SPACE CYBERSECURITY WEEKLY WATCH

Week 35

August 22 – 29, 2023

Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.
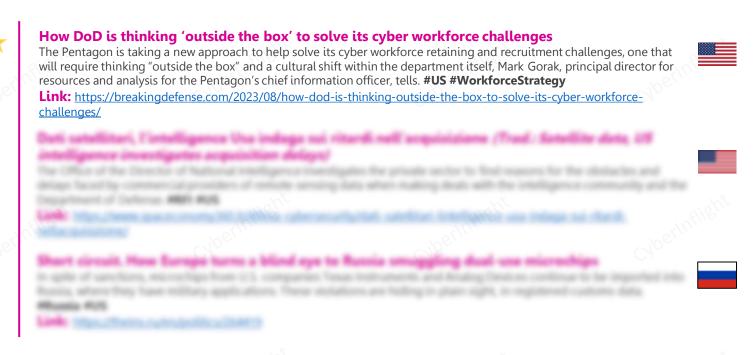
Timeframe : Weekly

# of articles identified : 19

Est. time to read : 35 minutes

- ■ **GEOPOLITIC**
- ■ **MARKET & COMPETITION**
- ■ **TECHNOLOGY**
- ■ **REGULATION**
- ■ **TRAINING & EDUCATION**
- ■ **THREAT INTELLIGENCE**
- ⭐ **IMPORTANT NEWS**

Overview

This week, the US DoD began proposing solutions to the problem of retaining and recruiting the cyber workforce. Also, an RFI has been set up by the US ODNI to find out the reasons for the obstacles and delays encountered by commercial companies when contracting with the DoD. On the market side, Eutelsat and OneWeb have voted and approved merger plans. The US government awarded a contract to Intelsat as well as to Mynaric. Finally, a consortium between ICEYE and PAR Government was awarded a multi-million dollars contract by the USSF. On the Threat Intelligence front, Australia has recognized space as a critical infrastructure and implemented several regulations to protect space assets. Also this week, Russia moved its spy satellite Luch/Olymp 2, and there has been a significant growth in jamming in the Middle East. On the subject of critical infrastructure, the US government agencies have published a guide entitled "Safeguarding the US Space Industry"

GEOPOLITIC

⭐
How DoD is thinking 'outside the box' to solve its cyber workforce challenges
The Pentagon is taking a new approach to help solve its cyber workforce retaining and recruitment challenges, one that will require thinking "outside the box" and a cultural shift within the department itself, Mark Gorak, principal director for resources and analysis for the Pentagon's chief information officer, tells. **#US #WorkforceStrategy**
Link: https://breakingdefense.com/2023/08/how-dod-is-thinking-outside-the-box-to-solve-its-cyber-workforce-challenges/

Dati satellitari, l'intelligence Usa indaga sui ritardi nell'acquisizione (Trad.: Satellite data, US intelligence investigates acquisition delays)
The Office of the Director of National Intelligence investigates the private sector to find reasons for the obstacles and delays faced by commercial providers of remote sensing data when making deals with the intelligence community and the Department of Defense. **#RFI #US**
Link: https://www.space.economy.it/cyber-cybersecurity/dati-satellitari-lintelligence-usa-indaga-sui-ritardi-nellacquisizione/

Short circuit: How Europe turns a blind eye to Russia smuggling dual-use microchips
In spite of sanctions, microchips from U.S. companies Texas Instruments and Analog Devices continue to be exported into Russia, where they have military applications. These violations are hiding in plain sight, in registered customs data. **#Russia #US**
Link: https://thebne.eu/sreplica/20473

1

MARKET & COMPETITION

Eutelsat and OneWeb board votes to seal merger plans
Eutelsat and key OneWeb shareholders are set to vote to seal the merger plans between te two international companies in an all-share transaction. According to reports, Eutelsat shareholders and OneWeb shareholders would each hold 50% of the Eutelsat shares. **#Eutelsat #OneWeb**
Link: https://spacewatchafrica.com/eutelsat-and-oneweb-board-votes-to-seal-merger-plans/

Intelsat Wins U.S. Defense Department Low Earth Orbit Satellite Opportunity
Intelsat, operator of one of the world's largest integrated satellite and terrestrial network, has been tapped to provide commercial satellite communications bandwidth, equipment and services to the U.S. Defense Department, as part of a 10-year Indefinite delivery, Indefinite quantity (IDIQ) U.S. Space Force contract. **#DoD #Satcom**
Link: https://www.satcom.digital/news/intelsat-wins-us-defense-department-low-earth-orbit-satellite-opportunity

Mynaric to design optical ground terminal for U.S. military constellation
SDA awarded Mynaric a two-year $3 million contract to design an optical ground terminal and demonstrate connections with space-based optical communications terminals. **#Mynaric #SDA**
Link: https://spacenews.com/mynaric-to-design-optical-ground-terminal-for-u-s-military-constellation/

PAR Government + ICEYE receive million$$$ USSF contract
PAR Technology Corporation announced their subsidiary, PAR Government Systems Corporation, in partnership with ICEYE, signed a prime contract award for the Proliferated Low Earth Orbit Satellite Based Services initiative led by the U.S. Space Force. The contract serves as a mechanism for satellite based services and capabilities to support all domains (space, air, land, maritime, cyber) with consistent, quality backed, low latency offerings. **#USSF #Contract**
Link: https://news.satnews.com/2023/08/24/par-government-iceye-receive-million-usd-contract/

TECHNOLOGY

Latest GPS/GNSS Products in 2023: August Edition
Global Positioning System (GPS) and Global Navigation Satellite System (GNSS) products are used in GPS/GNSS applications to determine precise positioning, navigation & timing (PNT) information, as well as used in GNSS testing purposes, GPS anti-jam function and other GPS/GNSS related purposes. **#GPS #GNSS**
Link: https://www.everythingrf.com/news/details/17593-latest-gps-gnss-products-in-2023-august-edition

REGULATION

US Agencies Call for Strengthened Cybersecurity in the Space Industry
The Federal Bureau of Investigation, the National Counterintelligence and Security Center (NCSC) and the Air Force Office of Special Investigations (AFOSI) released an advisory: Safeguarding the US Space Industry. The advisory recognizes the growing value of the global space economy and highlights the motivation for foreign intelligence entities to target the US space industry. **#Cybersecurity #SpaceIndustry**
Link: https://www.informationweek.com/security-and-risk-strategy/us-agencies-call-for-strengthened-cybersecurity-in-the-space-industry-
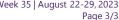
TRAINING & EDUCATION

Cyber Weapons Lab Online: Aerospace Cybersecurity & Satellite Hacking 101
On the 27th of August, join Angelina Tsuboi for an immersive online workshop "Aerospace Cybersecurity Satellite Hacking 101" where you will dive into the captivating world of satellite hacking while simultaneously discovering how to safeguard these crucial systems. **#Webinar #Cybersecurity**
Link: https://www.meetup.com/hushcon-meetups/events/295363996/?isFirstPublish=true

Webinar by Coditing on « Unlocking the cosmos – Journey into satellite pentesting »
Webinar on the intricacies of satellite technology and its vital connection to the world of cybersecurity.
#Satellite #Cybersecurity
Link: https://www.linkedin.com/posts/coditing_india-innovation-management-activity-7100707776443613184-gUu1/

THREAT INTELLIGENCE

Space systems as critical infrastructure assets – understanding the security obligations for space assets

The increasing reliance on space-based assets for navigation, communications, and remote sensing makes space infrastructure an attractive target for malicious cyber actors. With the democratisation of space and rapid growth of the commercial space industry, the Australian government has over the years stepped up the regulatory governance of Australia's critical infrastructure to manage strategic risks facing these assets. **#Australia #CriticalInfrastructure**

Link: https://hwlebsworth.com.au/space-systems-as-critical-infrastructure-assets-understanding-the-security-obligations-for-space-assets/

An Insider's Look at DEF CON's First On-Orbit Hacking Competition

Article by Robert McClellan about his experience at this year's Hack-A-Sat competition. **#Hack-A-Sat**

Link: https://www.bradadefcon.com/constellations/articles/an-insiders-look-at-def-cons-first-on-orbit-hacking-competition

Combat operations of Russian EW equipment boosts export demand — arms export agency

According to Rosoboronexport CEO Alexander Mikheev, Russian electronic warfare systems demonstrated their excellent performance during the special military operation. **#TASS #Russia**

Link: https://tass.com/defense/1661282

Spies and hackers are targeting the US space industry: report

U.S. intelligence agencies have issued a warning about foreign spies targeting the American space industry as well as cyberattacks against the nation's satellite infrastructure. **#US #Cyberattack**

Link: https://www.space.com/us-government-warning-space-industry-satellite-hacking

Russia has relocated its stalker satellite Luch/Olymp 2

Russia has relocated its stalker satellite Luch/Olymp 2 (2023-031A) to 8.9°E. This is in the immediate vicinity of Eutelsat 8A-SAT 5A (whose users were subject to the famous cyber attack bricking their modems on the eve of the Russian invasion of Ukraine) and Eutelsat 9B which besides 60 Ku-band/transponders carries a laser communication terminal (LCT) providing optical relay services to the European Commission's Sentinel earth observation satellites. **#Russia #Satellite**

Link: https://twitter.com/Marco_Langbroek/status/1694012129620016

The Critical Importance of Cyber Securing ISRO's Space Missions

With the technology, IT infrastructure, and software required to achieve this giant leap, assessing these missions from a cybersecurity perspective is critical. Space may be the "final frontier" for exploration, but it is also ripe for exploitation and is particularly susceptible to a range of cyber vulnerabilities and threats. **#ISRO #Cybersecurity**

Link: https://www.cnp.io.com/blog/the-critical-importance-cyber-securing-isros-space-missions/

Huge increase in Middle-East Jamming

The middle-east, long a hot spot for jamming, has seen a significant increase since the end of May. **#Jamming #MENA**

Link: https://www.skai-ai.com/pulse/huge-increase-middle-east-jamming-dana-goward/

Huge cyberattack disables telescopes in Hawaii and Chile

National Science Foundation funded telescopes in Chile and Hawaii have been the victim of a curious cyberattack, closing operations at many of them. **#Cyberattack #Telescopes**

Link: https://interestingengineering.com/science/hawaii-chile-nsf-telescopes-cyberattack