



# SPACE CYBERSECURITY WEEKLY WATCH

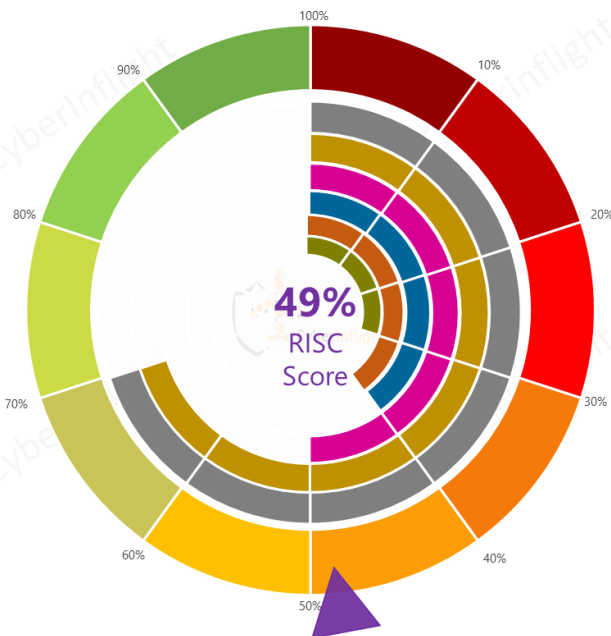
Week 43

October 17 – 23, 2023

Timeframe : Weekly  
# of articles identified : 26  
Est. time to read : 45 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
- MARKET & COMPETITION
- TECHNOLOGY
- THREAT INTELLIGENCE
- TRAINING & EDUCATION
- REGULATION
- ★ IMPORTANT NEWS



## Overview & RISC Score

This week's RISC score is 49%. There are several reasons for this score, including the publication by the UK of a PNT framework to protect critical infrastructures from satellite data disruptions.

Also this week, the USSF expressed its desire for closer collaboration with its allies, particularly in the event of shared threats.

On the market front, SDA signed a contract with SpiderOak to research the use of the company's software to protect ground systems that control military satellites.

ISRO is moving ahead with quantum technologies, with the ambition of creating hack-proof satellite communication, based on QKD or Quantum cryptography.

As for the threat intel this week, a second Russian Luch/Olymp satellite is now trailing Western systems in orbit.

Finally, the VOSS conference, organized by Space ISAC from October 17 to 20, highlighted the value of satellites as crucial infrastructure that forms the backbone of the modern digital economy and enables services critical for everyday life.





## GEOPOLITIC



### U.S. Space Force seeks to work closer with allies in face of shared threats

The procurement arm of the U.S. Space Force is making a major push to work more closely with allies abroad and is pressing the Pentagon to adjust classification policies to allow for more open sharing of information with trusted international partners. In this effort, for the first time, the U.S. will sell a satellite jammer known as Counter-Communications System to Australia. **#USSF #Allies**

**Link:** <https://spacenews.com/u-s-space-force-seeks-to-work-closer-with-allies-in-face-of-shared-threats/>



### 'Space war' between US and Russia looms with satellite and spacechip attacks

According to General Thomas Siffert, the Chief of Space Operations for the US Space Force, the space environment between the US and Russia is becoming a prime area for military competition. General Siffert warns that, as competition for space and the United States grows for control of space, the chances of other conflicts will increase. **#US Space Force**

**Link:** <https://spacenews.com/space-war-between-us-and-russia-looms-with-satellite-and-spacechip-attacks-in-cyber-war/>



## MARKET & COMPETITION



### Space Development Agency to evaluate SpiderOak cybersecurity software

The cybersecurity firm SpiderOak has signed an agreement with the U.S. Space Development Agency to research the use of the company's software to protect ground systems that control military satellites. **#SDA #SpiderOak**

**Link:** <https://spacenews.com/space-development-agency-to-evaluate-spideroak-cybersecurity-software/>



### Partnership leads to the stars to improve cybersecurity

A new partnership between IBM Cyber Security, a U.S. information data company, Space, and the University of South Florida is looking to the stars, literally, to create more secure and efficient communications.

**Partnership**

**Link:** <https://www.ibm.com/pressroom/en/pressreleases/ibm-to-the-stars-to-improve-cybersecurity>



### Observations della terra: Thales Alenia Space, Esa e Egit insieme nella Mission (Food) Earth observation: Thales Alenia Space, Esa and Egit together on Mission

The partnership aims to counter the threat of falsifying satellite images (FSS) with the help of artificial intelligence.

**Link:** [https://www.esa.int/Enabling\\_Support/Space\\_Education/ESA\\_and\\_Thales\\_Alenia\\_Space\\_together\\_on\\_Mission](https://www.esa.int/Enabling_Support/Space_Education/ESA_and_Thales_Alenia_Space_together_on_Mission)



### Cybersecurity as Enabler for Secure Satellite Communications and Resilient Applications

The new space systems for safety and security (SS) Call for Proposals aims to foster the development of innovative satellite communications technologies, products, systems and downstream applications which address these challenges.

**Link:** [https://www.esa.int/Enabling\\_Support/Space\\_Education/ESA\\_and\\_Thales\\_Alenia\\_Space\\_together\\_on\\_Mission](https://www.esa.int/Enabling_Support/Space_Education/ESA_and_Thales_Alenia_Space_together_on_Mission)



## TECHNOLOGY



### Securing the Final Frontier

While the Cyber Space Operations Program, maintaining the collaboration between space technology and cybersecurity. **Space Cybersecurity**

**Link:** [https://www.esa.int/Enabling\\_Support/Space\\_Education/ESA\\_and\\_Thales\\_Alenia\\_Space\\_together\\_on\\_Mission](https://www.esa.int/Enabling_Support/Space_Education/ESA_and_Thales_Alenia_Space_together_on_Mission)

### How India plans to make satellite communication hack-proof

The Indian Space Research Organisation (ISRO) aims to launch a satellite with ultra-secure quantum communication capabilities. The system is expected to be impenetrable by hackers. The satellite, based on Quantum Key Distribution (QKD) or quantum cryptography, will contribute to the creation of a communication network, which connects quantum computers processing information in unison. The agency is yet to announce a launch date. **#ISRO #QKD**

**Link:** <https://www.nature.com/articles/d44151-023-00155-4>





# THREAT INTELLIGENCE



## Second Russian Luch/Olymp satellite now trailing Western systems in orbit

Much like its predecessor launched nearly a decade ago, Russia's second Luch/Olymp satellite is stalking Western satellites across geosynchronous Earth orbit (GEO), according to private sector space watchers. **#Russia #Luch/Olymp**

**Link:** [https://breakingdefense.com/2023/10/second-russian-luch-olymp-satellite-now-trailing-western-systems-in-orbit/?\\_ga=2.233764190.1314624386.1697573524-289861297.1670254073](https://breakingdefense.com/2023/10/second-russian-luch-olymp-satellite-now-trailing-western-systems-in-orbit/?_ga=2.233764190.1314624386.1697573524-289861297.1670254073)



## A team from ESA joined one of the world's largest jamming testing campaigns Norway's "Jammerfest"

ESA's navigation testbed vehicle participated in a campaign organized by Norwegian governmental authorities to assess the impact of jamming and spoofing on satellite systems, and test countermeasures for detection and mitigation.

**ESA Jammerfest**

**Link:** [https://www.esa.int/Enabling\\_Support/Space\\_Engineering\\_Technology/Navigation/Navigation\\_Test\\_Beds/Navigation\\_Test\\_Beds\\_Jammerfest](https://www.esa.int/Enabling_Support/Space_Engineering_Technology/Navigation/Navigation_Test_Beds/Navigation_Test_Beds_Jammerfest)



## When GNSS Does Not Work

Article extract from GPS World, about its impact on society in case of failure, and what mitigations need to minimize these impacts. **#GNSS #GPS**

**Link:** <https://www.gpsworld.com/when-gnss-does-not-work/>

## Space Force Gen. Soltanman Proliferated LEO Shows Fleets in Ukraine

Proliferated low Earth orbit (LEO) constellations for communications and other services demonstrating that they can deliver and adapt to adversary attacks such as jamming, the head of U.S. Space Force suggested on Oct. 16. **#USAF #SpaceForce**

**USAF Proliferation**

**Link:** <https://www.defenseone.com/analysis/2023/10/16/us-space-force-gen-soltanman-proliferated-leo-shows-fleets-in-ukraine/>



## Professor in computer science and software engineering develops novel method to prevent cyber attacks on low earth orbit satellites

Tom Wu, associate professor in computer science and software engineering, has a plan that could prevent such a communications catastrophe and keep bad actors from obtaining the necessary information to hack into satellite systems.

**UCLA Cyberattack**

**Link:** <https://www.ucla.edu/news/2023/10/16/computer-science-engineering-method-to-prevent-cyber-attacks-on-satellites>

## Breadloaf Gap: Situation in Israel Is A Case (Trad. Gap Jamming Situation in Israel And Gaza)

This article reviews GPS jamming, focusing on how it's done, why it's used and the situation in Israel and Gaza.

**Jamming Israel**

**Link:** <https://www.space.com/531237-gps-jamming-situation-in-israel-and-gaza/>



## NASA just patched Voyager 2's software but spared Voyager 1 the risky rewrite

NASA patched its Voyager 2 spacecraft software to address a bug that last year nearly deleted generated corrupted telemetry data, but won't touch it to fix a similar - or somewhat critical code - until sometime after October 26.

**NASA Voyagers**

**Link:** <https://www.nasa.gov/news/2023/10/16/nasa-patches-voyager-2-software-but-spared-voyager-1-the-risky-rewrite/>



## Assessing and Responding to the ZIMT Ransomware Attack

This report provides an analysis of the ransomware attack suffered by ZIMT and recommendations for responding and preventing future attacks. **#ZIMT #Ransomware**

**Link:** <https://redhat.com/blog/redhat-communications-learning-and-responding-to-the-zimt-ransomware-attack/>

## La sécurité des communications par satellite: une infrastructure critique pour la transmission de données (Trad. Satellite communications security: a critical infrastructure for data transmission)

Satellites are attractive targets for malicious attacks, and the nature of their development influences their vulnerability. Several solutions are available to prevent and remediate attacks on them. **#Cybersecurity #Satellites**

**Link:** <https://www.enr.com/news/2023/10/16/la-securite-des-communications-par-satellite-une-infrastructure-critique-pour-la-transmission-de-donnees/>

## Attack on the NASA Blog Website

The post states that the NASA blog website has been targeted by a DDoS attack conducted by a threat actor known as DDoS-42. The post provides a link to a website that supposedly shows proof of the website's downtime. It also mentions that the attack was published on the Telegram network by the DDoS-42 group. The DDoS categorizes the attack as a DDoS attack and identifies the victims as NASA blogs, with the website being blogs.nasa.gov. The attack is said to have affected the Aviation & Aerospace industry and specifically targeted the United States. **#NASA #DDoS**

**Link:** <https://www.space.com/531237-nasa-blog-website-attack/>





# TRAINING & EDUCATION

## ★ Space industry group turns up volume on satellite vulnerabilities

The Space ISAC held a conference Oct. 17 in Colorado Springs to highlight the value of satellites as crucial infrastructure that forms the backbone of the modern digital economy and enables services critical for everyday life.

#VOSS #SpaceISAC

**Link:** <https://spacenews.com/space-industry-group-turns-up-volume-on-satellite-vulnerabilities/>



### ESA's Cyber Security Industry Day in 2023

On October 24, 2023, ESA will host an industry day at the European Space Operations Centre (ESOC), providing a unique opportunity for economic operators, both large companies and small to medium enterprises (SMEs), to explore collaboration possibilities. #ESA #ESAConference

**Link:** [https://www.esa.int/ESA/News/ESA\\_Cyber\\_Security\\_Industry\\_Day\\_2023\\_20231024](https://www.esa.int/ESA/News/ESA_Cyber_Security_Industry_Day_2023_20231024)

### Year 2023's maritime sector reeled from cyber attack

The 'Pan-Sea Floor' fishing vessel was held on 17 October at 200's nautical miles control centre in Denmark, Germany in collaboration with the Danish IT and ATISAC Centre. Its goal was to bring together, educate and inspire younger generations in the matter of cybersecurity. #Hacking #Maritime

**Link:** [https://www.esa.int/ESA/News/2023\\_Maritime\\_sector\\_reeled\\_from\\_cyber\\_attack](https://www.esa.int/ESA/News/2023_Maritime_sector_reeled_from_cyber_attack)

### Cyber Fundamentals: The key to unlocking the potential of SATCOM and space

This article discusses the dynamic SATCOM landscape and its evolving threat environment, the unique challenges related to protecting space-based networks, and ESA's core principles for effective space cybersecurity in 2023 and beyond. #Cybersecurity #ESA

**Link:** [https://www.esa.int/ESA/News/Cyber\\_fundamentals\\_the\\_key\\_to\\_unlocking\\_the\\_potential\\_of\\_satcom\\_and\\_space](https://www.esa.int/ESA/News/Cyber_fundamentals_the_key_to_unlocking_the_potential_of_satcom_and_space)

### Commercial Space Innovation, Regulation, and International Collaboration

The upcoming 2023 event – 'The Space Edge – Defining New Opportunities, Economics, and Risks' – will dig deep into the emerging opportunities, economics, and risks associated with the rapid development of space-based technologies, resource acquisition, and risk from the public to private sector. #ESA #ESAConf

**Link:** [https://www.esa.int/ESA/News/2023\\_Cyber\\_fundamentals\\_the\\_key\\_to\\_unlocking\\_the\\_potential\\_of\\_satcom\\_and\\_space](https://www.esa.int/ESA/News/2023_Cyber_fundamentals_the_key_to_unlocking_the_potential_of_satcom_and_space)

### ESA's Fight Against Space Cyber Threats

In a meeting speech at the 2023 conference for the Chairman of the Interplanetary Space Research Organization (ISRO), Germany, shed light on the growing cyber threats faced by India's space sector. Facing hundreds of daily cyberattacks on their networks, the urgent need for a strong defense against these threats cannot be overstated. #ESA #ESAConference

**Link:** [https://www.esa.int/ESA/News/ESA\\_fight\\_against\\_space\\_cyber\\_threats\\_2023](https://www.esa.int/ESA/News/ESA_fight_against_space_cyber_threats_2023)

### Inaugural Space Diplomacy Symposium 2023

As the number and types of space actors increase, the importance of diplomacy will increase in maintaining cooperation, coordination and collaboration in the space domain. The aim of the annual Space Diplomacy Symposium 2023 is to study diplomacy in the traditional categories of civilian, commercial and military space activities across all regions of the world. The conference will take place on 20 October 2023 at the UN School of Space. #ESA #ESAConference #SpaceDiplomacy

**Link:** [https://www.esa.int/ESA/News/Inaugural\\_Space\\_Diplomacy\\_Symposium\\_2023](https://www.esa.int/ESA/News/Inaugural_Space_Diplomacy_Symposium_2023)

# REGULATION

## ★ Critical services to be better protected from satellite data disruptions through new Position, Navigation and Timing framework

Sectors relying on Position, Navigation and Timing (PNT) satellite information such as emergency services and banks will be given added resilience through a new framework unveiled by Science Minister George Freeman. #UK #PNT

**Link:** <https://www.gov.uk/government/news/critical-services-to-be-better-protected-from-satellite-data-disruptions-through-new-position-navigation-and-timing-framework>



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](mailto:research@cyberinflight.com)