# SPACE CYBERSECURITY WEEKLY WATCH

## Week 28
## July 9 – 15, 2024

**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** : 39

**Est. time to read** : 90 minutes

■ **GEOPOLITIC**

■ **MARKET INTELLIGENCE**

■ **TRAINING & EDUCATION**

■ **THREAT INTELLIGENCE**

■ **TECHNOLOGY**

■ **REGULATION**

⭐ **IMPORTANT NEWS**

## Overview & Resilience Index for Space Cybersecurity (RISC)



**66%**
RISC Score

*9 percentage points of increase from last week (from 57% to 66%)*
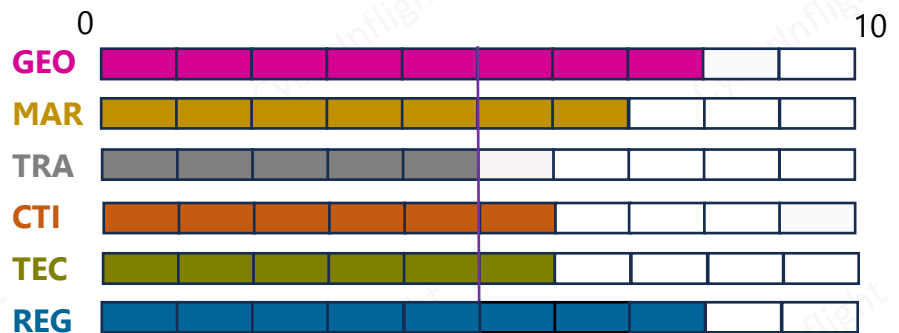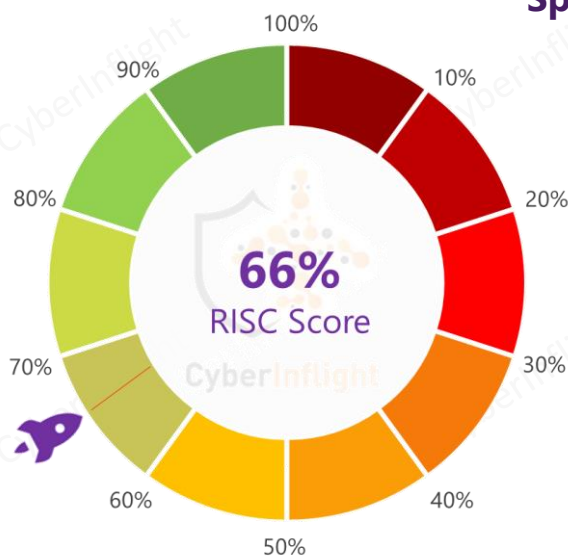


**RISC Score Evolution**



*After declining from W18, the RISC score (the tool assessing space cybersecurity resilience) was struggling to recover. It is finally back on the rise at W28.*

This week's RISC score is 66%. CyberInflight became an official member of the Aerospace Valley ecosystem after being approved by the Cluster Board of Directors. On the technology front, Microchip has unveiled its first devices in its PIC64 High-Performance Spaceflight Computing family of microprocessors. This new technology can balance cost-effectiveness with high fault tolerance crucial for round-the-clock service reliability and space asset cybersecurity. In addition, a paper entitled "Cyber and electromagnetic threats to space infrastructure" is published by the Istituto Affari Internazionali, an Italian think tank on international relations. On the geopolitical front, Japan and NATO have an accommodation in their world positions and individual security. This fact allows them to cooperate in enhancing the resilience of their own satellites to withstand jamming and spoofing. On the regulatory front, Beijing is said to have a program to jam broadcasts and falsify signals from EU satellites. The European Space Law would be helpful to counter these attacks, although it is still delayed as work on it is in progress at different stages. On the market front, Thales signed a contract with the French Army for the supply of 30 satellite communication stations. This contract aims to enable the French Army to manage satellite data with a high level of protection against jamming, cyberattacks and other risks. Lastly, the Japanese Space Exploration Agency discovered unknown cybersecurity vulnerabilities during the process of addressing a security incident while working with Microsoft to investigate a cyberattack on its systems in 2023. After the investigation, it was confirmed that no classified data on rockets, satellites or national security was compromised.

# 🎉 CYBERINFLIGHT'S NEWS 🎉

⭐ **CyberInflight is one of 36 new members of the Aerospace Valley ecosystem**
Following the cluster's last Board of Directors meeting, the Aerospace Valley competitiveness cluster is pleased to welcome 36 new members to its ecosystem in Occitanie, Nouvelle-Aquitaine & Other regions.
**#CyberInflight  #AerospaceValley**
**Link**: https://www.aerospace-valley.com/annuaire-des-membres/cyberinflight

# TECHNOLOGY

**64-bit MPUs advance space computing**
Microchip has launched the first devices in its PIC64 High-Performance Spaceflight Computing (PIC64-HPSC) family of microprocessors. One of them are the Radiation-tolerant PIC64-HPSC RT MPUs, which are tailored for the commercial space sector, particularly Low Earth Orbit (LEO) constellations. They balance cost-effectiveness with high fault tolerance crucial for round-the-clock service reliability and space asset cybersecurity. **#Microchip #Microprocessors**
**Link**: https://www.edn.com/64-bit-mpus-advance-space-computing/

# TRAINING & EDUCATION

⭐ **Cyber and electromagnetic threats to space infrastructure**
In this paper, the Italian international relations think tank Istituto Affari Internazionalihat (IAI) explains that the resilience of space systems can be achieved through a holistic approach that considers both the technological component, adopting the principle of security by design, and the human component, with particular attention to including cyber when training personnel. **#IAI #SpaceInfrastructure**
**Link**: https://www.iai.it/sites/default/files/iai2407.pdf

# GEOPOLITIC

### Japan-NATO ties: for what end?

In addition to the strengthening of practical areas of cooperation, Japan and NATO have increasingly shown alignment in their worldviews and the interconnectedness of their individual security. Thus, they could work on improving the resiliency of their own satellites to withstand jamming and spoofing. They could also work to integrate their separate Space Domain Awareness capabilities to ensure broader situational awareness for US-led activities. **#Japan #NATO**

**Link**: https://www.rand.org/pubs/commentary/2024/07/japan-nato-ties-for-what-end.html

### Sweden inks first military space strategy, looks to bolster role in global space race

Sweden's first own strategy for space defence is aimed building the capabilities of its armed forces to play a larger role as nations around the world gird for potential conflict in the heavens. **#Sweden #Space**

**Link**: https://breakingdefense.com/2024/07/sweden-inks-first-military-space-strategy-looks-to-bolster-role-in-global-space-race/

### An argument against establishing a US Cyber Force

Over the past twenty plus years, the Department of Defense has made significant progress normalizing cyberspace operations. After United States Cyber Command was established in 2010, DOD continued to conduct most facets of DOD cyberspace operations through the command. This Cybercom-centric approach, built on centralized authorities and control, has resulted in many significant operational outcomes for the nation. Despite that progress, DOD struggles with recruiting, training, retaining, and tracking operational readiness of its cyberspace forces. **#USCF #Cybersecurity**

**Link**: https://defensescoop.com/2024/07/11/argument-against-establishing-united-states-cyber-force/

### NATO sounds alarm on China's advances in space and nuclear, ties with Russia

NATO leaders gathered in Washington D.C. for the alliance's 75th anniversary summit, and they were alarmed by China's ambitions and aggressions in nuclear, space, and cyberspace on top of its deepening ties with Russia, regarding the rapid expansion and diversity of its nuclear arsenal with more warheads and a larger number of nuclear-tipped delivery systems. **#China #Russia**

**Link**: https://www.c4isrnet.com/nato-sounds-alarm-china-space-nuclear-russia/

### Digital ministry touts satellite signal progress

According to the Taiwanese Ministry of Digital Affairs, Taiwan has line of sight with low-Earth orbit satellites half of the time, a milestone in the nation's efforts to enhance signal resilience. The ministry began the two-year project to enhance signal resilience throughout the nation last year and tested 773 sites domestically and abroad to ensure that Taiwan's military and public or command system would maintain communication capabilities in an emergency. **#Taiwan #SatelliteResilience**

**Link**: https://www.taipeitimes.com/News/taiwan/archives/2024/07/11/2003820511

### Space Based Warfare America's dominance challenged

Both the US and Russia have communication satellites, the US is the only nation with a low-earth orbit (LEO) internet constellation, Starlink, consisting of over 5,000 satellites. While Starlink has provided the US and its allies with advantages seen on today's battlefield, these advantages have been countered, and similar capabilities are being developed by not only Russia but also China. **#Russia #China**

**Link**: https://finabestonic.com/en/?query_category/space-based-warfare-americas-dominance-challenged/

### NATO set to build new Cyber Defense Center

NATO's members have agreed to the construction of a new cyber defence facility designed to help the military alliance build resilience and better respond to digital threats. **#NATO #CyberDefense**

**Link**: https://www.infosecurity-magazine.com/news/nato-build-new-cyber-defense-center/

### Space is now a priority for NATO leaders, Euro leaders scramble to meet threats

When NATO leaders met on July 9-11, space is firmly on the agenda as allies work to build up a stronger collective infrastructure for coordination, and key European space players harden to develop new capabilities. **#NATO #Space**

**Link**: https://breakingdefense.com/2024/07/space-now-a-priority-for-nato-leaders-euro-leaders-scramble-to-meet-threats/

### Ariane 6 rocket successfully launches, flight in progress

The launch of Ariane 6 is a significant success for the European space program, reducing costs and providing strategic autonomy for European governments and companies. **#Ariane6 #EU**

**Link**: https://www.spaceflightnow.com/2024/07/09/ariane-6-rocket-successfully-launches-flight-in-progress/

# REGULATION

★ ### China to attack EU satellites, Breton: "European law will address security issue"

Beijing allegedly has a program to jam broadcasts and falsify information. EU runs for cover, but regulations lag behind. Thierry Breton glossed over the delays of EU space law. He said that works are in progress at different levels in parallel and Member States are developing receivers at the national level for the secure navigation service offered by Galileo, the European Union's civil satellite navigation and positioning system and Galileo. He also said that Galileo supplies state-of-the-art protection against spoofing and jamming, ensuring robust and reliable performance even under jamming conditions. **#EUSpaceLaw #China**

**Link**: https://www.eunews.it/en/2024/07/08/china-to-attack-eu-satellites-breton-european-law-will-address-security-issue/

### Enhancing Space Mission assurance to cyber threats: findings and recommendations for the US Space Force

In this report, the authors provide recommendations that will help USSF implement the guidance set forth in Space Policy Directive-5 to incentivize the commercial sector to adopt a cybersecurity strategy that will help ensure space mission assurance (SMA), which is a concept used to deter adversaries, counter risk from emerging man-made and natural threats to space, and pursue resilient space architectures. **#USSF #Assurance**

**Link**: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA/RRA2900/RR2900-1/RAND_RR2900-1.pdf

### Memorandum for the heads of Executive Departments and Agencies

This memorandum outlines the Administration's cross agency cybersecurity investment priorities for formulating fiscal year (FY) 2026 budget submissions to the Office of Management and Budget (OMB), consistent with spring guidance. **#Memorandum #Cybersecurity**

**Link**: https://whitehouse.gov/wp-content/uploads/2024/07/M-24-14-Cybersecurity-Priorities-Memo-Signed.pdf

### New CLUSIF's sheet the NIS2 directive

As soon as the European NIS-2 directive was implemented, CLUSIF set up a task force which produced a maturity self-assessment grid and a table of correspondence between the national transposition of NIS2 and the two versions of securities. **#NIS2 #CLUSIF**

**Link**: https://clusif.fr/publications/fiche-clusif-directive-nis2/

### With concerns over space warfare on the rise, existing international law may be the answer

As nations delay regulating the use of force in space, a new analysis says attacks on satellites and similar acts of space warfare may fall under existing international agreements. **#SpaceWarfare #Law**

**Link**: https://thenextweb.com/news/concerns-over-space-warfare-on-the-rise-existing-international-law-may-be-the-answer/

### Regulating outer space after Loper Bright

While space exploration began 67 years ago with the launch of Sputnik, the rules regulating commercial activities in outer space is many ways are just now being written. Agencies from the Federal Communications Commission (FCC) to the Federal Aviation Administration (FAA) to the National Institute of Standards and Technology (NIST) all have open proceedings affecting outer space. And without Chevron deference, all of these agency actions may be subject to challenge. **#OuterSpace #Regulation**

**Link**: https://spacenews.com/regulating-outer-space-after-loper-bright/

### NATO plans first commercial space strategy to spur tech innovation

NATO's members are planning to build a first-ever commercial space strategy to speed new technologies to their militaries, based in part on recommendations put together by a government-industry working group sponsored by NATO and the US Chamber of Commerce. **#NATO #Strategy**

**Link**: https://breakingdefense.com/2024/07/nato-plans-first-commercial-space-strategy-to-spur-tech-innovation/

### ESA White Paper takes PNT vision to 2035

The European Space Agency's Navigation Innovation and Support Program Advisory (Voluntary Statistic) has released a new white paper outlining its vision for the evolution of positioning, navigation, and timing (PNT) technology, applications, and services until 2035. **#ESA #PNT**

**Link**: https://insidegnss.com/esa-white-paper-takes-pnt-vision-to-2035/

### Congressman Maxwell Frost defends US Assets from China, Russia cyberattacks, introduces new bill to enhance cybersecurity of american spacecrafts

Congressman Maxwell Alejandro Frost (FL-10) with Congressman Don Beyer (VA-8) have introduced the Spacecraft Cybersecurity Act. This legislation would require the National Aeronautics Space Administration (NASA) to secure a cybersecurity plan from manufacturers applying to use federal dollars to build/deliver spacecrafts. **#US #Spacecraft**

**Link**: https://frost.house.gov/media/press-releases/congressman-maxwell-frost-defends-us-assets-from-china-russia-cyberattacks-introduces-new-bill-enhance-cybersecurity-of-american-spacecrafts

# MARKET & COMPETITION

### Thales gets contract to provide French Army with satellite communication stations

Thales won a contract to provide 30 satellite communication stations to the French Army. This order will allow the French Army to manage satellite data with a high level of protection from jamming, cyberattacks and other risks.

**#Thales #FrenchArmy**

**Link**: https://www.marketscreener.com/quote/stock/THALES-4715/news/Thales-Gets-Contract-to-Provide-French-Army-With-Satellite-Communication-Stations-47369423/

# THREAT INTELLIGENCE

**Global GPS system at risk of attack**

The Global Positioning System (GPS) is part of our daily lives. This technology is critical for location services, telecommunications, emergency, and even financial transactions. Even so it is at risk of attacks that can cause interruptions and even sending fake signals. **#GPS #Attack**

Link: https://cyberinflight.com/...

**Vulnerability remediation systems for space tech companies: protecting the final frontier**

Cyber threats pose significant challenges for space tech companies. From the speed and stealth of attacks to the difficulty of attributing them, the stakes are high. The days of "security by obscurity" for satellites are over. As these systems become more digitized and software driven, their vulnerability increases. **#Space #Cybersecurity**

Link: https://www.overtsec.io/.../vulnerability-remediation-systems-for-space-tech-companies/

**Hacking a Satellite harder than it looks?**

Last year's DEF CON event featured a demonstration of satellite hacking. In the hack-a-sat contest, which was organized by the US Air Force, teams of hackers were able to penetrate a cubesat called Moonlighter and bypass the satellite's restrictions on the ground targets it can observe. The success of the hackers prompted the Office of the Director of National Intelligence, the FBI, the National Counterintelligence and Security Center, and the Air Force Office of Special Investigations to issue a warning about cyber risks facing satellites in orbit. **#Satellite #Hacking**

Link: https://cusp.org/.../hacking-a-satellite-harder-than-it-looks/

**Russian jamming is wreaking havoc on GPS in Eastern Europe. But is it hybrid warfare?**

Amid unprecedented amounts of electronic warfare in Russia's war on Ukraine, there is no doubt that the Russians are jamming GPS and other satellite-based navigation systems around the Baltic Sea. Earlier this year, the interference forced the closure of a major civilian airport after flights had to be diverted en route. **#HybridWarfare #Baltics**

Link: https://www.sharabepollitics.com/...

**Russian offensive campaign assessment, July 11, 2024**

Finnish federal transport and communications agency Traficom told Finnish outlet Ilapleht on July 11 that GPS "malfunctions" have increased in the past week in reference to a specific incident in the east of Finland overnight on July 10-11. Russia's apparent GPS jamming is likely part of Russia's intensifying hybrid campaign directly targeting NATO states likely aimed at undermining support for Ukraine and NATO unity. **#Finland #Russia**

Link: https://www.iswresearch.org/.../russian-offensive-campaign-assessment-71124/

**Israel Defense Forces – Iran update, July 11, 2024**

An initial investigation published by the Israel Defense Forces (IDF) Home Front Command found that IDF GPS jamming intended to disrupt Hezbollah attacks, reportedly interfered with the couple's ability to receive attack warnings. The IDF Northern Command proposed revisions to its current attack warning system to allow users to receive notifications for a selected area of interest versus the location of the phone itself, bypassing the GPS jamming error. **#IDF #Hezbollah**

Link: https://www.understandingwar.org/.../israel-iran-update-july-11-2024

⭐ **Japanese space agency spotted zero-day attacks while cleaning up attack on M365**

Multiple malware attack saw personal data accessed, but rocket science remained safe. The Japanese Space Exploration Agency (JAXA) discovered unknown cybersecurity vulnerabilities during the process of addressing a security incident while working with Microsoft to probe a 2023 cyberattack on its systems. An investigation ensued, and saw networks taken offline to verify that no classified data on rockets, satellites, or national security was compromised. **#JAXA #Cyberattack**

Link: https://www.theregister.com/2024/07/11/jaxa_m365_zeroday_attacks/