



# SPACE CYBERSECURITY WEEKLY WATCH

Week 5

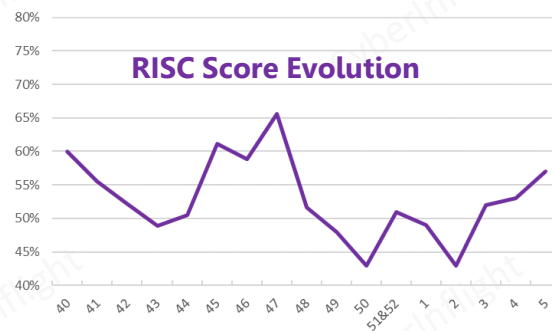
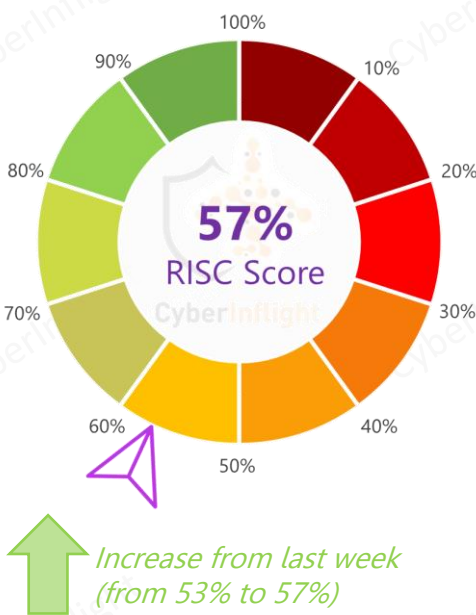
January 30 – February 5, 2024

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 : 19  
Est. time to read : 30 minutes

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

## Overview & RISC Score



*After a period of decline since the start of 2024, there has been an increase since W3.*

This week's RISC Score is 57%. This week, the project to create a jam-resistant military-only GPS signal for the United States Space Force (USSF) has been postponed to June 2025. The delay is attributed to the complexity of the project and the need for additional testing. Also on the market this week, the USSF is reviewing its acquisition strategy for secure narrow-band communications. To achieve this goal, the USSF has established eight working groups, each focused on a specific area of interest. One of these groups is a Cyber Working Group, which is responsible for identifying and mitigating potential cyber threats to the USSF's communication systems. Regarding the threat intelligence front, the Commander of the Estonian Defense Forces has announced at a conference that Russia is likely responsible for the increase in GPS jamming in Eastern Europe. Finally, the Institute of Electrical and Electronics Engineers (IEEE) is offering an online course on February 15th about the security of emerging satellite mega-constellations. The course will be taught by Gunes Karabulut Kurt and Gregory Falco, who are experts in this field. The course aims to educate individuals on the challenges and potential risks involved in developing and operating mega-constellations of satellites.

## GEOPOLITIC

### U.S. Space Force expresses concern over China's growing spy satellite capabilities

The U.S. Space Force is raising concerns over China's rapidly expanding spy satellite capabilities, including advanced optical and radar surveillance systems that could monitor U.S. and allied activities. #US #China

**Link:** <https://www.defense.com/analysis/space-force-expresses-concern-over-chinas-growing-spy-satellite-capabilities/>



## THREAT INTELLIGENCE

### Hundreds of Network Operators' Credentials Found Circulating in The Dark Web

In early January, an attacker going by the alias 'Iron Spook' leaked 100,000+ network operator credentials (NOC) across 100+ different servers. The credentials were associated with major organizations, including an Israeli communications satellite operator. #DarkWeb #CyberAttack

**Link:** <https://www.research.com/articles/hundreds-of-network-operators-credentials-found-circulating-in-dark-web/>

### US Frenchie targets the website of NATO

The French actor 'US Frenchie' targeted the NATO website on January 27. #NATO #France

**Link:** <https://www.research.com/articles/us-frenchie-targets-the-website-of-nato/>



### Estonian general: Russia likely responsible for uptick in GPS jamming in Eastern Europe

Russia is likely behind an increase in GPS jamming across Eastern Europe, said Martin Herem, the commander of the Estonian Defense Forces. #Jamming #Estonia

**Link:** <https://news.yahoo.com/estonian-general-russia-likely-responsible-105024581.html>



### As Baltic sea spikes in GPS jamming, NATO must respond - Breaking Defense

An uptick in GPS jamming in the Baltic Sea is a concern, prompting NATO to respond to Russia's threat and dangerous jamming activity. #NATO

**Link:** <https://www.breakingdefense.com/2024/01/27/as-baltic-sea-spikes-in-gps-jamming-nato-must-respond-breaking-defense/>



## MARKET & COMPETITION



### Space Force reexamining acquisition strategy for secure narrow-band communications

That study involves eight different working groups looking at all aspects of the question. Those are the: Technology Alternatives Working Group; Cost Analysis Working Group; Performance Effectiveness Analysis Working Group; Commercial Working Group; Enterprise Working Group; Threats/Scenarios Working Group; Cyber Working Group and the International Partner Working Group. #USSF #Resilience

**Link:** <https://breakingdefense.com/2024/01/space-force-reexamining-acquisition-strategy-for-secure-narrow-band-communications/>



### Dark Sky Technology, Inc. Joins Space IAC to Enhance Security in Space Systems Software

Dark Sky Technology, Inc. has announced its membership with the Space Information Sharing and Analysis Center (Space IAC). This collaboration will offer unparalleled software supply chain threat intelligence and analysis for critical space systems, contributing significantly to the security and reliability of software in the defense and aerospace sectors. #Space #DarkSkyTechnology

**Link:** <https://www.darkskyy.com/press-releases/dark-sky-technology-joins-space-iac-to-enhance-security-in-space-systems-software/>

### Space Force to put firms under contract for commercial reserves by 2025

The Space Force expects to begin identifying members for its Commercial Augmentation Space Force — an effort to scale up the use of commercial capabilities during a conflict — and get them under contract by 2025, if not sooner. #USSF #CommercialSpace

**Link:** <https://www.defense.com/analysis/space-force-to-put-firms-under-contract-for-commercial-reserves-by-2025/>



# TECHNOLOGY

## The European Quantum Communication Infrastructure (EuroQCI) Initiative

Europe continues to advance its incorporating quantum-based systems, providing an additional layer of security. The initiative utilizes quantum communication technologies developed by the EU-funded Quantum Technologies Flagship and involves industry partners to boost Europe's capabilities in cybersecurity and quantum technologies. #Quantum #EuroQCI

**Link:** <https://www.ec.europa.eu/digital-affairs/en/euroqci>



## Open Service Navigation Message Authentication (OSNMA) is a setback

As users depend on the accuracy and integrity of satellite navigation signals, the OSNMA is a setback. OSNMA is a critical element to the full suite of services provided by GPS. #OSNMA #GPS

**Link:** <https://www.ec.europa.eu/digital-affairs/en/osnma>



## GPS Systems reaches major development milestones with enhanced M-Code global test

The M-Code modernization program has two goals. The first is to develop an advanced security-certified M-Code for GPS, which provides assured Position, Navigation and Timing (PNT) in GPS jamming and spoofing environments, incorporates full dual-frequency capable system (DF-CA) receivers, and reduces power consumption. The capability will support military users and weapon systems in airborne, maritime, and ground domains. #MCode #GPS

**Link:** <https://www.ec.europa.eu/digital-affairs/en/m-code>



## Ground system for jam-resistant GPS delayed again to July 2025 at earliest, Pentagon tester says

The long-troubled ground system needed for the Space Force to have "full control" of the jam-resistant, military-only GPS signal is facing yet another delay — and now won't be ready for use until July 2025, according to the latest report by Pentagon's testing office. #JamResistant #USSF

**Link:** <https://breakingdefense.com/2024/02/ground-system-for-jam-resistant-gps-delayed-again-to-july-2025-at-earliest-pentagon-tester-says/>



## Korea's KASS satellite navigation system certified by national authorities - enters service

KASS, the second GPS system developed by South Korea, is derived from GPS. The European Galileo satellite navigation system. It is designed to improve the positioning and navigation performance of the existing GPS constellation and includes upgrades with the Galileo and GPS dual-frequency systems constellation. #KASS #GPS

**Link:** <https://www.ec.europa.eu/digital-affairs/en/kass>



# TRAINING & EDUCATION

## ISAC: Here's Your Opportunity to Become a Space Security Professional

ISAC is an international membership association for space and security professionals offering certified space security specialist professional (CSP) and other space cybersecurity certifications. #ISAC #Space

**Link:** <https://www.isac.org/>



## Security of Emerging Satellite Mega-Constellations

In this course, the instructors will begin with a discussion on the fundamental components of LEO mega-constellations. Three main vulnerability classes will be considered, these are: payload and inter-satellite link vulnerabilities; ground station/terrestrial network interconnection vulnerabilities; and signal vulnerabilities. #Courses #IEEE

**Link:** <https://www.comsoc.org/education-training/training-courses/online-courses/2024-02-security-emerging-satellite-mega>



## How NASA is Strengthening Cybersecurity in Space

In August 2023, the ISAC, along with the US National Counterintelligence and Security Center and the Air Force Office of Special Investigations warned that international intelligence bodies were launching hacking campaigns to infiltrate the American space industry. ISAC just launched its first cybersecurity best practices guide for the space industry. #ISAC #Cybersecurity

**Link:** <https://www.isac.org/>





# TRAINING & EDUCATION



## Decoding the European Space Conference: Key Insights from a Cybersecurity Perspective

The cybersecurity reports at ESA 2024 play a pivotal role in the secure operation of the infrastructure in Europe. With a budget of over 1.5 billion euros, the European Commission and ESA are cybersecurity especially in a crucial endeavor due to the increasing importance of Global Navigation Satellite Systems (GNSS) and the growing threats against these systems. #ConferenceESA24

[https://www.esa.int/Enabling\\_Support/Space\\_Conferences\\_and\\_Conferences\\_Key\\_Insights\\_from\\_Cybersecurity\\_Perspective](#)

## We Need Cybersecurity in Space to Protect Satellites

Selecting our critical satellites is essential to safeguard the very fabric of our interconnected world and thereby ensure the continued advancement of our progress in the digital age. Today, efforts to secure our satellites will protect our global infrastructure for future generations. #ResilienceHorizons

[https://www.esa.int/Enabling\\_Support/Space\\_Conferences\\_and\\_Conferences\\_Key\\_Insights\\_from\\_Cybersecurity\\_Perspective](#)

## The Download (Feb 05, 24) Space Money: When Nation States Target The Commercial Space Sector

This is the first in a series of episodes examining cyber attacks and space systems. Laura Winter speaks with Nick Saunders, Head of Cybersecurity and Data Officer for Government Systems, in his first all-down interview since the satellite communications company weathered a notorious cyberattack on February 28, 2022. In 2018, the space information sharing and analysis center (ISAC) and Frank Barker, CEO of iSpace, a company providing earth observation products to government and commercial customers. #Podcast #CyberInflight

[https://www.esa.int/Enabling\\_Support/Space\\_Conferences\\_and\\_Conferences\\_Key\\_Insights\\_from\\_Cybersecurity\\_Perspective](#)

*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)*