



SPACE CYBERSECURITY WEEKLY WATCH

Week 33

August 8 – 14, 2023

Timeframe : Weekly
of articles identified : 15
Est. time to read : 35 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**
- **TECHNOLOGY**
- **THREAT INTELLIGENCE**
- **REGULATION**
- **TRAINING & EDUCATION**
- ★ **IMPORTANT NEWS**

Overview

In this watch there aren't as many new articles in the field of space cybersecurity as in other weeks, and it's mainly US news, as there are several important conferences going on at the moment, such as Black Hat and Def Con. These two events have highlighted the need for cybersecurity on board satellites, via the Hack-A-Sat competition for Def Con and via a presentation by one of the researchers from Ruhr University Bochum in Germany for Black Hat. Also this week, DARPA decided to launch a new two-year competition to use artificial intelligence to help protect critical software and create new cybersecurity tools. Meanwhile, measures are being discussed in the US to protect commercial satellites. Another important piece of news this week is the release of the latest version of SPARTA, by the Aerospace Corporation. On the technological front, the Galileo project has developed an anti-spoofing service which will soon be available to the public. Japan has also launched a Quantum Cryptography Optical Communication Device.

GEOPOLITIC

DARPA, White House launch SSPA AI, cybersecurity challenge

The Defense Advanced Research Projects Agency (DARPA) and the White House have teamed up to announce a new two-year competition to use artificial intelligence to help protect critical software and create new cybersecurity tools to which DARPA is adding a cutting-edge high-stakes cybersecurity program: #HackTheSatellite #SpaceCyber

Link: <https://www.darpa.mil/press-releases/darpa-white-house-launch-sspai-cybersecurity-challenge>

U.S. intelligence agencies take steps to protect commercial satellites

The National Reconnaissance Office, the National Geospatial-Intelligence Agency and U.S. Space Command signed an agreement to improve threat intelligence sharing with commercial satellite operators. #Satellite #InformationSharing

Link: <https://spacenews.com/u-s-intelligence-agencies-take-steps-to-protect-commercial-satellite-operators/>

Irregular warfare in space is an ongoing threat - and the US must adapt

The war in Ukraine has proven how irregular warfare can work in the modern era. One of that modern forms operating in the "gray zone" when it comes to attacking and disrupting satellite systems, is the #CyberWarfare. US, Japan, Korea, and China are all working to adapt. #US #Military

Link: <https://www.defenseone.com/analysis/2023/08/irregular-warfare-space-ongoing-threat-us-must-adapt/230801/>

TECHNOLOGY

SPARTA, the latest in GPS anti-spoofing security

To further improve navigation reliability, the Aerospace Corporation, Galileo has developed the SPARTA anti-spoofing service which allows users and its equipment to receive signals from Galileo satellites to SPARTA (Secure Positioning, Authentication, Reliability, and Timing) service. Navigation Message Authentication (NMA) will soon be available for users and has security impact on the GPS timing phase. #SPARTA #Navigation

Link: <https://www.aerospacemission.com/2023/08/08/sparta-anti-spoofing-security/>



TECHNOLOGY

Japan takes global stage as QIPerfect announces successful launch of Quantum Cryptography Optical Communication System

QIPerfect 2023 Corporation announced the successful launch of the Quantum Cryptography Optical Communication System, which was built as the "Study and Development of Satellite-based Quantum Key Distribution (QKD) and Cryptography Technology in Satellite Communication" by the Minister of Internal Affairs and Communications (MIC), Quantum Cryptography

Link: [https://www.qiperfect.com/en/2023/08/08/qiperfect-announces-successful-launch-of-satellite-communication-system](#)



THREAT INTELLIGENCE



Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault

The cyberattack that crippled satellite communications on the eve of the Ukraine war was more broad than initially understood and carried out by attackers with detailed knowledge of the compromised system, an executive with Viasat, whose modems were targeted in the attack, revealed during a talk Thursday at the Black Hat cybersecurity conference in Las Vegas. **#Cyberattack #Viasat**

Link: <https://cyberscoop.com/viasat-ka-sat-hack-black-hat/>

Inside Russia's attempts to hack Ukrainian military operations

Security intelligence officials have revealed details to WH about an attempt by Russian state hackers to penetrate Ukrainian military planning and communications systems. **#Russia #Ukraine**

Link: [https://www.washingtonpost.com/technology/2023/08/11/russia-hack-ukraine-military-operations/](#)



Want to pwn a satellite? Turns out it's surprisingly easy

In a presentation at the Black Hat security conference in Las Vegas, Johannes Willbold, a PhD student at Germany's Ruhr University Bochum, explained he had been investigating the security of satellites. **#BlackHat**

Link: https://www.theregister.com/2023/08/11/satellite_hacking_black_hat/

For the first time, U.S. government lets hackers break into satellite in space

Hackers in a distant part of the world are getting a glimpse of cybersecurity at a U.S. government satellite in flight — and its exactly what the Pentagon wanted to happen. **#Space #Cybersecurity**

Link: [https://www.wired.com/story/2023-08-11-us-hackers-space-force-02-2023/](#)



A new era of space cybersecurity begins with Hack & Sat 4

Special edition of the world's top cybersecurity conference dedicated to telling you all about the revolutionary Hack & Sat competition. **#Space #Hack & Sat**

Link: [https://www.blackhathackingspace.com/cybersecurity-begins-hack-sat-4/](#)



REGULATION

SPARTA v1.4 – What's New?

The SPARTA framework offers space professionals a taxonomy of potential cyber threats to spacecraft and space missions, U.S. defense agencies and systems. **#SPARTA**

Link: [https://medium.com/@the-air-force/what-s-new-in-sparta-v1-4-what-s-new-3b9d7c0c0e0c](#)



📣 Release of SPARTA version 1.4 !

CyberInflight's analysis of the latest SPARTA version ! The evolution of SPARTA is a perfect illustration of how the cyber domain is increasingly taking into account the specificities of the space domain. This adaptation is carried out through multiple publications by NIST, MITRE and others. SPARTA is at the forefront of this trend and continues to include new elements to facilitate its use. **#SPARTA**

Link: <https://www.linkedin.com/feed/update/urn:li:activity:7095695005641490433>





TRAINING & EDUCATION

Hackers prepare to take on a satellite at DEF CON

Hackers at DEF CON will compete to break into a virtual satellite through a series of a hackathon the **Hack-A-Sat**

Link: <https://www.foxnews.com/tech/hackers-launch-cyberattacks-us-satellite-requested-pentagon>



The Cyber Satellite Threat with Mark Montgomery

Mark and I spoke with Mark Montgomery about the different physical and cyber threats faced by satellites and space systems. **What's Next?**

Link: <https://www.foxnews.com/tech/hackers-launch-cyberattacks-us-satellite-requested-pentagon>



Hackers launch cyberattacks against US satellite, requested by Pentagon

Hackers are competing to be the first to crack into a U.S. government satellite in a contest administered by the Pentagon. Officials with the Air Force and Space Force organized the Las Vegas competition to hack into a functioning satellite currently orbiting the globe, which will pay out a \$50,000 first prize. **#DEFCON #Hack-A-Sat**



Link: <https://www.foxnews.com/tech/hackers-launch-cyberattacks-us-satellite-requested-pentagon>

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