



SPACE CYBERSECURITY WEEKLY WATCH

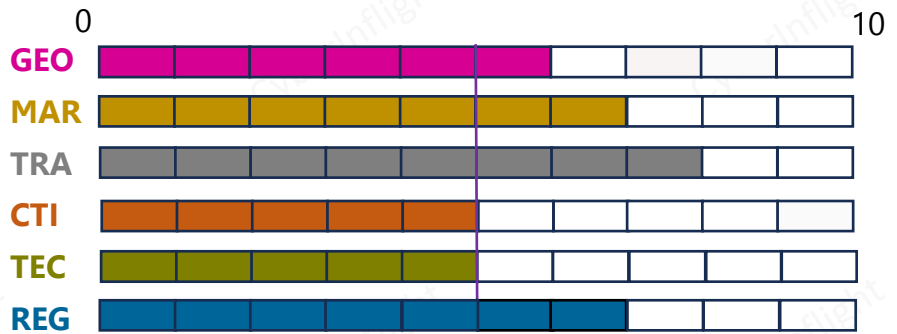
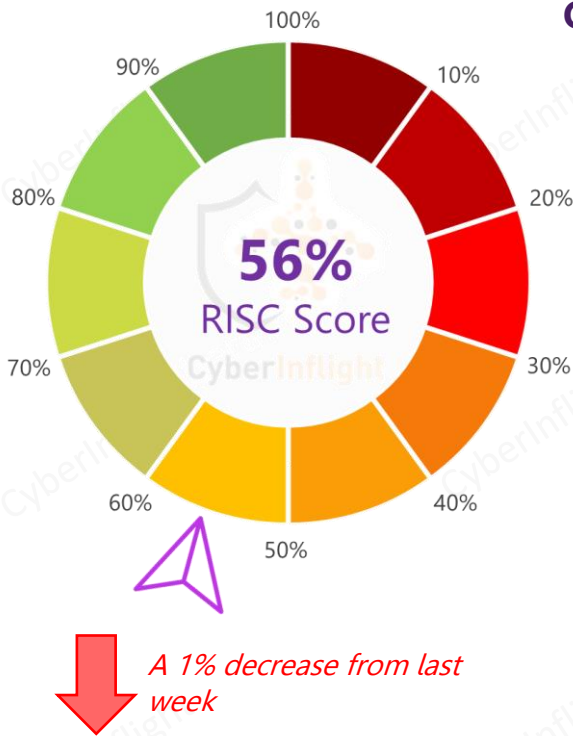
Week 20
May 14 - 20, 2024

Timeframe : Weekly
of articles identified : 27
Est. time to read : 45 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
- MARKET INTELLIGENCE
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- TECHNOLOGY
- REGULATION
- ★ IMPORTANT NEWS

Overview & RISC Score



RISC Score Evolution



This W20 shows a slight decrease from last week's RISC Score level. The tendency still remains constant, except for W17 which showed the highest score level of the year.

This week's RISC score is 56%. This week, France remains undecided about an offer from US Space Command to take part in Operation Olympic Defender, the US-led initiative to strengthen defense and deter hostility in space. In addition, the Federal Office for Information Security (BSI) unveils its cybersecurity framework for space applications. The office identified actions and goals to implement suitable measures for designing cybersecurity for space infrastructures. On the market front, Governor of Maryland and State of South Australian Premier signed a Memorandum of Understanding between Maryland & South Australia to collaborate in cybersecurity, outer space and high technology. In addition, China has emerged as a global leader in tackling critical infrastructure issues through its groundbreaking QKD technology, demonstrated by its quantum satellite program. On the technology front, SEALSQ announced that its post-quantum semiconductors solutions are designed to provide a reliable foundation for secure computing and transaction verification. The company stands at the forefront of integrating quantum computing and IoT, offering a unique and trusted cybersecurity platform. Finally, the Ukrainian military's Starlink terminals went down on the first day of the Russian offensive in Kharkiv Oblast on May 10th. They were jammed by Russian electronic warfare systems.



GEOPOLITIC



The US Air Force is leading 40 air campaigns aimed to cause IIRs just before and in future fight

The US Air Force is leading 40 air campaigns aimed to cause IIRs just before and in future fight operations and during. The campaigns are intended to be in the form of simulated IIRs, which are designed to cause IIRs in the form of simulated IIRs. The campaigns are intended to be in the form of simulated IIRs, which are designed to cause IIRs in the form of simulated IIRs.

Link: [https://breakingdefense.com/2024/05/france-undecided-on-us-offer-to-join-olympic-defender-space-effort/](#)



France undecided on US offer to join 'Olympic Defender' space effort

France remains undecided about an offer from US Space Command to take part in Operation Olympic Defender, the US-led initiative to strengthen defense and deter hostility in space – but says that if it does join up, it will not be turning over operational control of its military space capabilities to its US allies. **#France #OlympicDefender**

Link: <https://breakingdefense.com/2024/05/france-undecided-on-us-offer-to-join-olympic-defender-space-effort/>



Strong through Biden's IIR 22 weeks ongoing need to shore up critical infrastructure security and resilience

The Department of Defense (DoD) is currently conducting a series of IIRs to shore up critical infrastructure security and resilience. The IIRs are designed to be in the form of simulated IIRs, which are designed to cause IIRs in the form of simulated IIRs. The IIRs are designed to be in the form of simulated IIRs, which are designed to cause IIRs in the form of simulated IIRs.

Link: [https://breakingdefense.com/2024/05/france-undecided-on-us-offer-to-join-olympic-defender-space-effort/](#)



REGULATORY



Law to allow international legal cooperation on cyberattacks targeting space systems

The law to allow international legal cooperation on cyberattacks targeting space systems. The law is designed to be in the form of simulated IIRs, which are designed to cause IIRs in the form of simulated IIRs. The law is designed to be in the form of simulated IIRs, which are designed to cause IIRs in the form of simulated IIRs.

Link: [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/IT-Sicherheit-in-Luft-und-Raumfahrt/it-sicherheit-in-luft-und-raumfahrt_node.html](#)



The Federal Office for Information Security (BSI) unveils its cybersecurity framework for space applications

Satellite applications have become an integral part of everyday life. Space-based systems are also highly relevant for sovereign task. The BSI is responsible for strengthening the information security of such satellite systems and ensuring the availability of services via integral, authentic communications. The office identified actions and goals to implement suitable measures for designing cybersecurity for space infrastructures. The document is for now only available in German, but the English version is to be released soon. **#BSI #SpaceCybersecurity**

Link: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/IT-Sicherheit-in-Luft-und-Raumfahrt/it-sicherheit-in-luft-und-raumfahrt_node.html



The Belgian IIR law has been published

The Belgian IIR law has been published. The law is designed to be in the form of simulated IIRs, which are designed to cause IIRs in the form of simulated IIRs. The law is designed to be in the form of simulated IIRs, which are designed to cause IIRs in the form of simulated IIRs.





MARKET & COMPETITION

Space Space awarded \$1.6m contract to join UK's Civil Security Space program for civil security and crisis event

The UK Space Agency has awarded a contract to join the UK's Civil Security Space program for civil security and crisis event. The contract is for the development and testing of a satellite-based system for monitoring and detecting civil security and crisis events.

Link: [https://www.gov.uk/government/news/uk-space-agency-awards-contract-to-join-civil-security-space-program](#)



Advancing military and aerospace software testing with data-driven development strategy

The software development and testing process is being revolutionized by data-driven development (DD) strategies. DD is a software development approach that uses data to inform the development and testing process, leading to faster development and testing cycles.

Link: [https://www.cyberinflight.com/news/advancing-military-and-aerospace-software-testing-with-data-driven-development-strategy](#)



ESA's €1.6m in 14 defense industry projects through the European Defense Fund

The European Space Agency (ESA) has awarded a total of €1.6m in 14 defense industry projects through the European Defense Fund. The projects are aimed at supporting the development and testing of defense-related software and hardware.

Link: [https://www.esa.int/ESA/News/ESA_awards_14_defence_industry_projects_through_the_European_Defense_Fund](#)



Singapore's latest space cybersecurity software also supports

Singapore's latest space cybersecurity software also supports the development and testing of defense-related software and hardware. The software is designed to protect space-based systems from cyber threats.

Link: [https://www.cyberinflight.com/news/singapores-latest-space-cybersecurity-software-also-supports](#)



Maryland and South Australia officials sign Memorandum of Understanding to collaborate in cybersecurity, outer space and high tech

Governor Wes Moore and State of South Australian Premier, Peter Malinauskas, signed a Memorandum of Understanding between Maryland and South Australia to collaborate in cybersecurity, outer space and high tech. also there: Australian Ambassador Kevin Rudd, MD Sec. Commerce Kevin Anderson. #SouthAustralia #Maryland

Link: <https://x.com/SenatorSusanLee/status/1792360166127755674>



India to use and secure Global communication system project

India is set to use and secure the Global communication system project. The project is a satellite-based communication system that will provide secure and reliable communication services.

Link: [https://www.cyberinflight.com/news/india-to-use-and-secure-global-communication-system-project](#)



6 years later

Six years after its launch, the Global communication system project is still providing secure and reliable communication services. The project has been a success story for India's space program.

Link: [https://www.cyberinflight.com/news/6-years-later](#)



TRAINING & EDUCATION

Developing the criteria for detecting the spending and procurement characteristics of DHS agents using the experimental simulation model

The Department of Homeland Security (DHS) is developing the criteria for detecting the spending and procurement characteristics of DHS agents using the experimental simulation model. The model is designed to identify and track the spending and procurement patterns of DHS agents.

Link: [https://www.dhs.gov/news/2024/05/14/dhs-develops-criteria-for-detecting-the-spending-and-procurement-characteristics-of-dhs-agents](#)





TRAINING & EDUCATION



China's quantum satellites: paving the way for a global unhackable ground and space network infrastructure

In an era of escalating cyber threats and the increasing vulnerability of critical infrastructures, the need for secure communication systems has never been more critical. As cyber warfare targets essential information systems, nations are compelled to fortify their communication channels against potential breaches. Compounding this challenge is the looming threat of quantum computers, capable of rendering conventional cryptographic methods obsolete. China has emerged as a global leader in tackling these issues through its groundbreaking QKD technology, notably demonstrated by its quantum satellite program. **#QuantumSatellites #SpaceSecurity**

Link: <https://idstch.com/cyber/chinas-quantum-satellites-paving-the-way-for-a-global-unhackable-ground-and-space-network-infrastructure/>



TECHNOLOGY



SEALQ quantum computing and IoT: a transformative synergy with next-generation root of trust IoT

Leader in semiconductor, PKI and Post-Quantum technology development, SEALSQ, announced that its post-quantum semiconductor solutions are designed to provide a reliable foundation for secure computing and transaction verification in a world threatened by quantum computing capabilities. SEALSQ stands at the forefront of integrating quantum computing and IoT, offering a unique and trusted cybersecurity platform. It offers innovative solutions able to ensure the security and integrity of digital interactions and transactions across various industries including fintech, healthcare, automotive, defense and space research. **#SEALQ #QuantumComputing**

Link: <https://www.globenewswire.com/news-release/2024/05/14/2881407/0/en/SEALQ-Quantum-Computing-and-IoT-A-Transformative-Synergy-with-Next-Generation-Root-of-Trust-IoT.html>





THREAT INTELLIGENCE

System may disrupt US satellite by tracking ground stations

The US Space Force and other agencies are concerned about a satellite system that could track and disrupt US satellite ground stations. The system, known as the Russian Ground Station Tracking System (RGS), is believed to be capable of identifying and tracking US satellite ground stations and their locations. This information could be used to disrupt or destroy the ground stations, which would severely impact US satellite operations.

Link: [https://www.defense.gov/Newsroom/News-Transcripts/Transcript.aspx?TranscriptID=488888](#)

No other leader: military will need multiple systems to back up GPS

The US military is looking for a way to back up its GPS system in case it is disrupted. The military is currently using GPS for navigation and timing, but it is aware that GPS is a single point of failure. The military is looking for a way to back up GPS with other systems, such as inertial navigation systems and other satellite-based systems.

Link: [https://www.defense.gov/Newsroom/News-Transcripts/Transcript.aspx?TranscriptID=488888](#)

AI-powered technology is significantly worse than Russia's

The US military is aware that Russia is using AI-powered technology in its military operations. The US military is currently using AI for a variety of tasks, such as target identification and threat detection. However, the US military is aware that Russia is using AI-powered technology that is significantly worse than the US military's current capabilities.

Link: [https://www.defense.gov/Newsroom/News-Transcripts/Transcript.aspx?TranscriptID=488888](#)



Ukrainian military's Starlink terminals went down at beginning of Russian offensive in Kharkiv Oblast

The Ukrainian military's Starlink terminals went down on the first day of the Russian offensive in Kharkiv Oblast on May 10th. They were jammed by Russian electronic warfare systems. **#Ukraine #Starlink**

Link: <https://www.pravda.com.ua/eng/news/2024/05/17/7456272/>

Space systems face flight after alternative to GPS approved system found

The US military is looking for a way to back up its GPS system in case it is disrupted. The military is currently using GPS for navigation and timing, but it is aware that GPS is a single point of failure. The military is looking for a way to back up GPS with other systems, such as inertial navigation systems and other satellite-based systems.

Link: [https://www.defense.gov/Newsroom/News-Transcripts/Transcript.aspx?TranscriptID=488888](#)

Combating jamming and spoofing

The US military is aware that Russia is using jamming and spoofing techniques to disrupt US satellite operations. The US military is currently using a variety of techniques to combat jamming and spoofing, such as frequency hopping and spread spectrum techniques.

Link: [https://www.defense.gov/Newsroom/News-Transcripts/Transcript.aspx?TranscriptID=488888](#)

GPS spoofing is a new concern for global navigation security

The US military is aware that Russia is using GPS spoofing techniques to disrupt US satellite operations. The US military is currently using a variety of techniques to combat GPS spoofing, such as frequency hopping and spread spectrum techniques.

Link: [https://www.defense.gov/Newsroom/News-Transcripts/Transcript.aspx?TranscriptID=488888](#)

GPS jamming is a low priority and that's a mistake

The US military is aware that Russia is using GPS jamming techniques to disrupt US satellite operations. The US military is currently using a variety of techniques to combat GPS jamming, such as frequency hopping and spread spectrum techniques.

Link: [https://www.defense.gov/Newsroom/News-Transcripts/Transcript.aspx?TranscriptID=488888](#)

