlackHole in orbita?)

China achieves a major space feat by launching the world's first satellite with a blockchain imaging and tracking system. Developed by National Aerospace Technology Co, this revolutionary satellite opens up new prospects for blockchain. #China #Blockchain

[https://www.cyberinflight.com/2023/08/01/la-china-dispone-de-black-hole-en-orbita/](#)

Quelles sont ces quatre alternatives au positionnement GPS que développent les armées dans le monde? (Trad: What are the four alternatives to GPS positioning being developed by armies around the world?)

Today, there are 4 such technologies: inertial navigation, dual antenna GPS, signal of opportunity navigation and magnetic navigation. #GPS #GNSS

[https://www.cyberinflight.com/2023/08/01/quelles-sont-ces-quatre-alternatives-au-positionnement-gps-que-developent-les-armees-dans-le-monde/](#)



Orbit Launches the NetShroud+ Solution – New Cyber Security Capability for its Gaia100 Earth Observation Systems

Orbit Communications Systems Inc, a leading global provider of maritime and airborne SATCOM terminals, tracking ground station solutions and mission-critical airborne audio management systems, is proud to announce a major advancement in cybersecurity with the introduction of NetShroud+ for its Gaia100 Earth Observation systems.



#Orbit #Cybersecurity

[Link: https://www.satcom.digital/news/orbit-launches-the-netshroud-solution-new-cyber-security-capability-for-its-gaia100-earth-observation-systems](https://www.satcom.digital/news/orbit-launches-the-netshroud-solution-new-cyber-security-capability-for-its-gaia100-earth-observation-systems)

ESA, ESAE, ESAE and ST Engineering Direct launch in phase de développement d'un service satellite sécurisé (Trad: ESAE, ESAE and ST Engineering Direct launch the development phase of a secure satellite service)

The SecureSat (Secure & Sharing Satellite Services) project has entered the product development phase which will lead to commercialisation of the service in 2025, following a successful definition and technology phase. The project is co-financed by the European Space Agency (ESA) as part of its Advanced Research in Telecommunications (ART) program, with support from the Belgian Federal Public Service for Scientific Policy Programme (FPSRS). #ESA #ESAE

[https://www.esa.int/ESA/ST/ESAE_and_ST_Engineering_Direct_launch_in_phase_de_developpement_dun_service_satellite_securise](#)

THREAT INTELLIGENCE

Russia's Electronic Warfare Starts Jamming Starlink Signal in Luhansk - Military Expert

Russian electronic warfare systems has started to jam the Starlink satellite internet signal in the Luhansk sector. #Russia #Starlink



[https://www.cyberinflight.com/2023/08/01/russias-electronic-warfare-starts-jamming-starlink-signal-in-luhansk-military-expert/](#)



Could Russian Electronic Warfare Systems Mute Ukrainian Starlink?

Reports have popped up suggesting that Starlink has stopped operating in some parts of the Ukraine conflict zone. Earlier in the month a source familiar with the situation told Sputnik that Russia had developed a new electronic warfare (EW) system capable of disrupting spacecraft communications in geostationary orbit. #Russia #Starlink



[Link: https://www.theinteldrop.org/2023/08/01/could-russian-electronic-warfare-systems-mute-ukrainian-starlink/](https://www.theinteldrop.org/2023/08/01/could-russian-electronic-warfare-systems-mute-ukrainian-starlink/)

Space Pirates Turn Cyber Saboteurs as Russian, Serbian Organizations

Since late 2015, the Space Pirates cybercrime group has focused its efforts on espionage and data theft. But in recent months, researchers have noticed changes in their thinking, indicating the group has identified a treasure trove of new attack vectors. #CyberPirates #SpacePirates

[https://www.cyberinflight.com/2023/08/01/space-pirates-turn-cyber-saboteurs-as-russian-serbian-organizations/](#)



THREAT INTELLIGENCE

Satellites easier to hack than a Windows device

Researchers of one of the people looking for bugs of researchers from Ruhr University Bochum and the CISA National Center for Information Security (NCIS) researchers behind the paper, who also discovered that the team discovered subtle vulnerabilities in satellites. He says that malicious hackers could easily hack them using off-the-shelf equipment. He set them up with Windows devices satellite security and why on Earth a hacker would target a satellite. #SpaceCybersecurity #SatelliteSecurity

Western's invisible battle to join Russian weapons

In the early days of the invasion of Ukraine, reports were surprised at how poorly the Russian army's electronic warfare units performed, but nearly 18 months later they are causing significant problems for Ukraine's counter-offensive. #SpaceCybersecurity #Ukraine

TRAINING & EDUCATION

Indiana University launches space law courses, satellite cybersecurity program

The fall is also a launching course on space cybersecurity and a new space cybersecurity certificate program. University announced the fall space cybersecurity digital badge is the first program in the United States to offer a specialized focus on protecting the cybersecurity of space assets. #SpaceCybersecurity #Cybersecurity #US



"Whenever there's a paradigm shift, there are security issues": Examining Satellite Security

In their paper "Space Odyssey: An Experimental Software Security Analysis of Satellites", CISA Faculty Ali Abbasi and Thorsten Holz, along with researchers from Ruhr University Bochum, investigate the security issues that accompany the dawning of this "New Space Era". #UniversityPaper #SpaceCybersecurity

Link: <https://cispa.de/en/satellite-security>

EP 20: Securing Satellite Communications With Quantum Cryptography

Episode from our podcast where we talk about quantum cryptography and how it can be used to secure satellite communications. #Quantum #QuantumCryptography

Eric M. Miller, Executive Director of Space IAC, has been invited to speak at the NSA's 2nd Propulsion Laboratory Mission Cybersecurity Workshop

The workshop is an exceptional opportunity for cybersecurity experts from NSA centers, US industry, government, and academia to come together and share into the complexities of higher-risk assessment frameworks. The workshop is on August 22-24, 2023. #Workshop



The Risk to Space Satellite Communications Systems and Ground Networks as Attack Targets

Members of the NATO Blue Team Summit 2023 panel about the risk to space satellite communications systems and ground networks as attack targets. The panel was moderated by Scott Lynch. #Satellite #Space



ISU Space Cafe - Threats To and From Satellites with Jackie Wang

Conference with Jackie Wang is organized by the International Space University - USA Alumni Association's Washington DC Chapter. The event is on the 17 of August 2023 in Washington. #Workshop

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