

SPACE CYBERSECURITY WEEKLY WATCH

W22

May 27 – June 1, 2026

Timeframe: Weekly

of news identified: 42

Est. time to read: 85 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.

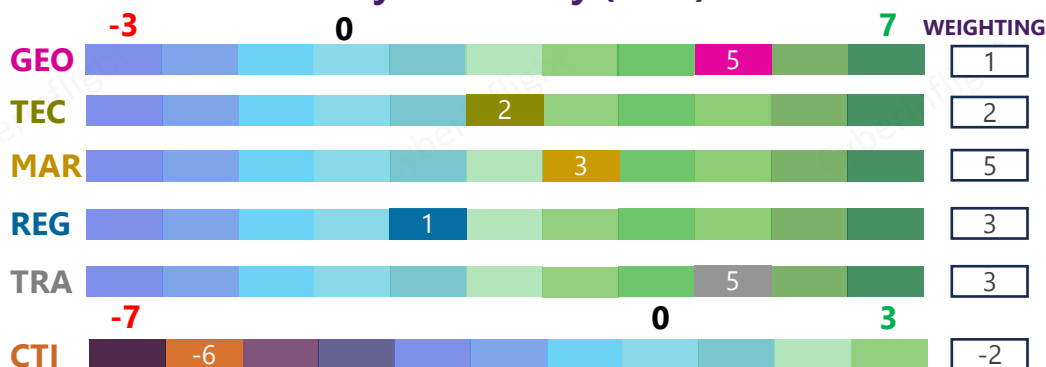
- GEOPOLITICS
- TECHNOLOGY
- MARKET & COMPETITION
- REGULATION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- ★ IMPORTANT NEWS

RISC Score Assessment

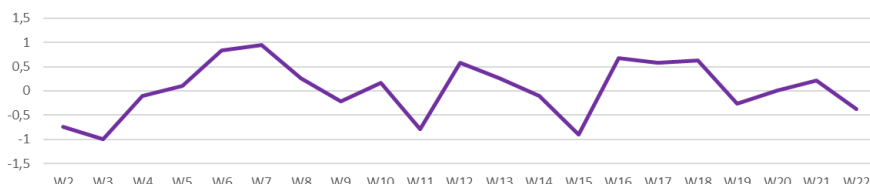


The RISC score for this watch is -0.37, a decrease of 0.58 points compared to the previous week. This is mainly due to a negative climate in Threat intel, with several alleged cyberattacks against the space domain reported.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



This week, on the geopolitical front, **European officials are calling for greater integration of cybersecurity into mission design.** Moreover, in the U.S., the top member on the House Armed Services subcommittee focused on cyber had a stark warning about **how China is positioning itself to overwhelm the U.S. military in cyberspace.** On the regulation side, this year's edition of the **ENISA NIS360 report shows improvement in cybersecurity maturity of EU critical sectors** while the level of criticality in sectors remains comparatively more stable. On the market front, the **EUSPA's EU Space Market Report 2026 was published** and presents key trends, forecasts and insights shaping the evolution of the global space economy. On the threat side, an article highlighting **407 cyberattacks against the space sector in 2025** was published by Air&Cosmos, highlighting that cyber-threats are gradually replacing kinetic threats on the list of concerns. These attacks take various forms and primarily target ground-based systems. Moreover, **a threat actor claims to have successfully breached the Spanish Space Agency and stolen a comprehensive dataset related to the XMM-Newton space telescope.** On the technological side, **experts at SmallSat Europe tried to decipher between the hype and reality of orbital data centers** — in terms of both technology and economics. On the training and education side, a **webinar by GSOA on Cybersecurity in Space: Hardening networks, supply chains & architectures was made available.** The discussion unpacked the evolving space cybersecurity threat landscape, with increasingly powerful threat actors seeking disruption on space infrastructure as it becomes critical for national security. With satellite systems becoming closely integrated with terrestrial networks, new layers of complexity are introduced, increasing the attack surface, but also opening new opportunities.

GEOPOLITICS

Challenges when collaborating with China on space research and technology

China's space program has a long history of collaboration with other nations, but its growing military capabilities have raised concerns. The United States and other nations are wary of China's intentions in space, particularly its growing military capabilities. This has led to a complex relationship between the two nations, with both sides seeking to balance cooperation and competition.

Report Writing

Source: [TechCrunch](#)



Cybersecurity: Critical delay in the European space sector

Cybersecurity has become a top priority amid the trend toward sovereign space infrastructure in Europe, which lags behind China and the United States in this area. Drawing on lessons learned from Ukraine, officials are calling for greater integration of cybersecurity into mission design. #Cybersecurity #SpaceSector

Source: [Air & Cosmos](#)



When space goes dark, the new frontlines of strategic rivalry

As the world's major powers vie for dominance in space, the competition is moving from the physical to the digital. The United States and China are the primary players in this new arena, with both nations seeking to establish a dominant position in the space domain.

Report Writing

Source: [TechCrunch](#)



In the cyber race against China, CYBERCOM bets on 'quality over quantity.'

The top member on the House Armed Services subcommittee focused on cyber had a stark warning about how America's greatest geopolitical rival is positioning itself to overwhelm the US military in cyberspace. #CYBERCOM #China

Source: [Breaking Defense](#)



Space forces need to secure the systems as cyber grows more embedded

As the world's major powers vie for dominance in space, the competition is moving from the physical to the digital. The United States and China are the primary players in this new arena, with both nations seeking to establish a dominant position in the space domain.

Report Writing

Source: [TechCrunch](#)



Space the new battleground, India must prepare new experts

As the world's major powers vie for dominance in space, the competition is moving from the physical to the digital. The United States and China are the primary players in this new arena, with both nations seeking to establish a dominant position in the space domain.

Report Writing

Source: [TechCrunch](#)



Cyber law deepens Australia-Japan partnership

As the world's major powers vie for dominance in space, the competition is moving from the physical to the digital. The United States and China are the primary players in this new arena, with both nations seeking to establish a dominant position in the space domain.

Report Writing

Source: [TechCrunch](#)



Space forces cyber expert says cyber policy must align with operational reality

As the world's major powers vie for dominance in space, the competition is moving from the physical to the digital. The United States and China are the primary players in this new arena, with both nations seeking to establish a dominant position in the space domain.

Report Writing

Source: [TechCrunch](#)



Space Italy and Japan launch bilateral strategic dialogue

As the world's major powers vie for dominance in space, the competition is moving from the physical to the digital. The United States and China are the primary players in this new arena, with both nations seeking to establish a dominant position in the space domain.

Report Writing

Source: [TechCrunch](#)



EU/US/EU European interview of Joseph Ruffinello about space cybersecurity

As the world's major powers vie for dominance in space, the competition is moving from the physical to the digital. The United States and China are the primary players in this new arena, with both nations seeking to establish a dominant position in the space domain.

Report Writing

Source: [TechCrunch](#)



REGULATION

★ **ENISA: EU critical sectors improve cybersecurity maturity under NIS2**

This year's edition of the ENISA NIS360 report shows improvement in cybersecurity maturity of EU critical sectors while the level of criticality in sectors remains comparatively more stable. The ENISA NIS360 aims to work as an annual assessment tool supporting national authorities, policymakers and other stakeholders in assessing the cybersecurity maturity and criticality of high criticality sectors under the NIS2 Directive. **#NIS2 #ENISA**

Source: [Insight EU Monitoring](#)



MARKET & COMPETITION

Spain Cybersecurity from Civilian to Defense: ENISA supports the "Shift" to Low Earth Orbit

In late March, the world's first satellite was launched for the Spanish cybersecurity program, which aims to provide an integrated, coordinated response to cyber threats. This is part of a wider strategy to protect national security in space, including those with critical infrastructure. **#ENISA #Spain**

Source: [ENISA](#)



Spain ENISA receives funding for defense, cybersecurity, satellite connectivity and space cooperation drive growth

The satellite connectivity program, which is part of the Spanish cybersecurity strategy, is now being implemented. The program will support the development of a secure, resilient and interoperable satellite network, which will be used to provide critical services to the defense, law enforcement and emergency services. **#ENISA #Spain**

Source: [ENISA](#)

Spain partners with ENISA to strengthen the use of artificial intelligence in security and emergency applications

Spain has signed a partnership agreement with ENISA to strengthen the use of artificial intelligence in security and emergency applications. The agreement will support the development of a secure, resilient and interoperable satellite network, which will be used to provide critical services to the defense, law enforcement and emergency services. **#ENISA #Spain**

Source: [ENISA](#)



★ **Unlock the latest EU Space Market insights**

The EUSPA's EU Space Market Report 2026 presents key trends, forecasts and insights shaping the evolution of the global space economy. Through data-driven analysis and sector-focused perspectives, the report explores how EO, GNSS, Secure SATCOM, and SSA are transforming industries, enabling resilience and supporting innovation across Europe and beyond. **#EUSPA #EUReport**

Sources: [EUSPA](#), [The Brussels Times](#)



THREAT INTELLIGENCE

Malware seen Russia use likely GPS signals up to 200 miles deep into the EU's borders

Malware seen Russia use likely GPS signals up to 200 miles deep into the EU's borders. The malware is designed to intercept and manipulate GPS signals, which are used by a wide range of applications, from navigation to critical infrastructure. **#Malware #Russia**

Source: [ENISA](#)



Malware seen Russia use likely GPS signals up to 200 miles deep into the EU's borders

Malware seen Russia use likely GPS signals up to 200 miles deep into the EU's borders. The malware is designed to intercept and manipulate GPS signals, which are used by a wide range of applications, from navigation to critical infrastructure. **#Malware #Russia**

Source: [ENISA](#)



THREAT INTELLIGENCE

USCJ's Global Maritime Operations group attacks defense, aerospace, telecom sectors using Russian malware

A report from the US Cyber Command (USCJ) states that the Russian Navy's Global Maritime Operations group (GMO) is actively engaged in cyber operations against defense, aerospace, and telecom sectors. The report highlights the group's use of Russian malware to compromise systems across the U.S., Europe, and the Middle East. The operations reportedly involve intercepting satellite communications and collecting data, information, and intelligence. The report also mentions that the group is using a variety of malware, including a new one called 'Magma', which is designed to steal data and disrupt operations. The report concludes that the group's activities pose a significant threat to the U.S. and its allies.

Source: [US Cyber Command](#)

Source: [US Cyber Command](#)

Spain's Navy highlighted space force's needs for distributed ops, 2026

The Spanish Navy's Space Force is planning to develop a distributed operations capability by 2026. The force is currently focused on satellite communications and navigation, but it is expanding its mission to include space situational awareness and missile defense. The force is also developing a new generation of satellites that will be able to operate in a more distributed manner. The force is also developing a new generation of space-based sensors that will be able to detect and track threats in space.

Source: [Spain's Navy](#)

★ 407 cyberattacks against the space sector in 2025

Cyber-threats are gradually replacing kinetic threats on the list of concerns. These attacks take various forms and primarily target ground-based systems. **#SpaceDomain #Cyberattacks**

Source: [Air&Cosmos](#)

Russian electronic warfare jammed satellite communications on a plane carrying the British defense secretary

A British Air Force aircraft carrying Defense Secretary John Healey was in flight when Russian electronic warfare systems jammed its satellite communications. The aircraft was flying over the North Atlantic when it was targeted by Russian electronic warfare systems. The jamming was brief but it caused significant disruption to the aircraft's communications.

Source: [Russia's Navy](#)

USCJ's Global Maritime Operations group attacks defense, aerospace, telecom sectors using Russian malware

A report from the US Cyber Command (USCJ) states that the Russian Navy's Global Maritime Operations group (GMO) is actively engaged in cyber operations against defense, aerospace, and telecom sectors. The report highlights the group's use of Russian malware to compromise systems across the U.S., Europe, and the Middle East. The operations reportedly involve intercepting satellite communications and collecting data, information, and intelligence. The report also mentions that the group is using a variety of malware, including a new one called 'Magma', which is designed to steal data and disrupt operations. The report concludes that the group's activities pose a significant threat to the U.S. and its allies.

Source: [US Cyber Command](#)

★ The alleged database of the Spanish Space Agency is on sale

A threat actor claims to have successfully breached the Spanish Space Agency and stolen a comprehensive dataset related to the XMM-Newton space telescope. **#SpanishSpaceAgency #DataLeak**

Sources: [SOC Radar](#), [X](#)

The alleged unauthorized XMM-Newton dataset is detected for a Japanese Aerospace Company

The Japanese Aerospace Company (JAXA) has detected an unauthorized dataset related to the XMM-Newton space telescope. The dataset is believed to be a copy of the data that was stolen from the Spanish Space Agency. JAXA is currently investigating the source of the dataset and has issued a warning to its employees not to use the data.

Source: [JAXA](#)

The alleged database of XMM-Newton is on sale

A threat actor has announced that the database of the XMM-Newton space telescope is for sale. The database is believed to be a copy of the data that was stolen from the Spanish Space Agency. The threat actor is asking for \$100,000 for the database.

Source: [JAXA](#)

The alleged data of Space Agency is leaked

The Spanish Space Agency (CSA) has announced that it has detected a leak of its data. The data is believed to be a copy of the data that was stolen from the Spanish Space Agency. The CSA is currently investigating the source of the leak and has issued a warning to its employees not to use the data.

Source: [JAXA](#)

The alleged data of the Space Agency System is leaked

The Spanish Space Agency (CSA) has announced that it has detected a leak of its data. The data is believed to be a copy of the data that was stolen from the Spanish Space Agency. The CSA is currently investigating the source of the leak and has issued a warning to its employees not to use the data.

Source: [JAXA](#)

THREAT INTELLIGENCE

Spain alleged unauthorized access to data bank is detected for the Spanish Air

An alleged unauthorized access to a data bank in Spain, involving the Spanish Air Force, has been detected. The access was detected by a Spanish security agency, the Spanish National Intelligence Center (CNI).

Report: [The Guardian](#)

Source: [The Guardian](#)



The Instagram account of the Chief Master Sergeant of the US Space Force got hacked

The Instagram account of the Chief Master Sergeant of the US Space Force was hacked. The account was hacked by a person who used the name "Master Sergeant".

Report: [The Guardian](#)



Sweden says trying to steal Western technology and defense secrets

Sweden says it is trying to steal Western technology and defense secrets. The Swedish government has accused a group of people of trying to steal Western technology and defense secrets.

Report: [The Guardian](#)

Source: [The Guardian](#)



The company Nordbørn in Sweden, Norway, discovered a tracking device under a company vehicle at their high security data center facility

The company Nordbørn in Sweden, Norway, discovered a tracking device under a company vehicle at their high security data center facility. The company discovered the device while conducting a security audit.

Report: [The Guardian](#)



India says it has used spyware to monitor

India says it has used spyware to monitor. The Indian government has accused a group of people of using spyware to monitor. The Indian government has accused a group of people of using spyware to monitor.

Report: [The Guardian](#)



TECHNOLOGY

Looking at security in 2026 powered by AI

Looking at security in 2026 powered by AI. The article discusses the challenges of security in 2026, powered by AI. The article discusses the challenges of security in 2026, powered by AI.

Report: [The Guardian](#)

New form of war: an invisible war of China's AI strategy to dominate warfare

New form of war: an invisible war of China's AI strategy to dominate warfare. The article discusses the challenges of security in 2026, powered by AI. The article discusses the challenges of security in 2026, powered by AI.

Report: [The Guardian](#)

Source: [The Guardian](#)



Orbital data centers must tackle chip lifespan, launch availability, and cybersecurity challenges

One of the big topics, especially in light of the SpaceX initial IPO documents, is the future of orbital data centers and the possibilities of moving compute to space. Experts at SmallSat Europe tried to decipher between the hype and reality of orbital data centers — in terms of both technology and economics. **#OrbitalDataCenters #SmallSatEurope**

Source: [National Cyber Security](#)



USCIS is exploring ways for future offensive cyber ops Chief Scientist

USCIS is exploring ways for future offensive cyber ops. The article discusses the challenges of security in 2026, powered by AI. The article discusses the challenges of security in 2026, powered by AI.

Report: [The Guardian](#)



TRAINING & EDUCATION

Following success in the Space 2025 satellite cyber security summit, CyberInflight is launching a new satellite cyber security training program.

The new program is a 12-week satellite cyber security training program that includes advanced satellite technology, with a focus on satellite cyber security, satellite cyber security, satellite cyber security, satellite cyber security, and satellite cyber security.

Source: [YouTube](#)



CyberInflight is launching a new satellite cyber security training program that includes advanced satellite technology, with a focus on satellite cyber security, satellite cyber security, satellite cyber security, satellite cyber security, and satellite cyber security.

Source: [YouTube](#)



The current state of satellite cyber security is a complex one, with many challenges and opportunities. The current state of satellite cyber security is a complex one, with many challenges and opportunities. The current state of satellite cyber security is a complex one, with many challenges and opportunities.

Source: [YouTube](#)



Space Cyber Security Summit 2025 is a leading event in the satellite cyber security community, bringing together experts from around the world to discuss the latest in satellite cyber security.

Source: [YouTube](#)



Space Security for a Resilient Future is a leading event in the satellite cyber security community, bringing together experts from around the world to discuss the latest in satellite cyber security.

Source: [YouTube](#)



Webinar: Cybersecurity in Space: Hardening networks, supply chains & architectures

The discussion unpacked the evolving space cybersecurity threat landscape, with increasingly powerful threat actors seeking disruption on space infrastructure as it becomes critical for national security. With satellite systems becoming closely integrated with terrestrial networks, new layers of complexity are introduced, increasing the attack surface, but also opening new opportunities. **#Webinar #GSOA**

Source: [Youtube](#)



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