SPACE CYBERSECURITY WEEKLY WATCH

Week 22

May 23 - 29, 2023

Timeframe: Weekly
# of articles identified: 31
Est. time to read : 1 hour

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
■ TECHNOLOGY
■ TRAINING & EDUCATION
■ THREAT INTELLIGENCE
■ MARKET & COMPETITION
★ IMPORTANT NEWS

Overview

This week was characterized by numerous contracts, including Viasat's acquisition of Inmarsat and ESA's new Call for Proposal. Also this week, the Chinese government announced the banning of certain American products over national security concerns. On the threat intelligence front, two significant data breaches were reported this week. The importance of satellite cybersecurity was also highlighted this week by the US DoD, as well as by the Ministry of Enterprise and Made in Italy. On the technology side, encryption and quantum are still important topics. Finally, a new online course about satellite mega-constellation presented by the IEEE ComSoc was created.

GEOPOLITIC

Pump up the jam!

For the first time, the Canadian Space Aggressor Team (CSAT) from 7 Space Operations Squadron conducted Global Positioning System (GPS) jamming during Exercises REFLEXE RAPIDE (Ex RR23) and MAPLE RESOLVE (Ex MR23), the Canadian's Army's largest training exercise. **#Canada #MilitaryExercice**

Link: https://www.canada.ca/en/department-national-defence/maple-leaf/rcaf/2023/05/space-pump-up-the-jam.html

Lifting our gaze: an update on the Australian space industry and satellite cyber security

The Australian space industry has cause for excitement after a joint statement issued by the Prime Minister of Australia and the President of the United States on 20 May 2023. This alert covers key elements of the joint statement as well as emerging issues in satellite cyber security. **#Australia**

https://www.lexology.com/library/detail.aspx?g=63aef398-2c65-4f01-bb5e-6a1ae5f69728

GNSS Interference: Getting to the Source

A look at algorithms developed for the real-time detection and localization of GNSS interference sources, and an investigation into last year's disruption at Dallas-Fort Worth International Airport. **#GNSS #Airports**

Link: https://insidegnss.com/gnss-interference-getting-to-the-source/

★ GCHQ warns of fresh threat from Chinese state-sponsored hackers

The UK's cybersecurity agency has urged operators of critical national infrastructure, including energy and telecommunications networks, to prevent Chinese state-sponsored hackers from hiding on their systems. **#UK #Cybersecurity**

Link: https://www.theguardian.com/technology/2023/may/25/experts-warn-against-china-sponsored-cyber-attacks-on-uk-networks

★ The Chinese government announced the ban on the products made by the US memory chip giant Micron Technology over national security concerns.

The Cyberspace Administration of China announced the ban on products made by US memory chip giant Micron Technology over security concerns. The ban is related to the use of company products in key infrastructure projects. **#China #MicronTechnology**

Link: https://securityaffairs.com/146511/security/china-bans-micron-products.html

Space Force Will Look At How to Hack Targets From Space

Two Space Force troops are helping the Air Force's information-warfare wing explore the future of offensive space operations, the leader of Space Operations Command said Wednesday. **#USSF #Hacking**

Link: https://www.defenseone.com/technology/2023/05/space-force-will-look-how-hack-targets-space/386755/

At GEOINT, Space Force and NGA lean into the metaverse, whatever that means

While Mark Zuckerberg and Microsoft already may have abandoned the metaverse as yesterday's news, the Defense Department and Intelligence Community continue to embrace the concept — with the theme of this year's annual US Geospatial Intelligence Foundation at St. Louis **#USSF**

Link: https://breakingdefense.com/2023/05/at-geoint-space-force-and-nga-lean-into-the-metaverse-whatever-that-means/

TECHNOLOGY

Viasat Next-Generation Ground-to-Space Encryption Solution Achieves National Security Agency Type-1 Certification

Viasat Inc., announced its next-generation ground-to-space encryption product, the KG-255XJ, is now National Security Agency (NSA) Type-1 certified. **#Viasat #Encryption**

Link: https://news.viasat.com/newsroom/press-releases/viasat-next-generation-ground-to-space-encryption-solution-achieves-national-security-agency-type-1-certification

Sending security to the stars

As quantum computing evolves, Guy Matthews examines how this advanced technology can be applied to satellite communications. **#Quantum #Encryption**

Link: https://www.capacitymedia.com/article/2boinh31lr5r4e6hhq1og/feature/sending-security-to-the-stars

Researchers developed a quantum sensor for GPS-free navigation

Researchers from The Imperial College London have developed a prototype of a quantum sensor that can enable GPS-free navigation, and they have tested a quantum sensor in collaboration with a Royal Navy ship. **#Quantum #GPS**

Link : https://www.inceptivemind.com/researchers-developed-quantum-sensor-gps-free-navigation-system/31042/

TRAINING & EDUCATION

★

Hack-A-Sat 2023: MOONLIGHTER

The fourth iteration of cybersecurity challenge poses the ultimate test: who can hack a satellite in space? **#Hack-A-Sat #Satellite**

Link: http://www.milsatmagazine.com/story.php?number=1911025006#

Meet a Teen Space Guardian Protecting the Cosmos from Evil using Aerospace Cybersecurity

Interview of Angelina Tsuboi, a programmer and aerospace cybersecurity researcher interning at NASA. **#Interview**

Link: https://hackernoon.com/meet-a-teen-space-guardian-protecting-the-cosmos-from-evil-using-aerospace-cybersecurity?source=rss

Security of Emerging Satellite Mega-Constellations

Presentation of the online course about satellite mega-constellations presented the IEEE ComSoc. **#Education**

Link: https://www.comsoc.org/education-training/training-courses/online-courses/2023-06-security-emerging-satellite-mega

THREAT INTELLIGENCE

VSAT Connectivity Comes With Cybersecurity Threats to Vessels

VSATs are targeted by attackers because they provide access to other vessel infrastructure, and they are also a target in themselves **#VSAT #Cybersecurity**

Link: https://www.maritime-executive.com/editorials/vsat-connectivity-comes-with-cybersecurity-threats-to-vessels

Nearly 300,000 people affected by data breach in DISH ransomware attack

A February ransomware attack against satellite broadcast giant DISH leaked the personal information of nearly 300,000 people, according to regulatory filings made by the company last week. **#DISH #Cyberattack**

Link: https://therecord.media/people-affected-by-dish-data-breach?hss_channel=lcp-3309477

★ Cybersecurity nello spazio: la tecnologia ipognac e la protezione dei dati a bordo di un satellite. Intervista a Giuseppe Vallone, Thinkquantum. *(Trad.: Cybersecurity in space: Ipognac technology and data protection aboard a satellite. Interview with Giuseppe Vallone, Thinkquantum.)* 🇪🇺

Interview of Giuseppe Vallone about the EU Cyber Solidarity Act and quantum key distribution. **#QKD #Cybersecurity**

Link: https://www.knowledge-share.eu/news/cybersecurity-nello-spazio-la-tecnologia-ipognac-e-la-protezione-dei-dati-a-bordo-di-un-satellite-intervista-a-giuseppe-vallone-thinkquantum/

Satelliti, Valentini: “Vanno protetti, minaccia cyber crescente” *(Trad.: Satellites, Valentini: "They must be protected, growing cyber threat”)* 🇪🇺

Deputy Minister of Enterprise and Made in Italy, Valentino Valentini, appealed for greater protection of satellites and space infrastructure. **#Italy #Cybersecurity**

Link: https://www.spaceconomy360.it/difesa-cybersecurity/satelliti-valentini-vanno-protetti-minaccia-cyber-crescente/

Unified and integrated: How Space Force envisions the future of data-sharing for space operations 🇺🇸

The Space Force over the next few years plans to build out its vision of what is essentially an everything network for space operations where it can receive data from just about any source in any format and make it available from a cloud-based repository to other organizations that use different systems and on different levels of classification.
#USSF #InformationSharing

Link: https://breakingdefense.com/2023/05/unified-and-integrated-how-space-force-envisions-the-future-of-data-sharing-for-space-operations/

NASA Laptop Data Breach Exposed 10,000 Employees’ Private Information 🇺🇸

NASA fell victim to a significant data breach, which resulted in the exposure of private information belonging to approximately 10,000 employees. **#NASA #DataBreach**

Link: https://fidelityheight.com/nasa-laptop-data-breach-exposed-employee-information/

DoD CIO Urges Vendors To Ensure Their Commercial Satellite Systems Are Cyber Secure 🇺🇸

The DoD ask to ensure that commercial satellite are protected from cyber threats. **#DoD**

Link: https://www.satellitetoday.com/cybersecurity/2023/05/25/dod-cio-urges-vendors-to-ensure-commercial-satellite-systems-are-cyber-secure/

★ Space Force to shift all cyber guardians to defending mission systems and performing ‘core’ tasks 🇺🇸

Guardians that are protecting the Space Force’s “base-level” networks will soon move onto conducting more critical operational cybersecurity missions. **#USSF #CyberGardians**

Link: https://defensescoop.com/2023/05/24/space-force-cyber-guardians/

Russia ‘Smashing’ 330 Ukrainian UAVs Per Day; UK Report Says Russian Electronic Warfare ‘Wreaks Havoc’ On Kyiv 🇷🇺

Researchers have revealed new Russian Electronic Warfare (EW) systems and capabilities that have been devastating for Ukrainian unmanned aerial vehicles (UAV) and encrypted radio communications in an alarmingly short period.
#RussiaUkaineWar #ElectronicWarfare

Link: https://eurasiantimes.com/russia-smashing-330-ukrainian-uavs-per-day-uk-report-says-russian-electronic-warfare-wreaks-havoc-on-kyiv/

MARKET & COMPETITION

NATO hunger for info driving deals for commercial satellite imagery

The unending appetite for intelligence, surveillance and reconnaissance within NATO is driving deals with commercial satellite imagery providers, according to one official. **#NATO #Satelliteprovider**

Link: https://www.defensenews.com/intel-geoint/isr/2023/05/23/nato-hunger-for-info-driving-deals-for-commercial-satellite-imagery/

★ Space Investment in 2023: Better Than Expected?

Overview of investments since the beginning of the year 2023. **#Investments**

Link: https://interactive.satellitetoday.com/via/june-2023/space-investment-in-2023-better-than-expected/

★ Cybersecurity as Enabler for Secure Satellite Communications and Resilient Applications

This new Space Systems for Safety and Security (4S) Call for Proposals aims to foster the development of innovative satellite communications technologies, products, systems and downstream applications which address these challenges. **#ESA #Proposal**

Link: https://business.esa.int/funding/call-for-proposals-artes-satcom-apps/cybersecurity-enabler-for-secure-satellite-communications-and

Innovation endorsement from ClassNK to Inmarsat's Fleet Secure Endpoint

ClassNK has granted their Innovation Endorsement to Inmarsat's Fleet Secure Endpoint, verifying the solution's fulfillment with functional elements that support effective, cyber risk management, as set out in the International Maritime Organization (IMO) 2021 regulation. **#Inmarsat #ClassNK**

Link: https://news.satnews.com/2023/05/26/innovation-endorsement-from-classnk-to-inmarsats-fleet-secure-endpoint/

Data accord signed between IFS and Lockheed Martin

Cloud enterprise provider IFS and defense giant Lockheed Martin announced a joint partnership intended to promote products and services to help defense and aerospace organizations turn data into actionable information for mission platforms. **#Lockheed Martin #IFS**

Link: https://militaryembedded.com/cyber/cybersecurity/data-accord-signed-between-ifs-and-lockheed-martin

Cyber security boost as CyberHive joins Inmarsat's ELEVATE programme

CyberHive, a leading cyber security software company, today announced it has joined Inmarsat's ELEVATE programme. **#CyberHive #Inmarsat**

Link: https://www.inmarsat.com/en/news/latest-news/enterprise/2023/cyberhive-joins-inmarsats-elevate-programme.html

BAE Systems gets contract to develop space-based surveillance tech

BAE Systems has secured a contract from a US government agency to develop an autonomous space-based surveillance technology **#BAESystem #DARPA**

Link: https://www.verdict.co.uk/bae-systems-surveillance-tech/

Viasat's Inmarsat acquisition clears all regulatory hurdles

Viasat has secured all regulatory clearances needed to buy British satellite operator Inmarsat after getting unconditional approval from the European Commission May 25. **#Viasat #Inmarsat**

Link: https://spacenews.com/viasats-inmarsat-acquisition-clears-all-regulatory-hurdles/

★ L3Harris wins $80 million Air Force contract for satcom experiments

The U.S. Air Force Research Laboratory awarded L3Harris Technologies a contract worth $80.8 million to conduct communications experiments using multiple commercial space internet services. **#L3Harris #US**

Link: https://spacenews.com/l3harris-wins-80-million-air-force-contract-for-satcom-experiments/

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