



SPACE CYBERSECURITY WEEKLY WATCH

Week 39

September 23 - 29, 2025

Timeframe: Weekly
of articles identified: 44
Est. time to read: 95 minutes

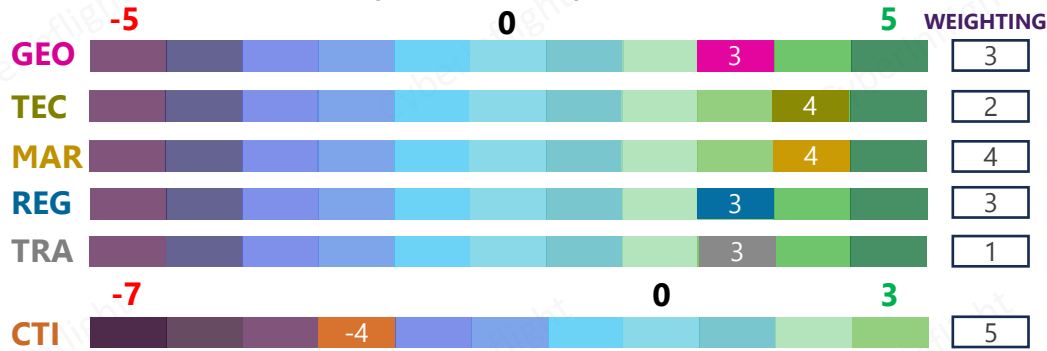
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

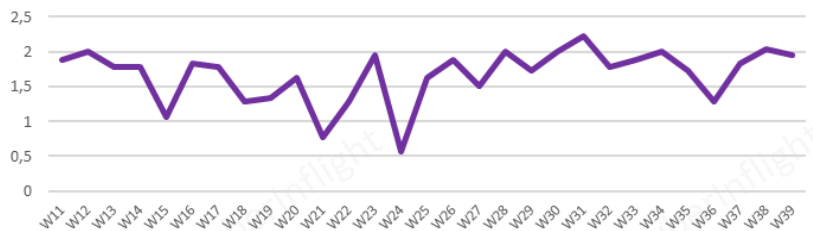
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



The RISC score for this watch is 1.95, indicating a slight decrease from last week. Nonetheless, it still represents a solid score overall. This trend can be attributed to a strong focus on both market and technological developments, despite significant activity in threat intelligence.

This week, German Defense Minister Boris Pistorius announced that Germany will invest €35bn in space-related defense projects by 2030, stepping up the country's technological independence and ability to protect its assets in orbit amid an increasing militarization of outer space. On the regulation front, the U.S. Department of War (DoW), formerly the Department of Defense, announced the implementation of a Cybersecurity Risk Management Construct (CSRMC). This transformative framework will deliver real-time cyber defense at operational speed, ensuring cyber survivability and mission assurance in every domain, including space and cyberspace. Additionally, the U.S. Space Force Space Systems Command achieved a major milestone for Future Operationally Resilient Ground Evolution (FORGE) processing, delivering its new Overhead Persistent Infrared (OPIR) capabilities to the Space Operations Command and the OPIR Battlespace Awareness Center (OBAC), marking a key advancement in missile threat response. On the market front, CS Group has welcomed AIKO to its GOSMIC ground segment product line, known for its expertise in AI and its gifted-GENE AI platform for telemetry analysis and predictive maintenance. This partnership will bring advanced autonomy into space operations. Regarding threat intelligence, during the Air, Space, & Cyber Conference organized by the Air & Space Forces Association in Maryland, several Pentagon officials identified China as the primary threat to American interests in space. Lt. Gen. Douglas Schiess, commander of U.S. Space Forces-Space, emphasized that Beijing is rapidly advancing its space capabilities at an "incredible pace," quickly closing the gap with the U.S. military's long-standing dominance. Lastly, the training & education section focuses on the new developments in China's military cyber education system, which will shape the future of China's information warfare forces.



CYBERINFLIGHT'S NEWS



Our report is out: "Space Cybersecurity Market Intelligence, Edition 2025"

As space becomes an unprecedented strategic and dual-use domain, space cybersecurity has never been more critical. Cyberthreats against the space sector are evolving and adapting rapidly, driven by increasingly complex geopolitical tensions. Our latest 370-page market intelligence report offers an unprecedented overview of this fast-changing topic.

#Report #Edition2025

Source: [CyberInflight](#)



Cybersecurity for the future of satcom

The ESA Cybersecurity Makerspace project has started its first activities to explore innovative approaches for securing satellite communications. The initiative aims to test Proof-of-Concepts in realistic environments, addressing challenges such as secure communication, anomaly detection, and vulnerability analysis. As part of this effort, CyberInflight contributes by analyzing the impacts of new cyber regulations on the Satcom ecosystem.

#ESA #CybersecurityMakerspace

Source: [Cybersecurity Makerspace](#)



GEOPOLITICS

Storage has an essential role in U.S. space domain awareness efforts

Storage has an essential role in U.S. space domain awareness efforts. The report highlights the importance of data storage in maintaining a clear and accurate record of space activities. It discusses the challenges of storing large volumes of data and the need for secure and reliable storage solutions. The report also mentions the importance of data backup and recovery in ensuring the availability of critical information.

Sources: [Defense News](#)



Germany pledges €35bn for space defense against Russia, China

Defense Minister Boris Pistorius said that Germany will invest €35bn (\$41bn) in space-related defense projects by 2030, stepping up the country's technological independence and ability to protect its assets in orbit amid an increasing militarization of outer space. This reflects a broader shift toward contested space domains. #Germany #Strategy

Sources: [Defense News](#), [WPN](#)



Leaders push for greater speed for Europe's ISS' construction

European leaders are pushing for greater speed in the construction of the International Space Station (ISS). They emphasize the need for efficient project management and increased collaboration between member states. The report also discusses the importance of ensuring the station's safety and security during its construction phase.

Sources: [Defense News](#)



Highlighting between satellites' recognizing space as a domain of war

The report highlights the growing recognition of space as a domain of war. It discusses the challenges of identifying and tracking satellites and the potential for conflict in space. The report also mentions the need for international cooperation to ensure the peaceful use of space.

Sources: [Defense News](#)



REGULATION



U.S. Department of War rolls out CSRMC to deliver real-time cyber defense

The U.S. Department of War (DoW) announced the implementation of a Cybersecurity Risk Management Construct (CSRMC), a transformative framework to deliver real-time cyber defense at operational speed. This five-phase construct ensures that U.S. warfighters maintain technological superiority against rapidly evolving and emerging cyber-threats. By institutionalizing this construct across the Department, the DoW is ensuring cyber survivability and mission assurance in every domain: air, land, sea, space, and cyberspace. #CSRMC #Framework

Sources: [Industrial Cyber](#), [DoW](#)



REGULATION

DoD updates security rules for satellite operations during and after launch events

The Department of Defense (DoD) is updating its satellite security framework to address risks to satellite communications and navigation services during and after launch events. The update includes...



Source: [DoD](#)

Securing aerospace & defense software: The critical role of SBIRs

Software, hardware, and defense systems are an increasingly complex software ecosystem that includes open source, third party, and state components. Space cybersecurity risks have heightened the need for tools, services, and...

Source: [DoD](#)

TECHNOLOGY

France unveils upgraded Hermes OTH radar ship

France's Hermes & Hermes has unveiled an enhanced version of Hermes, its upgraded OTH radar ship and which has been designed for defense applications. Hermes incorporates both primary and air warning capabilities...



Source: [DoD](#)

Space Development Agency plans to provide OTH capabilities

The new funding to build out additional OTH capacity in the Space Development Agency of the Department of Defense... which will comprise hundreds of satellites providing data relay and missile warning and tracking capabilities...



Source: [DoD](#)

US OTH - Next generation satellite OTH radar systems

Thanks to the program's 2017 launch, the OTH program, the first program led by the Space Development Agency... will be used to conduct OTH, and other activities, such as, and using OTH, a range of other...



Source: [DoD](#)

India plans to upgrade satellites to shield its space assets from debris and threats

India is considering the development of a new generation satellite designed to shield its space assets from debris and threats... including debris, and other threats, such as, and using OTH, a range of other...



Source: [DoD](#)



Space Systems Command achieves operational acceptance for Future Operationally Resilient Ground Evolution (FORGE) processing: delivers new OPIR capabilities to operators

The U.S. Space Force Space Systems Command's System Delta 84 achieved a major milestone, delivering the second FORGE Operational Acceptance (OA#2) with new OPIR capabilities to the USSF's Space Operations Command (SpOC) and the OBAC at Buckley Space Force Base, Colorado. This achievement marks a key advancement in missile threat response.



#SSC #FORGE

Source: [Space Systems Command](#)

Space Communication Systems (SPC) OTH radar

The Space Communication System, a leading provider of communication services, recently announced the launch of the SPC... which will be used to conduct OTH, and other activities, such as, and using OTH, a range of other...



Source: [DoD](#)

TECHNOLOGY

Machine learning cyber defense still an early effort

While machine learning (ML) is being used in cyber defense, it's still an early effort. ML is being used to detect anomalies in network traffic, but it's not yet being used to detect and respond to threats. The use of ML in cyber defense is still in the early stages, and it's not yet clear how effective it will be. However, it's being used to detect anomalies in network traffic, and it's being used to detect and respond to threats. The use of ML in cyber defense is still in the early stages, and it's not yet clear how effective it will be. However, it's being used to detect anomalies in network traffic, and it's being used to detect and respond to threats.



Source: [CyberInflight](#)

How AI and predictive analytics are making space traffic info easier to interpret

Artificial intelligence (AI) and predictive analytics are making space traffic information easier to interpret. AI is being used to analyze large amounts of data, and predictive analytics is being used to predict future events. This is making it easier for space agencies to understand and manage space traffic. AI is being used to analyze large amounts of data, and predictive analytics is being used to predict future events. This is making it easier for space agencies to understand and manage space traffic.

Source: [CyberInflight](#)

MARKET & COMPETITION

NASA and the South Korean government sign MOU to establish a joint quantum communications demonstration research and design center in 2026

NASA and the South Korean government have signed a Memorandum of Understanding (MOU) to establish a joint quantum communications demonstration research and design center in 2026. The center will focus on developing quantum communication systems and conducting research and design. The MOU was signed in Seoul, South Korea, on September 23, 2025.



Source: [CyberInflight](#)

Cybersecurity data joins the EU Space Bill

The EU Space Bill, which aims to establish a legal framework for space activities, now includes cybersecurity data. The bill was adopted by the European Parliament on September 23, 2025. The bill will be implemented by the end of 2026.



Source: [CyberInflight](#)

Space development agency to deliver next generation high accuracy images

The Space Development Agency (SDA) is developing a next generation high accuracy imaging system. The system will provide high resolution images of the Earth and other celestial bodies. The system is expected to be operational by 2028.



Source: [CyberInflight](#)

Contractors partner with funds for next generation connectivity

Contractors are partnering with funds to provide a next generation connectivity network. The network will provide high speed, low latency connectivity for space and ground-based users. The network is expected to be operational by 2030.



Source: [CyberInflight](#)

Software, operations launch EU Space Defense Fund at Satellite Europe 2025

The European Union (EU) has launched the Space Defense Fund at the Satellite Europe 2025 conference. The fund will support the development and operation of space-based defense systems. The fund is expected to be operational by 2026.



Source: [CyberInflight](#)

2025 Space Resilience program to support 67 startups across Australia, India, and Japan

The 2025 Space Resilience program will support 67 startups across Australia, India, and Japan. The program will provide funding and technical support for the development and operation of space-based resilience systems. The program is expected to be operational by 2026.



Source: [CyberInflight](#)

MARKET & COMPETITION

ESA's competition leads off government process for ground segment

The European Commission is leading the competition to select the ground segment for the Galileo system. The contract will be awarded to the contractor that can best meet the needs of the system. [ESA's competition leads off government process for ground segment](#)

Source: [ESA's competition leads off government process for ground segment](#)



Space Space address partner (SPP) level 2 users with allSPP as strategic partner

Space Space has signed a partnership agreement with allSPP, a leading provider of satellite-based services. The partnership will focus on developing and delivering advanced services to customers. [Space Space address partner \(SPP\) level 2 users with allSPP as strategic partner](#)

Source: [Space Space address partner \(SPP\) level 2 users with allSPP as strategic partner](#)



★ Great news from Toulouse: CS Group and AIKO are teaming up

CS Group welcomed AIKO, which brings its renowned expertise in AI and its gifted-GENE AI platform for telemetry analysis and predictive maintenance, to its GOSMIC ground segment product line. This partnership is the launchpad of a long-term collaboration, bringing advanced autonomy into space operations and shaping a future where complexity is managed, resilience is built in, and innovation never stops. [Great news from Toulouse: CS Group and AIKO are teaming up](#)

Source: [CS Group](#)



THREAT INTELLIGENCE

USAF, NSA address partner selected by government group

The US Air Force and NSA have selected a partner to develop and deliver advanced services to customers. The partnership will focus on developing and delivering advanced services to customers. [USAF, NSA address partner selected by government group](#)

Source: [USAF, NSA address partner selected by government group](#)



Aviation conference to see impact of a risk for air transport with

The aviation conference will see the impact of a risk for air transport with. The conference will focus on developing and delivering advanced services to customers. [Aviation conference to see impact of a risk for air transport with](#)

Source: [Aviation conference to see impact of a risk for air transport with](#)



Inside the Space Force as it prepares for a new kind of war

Space and other key elements that they can use out of context with the satellite operated by the military and intelligence agencies. The report will focus on developing and delivering advanced services to customers. [Inside the Space Force as it prepares for a new kind of war](#)

Source: [Inside the Space Force as it prepares for a new kind of war](#)



Cybernetics by Indian Institute group

The Indian Institute group has developed a new kind of cybernetics. The report will focus on developing and delivering advanced services to customers. [Cybernetics by Indian Institute group](#)

Source: [Cybernetics by Indian Institute group](#)



High above the equator, Russia is building satellite used by NATO armed forces

Russia is building a satellite used by NATO armed forces. The satellite will focus on developing and delivering advanced services to customers. [High above the equator, Russia is building satellite used by NATO armed forces](#)

Source: [High above the equator, Russia is building satellite used by NATO armed forces](#)



THREAT INTELLIGENCE

Government group identifies 100 of Russian employees

In a new report, the U.S. government has identified 100 of Russian employees working in the U.S. — the latest addition to a government effort conducted by the group known as the Cyber Threat Intelligence. The report, released on September 18, identifies the names and roles of government employees whose credentials were hacked in late August. A list of names, addresses, dates of birth, and other data is being made public by the Cyber Threat Intelligence team.



Sources: [Wired](#), [The Washington Times](#)

Washington Cyber IPT reports global exposure to U.S. military networks and track down

The Cyber Threat Intelligence (CTI) team has reported that global adversaries have significantly increased their efforts to compromise U.S. military networks and track down sensitive information. The team has identified several new threats and has been working to track down the individuals and organizations responsible for these attacks.



Sources: [Wired](#)

★

US Space Force warns of China's growing orbital threat

In a stark assessment delivered at the Air, Space & Cyber conference, Lt. Gen. Douglas Schiess, commander of U.S. Space Forces-Space, declared China the preeminent threat to American interests in orbit. He emphasized that Beijing is advancing its space capabilities at an "incredible pace," rapidly closing the gap with the U.S. military's longstanding dominance. Gen. Sidari, deputy chief of space operations for intelligence, appeared alongside other top intelligence officials at the conference and outlined that China has accelerated its development to defeat the joint force.



#USSF #Rivalry

Sources: [WPN](#), [The Washington Times](#)

Spotify is allegedly a hard worker

In the music world, Spotify is often seen as a hard worker. The company has been working on security updates and other improvements to ensure it remains a secure platform for its users. The company has been working hard to ensure its services are always available and secure.



Sources: [Wired](#)

Industry groups push U.S. government for rapid action on AI privacy, security

A coalition of industry organizations has urged the U.S. executive branch, Congress, and state legislatures to take prompt action on AI privacy and security. The coalition is concerned about the potential for AI to be used in ways that could compromise privacy and security. They are calling for the government to take steps to address these concerns and to ensure that AI is used in a responsible and secure manner.



Sources: [Wired](#), [The Washington Times](#), [The Washington Post](#)

AI-based platform in European countries has failed to track activities during operation Berlin

During the 2024 Berlin cyber exercise, a European-based AI platform failed to track activities during the operation. The platform was designed to monitor and track cyber threats, but it was unable to identify several key threats that were active during the exercise. This failure highlights the need for improved AI-based threat detection and response capabilities.



Sources: [Wired](#), [The Washington Times](#)

TRAINING & EDUCATION

Government officials are looking at ways to improve the training of the U.S. Cyber Corps. The focus is on ensuring that cyber operators have the skills and knowledge needed to defend the nation's digital infrastructure.

The U.S. Cyber Corps is working to improve the training of its operators. The focus is on ensuring that cyber operators have the skills and knowledge needed to defend the nation's digital infrastructure. This includes providing them with the latest information on emerging threats and the tools and techniques needed to respond to these threats.



Sources: [Wired](#)



TRAINING & EDUCATION



The PLA goes back to school: Mapping new developments in China's military cyber education system

In China, cyber-track cadets are heading into classrooms that don't look quite like last year's. The People's Liberation Army (PLA) has recently reshuffled its military cyber education system and that shake-up is going to shape the future of China's information warfare forces. **#PLA #School**

Source: [Margin Research](#)



Highlights from 2024 Academy training courses

In the last few months, the Academy has delivered an extraordinary range of training courses and workshops, covering a wide range of topics from cyber operations to space operations. The Academy has also been instrumental in the development of new training and education programs for the PLA, including the development of a new training and education program for the PLA's cyber operations and space operations. **#PLA #School**



2024 Academy the focus on Cyber Space

The Academy has been the focus of many reports, including those from the PLA's own media. The Academy has been instrumental in the development of new training and education programs for the PLA, including the development of a new training and education program for the PLA's cyber operations and space operations. **#PLA #School**



World's first cyber-intelligence satellite constellation from 2024

The world's first cyber-intelligence satellite constellation is set to be launched from space with a focus on providing cyber intelligence to the PLA. The constellation will consist of several satellites and will be used to provide cyber intelligence to the PLA's cyber operations and space operations. **#PLA #School**



2024 Academy intelligence based on cyber space differences and intelligence collection

The Academy has been instrumental in the development of new training and education programs for the PLA, including the development of a new training and education program for the PLA's cyber operations and space operations. The Academy has also been instrumental in the development of a new training and education program for the PLA's cyber operations and space operations. **#PLA #School**



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