



SPACE CYBERSECURITY WEEKLY WATCH

Week 47

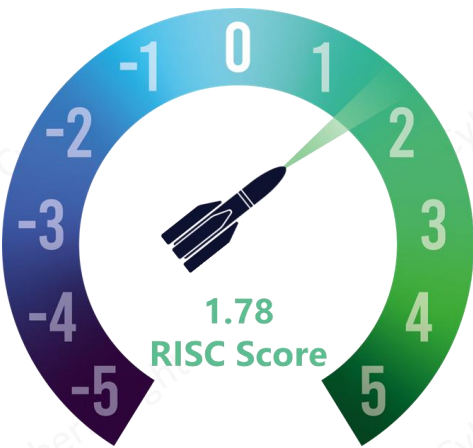
November 18- 24, 2025

Timeframe: Weekly
of articles identified: 45
Est. time to read: 90 minutes

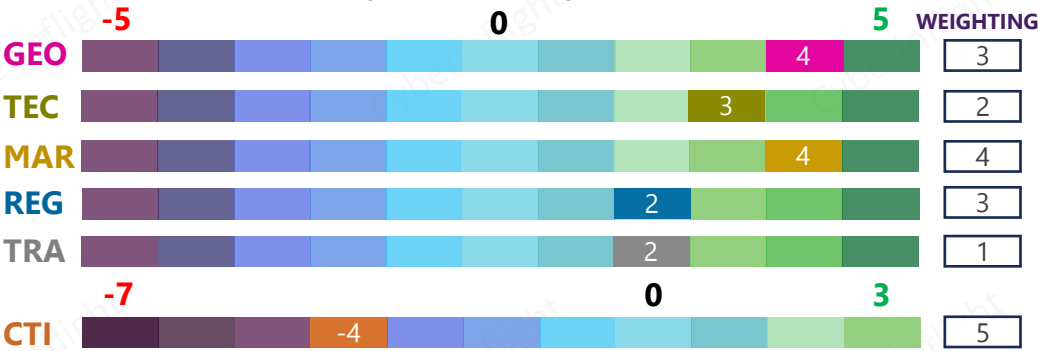
Articles, company’s communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

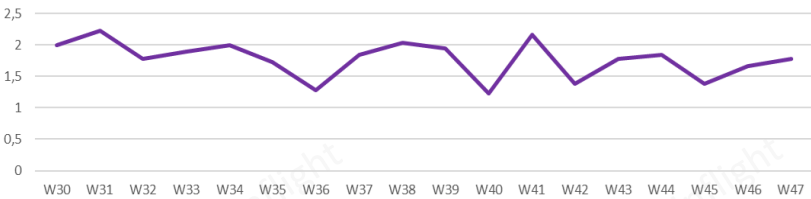
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



↑ The RISC score for this watch has slightly increased to 1.78. Despite enhancements in nearly all areas, partly driven by advancements announced at recent international events focused on space cybersecurity, the threat intelligence section balanced the score.

This week, Germany unveiled its first national space security strategy, with Defense Minister Boris Pistorius vowing to expand both military and civilian capabilities in orbit. The strategy covers all areas relevant to Germany’s security, from spaceflight projects to the expansion of satellite networks and promoting responsible state behavior in space. On the regulatory front, attention turns to the new rules recently issued by the Pentagon, which require commercial satellite operators to employ specific measures if U.S. intelligence agencies or military services utilize their products or services. On the technological front, the U.S. Department of Homeland Security (DHS) and Aerospace Corp. want satellite operators to volunteer to test out new tools they’re building to detect cyberattacks on spacecraft, officials said at the CyberSat conference. From a technological standpoint, the Department of Homeland Security (DHS) and Aerospace Corp. want satellite operators to volunteer to test out new tools they are building to detect cyberattacks on spacecraft, officials said at the same conference. On the market side, the United Arab Emirates Space Center and Thales Alenia Space signed a partnership to explore opportunities in low-Earth orbit (LEO) space navigation systems. The collaboration aims to enhance the robustness and sovereignty of future navigation services while deepening international cooperation and knowledge exchange. Meanwhile, on the threat intelligence front, coverage focuses on a Chinese study that shows how China could potentially jam Elon Musk’s Starlink satellites if it were to invade Taiwan. It indicates that the PLA could achieve this complex task on an immense scale, using approximately 1,000 to 2,000 specialized signal-jamming drones. Lately, on the threat & education front, YouTuber Rob VK8FOES has uploaded a video showing how to install and use the “dontlookup” open-source Linux Python research tool for evaluating satellite IP link security.



GEOPOLITICS

Germany's Ministry of Transport and Communications strengthens the resilience of its satellite navigation system against hybrid threats

According to the newly adopted Transport and Communications Security Strategy, it is essential for the German state to reach an agreement on a specific action plan that would enable a coordinated response to hybrid threats, including from adversaries to satellite navigation systems. Within the state, the state authorities are responsible for ensuring the resilience of the system and a functioning emergency response and crisis management.

Sources: [BZ](#)



ESA establishes space cyber program after last month's Romanian Space Force exercise

The European Space Agency (ESA) has established a new space cyber program to coordinate space cyber efforts across the agency. ESA officials stated that today's meeting focused on the mission integration of cyber and space systems. From the start, the cyber team has been collaborating with the ground segment, where a cyber team would not get along with the satellite. The program encompasses the need for cyber resilience, and security operations, as essential components such as cyber threat detection or cyber threat attribution will not be completely fulfilled without a space system. **ESA CyberProgram**

Sources: [ESA](#)



US considers C/ESAs to protect critical positioning and timing signals

The US government has adopted critical signals to strengthen the satellite positioning, navigation and timing (PNT) infrastructure, aiming to protect against threats from adversaries to critical signals, such as GPS. The signals are being developed in collaboration with the European Space Agency (ESA) and are designed to be used in critical signals and to be used in critical signals. **ESA CyberProgram**

Sources: [US DoD](#), [ESA](#)



The German Federal Government presents the first Space Safety and Security Strategy

Germany unveiled the country's first national space security strategy, with Defense Minister Boris Pistorius vowing to expand military and civilian capabilities in orbit. The strategy covers all areas relevant to Germany's security, from spaceflight projects to the expansion of satellite networks and promoting responsible state behavior in space. The objective is to become more capable of action also in space with partners in the EU, NATO and other partners around the world. The strategy comes weeks after Pistorius announced plans for the Armed Forces to spend €35bn (\$41bn) by 2030 on space defenses, citing growing threats posed by Russia and potentially China. **#SpaceSecurity #Strategy**

Sources: [Breaking Defense](#), [German Government](#)



Germany plans to boost funding for European Space Agency, says minister

Germany plans to significantly increase funding for the European Space Agency, with Defense Minister Boris Pistorius stating that the government will increase its contribution to the ESA budget. Pistorius stated that the government will increase its contribution to the ESA budget, which will be used to fund the ESA's space programs. The funding will be used to fund the ESA's space programs, which will be used to fund the ESA's space programs. **ESA CyberProgram**

Sources: [BZ](#)



ESA's new staff, ESA poised to take on defense role

The new staff of the European Space Agency (ESA) is being established, with the agency poised to take on a defense role. The new staff will be responsible for the ESA's space programs, which will be used to fund the ESA's space programs. The funding will be used to fund the ESA's space programs, which will be used to fund the ESA's space programs. **ESA CyberProgram**

Sources: [ESA](#), [ESA](#)



REGULATION

EU's new cyber law strengthens cyber security against cyberattacks in space

The European Union (EU) has adopted a new cyber law to strengthen cyber security against cyberattacks in space. The new law will be used to fund the EU's space programs, which will be used to fund the EU's space programs. The funding will be used to fund the EU's space programs, which will be used to fund the EU's space programs. **ESA CyberProgram**

Sources: [BZ](#)



ESA's new staff, ESA poised to take on defense role

The new staff of the European Space Agency (ESA) is being established, with the agency poised to take on a defense role. The new staff will be responsible for the ESA's space programs, which will be used to fund the ESA's space programs. The funding will be used to fund the ESA's space programs, which will be used to fund the ESA's space programs. **ESA CyberProgram**

Sources: [BZ](#)



REGULATION

★ New cybersecurity rules for Pentagon's commercial satellite vendors

The Pentagon recently issued new rules on cybersecurity measures that commercial satellite operators must employ if their products or services are used by U.S. intelligence agencies or military services. The rules, from the Pentagon-led interagency Committee on National Security Systems contain important new provisions, Brandon Bailey from Aerospace Corp., a federally funded research and development nonprofit, told the annual CyberSat conference. **#Pentagon #Rules**

Source: [Air & Space Forces Magazine](#)



Preparing up our rules in cybersecurity management, DHS Secretary (DHS News)

The Department of Homeland Security (DHS) is working to update its cybersecurity management and operations (CISO) Program. This program is a critical part of DHS's efforts to protect its information systems, its people, and its mission. The program is being updated to reflect the latest threats and the need for more robust cybersecurity measures. **#DHS #CyberTools**



TECHNOLOGY

★ DHS wants satellite volunteers to test new cyber tools

The Department of Homeland Security (DHS) and Aerospace Corp. want satellite operators to volunteer to test out new tools they're building to detect cyberattacks on spacecraft, officials said at CyberSat conference. As part of its mission to protect critical infrastructure, DHS is working to develop cyber resilience tools for satellites that provide vital resources including position, navigation and timing (PNT) services like GPS, as well as communication channels like phone and internet. **#DHS #CyberTools**

Source: [Via Satellite](#)



Big Technology satellite launch is first step to enable emergency broadcast message from space

The technology is a satellite-based system that will allow satellite operators to provide an emergency broadcast message from space. The system is being developed by a consortium of satellite operators and is expected to be operational by 2025. The system will allow satellite operators to broadcast emergency messages from space, providing a critical link between ground-based emergency services and satellite-based emergency services. **#DHS #CyberTools**



Source: [Via Satellite](#)

USDA satellite system defined DHS mission needs for Critical Infrastructure

A report issued by the Department of Homeland Security (DHS) and the Department of Agriculture (USDA) outlined the needs of the Critical Infrastructure (CI) system. The report is a key part of the DHS's efforts to protect its information systems, its people, and its mission. The report is being updated to reflect the latest threats and the need for more robust cybersecurity measures. **#DHS #CyberTools**



Source: [Via Satellite](#)

Quantum Computer New satellite system are enabling military intelligence beyond GPS

A new satellite system is being developed by a consortium of satellite operators and is expected to be operational by 2025. The system will allow satellite operators to broadcast emergency messages from space, providing a critical link between ground-based emergency services and satellite-based emergency services. **#DHS #CyberTools**



Source: [Via Satellite](#)

DHS satellite system ground quantum communication network

A new satellite system is being developed by a consortium of satellite operators and is expected to be operational by 2025. The system will allow satellite operators to broadcast emergency messages from space, providing a critical link between ground-based emergency services and satellite-based emergency services. **#DHS #CyberTools**



Source: [Via Satellite](#)

University of Illinois researcher developing radio frequency interference solutions

A new satellite system is being developed by a consortium of satellite operators and is expected to be operational by 2025. The system will allow satellite operators to broadcast emergency messages from space, providing a critical link between ground-based emergency services and satellite-based emergency services. **#DHS #CyberTools**



Source: [Via Satellite](#)

TECHNOLOGY

ESA's Galileo LEO-PNT program advances - Thales Alenia Space delivers navigation payload antenna

In the first step towards developing and testing LEO-PNT antenna systems, Europe's leading space antenna manufacturer, Thales Alenia Space, has delivered a key component of one of the two antennas supporting the LEO-PNT program. The antenna system will be designed and delivered by the antenna supplier, including the navigation payload antenna. The antenna system will be designed and delivered by the antenna supplier, including the navigation payload antenna. The antenna system will be designed and delivered by the antenna supplier, including the navigation payload antenna.

Source: [ESA](#)



Thales Alenia Space in joint quantum GNSS-like, navigation, ready to deliver satellite communication services

In the framework of the joint quantum GNSS-like, navigation, ready to deliver satellite communication services, Thales Alenia Space is working on the development of a quantum navigation system. The system will be designed and delivered by the antenna supplier, including the navigation payload antenna. The antenna system will be designed and delivered by the antenna supplier, including the navigation payload antenna.

Source: [ESA](#)



Europe launching the Quantum Europe Strategy for 2040

The Quantum Europe Strategy is a key element of the European Union's strategy for 2040. The strategy will be designed and delivered by the antenna supplier, including the navigation payload antenna. The antenna system will be designed and delivered by the antenna supplier, including the navigation payload antenna.

Source: [European Commission](#)



MARKET & COMPETITION



UAE Space Center, Thales Alenia Space partner on LEO-PNT navigation system

The National Space Science and Technology Center (NSSTC) and Thales Alenia Space are cooperating to explore opportunities in low-Earth orbit (LEO) space navigation systems. The collaboration reflects a vision to explore pathways that can enhance the robustness and sovereignty of future navigation services while deepening international cooperation and knowledge exchange between the United Arab Emirates and Europe in the field of space technology.

#UAESpaceCenter #Cooperation

Source: [GPS World](#)



France and Quantum Systems partner on joint satellite and drone monitoring capabilities for European defense missions

France and Quantum Systems have announced a strategic partnership to develop joint satellite and drone monitoring capabilities for European defense missions. The partnership will be designed and delivered by the antenna supplier, including the navigation payload antenna. The antenna system will be designed and delivered by the antenna supplier, including the navigation payload antenna.

Source: [France 24](#)



USAF uses GPS to test GPS alternatives for critical infrastructure

The US Air Force has conducted a series of tests to evaluate GPS alternatives for critical infrastructure. The tests will be designed and delivered by the antenna supplier, including the navigation payload antenna. The antenna system will be designed and delivered by the antenna supplier, including the navigation payload antenna.

Source: [USAF](#)



India is developing quantum resistant secure processor with the US looking for US applications

India is developing a quantum resistant secure processor with the US looking for US applications. The processor will be designed and delivered by the antenna supplier, including the navigation payload antenna. The antenna system will be designed and delivered by the antenna supplier, including the navigation payload antenna.

Source: [India Today](#)



MARKET & COMPETITION

UAE to build its first space to ground quantum communication network

The Technology Innovation Institute (TII) has unveiled the first quantum communication network (QCN) in collaboration with the UAE Ministry of Defense and the UAE Space Agency (UAE SA). The network, which will connect the UAE's first quantum communication satellite, the QCN-1, to the ground-based quantum communication network, will be the first of its kind in the world. The network will be used to secure the communication of the UAE's first quantum communication satellite, the QCN-1, to the ground-based quantum communication network, which will be the first of its kind in the world. The network will be used to secure the communication of the UAE's first quantum communication satellite, the QCN-1, to the ground-based quantum communication network, which will be the first of its kind in the world.

Source: [UAE Ministry of Defense](#)



US to create table understanding intelligence with the space-based fleet

The US Space Force is creating a table understanding intelligence with the space-based fleet. The table understanding intelligence is a new type of intelligence that is created by the US Space Force. The table understanding intelligence is a new type of intelligence that is created by the US Space Force. The table understanding intelligence is a new type of intelligence that is created by the US Space Force. The table understanding intelligence is a new type of intelligence that is created by the US Space Force. The table understanding intelligence is a new type of intelligence that is created by the US Space Force.

Source: [US Space Force](#)



Creating the table for resilient, secure space-based communication

The US Space Force is creating a table for resilient, secure space-based communication. The table for resilient, secure space-based communication is a new type of communication that is created by the US Space Force. The table for resilient, secure space-based communication is a new type of communication that is created by the US Space Force. The table for resilient, secure space-based communication is a new type of communication that is created by the US Space Force. The table for resilient, secure space-based communication is a new type of communication that is created by the US Space Force.

Source: [US Space Force](#)



Winning the space cyber war requires continuous investment, vigilance, and collaboration

In the article, Dr. Hani, who is president of the US Space Force, states that a cyber threat to the space-based fleet is a real threat. The cyber threat to the space-based fleet is a real threat. The cyber threat to the space-based fleet is a real threat. The cyber threat to the space-based fleet is a real threat. The cyber threat to the space-based fleet is a real threat.

Source: [US Space Force](#)



SpaceX and U.S. Navy announce strategic partnership manufacturing alliance

SpaceX, the world's leading private space exploration company, and the US Navy have announced a strategic partnership manufacturing alliance. The partnership manufacturing alliance is a new type of alliance that is created by SpaceX and the US Navy. The partnership manufacturing alliance is a new type of alliance that is created by SpaceX and the US Navy. The partnership manufacturing alliance is a new type of alliance that is created by SpaceX and the US Navy. The partnership manufacturing alliance is a new type of alliance that is created by SpaceX and the US Navy.

Source: [SpaceX](#)



SpaceX awarded contract to provide advanced space surveillance and tracking

SpaceX has been awarded a contract to provide advanced space surveillance and tracking. The contract is a new type of contract that is created by SpaceX. The contract is a new type of contract that is created by SpaceX. The contract is a new type of contract that is created by SpaceX. The contract is a new type of contract that is created by SpaceX. The contract is a new type of contract that is created by SpaceX.

Source: [SpaceX](#)



USAF says Russia is building world's first air-breathing satellite for very low Earth orbit

The US Air Force (USAF) has announced that Russia is building a world's first air-breathing satellite for very low Earth orbit. The air-breathing satellite is a new type of satellite that is created by Russia. The air-breathing satellite is a new type of satellite that is created by Russia. The air-breathing satellite is a new type of satellite that is created by Russia. The air-breathing satellite is a new type of satellite that is created by Russia. The air-breathing satellite is a new type of satellite that is created by Russia.

Source: [US Air Force](#)



THREAT INTELLIGENCE

THREAT INTELLIGENCE



China simulates jamming Starlink over Taiwan, mission to require over 1,000 drones

Instead of focusing on whether Starlink can be jammed in theory, Chinese military planners are increasingly concerned with how such a feat could be attempted in a real conflict over Taiwan. The challenge is staggering: Taiwan and its allies could rely on a constellation of more than 10,000 satellites that hop frequencies, reroute traffic and resist interference in real time. However, a recent simulation study by Chinese researchers delivers the most detailed public attempt yet to model a potential countermeasure. It concludes that disrupting Starlink across an area comparable to Taiwan is technically achievable – but only with a massive electronic warfare (EW) force. **#Starlink #Jamming**

Sources: [Interesting Engineering](#), [South China Morning Post](#)



Source suggested by a third party

Source: [Interesting Engineering](#), [South China Morning Post](#)



TRAINING & EDUCATION

Enhancing cyber security leaders to address resilience, compliance and threat intelligence

Enhancing cyber security leaders to address resilience, compliance and threat intelligence. The course is designed to provide a comprehensive overview of the current cyber security landscape, including the latest threats and vulnerabilities. It covers the fundamentals of cyber security, from network security to cloud security, and provides a deep dive into the latest trends and challenges. The course is designed for professionals who are looking to enhance their skills and knowledge in cyber security.



International satellite data and China's cyber threat

The course is designed to provide a comprehensive overview of the current cyber security landscape, including the latest threats and vulnerabilities. It covers the fundamentals of cyber security, from network security to cloud security, and provides a deep dive into the latest trends and challenges. The course is designed for professionals who are looking to enhance their skills and knowledge in cyber security.



Quantum Computing in Space

Quantum Computing in Space. This course is designed to provide a comprehensive overview of the current cyber security landscape, including the latest threats and vulnerabilities. It covers the fundamentals of cyber security, from network security to cloud security, and provides a deep dive into the latest trends and challenges. The course is designed for professionals who are looking to enhance their skills and knowledge in cyber security.



Building a Quantum Computing in Space International (QI) Space Data Space Competition and International Meeting

Building a Quantum Computing in Space International (QI) Space Data Space Competition and International Meeting. This course is designed to provide a comprehensive overview of the current cyber security landscape, including the latest threats and vulnerabilities. It covers the fundamentals of cyber security, from network security to cloud security, and provides a deep dive into the latest trends and challenges. The course is designed for professionals who are looking to enhance their skills and knowledge in cyber security.



Using the Don't Look Up tool to eavesdrop on insecure private satellite communications

Over on YouTube, Rob VK8FOES has uploaded a video showing how to install and use the "dontlookup" open-source Linux Python research tool for evaluating satellite IP link security. In the video, he discusses the new dontlookup tool, which is an excellent one-stop shop open-source tool for parsing IP data from these satellites. He goes on to show the full steps on how to install and use the tool in Linux. The end result is private internet satellite data being visible in Wireshark.

#DontLookUp #Video

Source: [RTL-SDR](#)



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