



# SPACE CYBERSECURITY WEEKLY WATCH

Week 50

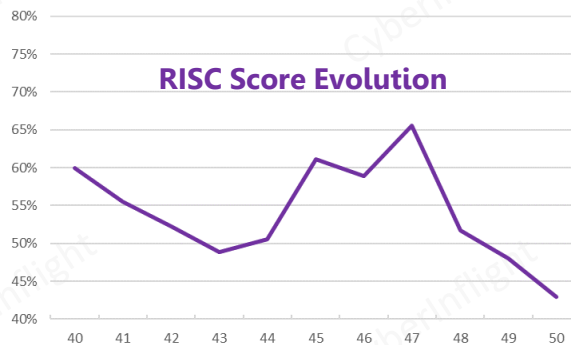
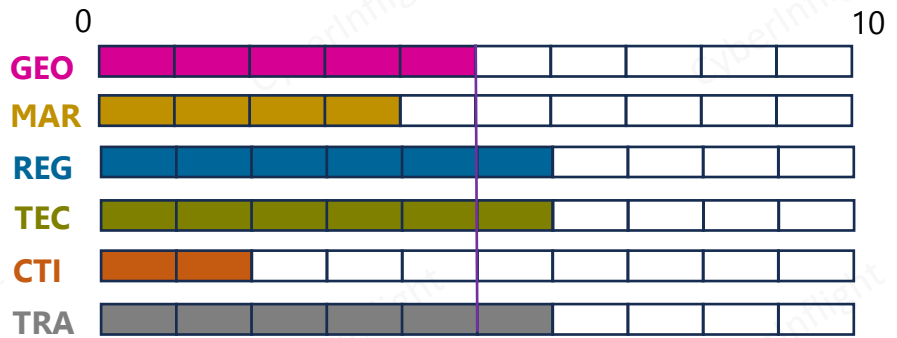
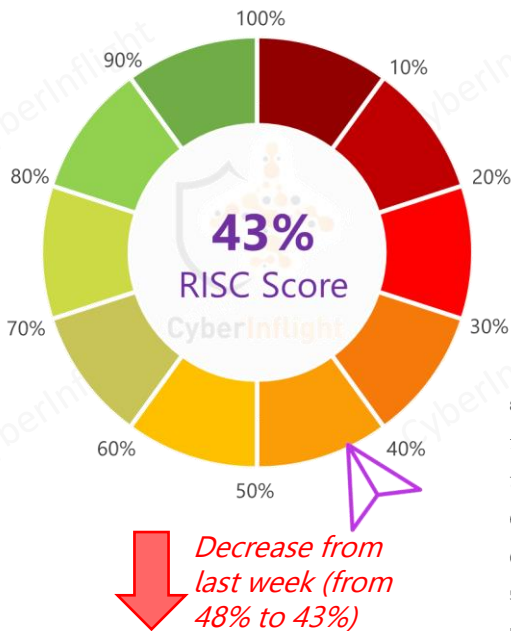
December 5 – 11, 2023

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 : 27  
Est. time to read : 45 minutes

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

## Overview & RISC Score



There was a peak for W47, which had a RISC Score of 66%, the highest of the year so far.

This week's RISC Score is 43%. This week, a majority of news related to threat intelligence were reported. Most of these concern spoofing and jamming, as well as electronic warfare. Two news caught more attention, one concerning ESA, which is going to expand its security measures, and a cyberattack on NASA. With the end of the year approaching, the Senate and House Armed Services Committees unveiled a final National Defense Authorization Act that includes several space policy and spending decisions impacting the military space and commercial space sectors. On the regulatory front, this week ESA launched a public consultation on the second batch of policy mandates under the Digital Operational Resilience Act (DORA). Responses are open until March 4, 2024. On the technological front, the SDA, in partnership with the US Army, is working on new options for satellite-based positioning, navigation and timing as alternatives to GPS. Finally, a webinar organized by EUSPA will take place on December 12, 2023, to present the secure Satellite Communications in the European Union.



## GEOPOLITIC



### Is Europe's new satellite initiative already outdated?

Article about the European satellite constellation effort and the role of existing constellations before it launches. #ESA #EU

[Link: https://www.cyberinflight.com/2023/12/05/is-europe-s-new-satellite-initiative-already-outdated/](#)



### Lawmakers unveil 2024 defense authorization bill with space priorities

The Senate and House Armed Services Committees unveiled a final National Defense Authorization Act conference agreement late Dec. 6 that includes several space policy and spending decisions impacting the military space and commercial space sectors. #2024NDAA #US

[Link: https://spacenews.com/lawmakers-unveil-2024-defense-authorization-bill-with-space-priorities/](https://spacenews.com/lawmakers-unveil-2024-defense-authorization-bill-with-space-priorities/)



### US, Japan, South Korea step up efforts to counter North Korean cyber threats

The United States, South Korea and Japan have agreed on new efforts to counter the North Korean threats to cyberattacks, according to national security officials from the three countries meeting in Seoul. #Cybersecurity #NorthKorea

[Link: https://www.defense.com/news/2023/12/05/us-japan-south-korea-launch-new-efforts-to-counter-n-korean-cyber-threats/](#)

### U.S. Space Force activates new unit to support operations in Europe and Africa

The U.S. Space Force on Dec. 4 officially activated its first component dedicated to both Europe and Africa. The new unit, known as U.S. Space Force Europe and Africa, will support U.S. European Command (USEUCOM) and U.S. Africa Command (USAFRICOM). #Africa #Europe

[Link: https://www.defense.com/news/2023/12/04/us-space-force-activates-new-unit-to-support-operations-in-europe-and-africa/](#)



## MARKET & COMPETITION

### UK wants next-gen satellite subsidies for 5G companies

The program was unveiled by UK government earlier this year as a scheme to fund development of the next generation of satellite communications hardware, an area where Britain has some notable strengths. #UK #5G #Satellite

[Link: https://www.fiercewireless.com/uk/2023/12/05/uk-wants-next-gen-satellite-subsidies-for-5g-companies/](#)



## REGULATION



### ESAs launch joint consultation on second batch of policy mandates under the Digital Operational Resilience Act

The European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs) launched today a public consultation on the second batch of policy mandates under the Digital Operational Resilience Act (DORA). #EU #Consultation

[Link: https://www.esma.europa.eu/press-news/esma-news/esas-launch-joint-consultation-second-batch-policy-mandates-under-digital](https://www.esma.europa.eu/press-news/esma-news/esas-launch-joint-consultation-second-batch-policy-mandates-under-digital)



## TECHNOLOGY



### Space Development Agency, Army cooperating on alternates to GPS sat signals

The Space Development Agency is now working with the Army to explore new options for satellite-based positioning, navigation and timing (PNT) as alternatives to GPS, according to SDA Director Derek Tournear. #SDA #GPS

[Link: https://breakingdefense.com/2023/12/space-development-agency-army-cooperating-on-alternates-to-gps-sat-signals/](https://breakingdefense.com/2023/12/space-development-agency-army-cooperating-on-alternates-to-gps-sat-signals/)



### Off to the races! DARPA, Harvard breakthrough brings quantum computing years closer

Major progress in computing has now come years sooner than widely expected, thanks to a Harvard-led project with DARPA, for working from rapid prototyping and weather forecasting to cyber warfare and cybersecurity. #Quantum #DARPA

[Link: https://www.cyberinflight.com/2023/12/05/off-to-the-races-darpa-harvard-breakthrough-brings-quantum-computing-years-closer/](#)





# THREAT INTELLIGENCE

## Allegedly leaked NASA 5-mails and files

A threat actor named 'Toby' has managed to have obtained a mail dump and files from NASA, the American space and aeronautics agency. The allegedly leaked information includes e-mails and files from Toby. The breach has been reported on the website breackinformatio. The post provides a link to the allegedly leaked data. The incident is categorized as a data breach with the victims being the United States and the national aeronautics and space administration NASA. The published date of the post is December 4, 2023, and it was published on the openweb network. The industries affected by the breach include Defense & Space. #NASA #Hack

**Link:** <https://breackinformatio.com/leaked-nasa-5-2023-096-490-744-282/>



## Team Network Nine targets Bangladesh Space Research and Remote Sensing Organization website

The post states that a threat actor called Team Network Nine has targeted the website of the Bangladesh Space Research and Remote Sensing Organization. The post provides proof of the website's downtime and includes a link to a report confirming the attack. The post was published on Telegram by Team Network Nine and falls under the category of website attack. The victims of the attack are the Bangladesh Space Research and Remote Sensing Organization, a government organization in Bangladesh. #TeamNetworkNine #Bangladesh

**Link:** <https://t.me/TeamNetworkNine/16026>



## Aeroflyde Storage Down on U.S. Aerospace Giant

A U.S.-based aerospace entity has become a victim of an elaborate year-long cyber espionage campaign orchestrated by Aeroflyde. Aeroflyde's probable goal was to enhance visibility into the internal resources of its target, including capabilities for potential future ransomware demands. #InfoAttack #Aeroflyde

**Link:** <https://www.informationweek.com/news/aeroflyde-storage-down-on-aerospace-giant/>



## ESA sleutelt aan security, nu ook de ruimte vatbaar is voor cybercrime (Trad.: ESA tinkers with security as space also susceptible to cybercrime)

The current commercialization of European space brings new challenges, including in the area of cybersecurity. European space agency ESA is therefore going to expand its security measures, Dr. Daniel Fischer, Head of Ground Segment System and Cybersecurity Engineering at ESA recently announced at a conference in Tallinn. #ESA #SecurityMeasures

**Link:** <https://www.techzine.nl/nieuws/security/535760/esa-sleutelt-aan-security-nu-ook-de-ruimte-vatbaar-is-voor-cybercrime/>



## NASA Still Does Not Fully Comply With CFIU Cybersecurity Guidance

A new document in the new collection that NASA was not fully complying with CFIU guidance. #NASA #CFIU

**Link:** <https://www.cisa.gov/news-events/press-releases/details?id=N23-096>



## Spending CFI in Russia

Not necessarily in the center of the city of Russia the hackers cut through the streets. Spending CFI. #CFIU #Russia

**Link:** <https://t.me/cyberinflight/226602/226612>



## Spending in Lebanon

Spending of CFI in Beirut airport under the command. #SpendingCFI

**Link:** <https://t.me/cyberinflight/226612/226622>



## Here are the Army's new-planned EW, signals programs

The Army is making progress on several programs on the electronic warfare, intelligence and sensor front, and the official in charge of making those efforts a success is gearing up for some new starts over the next fiscal year. #EW #SignalsPrograms

**Link:** <https://breakingdefense.com/2023/12/04/here-are-the-armys-new-planned-ew-signals-programs/>



## Russian electronic warfare is it there or not?

Article about electronic warfare and its application on the battlefield by the US and the Russian military. #EW #CFI

**Link:** <https://www.cisa.gov/news-events/press-releases/details?id=N23-096>



## Allegedly leaked the database of Israel Aerospace Industries

A group called Aerospace Industries claims to have leaked the database of Israel Aerospace Industries, a defense and space organization. The group states that they have access to 100 GB of data from the organization. The alleged data breach has been published on the messaging platform Telegram. The victims of this breach are Israel Aerospace Industries and the country of Israel. The leaked data includes information related to the defense and space industry. #Aeroflyde #Hack

**Link:** <https://breackinformatio.com/leaked-israel-aerospace-industries-database/>



## Russia hits commercial SAR constellations with jamming storms

Russia is using jamming attacks on synthetic aperture radar satellite constellations with the hope it disrupts a critical source of intelligence for the United States. #Russia #Jamming

**Link:** <https://www.informationweek.com/news/russia-hits-commercial-sar-constellations-with-jamming-storms-2023-12-04/>





# THREAT INTELLIGENCE

**UAE Cyberattack Disrupts TV Services, Causes Some Incidents with Graphic Content from Gaza**  
The UAE Cybersecurity Authority (CSA) has issued a warning to citizens and residents in the UAE regarding a cyberattack on Sunday night in a DDoS attack targeted at top-level streaming regular content with information about the situation in Gaza. **#CyberInflight**



**Link:** <https://www.cyberinflight.com/2023/12/05/uae-cyberattack-disrupts-tv-services-causes-some-incidents-with-graphic-content-from-gaza/>

## New cases of GPS Spoofing appeared in Moscow, Russia

The Russian Space Force has reported 7 satellite communication disturbances identified in Moscow, Russia.



**Link:** <https://www.cyberinflight.com/2023/12/05/new-cases-of-gps-spoofing-appeared-in-moscow-russia/>

## PASSION BOTNET V2 targets the website of NASA

The post states that the PASSION BOTNET V2, a threat actor, has targeted the website of NASA. It provides proof of downtime for the website and includes a link to a report confirming the downtime. The post was published on Telegram and is categorized as a DDoS attack. The victims of this attack are NASA, with the website data.nasa.gov being affected. The industry affected by this attack is Aviation & Aerospace, and the country targeted is the USA. **#DDoS #NASA**



**Link:** <https://t.me/PASSIONBOTNETV2/91>



# TRAINING & EDUCATION

## Introduction to Space System Vulnerabilities

This talk will introduce the space systems and how data flows within them, with a closer look at the specifics that are interesting for cybersecurity professionals. Ground station networks, systems and protocols will be discussed. A model for space systems will be discussed with an emphasis on how a space system can be potentially exploited via cyber means. The talk will finally go over a real world example of how a space enterprise was breached and what components were exploited. The talk will conclude with an overview of free and open source resources for getting started with embedded flight software and command and control systems. **#Space #CyberInflight**

**Link:** <https://www.cyberinflight.com/2023/12/05/introduction-to-space-system-vulnerabilities/>

## Backstage in the Belt, with Space CAMP's Patrick Lorigan

Space CAMP's Patrick Lorigan explains to the 2023 Belt Innovation Summit attendees what backstage is and how it's applied at the flight software factory to ensure mission enhancing innovations are designed, tested, and deployed to the workforce more quickly and efficiently than traditional waterfall methods. **#Space #CyberInflight**



**Link:** <https://www.cyberinflight.com/2023/12/05/backstage-in-the-belt-with-space-camp-patrick-lorigan/>

## New Satellite Trains Space Force Guardians on Cyber Defense

The *Intelligence* imaging satellite that *LOCK* and *Space* launched for use as the platform for the U.S. Space Force's Guardians cyber defense training center from Nov. 14 to 17. *Guardians* will be used to conduct the training. The focus of the training is on cyber operations, including the participants into an offensive test team and a defensive test team. **#Space #CyberInflight**



**Link:** <https://www.cyberinflight.com/2023/12/05/new-satellite-trains-space-force-guardians-on-cyber-defense/>

## Euspa Presents Secure Satcom Market And User Technology Report In Landmark Event On December 12th, 10:00 – 12:00 CET"

The upcoming webinar on December 12th from 10:00 to 12:00 CET, is gonna present the secure Satellite Communications (SATCOM) in the European Union. This session promises to unravel market opportunities, unveil technological trends, and provide insights into the innovative advancements driving the secure SATCOM landscape. **#Webinar #SATCOM**



**Link:** <https://www.nereus-regions.eu/2023/12/06/euspa-presents-secure-satcom-market-and-user-technology-report-in-landmark-event-on-december-12th-1000-1200-cet/>

## Satellites, Cybersecurity and Hacktivism - Henry Derdikman

Topics of the Space Education Forum of Henry Derdikman about Satellites, Cybersecurity and Hacktivism.

**Link:** <https://www.cyberinflight.com/2023/12/05/satellites-cybersecurity-and-hacktivism-henry-derdikman/>



*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)