



SPACE CYBERSECURITY WEEKLY WATCH

Week 46

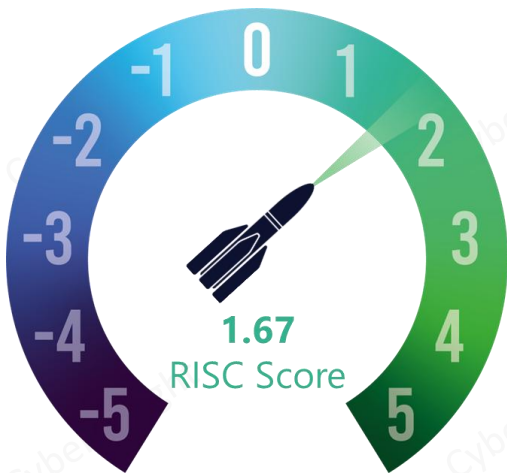
November 11- 17, 2025

Timeframe: Weekly
of articles identified: 33
Est. time to read: 70 minutes

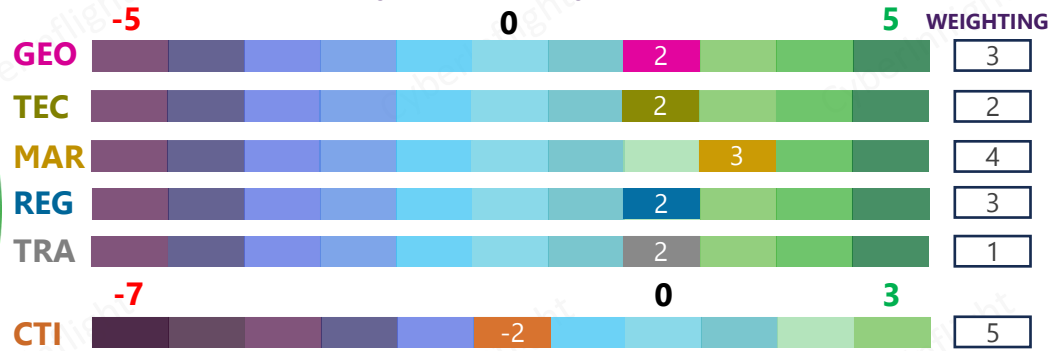
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

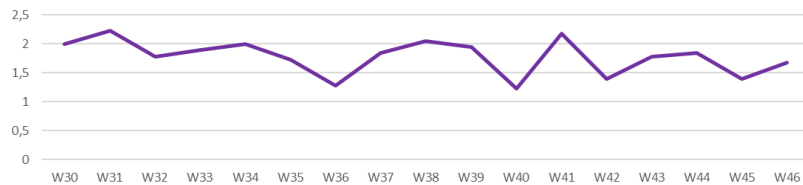
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



↑ The RISC score for this watch is 1.67, an increase from last week. This difference is due to an improvement on the regulation and technology fronts.

This week, CyberInflight October Monthly Watch went out. This Monthly report is part of CyberInflight's commercial intelligence services and offers a clear, structured view of the month's most important market, geopolitical, and threats developments. Moreover, this week, on the geopolitical front, French President Emmanuel Macron on Wednesday announced a planned increase of €4.2bn (\$4.9bn) in military space spending between 2026 and 2030. On the regulatory side, Aerospace Corporation issued SPARTEND, short for SPARTA Telemetry Encoder Neural Network to DARS (Detection And Reporting System). Its purpose is to merge the strategic insights provided by SPARTA with the anomaly detection capabilities of DARS. On the technological front, Irish quantum computing startup Equal1 has been selected by the European Space Agency (ESA) to install its Bell-1 Quantum Computer at ESA's Φ-lab (pronounced 'Phi-Lab'). On the market side, officials of the Battle Management Command, Control, and Communications (BMC3) office of the Space Force's Space Systems Command (SSC), issued a commercial solutions opening for the Kronos Family of Systems Commercial Solutions Opening project. On the threat intel side, an article about APT33 also called Elfin, Refined Kitten, and Magnallium, one of Iran's most active and long-lasting cyber-espionage groups in Iran, has been issued. Lastly, in the Training and education section, an article about the Czech region Brno, one of Europe's most dynamic tech hubs, has been posted.

CYBERINFLIGHT'S NEWS

★ **CyberInflight October Space Cybersecurity Monthly Watch is out!**

CyberInflight October Monthly Watch is out. This Monthly report is part of CyberInflight's commercial intelligence services and was created for people and organizations who want to stay informed without having to follow the news week after week. It offers a clear, structured view of the month's most important market, geopolitical, and threats developments.



#MonthlyWatch #CyberInflight

Source: [LinkedIn](#)

GEOPOLITICS

How Europe is preparing for a space war

The European Union is preparing for a space war by developing a space-based military capability. This involves the development of a space-based military capability, which is a key element of the EU's strategy for space security. The EU is also working on a space-based military capability, which is a key element of the EU's strategy for space security. The EU is also working on a space-based military capability, which is a key element of the EU's strategy for space security.



★ **France announces almost \$5bn in new military space funding**

French President Emmanuel Macron on Wednesday announced a planned increase of €4.2bn (\$4.9bn) in military space spending between 2026 and 2030. Macron warns that space is no longer a sanctuary, announcing major new space defense investments and says he wants 'New Space' French startups to help counter rising orbital threats from Russia and other hostile powers. #Funding #NationalSpaceStrategy



Sources: [Breaking Defense](#), [FrenchTech Journal](#), [Kyiv Post](#)

Germany's DLR has an military space capability

Germany's DLR has an military space capability. This involves the development of a space-based military capability, which is a key element of the EU's strategy for space security. The EU is also working on a space-based military capability, which is a key element of the EU's strategy for space security. The EU is also working on a space-based military capability, which is a key element of the EU's strategy for space security.



REGULATION

What does the cybersecurity of space?

What does the cybersecurity of space? This involves the development of a space-based military capability, which is a key element of the EU's strategy for space security. The EU is also working on a space-based military capability, which is a key element of the EU's strategy for space security. The EU is also working on a space-based military capability, which is a key element of the EU's strategy for space security.



European defense leaders call for a collective military AI/ML framework

European defense leaders call for a collective military AI/ML framework. This involves the development of a space-based military capability, which is a key element of the EU's strategy for space security. The EU is also working on a space-based military capability, which is a key element of the EU's strategy for space security. The EU is also working on a space-based military capability, which is a key element of the EU's strategy for space security.



★ **Aerospace's SPARTEND integrates space-cyber threat knowledge with autonomous detection**

Merging the strategic insights provided by SPARTA with the anomaly detection capabilities of DARS is critical to real onboard intrusion detection and mitigation capability. This is the purpose of SPARTEND, short for SPARTA Telemetry Encoder Neural Network to DARS. #AerospaceCorporation #SPARTA



Source: [Aerospace Corporation](#)



TECHNOLOGY



European Space Agency to install Equal1 Bell-1 quantum computer for Earth Observation data processing

Irish quantum computing startup Equal1 has been selected by the European Space Agency (ESA) to install its Bell-1 Quantum Computer at ESA's Φ -lab (pronounced 'Phi-Lab'). The installation will be carried out as part of the ESA's FutureEO flagship program under its Quantum Computing for Earth Observation initiative (QC4EO), which aims to use quantum technologies to accelerate the processing of Earth Observation data structures. #ESA #QC4EO



Source: [Data Center Dynamics](#)

Space Force launches QFT-1 - A next-generation QFT experiment value flight

Space Force has announced the launch of its first quantum flight experiment, QFT-1, on the SpaceX Falcon Heavy. The experiment will test the feasibility of using quantum technologies for secure communications and navigation in space. The mission will involve the deployment of a quantum key distribution (QKD) system and a quantum clock. The system will be used to demonstrate the ability to generate and distribute quantum keys for secure communication and to measure the time delay between two distant locations. The mission is expected to launch in late 2025.



Source: [Space.com](#)

Building the Golden Gate with cyber resilience: Why security must start at the drawing board

The construction process of the Golden Gate Bridge is a complex task that requires a high level of precision and coordination. Similarly, the development of a secure system requires a high level of precision and coordination. The process starts at the drawing board, where the system's architecture is defined. This includes the selection of the hardware and software components, the design of the system's security features, and the implementation of the system. The process is iterative, with frequent communication and collaboration between the system's designers and the system's users. The result is a secure system that is built to last.



Source: [CyberInflight](#)

IBMQ integrates the scalable NISQ Quantum Compiler, allowing Quantum programming across languages

IBM Quantum has announced the integration of its new Quantum Compiler, which allows users to write quantum programs in a variety of languages, including Qiskit, Cirq, and Q#. The compiler is designed to optimize quantum programs for execution on IBM's NISQ (Noisy Intermediate-Scale Quantum) hardware. The compiler will be available to users through the Qiskit ecosystem. The compiler is a key component of IBM's Quantum ecosystem, which includes the Qiskit software stack, the IBM Quantum hardware, and the Qiskit ecosystem. The compiler is expected to be released in late 2025.



Source: [IBM](#)

IBMQ launches U.S. based Pure Quantum team of Trust to define quantum resistant PKI and derive identity services as part of the FedRAMP strategy

IBM Quantum has announced the launch of its new Pure Quantum team of Trust. The team is focused on defining quantum resistant PKI (Public Key Infrastructure) and deriving identity services as part of the FedRAMP strategy. The team will be working with the U.S. government to develop quantum resistant PKI and identity services. The team is expected to be active in late 2025.



Source: [IBM](#)

Advanced Cybersecurity Toolkit

The advanced cybersecurity toolkit provides a comprehensive set of tools and services for protecting your organization's data and systems. The toolkit includes a variety of security solutions, including intrusion detection and prevention, endpoint protection, and cloud security. The toolkit is designed to be easy to use and integrate with your existing security infrastructure. The toolkit is expected to be released in late 2025.



Source: [CyberInflight](#)

MARKET & COMPETITION

EU "Quantum 2025" - QFT-1 - QFT-2 Quantum value flight

The EU has announced a plan to launch a series of quantum flight experiments, including QFT-1 and QFT-2. The experiments will test the feasibility of using quantum technologies for secure communications and navigation in space. The experiments are expected to launch in late 2025.



Source: [CyberInflight](#)

MARKET & COMPETITION

U.S. Space Force eyes space battle management using Artificial Intelligence (AI) and cybersecurity

U.S. Space Force battle-management experts are surveying the industry for products, technologies, and services in command and control, battle management, and space intelligence. Officials of the Battle Management Command, Control, and Communications (BMC3) office of the Space Force's Space Systems Command (SSC) in El Segundo, Calif., issued a commercial solutions opening (FA8806-26-S-0001) on Wednesday for the Kronos Family of Systems Commercial Solutions Opening project. This office is responsible for developing, modernizing, and sustaining integrated command, control, and communications for space operations. #Opening #USSF



Source: [Military Aerospace](#)

Space Force eyes space battle management using Artificial Intelligence (AI) and cybersecurity

U.S. Space Force battle-management experts are surveying the industry for products, technologies, and services in command and control, battle management, and space intelligence. Officials of the Battle Management Command, Control, and Communications (BMC3) office of the Space Force's Space Systems Command (SSC) in El Segundo, Calif., issued a commercial solutions opening (FA8806-26-S-0001) on Wednesday for the Kronos Family of Systems Commercial Solutions Opening project. This office is responsible for developing, modernizing, and sustaining integrated command, control, and communications for space operations. #Opening #USSF



Source: [Military Aerospace](#)

European Space Agency and European Union set up a subcommittee for ISS project

The European Space Agency (ESA) and the European Union (EU) have set up a subcommittee to coordinate the implementation of the International Space Station (ISS) project. The subcommittee will be responsible for developing, modernizing, and sustaining integrated command, control, and communications for space operations. #Opening #USSF



Source: [Military Aerospace](#)



Space Force eyes space battle management using Artificial Intelligence (AI) and cybersecurity

U.S. Space Force battle-management experts are surveying the industry for products, technologies, and services in command and control, battle management, and space intelligence. Officials of the Battle Management Command, Control, and Communications (BMC3) office of the Space Force's Space Systems Command (SSC) in El Segundo, Calif., issued a commercial solutions opening (FA8806-26-S-0001) on Wednesday for the Kronos Family of Systems Commercial Solutions Opening project. This office is responsible for developing, modernizing, and sustaining integrated command, control, and communications for space operations. #Opening #USSF



Source: [Military Aerospace](#)

U.S. Space Force eyes space battle management using Artificial Intelligence (AI) and cybersecurity

U.S. Space Force battle-management experts are surveying the industry for products, technologies, and services in command and control, battle management, and space intelligence. Officials of the Battle Management Command, Control, and Communications (BMC3) office of the Space Force's Space Systems Command (SSC) in El Segundo, Calif., issued a commercial solutions opening (FA8806-26-S-0001) on Wednesday for the Kronos Family of Systems Commercial Solutions Opening project. This office is responsible for developing, modernizing, and sustaining integrated command, control, and communications for space operations. #Opening #USSF



Source: [Military Aerospace](#)

Germany's foreign ministry calls on Russia to stop jamming European satellite signals

Germany's foreign ministry has called on Russia to stop jamming European satellite signals. The ministry said that the jamming is a violation of international law and is a threat to the security of European countries. #Opening #USSF



Source: [Military Aerospace](#)

THREAT INTELLIGENCE

Germany's foreign ministry calls on Russia to stop jamming European satellite signals

Germany's foreign ministry has called on Russia to stop jamming European satellite signals. The ministry said that the jamming is a violation of international law and is a threat to the security of European countries. #Opening #USSF



Source: [Military Aerospace](#)

U.S. Space Force eyes space battle management using Artificial Intelligence (AI) and cybersecurity

U.S. Space Force battle-management experts are surveying the industry for products, technologies, and services in command and control, battle management, and space intelligence. Officials of the Battle Management Command, Control, and Communications (BMC3) office of the Space Force's Space Systems Command (SSC) in El Segundo, Calif., issued a commercial solutions opening (FA8806-26-S-0001) on Wednesday for the Kronos Family of Systems Commercial Solutions Opening project. This office is responsible for developing, modernizing, and sustaining integrated command, control, and communications for space operations. #Opening #USSF



Source: [Military Aerospace](#)



THREAT INTELLIGENCE

★ **APT33 (Elfin / Refined Kitten): Iran's longstanding cyber-espionage arm**

APT33 also called Elfin, Refined Kitten, and Magnallium is one of Iran's most active and long-lasting cyber-espionage groups. It has been operational since at least 2013 and has demonstrated persistence in campaigns against targets in the aerospace, energy, and defense industries. Analysts associate APT33 with Iran's Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence and Security (MOIS) and view its activities as consistent with Iran's strategic and military ambitions. **#APT33 #Iran**

Source: [BrandDefense](#)



Iran's Revolutionary Guard Corps strikes with hacked files sent to Spanish and Canadian officials

The Revolutionary Guard Corps (IRGC) of Iran has hacked files from the email accounts of Spanish and Canadian officials, according to a report from BrandDefense.

Source: [BrandDefense](#)



India claims that the delivery of hackers' IP address collapsed after ransom payment

The cyber village of address in the targeted IP of a hacker in India's capital was announced by a communication network that will merge with the IP address of a hacker group known as 'Elfin'. The IP address was found to be the same as the IP address of the hacker group known as 'Elfin'. According to the report, the IP address was found to be the same as the IP address of the hacker group known as 'Elfin'. The IP address was found to be the same as the IP address of the hacker group known as 'Elfin'.

Source: [BrandDefense](#)



Iran's cyber-espionage arm may be in space

The cyber intelligence for global security may not be on earth, but it is in the satellite orbiting around the planet and looking to monitor, intercept, and collect sensitive information from the ground and in the air.

Source: [BrandDefense](#)

India and Singapore intensify cyber-espionage

The cyber intelligence for global security may not be on earth, but it is in the satellite orbiting around the planet and looking to monitor, intercept, and collect sensitive information from the ground and in the air.

Source: [BrandDefense](#)



TRAINING & EDUCATION

China's cyber-espionage arm may be in space

The cyber intelligence for global security may not be on earth, but it is in the satellite orbiting around the planet and looking to monitor, intercept, and collect sensitive information from the ground and in the air.

Source: [BrandDefense](#)



★ **Brno reaches for space: local innovators showcase Czech space excellence at Europe's largest space expo**

The Brno region has become one of Europe's most dynamic tech hubs, uniting leading players across the local ecosystem. This collaborative platform is now taking Czech space excellence to the international stage at Space Tech Expo Europe in Bremen. TRL Space, Zaitra, and Groundcom will, for example, unveil new products. Beyond these exhibitors, the Brno Space Cluster brings together a group of companies and research organizations active in electronics and cybersecurity.

#Brno #SpaceTechExpo

Source: [The AI Journal](#)



European Commission first to admit satellite hacking challenge to test space cybersecurity

The European Commission has admitted satellite hacking challenge to test space cybersecurity.

Source: [BrandDefense](#)





TRAINING & EDUCATION

Space Cybersecurity Watch: Artificial Intelligence for Space
The capabilities of AI for the space sector are rapidly increasing as the technology continues to advance. This week's report covers the latest in AI, machine learning, and deep learning, providing an overview of the current state of the technology and its potential applications in the space sector. [Read the full report](#)



A CyberInflight enabled International Space Station partnership for security education in satellite operations and Space Operations Engineering and Technical Training
CyberInflight is proud to announce a new partnership with the International Space Station (ISS) to provide training and education in satellite operations and space operations engineering and technical training. This partnership will provide a unique opportunity for students and professionals to learn from the experts in the field of space operations and satellite technology. [Read the full report](#)



Space Cybersecurity Watch: Space Operations for a secure space economy (SatOps Security)
In the context of satellite security, operations, and technical training, this report provides an overview of the current state of the technology and its potential applications in the space sector. [Read the full report](#)



*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*

