

SPACE CYBERSECURITY WEEKLY WATCH

W18

April 28 – May 4, 2026

Timeframe: Weekly

of articles identified: 27

Est. time to read: 55 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

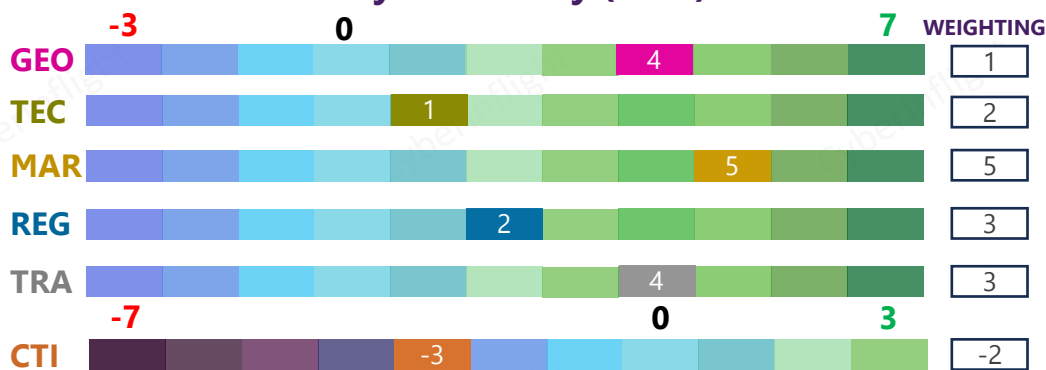
RISC Score Assessment



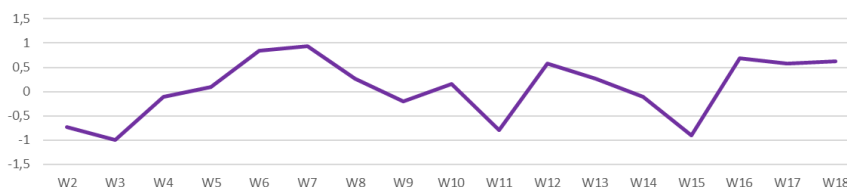
0.63
RISC Score

The RISC score for this watch is 0.63, up 0.5 from last week. This is due to several positive market, geopolitical, and training announcements.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2026



This week, on the geopolitical front, **the U.S. Space Force would receive an additional \$2.9bn over current funding for national security space launches.** Meanwhile, on the European side, **Italian and Spanish institutional and private space stakeholders met in Madrid to foster, together, with the embassy, contacts between Italian and Spanish companies in the space sector.** On the regulation side, the **EEA EFTA States made comments on the proposed EU Space Act**, underlining that a successful Space Act should enhance Europe's competitiveness by fully utilizing the potential of the Internal Market of 30 States. On the market front, **the UK Ministry of Defence has awarded a £6m contract to QinetiQ-led Team Elaris** to develop a deployable solution concept for enhanced Long-Range Navigation, an alternative to satellite-based positioning systems that can continue to function when GPS signals are jammed or spoofed by adversaries. In the threat intel category, an **alleged data leak targeted Blue Origin**, the U.S. space company. The attackers alleged a total of 492GB of sensitive company documents have been leaked, and they are demanding a ransom of \$250K. On the technological front, **Telepix and S2W, by signing a Memorandum of Understanding, are set out to build 'Multi-Domain Security AI' combining satellite and dark web.** Lastly, in the training and education side, **VisionSpace announced it will perform a Satellite Radio Analysis & Disruption (S-RAD) training at DEF CON 34.** Participants will work through how satellite links are structured, how signals can be analyzed and manipulated, and how disruptions arise from protocol design, signal-processing assumptions, and operational workflows.

GEOPOLITICS

Informational: Defense Dept. continues working on combating cyber threats to defense networks, data centers, satellites

The Department of Defense continues its efforts to protect its networks, data centers, and satellites from cyber threats. The Department is working with the private sector and other government agencies to develop and implement cybersecurity measures. The Department is also working to improve its ability to detect and respond to cyber threats.

Source: [Defense Dept.](#)



Budget request directs record \$338.8bn to Air Force and Space Force to meet “challenges of today and tomorrow”

Another \$500m will be directed to cyber warfare operations to safeguard satellites. The Space Force would also receive an additional \$2.9bn over current funding for National Security Space Launches. That boost in funding will procure 22 launches. #USSF #Budget

Source: [SpaceForce](#)



USAF: \$2.9Bn Space resilience is critical. So why are satellites still so exposed?

The newly funded Space Force is critical to the nation's security. It is responsible for ensuring the resilience of our satellites and the data they collect. The Space Force is working to improve its ability to detect and respond to threats to our satellites.

Source: [USAF](#)



Italy-Spain institutional and industrial meetings in the space sector

Meetings took place on April 28 and 29 in Madrid, led by the head of the Space Unit at the Office of the Military Advisor to the Prime Minister, Gen. Luigi Riggio, the Director of Space and Science at the Ministry of Foreign Affairs and International Cooperation (MAECI), Minister Plenipotentiary Lamberto Moruzzi, and Lt. Col. Nicola Donati Guerrieri of the Joint Cyber Intelligence Command of the Ministry of Defense, with the aim of fostering, together with the embassy, contacts between Italian and Spanish companies in the space sector. #Europe #Dialogue

Source: [ANSA](#)



Germany launches €1.6bn military space program

Germany is launching a €1.6bn military space program. The program is designed to protect Germany's satellites and the data they collect. The program is also designed to improve Germany's ability to detect and respond to threats to its satellites.

Source: [Germany](#)



U.S. warns of China, Russia threats to space force battlefield

The United States is warning of threats to its space force battlefield from China and Russia. The threats include the use of cyber attacks, kinetic attacks, and other means to disrupt or destroy U.S. satellites and the data they collect.

Source: [U.S.](#)



EU steps up space security as espionage and interference rise

The European Union is stepping up its efforts to protect its space assets from espionage and interference. The EU is working to improve its ability to detect and respond to threats to its satellites and the data they collect.

Source: [EU](#)



Orbits of influence: Emerging threats to U.S. space security and foreign policy implications

The United States is facing emerging threats to its space security and foreign policy implications. The threats include the use of cyber attacks, kinetic attacks, and other means to disrupt or destroy U.S. satellites and the data they collect.

Source: [U.S.](#)



REGULATION

House: 2025 official estimates for restoring the National Space Council to monitor satellite cyber threats

The House is working to restore the National Space Council to monitor satellite cyber threats. The Council is responsible for ensuring the resilience of our satellites and the data they collect. The Council is also responsible for improving our ability to detect and respond to threats to our satellites.

Source: [House](#)



REGULATION



EEA EFTA Comment on the EU Space Act Proposal

The EEA EFTA States welcome the EU Space Act proposal and its objective to strengthen the safety, resilience, and sustainability of space activities in the Internal Market. They underline that a successful Space Act should enhance Europe's competitiveness by fully utilizing the potential of the Internal Market of 30 States. **#EFTA #EUSpaceAct**

Source: [EFTA](#)



MARKET & COMPETITION



UK funds QinetiQ-led GPS alternative to protect from jamming

The Ministry of Defence has awarded a £6m contract to QinetiQ-led Team Elaris to develop a deployable solution concept for enhanced Long-Range Navigation, an alternative to satellite-based positioning systems that can continue to function when GPS signals are jammed or spoofed by adversaries, according to QinetiQ. **#QinetiQ #UKMoD**

Sources: [Ukdj](#), [MSN](#)



Belgium, Poland & France's plan to secure military satellites

France and Belgium are developing a secure military satellite system with Belgium, Poland and France. The system will be used for military operations and will be able to provide secure communication at the level of the group. The system will be developed by a consortium of the three countries. The system will be able to provide secure communication at the level of the group. The system will be developed by a consortium of the three countries.

Sources: [Le Monde](#), [The Guardian](#), [The New York Times](#)



Completion of Horizon and Horizon 2020

France, Germany, and the United Kingdom have announced that they have completed the development of a secure military satellite system. The system will be used for military operations and will be able to provide secure communication at the level of the group. The system will be developed by a consortium of the three countries. The system will be able to provide secure communication at the level of the group. The system will be developed by a consortium of the three countries.

Sources: [The Guardian](#), [The New York Times](#)



THREAT INTELLIGENCE

How electronic warfare is creating confusion in satellites

The development of electronic warfare (EW) systems is a major priority for the military. EW systems are used to disrupt the operations of enemy electronic systems. EW systems are used to disrupt the operations of enemy electronic systems. EW systems are used to disrupt the operations of enemy electronic systems. EW systems are used to disrupt the operations of enemy electronic systems.

Sources: [The Guardian](#), [The New York Times](#)

THREAT INTELLIGENCE

★ The alleged hack announcement is detected for Blue Origin

A total of 492GB of sensitive company documents have allegedly been leaked, and attackers are demanding a ransom of \$250K. **#DataLeak #BlueOrigin**

Source: [SOCRadar](#)



★ All Anonymous targets the website of Blue Origin Network

All Anonymous targets the website of Blue Origin Network, which is a space exploration company. **#AllAnonymous**

Source: [CyberInflight](#)



★ A data breach within the United Kingdom Air Force has raised concerns about cyber espionage within the networks of NATO, USA, and EU

A data breach within the United Kingdom Air Force has raised concerns about cyber espionage within the networks of NATO, USA, and EU. The breach involved the theft of sensitive information, including intelligence reports and operational plans. The UK Air Force has confirmed the breach and is working to contain the damage. The breach is believed to have been carried out by a group of cyber attackers, possibly linked to a state-sponsored group. The breach has raised concerns about the security of the UK's cyber infrastructure and the ability of the UK to protect its sensitive information. The breach has also raised concerns about the security of the networks of NATO, USA, and EU, which are all interconnected with the UK's networks. The breach is a serious threat to the security of the UK and its allies.

Source: [CyberInflight](#)

TECHNOLOGY

★ Telepix and S2W set out to build 'Multi-Domain Security AI' combining satellite and dark web

Cooperation in next-generation security technologies combining space data and cyber intelligence is set to begin in earnest. TelePIX, a space AI solution company, announced that it has signed a Memorandum of Understanding (MOU) with S2W, a big data AI company, to advance security intelligence. **#TelePIX #S2W**

Source: [VentureSquare](#)



★ Accelerating space power through software defined mission planning

As space becomes a contested domain, a software defined mission planning (SDMP) approach is being developed to accelerate space power. SDMP is a software-defined approach to mission planning that allows for rapid reconfiguration of mission plans in response to changing conditions. SDMP is being developed by a team of experts from the US Air Force and the US Space Force. SDMP is a key enabler for the development of next-generation space capabilities. SDMP is a software-defined approach to mission planning that allows for rapid reconfiguration of mission plans in response to changing conditions. SDMP is being developed by a team of experts from the US Air Force and the US Space Force. SDMP is a key enabler for the development of next-generation space capabilities.

Source: [CyberInflight](#)

TRAINING & EDUCATION

United Nations: The United Nations is working to develop a framework for the use of space in the context of international law. The framework is being developed by a team of experts from the United Nations Office for Outer Space Affairs (UNOOSA). The framework is a key enabler for the development of next-generation space capabilities. The framework is being developed by a team of experts from the United Nations Office for Outer Space Affairs (UNOOSA). The framework is a key enabler for the development of next-generation space capabilities.

Source: [CyberInflight](#)



★ Satellite Radio Analysis & Disruption (S-RAD) training at DEF CON 34

This training is built around real satellite radio systems, not just theory. You will work through how satellite links are structured, how signals can be analyzed and manipulated, and how disruptions arise from protocol design, signal-processing assumptions, and operational workflows. **#VisionSpace #DEFCON**

Source: [LinkedIn](#)



★ The role of cybersecurity in building satellite communications for national security

The role of cybersecurity in building satellite communications for national security is a key focus of the US Space Force. The US Space Force is working to develop a framework for the use of space in the context of international law. The framework is being developed by a team of experts from the US Space Force. The framework is a key enabler for the development of next-generation space capabilities. The framework is being developed by a team of experts from the US Space Force. The framework is a key enabler for the development of next-generation space capabilities.

Source: [CyberInflight](#)





TRAINING & EDUCATION

Assessing Space Security in the Context of AI

As reported in the article earlier this week, there is a growing concern that AI will be used to develop more sophisticated cyberattacks. The use of AI in cyberattacks is a complex issue, and it is important to understand the risks and opportunities associated with it. A single AI agent can be used to perform a wide range of tasks, from reconnaissance to attack. This makes it difficult for defenders to keep up with the pace of the attacks. The complexity of AI attacks makes it difficult for defenders to keep up with the pace of the attacks. The complexity of AI attacks makes it difficult for defenders to keep up with the pace of the attacks. The complexity of AI attacks makes it difficult for defenders to keep up with the pace of the attacks.



Source: [The New York Times](#)

US Satellite Launching Key Data From Submarine Fleet at Space Symposium

A new satellite launching on Tuesday will be used to monitor the submarine fleet of the United States. The satellite will be used to monitor the submarine fleet of the United States. The satellite will be used to monitor the submarine fleet of the United States. The satellite will be used to monitor the submarine fleet of the United States. The satellite will be used to monitor the submarine fleet of the United States.



Source: [The New York Times](#)

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