SPACE CYBERSECURITY WEEKLY WATCH

Week 5

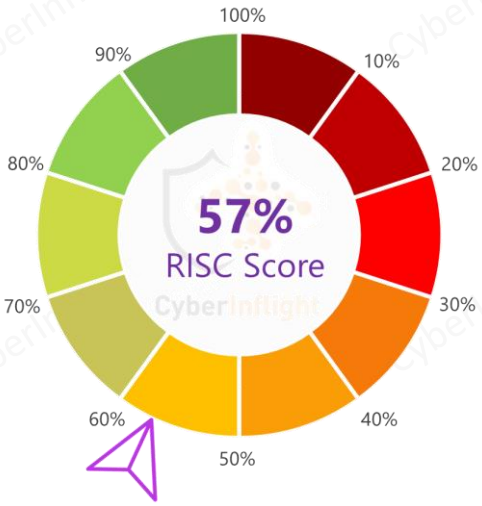
January 30 – February 5, 2024

Timeframe : Weekly
# of articles identified : 19
Est. time to read : 30 minutes

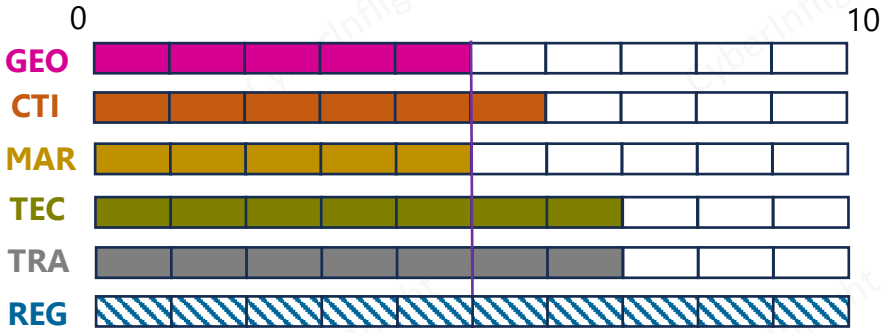
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

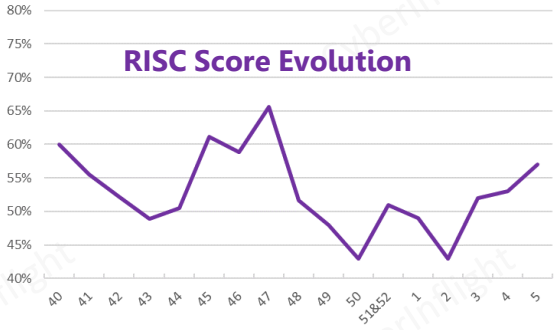
- GEOPOLITIC
- THREAT INTELLIGENCE
- MARKET & COMPETITION
- TECHNOLOGY
- TRAINING & EDUCATION
- IMPORTANT NEWS

Overview & RISC Score



Increase from last week (from 53% to 57%)





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

[illegible]

THREAT INTELLIGENCE

[illegible]

★ **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

[illegible]

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/

[illegible]

TECHNOLOGY

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/

TRAINING & EDUCATION

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

TRAINING & EDUCATION

Decoding the European Space Conference: Key Insights from a Cybersecurity Perspective
The cybersecurity experts at DLR CSR play a pivotal role in the secure operation of the infrastructure in Oberpfaffenhofen, catering to over 1.1 billion Galileo users, the European Commission, and EUSPA. Cybersecurity, especially, is a crucial cornerstone due to the increasing importance of Global Navigation Satellite Systems (GNSS) and the growing threats against these systems. **#Conference #GNSS**
Link: https://www.linkedin.com/pulse/decoding-european-space-conference-key-insights-from-cybersecurity-z1mfc/

We Need Cybersecurity in Space to Protect Satellites
Protecting our celestial sentinels is essential to safeguard the very fabric of our interconnected world and thereby ensure the continued advancement of human progress in the digital age. Today's efforts to secure our satellites will protect our global infrastructure for future generations. **#Resilience #Satellite**
Link: https://www.scientificamerican.com/article/we-need-cybersecurity-in-space-to-protect-satellites/

The Downlink (Feb 01, 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, Viasat's Chief Cybersecurity and Data Officer for Government Systems, in his first sit-down interview since the satellite communications company weathered a notorious cyberattack on February 24, 2022. Erin Miller, the Space Information Sharing and Analysis Center's Executive Director, and Frank Backes, CEO of Capella Space, a company providing earth observation products to government/commercial customers. **#Podcast #Cyberattacks**
Link: https://defensescoop.com/2024/02/01/the-downlink-feb-01-24-space-money-when-nation-states-target-the-commercial-space-sector/