



SPACE CYBERSECURITY WEEKLY WATCH

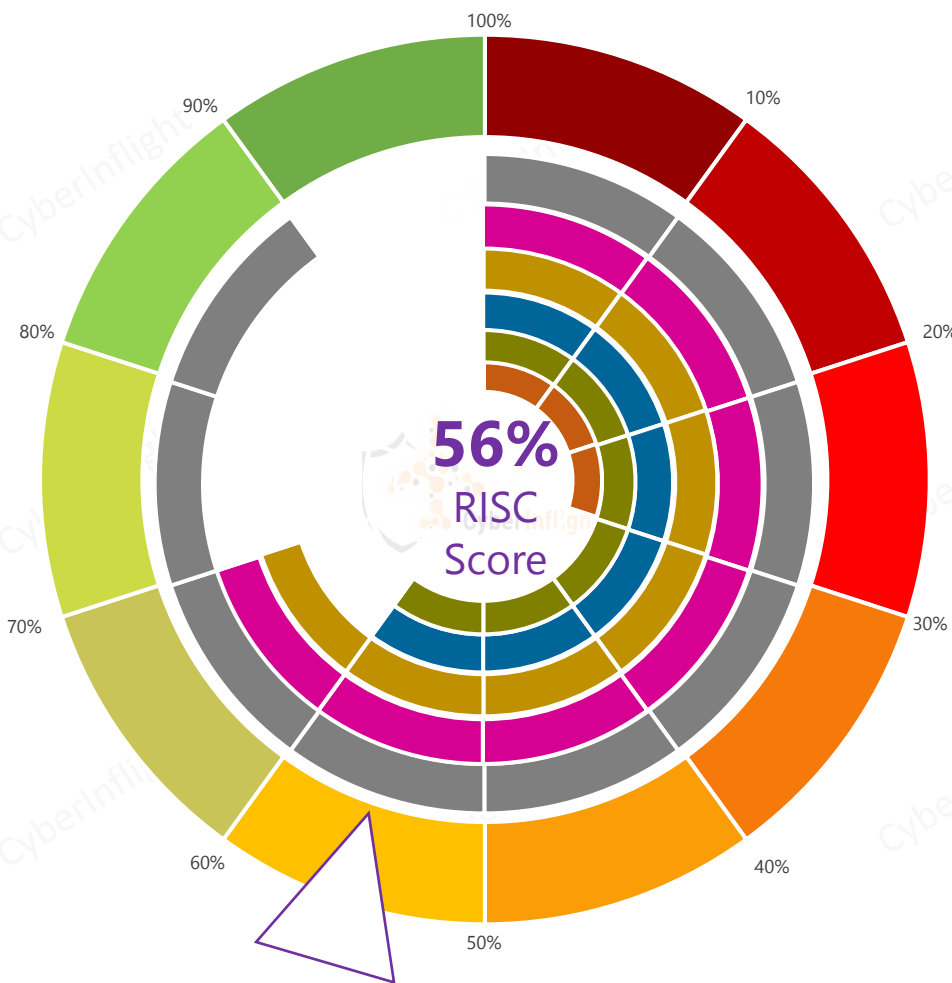
Week 41

October 3 – 9, 2023

Timeframe: Weekly
of articles identified: 40
Est. time to read: 1 h 30 min

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
- MARKET & COMPETITION
- THREAT INTELLIGENCE
- TRAINING & EDUCATION
- REGULATION
- ★ IMPORTANT NEWS



Overview & RISC Score

This week's RISC score is 65% for several reasons, the first one being the launch by EUSPA and DG DEFIS of a Call for Expression of Interest for the creation of an EU Space ISAC. This Call for Interest must be completed by November 3, 2023, for those interested in becoming founding members, but it will be possible to apply to become a member of the EU Space ISAC until October 31, 2025.

Also on the regulatory front, the DoD, GSA and NASA are currently examining how to implement new revisions to the Federal Acquisition Regulation (FAR) to standardize cybersecurity requirements for government contractors.

Meanwhile, Booz Allen won a contract with the USSF to support Space Systems Command's Program Executive Office for Space Sensing.

On the Market Intel front this week, several contracts with US authorities were won, and an ESA Call for Proposal is underway for the 4S mission.

On the Threat Intel front, there were several attacks this week, more than we've reported in recent weeks. One of these was an attack on Infrastat which was asked for \$60,000 not to disclose sensitive data.

On the technology front, the US DoT is looking for industry insight on how to best complement and support its PNT functions with new technology that does not depend on traditional GPS tech.

Lots of Training & Education news this week, including the BE-CYBER Conference on October 26 and the launch of a two-day workshop on Cybersecurity Principles for Satellite and Space Systems by Tonex.



GEOPOLITIC



Reinforcing European space autonomy with the EU Space Information Sharing Centre (ISAC)

Launch by EUSPA and the DG DEFIS, a Call for Expression of Interest for the new #EUSpace ISAC (Information Sharing Analysis Centre). The ISAC will serve as the primary communication channel for the #EUSpace sector regarding security-related information and sharing of best practices. It will be a membership-driven platform looking to engage industry, public sector and academia. #EUSPA #SpaceISAC #CallforInterest

Link: <https://www.euspa.europa.eu/newsroom/news/reinforcing-european-space-autonomy-eu-space-information-sharing-centre-isac>



Taiwan ramps up backup satellite network plans in island defense strategy

Taiwan is developing a backup satellite network to ensure its communications plans with the outside world in the event of a crisis. #Taiwan #Space #Military

Link: <https://www.scoop.international.com/2023/10/03/taiwan-ramps-up-backup-satellite-network-plan-2023-defense-strategy/>

ISRO chairman calls for strong cybersecurity knowledge base

Indian Space Research Organisation (ISRO) Chairman, S. Somnath has called for a strong cybersecurity understanding and knowledge base to ensure the security of the nation. #ISRO #Cybersecurity

Link: <https://www.isro.gov.in/News-Events/Chairman-calls-for-strong-cybersecurity-knowledge-base-2023-10-03>

TECHNOLOGY



DoT Looking For Industry Input on GPS Tech Alternatives

The U.S. Department of Transportation (DOT) is looking for industry insight on how to best complement and support its Positioning, Navigation, and Timing (PNT) functions with new technology that does not depend on traditional Global Positioning System (GPS) tech. #DoT #RFI

Link: <https://www.meritalk.com/articles/dot-looking-for-industry-input-on-gps-tech-alternatives/>



Technicians test the satellite use of super cloud Leonardo Galileo (Prod. Data transfer between satellites off to the Leonardo Galileo super cloud)

Leonardo will be the first company in the aerospace, defense and security industry to use the geo-distributed cloud technology developed by Galileo, a kind of "cloud" that is super-protected from cyber attacks and natural disasters, with over the replication of some next-generation designs, such as data transfer between satellites. #Leonardo #Cybersecurity

Link: <https://www.aerospace.com/leonardo-technicians-test-the-satellite-use-of-super-cloud-leonardo-galileo>

The University of Alabama in Huntsville demonstrates cybersecurity software aboard a Lockheed Martin technology demonstrator CubeSat

The University of Alabama in Huntsville has announced that it developed a cybersecurity software for the U.S. Army Space and Missile Defense Command. The software began performance testing on one of Lockheed Martin's space upgrade satellite system (SM-160) technology demonstrator CubeSat. The software, Small Satellite Sentinel, is an intrusion detection system designed for small satellites. #UniversityofAlabama #LockheedMartin

Link: <https://www.uah.edu/news/2023/for-university-of-alabama-in-huntsville-demonstrates-cybersecurity-software-aboard-a-lockheed-martin-technology-demonstrator-cubesat>

Russian Cyberwarfare at Space & S-400 Capabilities

S-400 are primarily designed to be computerized defense against aerospace security threats to undermine the cybersecurity within S-400 changes the shape of the war, and dominance of space technology, dynamics of the conflict. War changed with space and cyber and electronic warfare cyber attacks to cyber security of S-400 as defense mode system is provided. #Russia #CyberWarfare

Link: <https://www.intel.com/resources/journals/space-s-400-capabilities-by-ivan>

ISRO focused on developing onboard cyber technology for spacecraft

The Indian Space Research Organisation (ISRO) is taking proactive steps to address the growing threat of cyber attacks by developing onboard cyber technology. ISRO Chairman S. Somnath unveiled the strategic initiative during his keynote address. #ISRO #CyberTechnology

Link: <https://www.isro.gov.in/News-Events/ISRO-Chairman-S-Somnath-unveils-strategic-initiative-during-keynote-address-2023-10-03>



MARKET & COMPETITION



Leonardo, Congelanti: "Cybersecurity e Spazio i due pilastri del nuovo piano industriale" (Frank)
Leonardo, Congelanti: "Cybersecurity and Space the two pillars of the new business plan")
Cybersecurity and Space are the two pillars of Leonardo's business plan to be unveiled early 2024. This was anticipated by CEO Roberto Congelanti on the sidelines of the January 10 CyberTech Europe 2023. **Leonardo Cybersecurity**
Link: <https://www.leonardocorporation.it/it/area-azienda/leonardo-espone-cybersecurity-e-spazio-i-due-pilastri-del-nuovo-piano-industriale>



Booz Allen nabs \$630M integration contract for Space Force missile warning, weather programs
The contract, will support Space Systems Command's Program Executive Office for Space Sensing, which is responsible for the service's missile warning, weather monitoring and "persistent tactical surveillance" programs, according to a Space Force fact sheet. Disciplines include but are not limited to: Cybersecurity, Architecture/Design, Integration Planning & Execution, Test & Evaluation, Technical Baseline Management, Risk Management, Digital Engineering & Modeling Simulation & Analysis. **#BoozAllen #USSF**
Link: <https://breakingdefense.com/2023/10/booz-allen-nabs-630m-integration-contract-for-space-force-missile-warning-weather-programs/>



Cybersecurity As Enabler For Secure Satellite Communications And Resilient Applications
This new Space Systems for Safety and Security (SS3) Call for Proposals aims to foster the development of innovative satellite communications technologies, products, systems and downstream applications which address these challenges. **SS3 Call for Proposals (CFP)**
Link: <https://www.nasa.gov/press/20231001/nasa-announces-call-for-proposals-for-space-systems-for-safety-and-security/>



MOBATEMS and DHS Digital Solutions Partnership
MOBATEMS entered into partnership with DHS Digital Solutions for advancements in DHS security technologies. The partnership enables a stronger synergy in DHS security, especially in dealing with jamming and spoofing. **DHS Partnership**
Link: <https://www.mobatems.com/news/2023/10/01/mobatems-partners-with-dhs-digital-solutions/>

Spain: Iberdrola se contracta de filiar en Occidente, según le nombraron (Frank)
Spain: Iberdrola wins a regional industry contract in Occidentia, after the digital sector
In addition to supporting the 5G/6G roll in the digital sector in Occidentia, through the launch of 5G projects in areas such as artificial intelligence and cybersecurity, the challenge of this contract will be to train more people in the professions that make up the sector. **Iberdrola Contract**
Link: <https://www.iberdrola.com/actualidad/2023-10-01-iberdrola-contrata-un-contrato-de-filial-en-occidentia-despues-de-digital/>



US Army Set For Elon Musk's SpaceX 'Starshield' Trials; USAF To Become 1st Unit To Adopt The System
A Space Force spokesperson officially confirmed the contract, valued at \$18.75 million, and spanning a one-year duration. The collaboration marks a notable step for the military branch engaging with the private sector to advance its capabilities in space operations. **Starshield Military**
Link: <https://www.spaceforce.mil/News/2023-10-01-us-army-set-for-elon-musk-spacex-starshield-trials-usaf-to>



CACI awarded million\$111 AFRL contract to advance CSIR
Under the contract, CACI will implement agile and adaptable processes to develop mission software and data analysis capabilities to advance and modernize command, control, communications, computers, cyber, intelligence, surveillance, and reconnaissance (C3IC2) programs. These capabilities will enhance information dissemination and decision making across the U.S. Air Force and intelligence community, improve information security, and meet program mission objectives. **CACI AFRL**
Link: <https://www.cacigroup.com/2023/10/01/caci-awarded-million-111-afml-contract-to-advance-csir/>





THREAT INTELLIGENCE

Addressing Canada's Exposure to Space Cyber Threats

Report by the Center for International Communications Innovation about Canada's exposure to Space Cyber Threats by Cyber Threats: #Canada #Space #CyberThreats

[Link: https://www.cicim.org/publications/CIIC%20-%2017.html](#)



ISACA sets up panel to check GPS spoofing in Indian airspace

Directorate General of Civil Aviation (DGCA) has constituted a committee for monitoring Global Navigation Satellite System spoofing in Indian airspace. The committee will study various incidents of GNSS interference such as spoofing, jamming. The DGCA office stated in an order issued on Wednesday. #India #Spoofing

[Link: https://www.bbc.com/news/technology-66812141](#)



Russian Jamming Causing As Much Anxiety as Protection?

John Whisman on 8 Twitter relayed comments from Russian pilots of small aircraft and others worried about flying and being in and around Moscow. #Russia #Jamming

[Link: https://theflight.org/2023/10/08/russian-jamming-causing-as-much-anxiety-as-protection/](#)



Attack of B2E Systems by Hackers

The post states that the hackers from their threat actor targeted the website of B2E Systems, a defense and space organization based in the UK. The post includes two links as proof of the website's downtime. The post was published on Telegram and includes information about the victims, including the countries affected, organizations targeted, websites impacted, and the industry involved. The category of the attack is identified as a DDoS attack. The post also includes a link to the original source. #B2ESystems #Hackers

[Link: https://www.cicim.org/2023/10/08/](#)



Russian Launch (Dymov) 2 Satellite Approaching Multiple GPS Satellites

In recent days, Starlink's machine learning based object profiling engine has identified multiple maneuvers by the new Launch (Dymov) 2 satellite that are highly reminiscent of the behavior exhibited by its predecessor – suggesting that perhaps Launch (Dymov) 2 is now picking up where Launch (Dymov) 1 left off. #Satellite #Russia

[Link: https://theinformationsec.com/2023/10/08/](#)



Hackers threaten Infracast with demand of 60 thousand USD to not disclose sensitive data

Infracast, a telecommunications company, was the victim of a computer attack last week, as determined by an internal source to the newspaper Valor Económico. #Infracast #Ransomware

[Link: https://www.menosfios.com/en/hackers-ameacam-infracast-com-exigencia-de-60-mil-usd-para-nao-divulgar-dados-sensiveis/](https://www.menosfios.com/en/hackers-ameacam-infracast-com-exigencia-de-60-mil-usd-para-nao-divulgar-dados-sensiveis/)



Major Cyber Incident EA SAT 56

Report analyzing the EA SAT 56 incident by European Repository of Cyber Incidents. #CyberAttack #Report

[Link: https://www.eu-cyber.eu/en/2023/10/08/ea-sat-56-incident-report/](#)



Starlink Account Hacking Sparks Calls for Multi-Factor Authentication

Starlink's Starlink features a 2FA (two-factor authentication) but unfortunately it doesn't offer a built-in multi-factor authentication (MFA) for user logins. The security gap is coming under scrutiny following several incidents involving hackers breaking into Starlink user accounts to make fraudulent charges. #Starlink #Hacking

[Link: https://www.cicim.org/2023/10/08/starlink-account-hacking-sparks-calls-for-multi-factor-authentication/](#)



ISRO fights over 100 cyber attacks every day, reveals chairman Somanath

The Indian Space Research Organisation (ISRO) is facing more than 100 cyber attacks daily, its chairman Somanath revealed here on Saturday. #ISRO #CyberAttacks

[Link: https://www.cicim.org/2023/10/08/isro-fights-over-100-cyber-attacks-every-day-reveals-chairman-somanath-on-sat/](#)



Attack of Rafael Advanced Defense Systems by Green Team

The post states that the cyber threat actor targeted the website of Rafael Advanced Defense Systems, an Israeli organization in the defense and space industry. The post provides proof of downtime for the website and includes a link to a report confirming the attack. The information was published on Telegram by the cyber threat actor. #Rafael #Hackers

[Link: https://theinformationsec.com/2023/10/08/](#)





TRAINING & EDUCATION

Protecting the Space Economy: Cyber Defenses and National Security

This article is part of the US Cyber Future Space Economy editorial series. In Part 1 of this discussion, we discuss the legal framework and policies needed to protect the future space economy. Part 2 of the discussion will focus on the software, tools, and technological solutions needed to protect space interests. #Protect #SpaceEconomy

[https://www.cyberinflight.com/blog/2023/10/protecting-the-space-economy-cyber-defenses-and-national-security/](#)

Building more cyber resilient satellites begins with a strong network

How might we effect the importance of a strong space cybersecurity posture right from the start of satellite management and development? Cybersecurity for satellites begins with the design of an endpoint. In the case of satellites, they need to be able to work from the start to end of their life cycle. From the start of applications to mission they are the ultimate end-to-end solution. #Satellite #Cybersecurity

[https://www.cyberinflight.com/blog/2023/10/building-more-cyber-resilient-satellites-begins-with-a-strong-network/](#)



Cybersecurity Principles for Satellite and Space Systems | Training Workshop

Cybersecurity Principles for Satellite and Space Systems, Training Workshop is a 2-day interactive workshop designed to provide a unique learning experience on space and satellite vulnerabilities that are commonly exploited. Participants will discover techniques and strategies for integrating cybersecurity measures into space and SATCOM systems, networks, products and critical missions from the start. #Workshop #SpaceCybersecurity

[Link: https://www.tonex.com/training-courses/cybersecurity-principles-for-satellite-and-space-systems-training-workshop/](https://www.tonex.com/training-courses/cybersecurity-principles-for-satellite-and-space-systems-training-workshop/)



Global defense and space program kicks off

The first round of the current of Australia's new Global Security Hub in Defense and Space, a program specially designed to build highly qualified talent across the AUKUS alliance. #Australia #Cyber

[https://www.cyberinflight.com/blog/2023/10/global-defense-and-space-program-kicks-off/](#)

ISS workshop about the "Secure Communications via Satellite: Regulation and Technology"

Join the next workshop about "Secure Communications via Satellite: Regulation and Technology" hosted by ISSA in 2024 at the ISSA HQ on October 20-21. #Workshop #Satellite

[https://www.cyberinflight.com/blog/2023/10/iss-workshop-about-the-secure-communications-via-satellite-regulation-and-technology/](#)

SPACEMAX 2023: Cybersecurity Edition

Competition by the University of Canberra on October 17-18, 2023. This hackathon's challenge has six focus areas, five of which address a unique aspect of space cybersecurity and one representing a wild and open challenge. They are looking for innovations that can be turned into viable space tech, cyberspace tech, business or can be offered to existing companies. #SpaceHack #Competition

[https://www.cyberinflight.com/blog/2023/10/spacemax-2023-cybersecurity-edition/](#)



Space grand challenge: satellite week October 18-21, 2023

The Space Grand Challenge 2023 Program is a global virtual game-based cybersecurity competition for middle and high school students built by Cal Poly SLO. #CalPoly #Competition

[https://www.cyberinflight.com/blog/2023/10/space-grand-challenge-satellite-week-october-18-21-2023/](#)



NSS 2023 - SpaceSec Highlights

Recap of the Session 4: Workshop about Security of Space and Satellite Systems which takes place at the Network and Distributed System Security (NDSS) Symposium 2023, 27 February - 3 March 2023 in San Diego, California. #NDSS #SpaceSec

[https://www.cyberinflight.com/blog/2023/10/nss-2023-spacesec-highlights/](#)



Top ISSO, NATO officials to share knowledge on cybersecurity of space in India

Indian Space Research Organisation (ISRO) Chairman, National Space Research Organisation Chairman, Australian Space and National Cyber Security Coordinator or General M. A. P. will be among the prominent speakers at the 10th edition of the conference which will be held from October 4 to 7. #ISSO #Conference

[https://www.cyberinflight.com/blog/2023/10/top-issso-nato-officials-to-share-knowledge-on-cybersecurity-of-space-in-india/](#)



Space remains vulnerable to cyber attack

Interview of Professor de Oliveira, a leader and PhD candidate at Florida University, about how space remains vulnerable to cyberattacks and how to change that. #Research #Space #Cybersecurity

[https://www.cyberinflight.com/blog/2023/10/space-remains-vulnerable-to-cyber-attack/](#)





Satellite Open Source Intelligence with ChatGPT

A quick video about using ChatGPT to generate your satellite open source intelligence gathering methodology using Open Source Intelligence (OSINT).

Link: [https://www.youtube.com/watch?v=3W15v0G1p78](#)

A Decade of Cybersecurity Challenges and Solutions for Satellite Systems

This article delves into the dynamic landscape of cybersecurity threats on satellites over the last ten years, shedding light on the escalating risks faced by these indispensable space assets. The exploration not only highlights the existing threat landscape but also offers insights into the vulnerabilities and countermeasures that define the contemporary satellite cybersecurity landscape. #Satellite #Cybersecurity

Link: [https://www.linkedin.com/pulse/cybersecurity-satellite-systems-rob-ross](#)



BE-CYBER Experience Sharing Day

Conference on the 26th of October, 2023, in Brussels about Security in Space #Conference #BE-CYBER

Link: <https://be-cyber.be/>



REGULATION

'Government must lead' on 5G - UK Preparedness Commission Report

For the first time, the UK's 2022 National Risk Register (NRR) includes a warning on the risks from a loss of provision of 5G services. The previous NRR only highlighted the risk to provision and timing services from satellite space assets. This wider recognition is a welcome and important step in government leadership and national preparedness. A government announcement is anticipated with further details. #UK #5G

Link: [https://www.parliament.uk/business/committees/committees-a-z/commons-select/preparedness-commission/pages/5g-services-are-critical-to-uk](#)



Agencies Looking to Standardize Cyber Requirements for Federal Contractors

The Department of Defense (DoD), the General Services Administration (GSA), and NASA are looking to implement new revisions to the Federal Acquisition Regulation (FAR) to standardize cybersecurity requirements for government contractors. The proposed rule, published in the Federal Register today, would develop standardized contract language for unclassified Federal Information Systems (FIS) and help to mitigate any potential risks associated with having no streamlined requirements. #US #CyberRequirements

Link: <https://www.meritalk.com/articles/agencies-looking-to-standardize-cyber-requirements-for-federal-contractors/>



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