



SPACE CYBERSECURITY WEEKLY WATCH

Week 31

July 25 – 31, 2023

Timeframe : Weekly
of articles identified : 27
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**
- **THREAT INTELLIGENCE**
- **TRAINING & EDUCATION**
- **REGULATION**
- **TECHNOLOGY**
- ★ **IMPORTANT NEWS**

Overview

One of this week's highlights is the publication of the introductory report "Cybersecurity for Commercial Satellite Operations", NIST IR 8270. On the geopolitical front, the US government and the US Space Force are seeking cooperation with the rest of their European allies, including a proposed partnership around Anti-Satellite Attacks. A US-Italy summit also took place this week. Regarding satellite attacks, the US is challenged by China's rapid advances in space technology. New details of the Dozor-Teleport attack were published this week, and a new Russian attack on Brazilian satellites occurred. The attacker claims to have hacked into the cyber systems of INPE, the Brazilian research institute. Furthermore, this week Thales announced its participation in the European Galileo project with Quantum-Ready Cybersecurity measures. Quantum sensors is foreseen as a tool that will eventually replace GPS systems, according to research by the Naval Research Laboratory. For the European Commission, finding alternatives to GNSS is also a project for which tests are underway. Finally, on the market side, the EU, via EDF, has provided funding for 18 projects run by Leonardo. The EU has also awarded a contract to Spire as part of the Euralio project (within ARTES). CyberOps has won a major \$2.5 million contract with the Australian Department of Defense. In parallel, the Australian's Defense Research Funding Applications are currently open.

GEOPOLITIC

New STABCOM 'orbital warfare' exercise delayed towards end of year

The Space Force's first 'orbital warfare' exercise, called Star Wars, has been delayed from this summer towards the end of the year, according to Space Training and Readiness Command (STR) Chief of Staff Lt. Gen. Stephen Whiting.

[Link: https://spacenews.com/star-wars-exercise-delayed-towards-end-of-year/](#)

New Space : les enjeux de cybersécurité et de souveraineté (Fr.). New Space : cybersecurity and sovereignty issues

The challenges of cybersecurity in the space industry can be traced back to the complexity of satellite constellations and their occupation of the sky at different altitudes. An attacker will be more interested in attacking a satellite by cyber means than in destroying it, simply because this type of attack is anonymous and does not generate direct consequences.

[Link: https://www.esa.int/Enabling_Support/Space_Engineering_Technology/Space_Security/Space_Security/Space_Security](#)

Space Command nominee: U.S. has to prepare to respond to aggression against satellites

The U.S. military is being challenged to counter China's rapid advances in space technology, Lt. Gen. Stephen Whiting told the Senate Armed Services Committee. **#US #SPACECOM**

[Link: https://spacenews.com/space-command-nominee-u-s-has-to-prepare-to-respond-to-aggression-against-satellites/](https://spacenews.com/space-command-nominee-u-s-has-to-prepare-to-respond-to-aggression-against-satellites/)





AFI team wins AFCEA's annual writing contest on CSM

The Air Force Research Laboratory team took first place in the Armed Forces Communications and Electronics Association International's AFCEA's Cyber Writing Contest for 2023. The winning team is "Building the High Ground: A2C2 M2A2C2".

Link: <https://www.afceainternational.com/2023/07/25/afi-team-wins-afcea-annual-writing-contest-on-csm/>



Space summit Edoes Meloni: "new dialogue" Usa Italia (Trad.: Space Summit Edoes Meloni: "new dialogue" US Italy)

U.S. president and Italian premier reach agreement to strengthen cooperation on space security by promoting industrial partnerships between the two sides of the ocean with support from administrations. #July 2023

Link: <https://www.spaceconomy360.it/2023/07/25/spacesummit-edoes-meloni-usa-italia/>



★ Space Force Offering Europe Protection from Anti-Satellite Attacks

Chief of space operations Gen. Chance Saltzman expressed his support for defending European allied satellites against attacks and even warned that any destruction of a friendly satellite will be considered an act of war. Saltzman mentioned possible collaboration between Space Force and European partners revolving around equipment, training and policy, and added that such collaboration is much "less complicated" to plan and discuss compared to joint procurements.

#USSF #Cooperation

Link: <https://i-hls.com/archives/120122>



MARKET & COMPETITION

★ European Defence Fund, Leonardo si aggiudica 18 progetti: sul piatto 614 milioni (Trad.: European Defence Fund, Leonardo wins 18 projects: 614 million in the pot)

The Italian company won funding for research and development activities in 11 categories related to the fields of electronics, aircraft, cyber and space, leading, in particular, the Tiresyas (Technology Innovation for euRopEan radar SYstem ApplicationS) program. Five winning projects also feature investee companies: Telespazio, Larimart, Elettronica, MbdA Italia and Creo Consortium. #Leonardo #EDF

Link: <https://www.spaceconomy360.it/difesa-cybersecurity/european-defence-fund-leonardo-si-aggiudica-18-progetti-sul-piatto-614-milioni/>



Spain to develop CSM's independent aircraft tracking satellites for ESA

Spain will develop and operate a satellite surveillance system under a 16 million euro contract. The contract covers the development of the mission and system design, in addition to designing, developing, and operating a demonstrator to prove its performance and critical technologies. #Space #ESA

Link: <https://www.spaceconomy360.it/2023/07/25/spain-to-develop-csm-independent-aircraft-tracking-satellites-for-esa/>



18 Companies Chosen for Space Systems Command LEO Communications

Under a five-year, low-earth-orbit satellite-based services program that may be worth \$200 million, the Defense Information Systems Agency (DISA) and the U.S. Space Force's Space Systems Command have awarded 18 companies five-year contracts to establish commercial communications for military use. #Space #USAF

Link: <https://www.spaceconomy360.it/2023/07/25/18-companies-chosen-for-space-systems-command-leo-communications/>



Australia's CyberOps scores \$2.5 million space cybersecurity deal with Defense

Australia-based cybersecurity specialist CyberOps has secured a \$2.5 million deal with the Department of Defense to develop a dedicated cyber testing and training facility for Australia's space sector. #Cybersecurity #Australia

Link: <https://www.spaceconomy360.it/2023/07/25/australias-cyberops-scores-2-5-million-space-cybersecurity-deal-with-defense-2023/>



Defense Research Funding Applications Open

Applications are now being sought to receive funding from Defense Innovation Partnership's Collaborative Research Fund (CRF). Successful applicants will receive grants of up to \$10,000 to support genuine collaboration across government, academia and industry for early stage defense-related research, development and innovation. #Space #Australia

Link: <https://www.spaceconomy360.it/2023/07/25/defense-research-funding-applications-open/>





THREAT INTELLIGENCE

Satellites Are Logging Years Behind on Cybersecurity

New academic research sheds light on the practice of satellite manufacturers may be neglecting basic cybersecurity considerations in their haste to blast new satellites up into orbit. **Cybersecurity Watch**

Link: [Manufacturers' satellites are logging years behind on cybersecurity | MITRE](#)

Briefing 11: Russian Satellite Service Provider Dozor-Teleport Targeted by Cyberattack

Briefing about the Dozor-Teleport cyberattack. This attack represents the second major cyber incident affecting a satellite communications company; following the major disruption of a US satellite company in February 2022, when Viasat's KA-sat was disrupted at the onset of the Russian invasion of Ukraine. **#Cyberattack**

Link: <https://www.kratosdefense.com/constellations/space-isac>

Unhackable quantum satellite based QKD network now among China, Japan, United States, Canada, and EU

Quantum communication technology is considered to be unhackable and impossible to track. However long distance national quantum communication technology requires quantum satellite based communication networks. Many other countries like United States, Canada, Japan, Korea and some EU countries are all racing to develop quantum communication networks as they are actually unhackable. **Quantum Watch**

Link: [Quantum communication satellite network will be first to attack our most important data, experts say](#)

Was a Russian espionage satellite spyware compromised system (Trad.: How I hacked into Brazil's national institute for space research)

In this article you will learn about the process of detecting spy and hacker satellite operations, the process of their exploitation, and thanks to this, it will help to understand how to protect data from such attacks. **Hack Watch**

Link: [How I hacked into an orbital espionage satellite system | Hackers Weekly #17](#)

Hacker russo diz ter invadido satélites do INPE (Trad.: Russian hacker says he hacked INPE satellites)

A cybercriminal known as Samurai (from the Russian group SecDet) claims to have hacked into the cyber systems of INPE (National Institute for Space Research) last week. In addition to gaining access to confidential data, the attacker allegedly managed to access information from Brazilian satellites. **#Hacker #Russia #Brazil**

Link: <https://www.tecmundo.com.br/seguranca/266902-hacker-russo-diz-ter-invadido-satelites-inpe.htm>

TRAINING & EDUCATION

DEFCON 31 Talk Schedule

Schedule of the Defcon conference for the 10th and 11th of August 2023. **DEFCON**

Link: [https://www.defcon.org/defcon-31/schedule](#)

Space Cafe Radio – EUSPA Ep.01 – with Piotr Sitek

In this Space Café Radio – SpaceWatch.Global's Dr. Emma Gatti spoke with Piotr Sitek, governmental and new components, security governance officer in the security authority department of EUSPA. **#EUSPA #Podcast**

Link: <https://spacewatch.global/2023/07/space-cafe-radio-euspa-ep-01-with-piotr-sitek/>

Meet the Space Industry in Silicon Valley

The Silicon Valley Space Week is going to be held on October 17-20, 2023. This event will bring together over 200 speakers and more than 70 participants, including a large number of Silicon Valley players with an interest in space. **Space**

Link: [How to attend the Silicon Valley Space Week](#)

Acronspace Cybersecurity: Satellite Hacking

This course is meant for anyone who wants to learn more about space-related cybersecurity specifically in relation to satellite systems. An expert of any skill level who is interested in expanding their skill set in satellite communication and vulnerability analysis. **Cybersecurity Watch**

Link: [Acronspace Cybersecurity: Satellite Hacking](#)





REGULATION

★ Introduction to Cybersecurity for Commercial Satellite Operations

NIST Interagency Report (IR) 8270, Introduction to Cybersecurity for Commercial Satellite Operations, presents a specific method for applying the Cybersecurity Framework (CSF) to commercial space business and describes an abstract set of cybersecurity outcomes, requirements, and suggested controls. **#NIST #Cybersecurity**



Link: <https://csrc.nist.gov/pubs/ir/8270/final>

Argentina signs Artemis Accords

Argentina signed the U.S.-led Artemis Accords outlining best practices for space exploration part of a recent surge of countries joining the agreement. The Accords, rolled out in 2020, outline best practices and norms of behavior for space activities, building upon the Outer Space Treaty and other agreements. They address additional topics, such as exchange of scientific data and utilization of space resources. **#Argentina #ArtemisAccords**



TECHNOLOGY

One solution ID 6888 secures data for communications per satellite at conditions ID6888 (Final: Secure ID 6888 solution for satellite communications and ID6888 conditions)

The satellite network is a major part in many aspects. It is, for example, an essential element in building a global satellite network that operates in adverse conditions and under ID6888 conditions. This applies in particular to defense applications, where operations take place in difficult conditions, such as the distance of cable networks, line of sight jamming, etc.

Link: <https://www.cyberinflight.com/satellite-communications-secure-data-at-conditions-id6888/>

★ Thales announces Quantum-Ready Cybersecurity measures for Galileo

Thales's solution is set to be based on a scalable, flexible architecture, derived from its Cybels security supervision products, and equipped with big data capabilities. The objective is to protect the system against increasingly sophisticated threats, including the potential vulnerabilities introduced by quantum computing. **#Quantum #Galileo**



Link:

https://www.spacedaily.com/reports/Thales_announces_Quantum_Ready_Cybersecurity_measures_for_Galileo_999.html

Beyond Gravity to Provide Constellation On Board Computer to Quantum Space

Beyond Gravity, a leader in the space industry, announced it will provide its constellation on board computer with the Quantum Space's inaugural flight of its larger multi-purpose vehicle, which will take payload to geostationary and orbital orbits. **#Quantum #BeyondGravity**



Link: <https://www.beyondgravity.com/news/beyond-gravity-constellation-on-board-computer-quantum-space/>

Quantum Sensors Have Potential to Replace GPS

Work done by Naval Research Laboratory's research project Quantum Navigation Foundation for GPS, leading to the launch of GPS-3, the first satellite to transmit GPS signals in 2017. Using the GPS-3's location-based Quantum Navigation, Adam Black is among those adopting quantum sensors for an alternative navigation technique that provides GPS — inertial navigation. **#Quantum #GPS**



Link: <https://www.nrl.navy.mil/Research/quantum-navigation-quantum-sensors-have-potential-to-replace-gps/>

★ Backing Up GNSS

The Joint Research Centre of the European Commission tested seven advanced alternative sources of positioning navigation and timing (A-PNT) platforms through a performance assessment campaign, proving there are viable alternatives to GNSS available in the commercial market today. **#GNSS #EuropeanCommission**



Link: <https://insidegnss.com/backing-up-gnss/>

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