



SPACE CYBERSECURITY WEEKLY WATCH

Week 26

June 20 – 26, 2023

Timeframe : Weekly
of articles identified : 30
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
- MARKET & COMPETITION
- REGULATION
- THREAT INTELLIGENCE
- TECHNOLOGY
- TRAINING & EDUCATION
- ★ IMPORTANT NEWS

Overview

A number of significant news occurred this week. India and Ecuador signed the Artemis agreement. Also, Japan released its new space security strategy. Furthermore, Japan is considering the use of the Starlink constellation for its military communications. On the geopolitical front, the visit of Foreign Minister Dr Vivian Balakrishnan in Washington is a sign of a closer relationship between the US and Singapore. On the market front, SAIC was awarded a \$64 million contract by the SDA to build and maintain a cloud-based "application factory". Also, South Korea decided to invest 3.4 billion KRW in maritime and space security. Several cyberattacks took place this week. The first allegedly saw Compas Cable hacked by SiegedSec ransomware group. In the second, a Russian hacker posted an offer to sell access to a US military satellite. On the technology front, a new high-precision testing and operator training solution for cybersecurity in space has been launched. Also, a British partnership has begun to push the limits of quantum technologies in space.

GEOPOLITIC



Space Defence: Challenges for the French Space Command

Paper about the challenges for the French Space Command by French Space Commander. #CDE #France

Link: [https://www.defnat.com/pdf/cahiers/CAH098/15.%20Adam%20\(Paris%20Air%20Show%202023\).pdf](https://www.defnat.com/pdf/cahiers/CAH098/15.%20Adam%20(Paris%20Air%20Show%202023).pdf)



Minister for Foreign Affairs Dr Vivian Balakrishnan's Meetings in Washington D.C., 28 June 2023

During a visit to Washington D.C. on 28 June 2023, Minister for Foreign Affairs Dr Vivian Balakrishnan met with US Secretary of State Antony Blinken and US Deputy Secretary of State Kamala Harris. The two sides discussed the current state of space security and the need for further agreements. The Minister also met with US Under Secretary of State for Security Affairs, and the two sides discussed the current state of space security and the need for further agreements. #SingaporeMFA

Link: <https://www.mfa.gov.sg/newsroom/press-statements-statements-and-photos/2023/06/28/28-June-Meetings-in-Washington-DC>



The Evolution and Expanding Role of French Intelligence in Global Telecommunications Surveillance

In terms of global monitoring, the French intelligence community is expanding its reach to the world's largest American National Security Agency and the British GCHQ in telecommunications interception capabilities. #France

Link: <https://www.lesdevoirs.com/france/actualites/actualites-et-actualites/actualites-et-actualites/actualites-et-actualites>



South Arabia to establish institute for Global Cybersecurity Forum

South Arabia King Salman has issued an order to establish a new institute for the Global Cybersecurity Forum (GCF) in Riyadh, with the aim of enhancing the country's cybersecurity capabilities. #Cybersecurity #SaudiArabia

Link: <https://www.spa.gov.sa/en/1044444>





La Russie prête à partager son expertise en construction de satellites (Trad. Russia ready to share its satellite building expertise)

According to the CEO of the Russian space agency Roscosmos, Russia is ready to share its experience and expertise in satellite construction with its neighbors. South Korea, China and India are interested. **#Russia #Satellite**

Link: <https://www.space.com/53163-roskosmos-is-ready-to-share-its-satellite-building-expertise>



Japan's Self Defense Forces consider adopting South Korea's Starlink satellite service

Japan's military is reportedly considering the adoption of South Korea's Starlink satellite internet service as the country seeks to enhance its communication capabilities. While it is considered, there are also challenges such as integration with existing systems and infrastructure, compatibility with other communication networks, and cybersecurity concerns that will need to be thoroughly assessed. **#Japan #Starlink**

Link: <https://breakingdefense.com/2023/06/japans-self-defense-forces-consider-adopting-south-koreas-starlink-satellite-service/>



MARKET & COMPETITION

★ SAIC to build software app factory for Space Development Agency

The Space Force's Space Development Agency has tapped SAIC to build and maintain a cloud-based "application factory" to design, develop, test and deploy "cyber-resilient" battle management, command, control communications (BMC3) software for its planned satellites in low Earth orbit, according to SDA and company officials. The SDA contract is worth up to \$64 million over four years. **#SAIC #SDA**

Link: <https://breakingdefense.com/2023/06/saic-to-build-software-app-factory-for-space-development-agency/>



▲▲▲ AT&T Partners with Oneida Space Networks for Mission Critical Connectivity

Oneida Space Networks (OSN) and AT&T Intellectual Property have announced the signing of a memorandum of understanding (MOU) and a letter of intent (LOI) to bring a new level of high quality, secure, and reliable satellite connectivity to the government and defense sectors. **#ATandT #SpaceNetworks**

Link: <https://www.atandt.com/newsroom/2023/06/at-and-t-partners-with-oneida-space-networks-for-mission-critical-connectivity>



★ South Korea invests 3.4 billion won to boost maritime and space security

The South Korean government is providing 3.4 billion won (\$2.6 million) in funding for private companies as part of a pilot program to enhance security capabilities across maritime and space. **#SouthKorea #Investment**

Link: <https://thereadable.co/south-korea-invests-3-4-billion-won-to-boost-maritime-and-space-security/>



▲▲▲ One Network and SpaceOne Collaborate to Secure Spatial Data and Analytics for AgriTech Industry

One and SpaceOne announced a collaboration to unlock actionable intelligence and data from space for the benefit of sustainability efforts, beginning with the AgriTech industry. **#OneNetwork #SpaceOne**

Link: <https://www.onenetwork.com/news/2023/06/01/onenetwork-one-network-and-spaceone-collaborate-to-secure-spatial-data-and-analytics-for-agritech-industry>

REGULATION

▲▲▲ GNSSATCOM implementation continues to advance

The implementation of GNSSATCOM, Europe's Governmental Satellite Communications programme, continues to move forward. Recently, the European Commission adopted three implementing Acts. These Acts provide the legal foundation for the services that GNSSATCOM, along with GSC, will offer. **#GNSSATCOM #Space**

Link: https://www.ec.europa.eu/commission/press-materials/press-releases/ip-23-1000_en



▲▲▲ Ecuador signs Artemis Accords

Ecuador signed the governing instrument for the Artemis Accords for safe and sustainable space exploration. **#Ecuador #ArtemisAccords**

Link: <https://www.ecuador.gob.ec/ecuador-signa-acordos-artemis/>



★ Space Security in Japan's New Strategy Documents

This commentary looks at how Japan's space security policy will change in the future. **#Japan #SpaceStrategy**

Link: <https://www.csis.org/analysis/space-security-japans-new-strategy-documents>



▲▲▲ India signs Artemis Accords, tightening ties with US in space race with China

India has signed the Artemis Accords designed to set norms for exploration and exploitation of the Moon, Mars and potentially several other asteroids, in what Indian administration officials and experts say is a strategic tilt for US space. **#India #Artemis**

Link: <https://www.space.com/53163-india-signs-artemis-accords-tightening-ties-with-us-in-space-race-with-china>





THREAT INTELLIGENCE

The implications of the UK's National Space Strategy on special operations

The National Space Strategy (NSS) of the British Government is a testament to the critically and potential opportunities presented by space. This document positions Great Britain as a pioneering force within the international spacefaring community, showcasing the UK government's commitment to space exploration, technology, and research.

#UK #NationalSpaceStrategy

Link: <https://www.gov.uk/government/consultations/national-space-strategy>



Comcast Cable has been allegedly hacked by Singapore

The Singapore claims to have shut down that US satellite after saying this, withdrawing all logs and disconnecting the receiver.

#CyberAttack

Link: <https://www.hackread.com/singapore-hacked-comcast-cable/>



★ Military Satellite Access Sold on Russian Hacker Forum for \$15,000

A hacker active on a Russian-language hacker forum has posted an advertisement offering access for sale to a military satellite operated by Maxar Technologies. The hacker's claim suggests that the potential buyers could gain access to sensitive information regarding the US military and strategic positioning. **#Hacking #MilitarySatellite**

Link: <https://www.hackread.com/military-satellite-access-russian-hacker-forum/>



Q&A: Are Satellites Vulnerable to IoT Cyber Attacks?

As the use of IoT devices on the earth continues to grow, satellites will continue to be a concern for government and industry. What type of attacks to expect? Increase in quantity in the future. **#Cybersecurity #Satellite**

Link: <https://www.hackread.com/qa-are-satellites-vulnerable-to-iot-cyber-attacks/>

Why CISOs should be concerned about space based attacks

Space based data communications are reliable and useful tools for users, but they're also tempting targets for hackers and other hostile actors. CISOs and CEOs need to be aware of their organization's exposure. **#Cybersecurity**

Link: <https://www.hackread.com/why-ciso-should-be-concerned-about-space-based-attacks/>

Hackers Are Trying To Breach U.S. Space Satellite

Hack & Sat 4 will pit teams of hackers from all over the world against each other in a daily attempt to breach the satellite. **#Hack & Sat #Hacking**

Link: <https://www.government.com/hackers-try-to-breach-us-space-satellite/>



Satellite Security Showdown: DODCOM's Hack & Sat Competition Highlights the Rising Status of Space Based Cybersecurity

As industries from agriculture to banking increasingly depend on space based capabilities, safeguarding satellites from cyber threats has become paramount. In a groundbreaking move to address this, the U.S. military will stage Hack & Sat 4. **#Hack & Sat #Hacking**

Link: <https://www.government.com/satellite-security-showdown-dodcom-hack-sat-competition-highlights-the-rising-status-of-space-based-cybersecurity/>



Securing the Skies: The Importance of Satellite Based Cybersecurity

With the increasing reliance on technology, the threat of cyber attacks has become more significant than ever before. One area that has been gaining attention in recent years is satellite based cybersecurity. **#Cybersecurity #Satellite**

Link: <https://www.government.com/securing-the-skies-the-importance-of-satellite-based-cybersecurity/>



TECHNOLOGY

Chinese chips have made their way into US government agencies

It seems that Chinese (Taiwan) chips have made their way into US government agencies and international military organizations, as per a report by Wired. #China #Chip

[Link: https://www.wired.com/story/chinese-chips-into-us-government-agencies/](#)



True Anomaly launches new solutions to enhance cybersecurity in space

Space security company True Anomaly Inc. has today unveiled two new solutions that provide robust environments for high precision testing and operator training for cybersecurity in space. #Cybersecurity #Training

[Link: https://www.trueanomaly.com/news/true-anomaly-launches-two-new-solutions-for-space-cybersecurity](#)



SpiderOak demonstrates cybersecurity software on orbit

Cybersecurity specialist SpiderOak reported successful on-orbit testing June 22 of its OrbitSecure software running on a Ball Aerospace payload. #Cybersecurity #SpiderOak

[Link: https://spacenews.com/spideroak-demonstrates-cybersecurity-software-on-orbit/](https://spacenews.com/spideroak-demonstrates-cybersecurity-software-on-orbit/)



How can space quantum technology be advanced?

In partnership with the University of Bristol, the Southgate team is using recent developments in the fabrication and device integration of atom-trapped ions to advance space quantum technology. #Quantum

[Link: https://www.southgate.ac.uk/news/how-can-space-quantum-technology-be-advanced-14550](#)



Spacenet Demonstrates Groundbreaking Signal Simulator for LEO PNT Satellite Constellations

Spacenet demonstrated the first fully certified space satellite constellation signal simulator, SimSat, at the 2023 IEEE Aerospace Conference (AAS) in San Diego, CA from June 12-15, 2023. #PNT #Satellite

[Link: https://www.spacenet.com/news/2023/06/15/spacenet-demonstrates-groundbreaking-signal-simulator-for-its-leo-satellite-constellation](#)



Space Tech To Strive As The Limits Of Quantum Physics Are Tested On Earth And Beyond

Scientists are to build technologies to use and study nanoparticles in space – pushing the limits of quantum technologies. A UK wide consortium is developing technologies to use nanoparticles in state of the art sensors on small, medium sized satellites known as CubeSats. #UK #Quantum

[Link: https://www.ukri.ac.uk/news/2023/06/15/ukri-announces-space-tech-to-strive-as-the-limits-of-quantum-physics-are-tested-on-earth-and-beyond](#)



US Global Positioning Systems Under Threat: The Emerging Pegasus Could Take Over The GPS Role

The advent of the Global Positioning System (GPS) made navigating much simpler. All existing systems are satellite based and are in use not only by pilots in the air but also by drivers on the ground. #GPS #Pegasus

[Link: https://www.foxnews.com/global-positioning-systems-under-threat-the-emerging-pegasus-could-take-over-the-gps-role](#)



TRAINING & EDUCATION

ICSIW's Online™ Seminar: Space Asset Security and Resiliency

This seminar will discuss the status of cybersecurity within the space domain, past facts, attack vectors and mitigation approaches of experts. The seminar will also discuss the cyber security and space asset resiliency range and how it will be used to test and validate the assets' security and resiliency products. Finally, the seminar will identify the current state of cybersecurity space policies and standards. #Cybersecurity #Webinar

[Link: https://www.icsiw.com/online-seminar-space-asset-security-and-resiliency-2023/](#)

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