

SPACE CYBERSECURITY WEEKLY WATCH

Week 38

September 16 - 22, 2025

Timeframe: Weekly

of articles identified: 53

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.

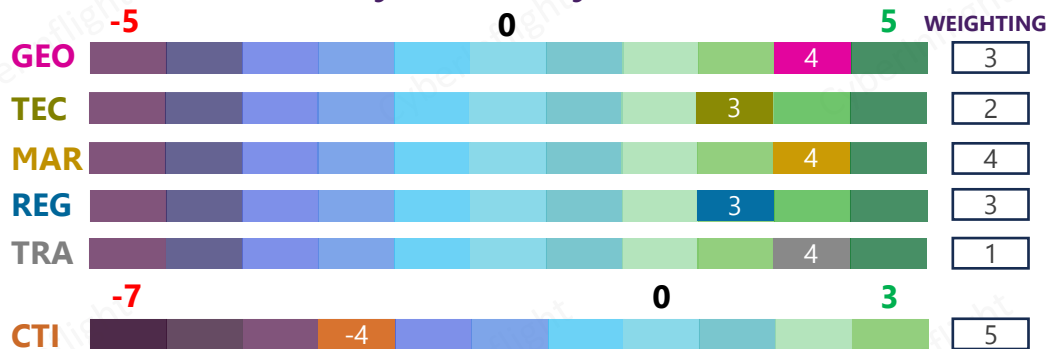
- **GEOPOLITICS**
- **TECHNOLOGY**
- **MARKET & COMPETITION**
- **REGULATION**
- **TRAINING & EDUCATION**
- **THREAT INTELLIGENCE**
- ★ **IMPORTANT NEWS**

RISC Score Assessment



The RISC score for this watch is 2.06, which has increased since last week. This slight change can be attributed to strong market attention and significant media coverage in the space cybersecurity domain.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



This week, U.S. Chief of Space Operations Gen. B. Chance Saltzman spoke to Air & Space Forces Magazine about the future of the U.S. Space Force. He noted that the Space Force is expanding its size and mission to stay ahead of China and Russia, but emphasized the need for careful management to address emerging threats while managing its growth. On the regulation front, the GSMA launched a new public policy paper on spectrum considerations for device-to-device (D2D) services, providing governments with guidance for this emerging technology. Moreover, on the technological front, the Luxembourg-based satellite player SES detailed plans to explore a method of transmitting data to ground stations without using radio, looking into the potential to increase data rates and security. The market showed strong performance this week, particularly with Viasat being selected to provide a space cryptography solution for the U.S. Space Force. This multi-year contract aims to enhance the protection of critical satellite assets against cybersecurity threats. Additionally, the SpaceRISE consortium, responsible for operating the IRIS² space constellation launched by the European Commission, has awarded Thales Alenia Space a risk mitigation contract worth over €400m for the development of onboard technologies. The threat intelligence landscape was highlighted by Major General Vincent Chusseau's first interview with international media since he took command of the French Space Command last month. He emphasized that the conflict in Ukraine has turned space into a "fully-fledged operational domain." He noted that there has been an escalation in attempts to jam satellites, blind them with lasers, and launch cyberattacks. Furthermore, CYSAT will take place as a satellite event during the CBC in Toulouse, on November 27. It will bring together leading experts in space, cybersecurity, and innovation, such as Florent Rizzo from CyberInflight, who will be a panel speaker.

GEOPOLITICS

Moving toward a realistic appraisal of China's potential in space

The article questions the position of the US in relation to China's potential in space. It says that China's capabilities are under development and that it is not clear if it will be able to compete with the US in the future. It also mentions that China's space program is a significant threat to the US and that the US should be prepared for a potential conflict in space.

Source: [The Atlantic](#)



US must 'control space' as white dominance rises, says US Space Command Chief

Speaking at the Defense and Security Leadership Conference (DSL) 2025, US Space Command Chief, Gen. John W. "Jack" Raymond, said that the US must be able to control space. He said that the US must be able to control space in order to maintain its dominance in the world.

Source: [The Atlantic](#)



Space and cybersecurity: A strategic partnership for the future

The article discusses the relationship between space and cybersecurity. It says that space and cybersecurity are closely linked and that a strategic partnership between the two is essential for the future. It also mentions that the US and other countries are working together to strengthen their space and cybersecurity capabilities.

Source: [The Atlantic](#)



Major military conference to host Pentagon officials, defense industry leaders at crucial moment

The article discusses a major military conference that will be held in the near future. It says that the conference will be a crucial moment for the defense industry and the Pentagon. It also mentions that the conference will be attended by high-ranking officials from both the defense industry and the Pentagon.

Source: [The Atlantic](#)



CSO Saltzman looks at the future of the Space Force

The U.S. Space Force is growing in size and mission as it seeks to stay ahead of the likes of China and Russia. But it will require careful management in the years to come for the new service to both keep up with threats and manage its growth, Chief of Space Operations Gen. B. Chance Saltzman told Air & Space Forces Magazine. **#USSF #Doctrine**

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



REGULATION



GSMA releases guidance to support new direct-to-device (D2D) satellite services

The GSMA launched a new public policy paper on spectrum considerations for D2D services, providing governments with guidance for this emerging technology. D2D can have a positive impact if national regulations protect against harmful interference into mobile networks, which serve 5.8bn people globally. **#GSMA #D2D**

Sources: [WebWire](#), [GSMA](#)



Space traffic management in the US Space Act: Beneficial commercialization for regulating foreign commercial activity

The article discusses the US Space Act and its impact on space traffic management. It says that the act is a significant step forward in addressing the regulatory needs of space traffic management. It also mentions that the act is a key element of the US strategy for promoting space commerce and ensuring the safety of space operations.

Source: [The Atlantic](#)



Policy initiatives being taken for space, cyber warfare equipment development (CSE)

During the last two sessions held in Berlin, NATO leaders and officials discussed the urgent need for developing capabilities in space and cyber warfare equipment. The discussion focused on the urgent need for developing capabilities in space and cyber warfare equipment and the growing importance of a coordinated effort to develop such capabilities.

Source: [The Atlantic](#)



National Space Strategy Update

The National Space Strategy Update was recently published by the White House. It says that the update is a key element of the US strategy for promoting space commerce and ensuring the safety of space operations. It also mentions that the update is a key element of the US strategy for promoting space commerce and ensuring the safety of space operations.

Source: [The Atlantic](#)



Satellite player SES detailed plans to explore a method of transmitting data to ground stations without using radio, looking into the potential to increase data rates and security. SES stated it plans to test optical ground stations constructed by France-based Cailabs, a specialist in laser light technology for sectors including aerospace and defense, welding and manufacturing, and fibre networks. **#Data #GroundStation**



The 2008 Test Operations, a part of the Flight Test Series, is the first Department of Defense service operation to include flight testing development and operational testing for all years and all platforms across the joint services.



For instance, an individual's self-reported health status increases the likelihood of a diagnosed, self-reported condition. Moreover, individuals with self-reported poor health status tend to be more likely to report having a diagnosed condition, regardless of whether they actually do. This suggests that self-reported health status is a strong predictor of diagnosed health status, and that self-reported health status is a strong predictor of diagnosed health status.



Copyright © 2009 by John Wiley & Sons, Inc.



© 2008 Cyberbit Corporation. All rights reserved. Cyberbit Corporation is a registered trademark of Cyberbit Corporation. All other trademarks are the property of their respective owners. The information in this document is subject to change without notice. The information in this document is provided "as is" without any warranty, express or implied. The information in this document is not intended to be used for any purpose other than that for which it was created. The information in this document is not intended to be used for any purpose other than that for which it was created. The information in this document is not intended to be used for any purpose other than that for which it was created.

[illegible]

MARKET & COMPETITION

Other multi-agent or agent communities provide support in solving the target information sharing and analysis tasks. Open networks, stating that the objective of agents participation is to coordinate with other collaboration and better evidence is given and shared system. **Researcher's View**



Julius Electronics & Software and Quantic have entered into a strategic partnership to deliver coverage and content for training, navigation and timing (PNT) solutions for the United Kingdom Ministry of Defense (MoD). The partnership offers advanced protection against jamming, spoofing and other electronic warfare (EW) threats. **EWAT Partnership**



© 2015 IEEE. All rights reserved. This article is intended solely for the personal use of the individual user and is not to be disseminated broadly.



MARKET & COMPETITION



Viasat selected to deliver space crypto solution for U.S. Space Force Space Systems Command

Viasat, Inc. is developing a new, space-based encryption solution to support data security for U.S. Space Force (USSF) Space Systems Command (SSC). Under this multi-year development award, Viasat's encryption team within its Defense and Advanced Technologies segment will build a next-generation cryptography solution for satellite applications, allowing the government to better protect critical space assets from cybersecurity threats. #Viasat #SSC

Sources: [Satnews](#), [Satcom Digital](#)



IRIS² : Thales remporte un premier grand contrat pour le développement de la constellation spatiale (Trad.: IRIS²: Thales wins first major contract for the development of the space constellation)

The SpaceRISE consortium, which will operate the IRIS² space constellation launched by the European Commission, has awarded Thales Alenia Space a risk mitigation contract worth over €400m for the development of onboard technologies.

#SpaceRISE #Contract

Source: [La Tribune](#)



MARKET & COMPETITION

USAF Space Systems Command officials reveal critical space system command centers as a battle, adding military to space and cyber technologies to counter emerging space threats. The intent is to gain a better understanding of requirements for managing space operations, maintain and plan, while addressing the need for integrated space and cyber systems. [USAF Media](#)

The US Space Systems Command officials reveal critical space system command centers as a battle, adding military to space and cyber technologies to counter emerging space threats. The intent is to gain a better understanding of requirements for managing space operations, maintain and plan, while addressing the need for integrated space and cyber systems. [USAF Media](#)

Source: [USAF Media](#)



The operations maintain that a new computing paradigm is reducing the size of the proposed facility

The operations maintain that a new computing paradigm is reducing the size of the proposed facility. The operations maintain that a new computing paradigm is reducing the size of the proposed facility. The operations maintain that a new computing paradigm is reducing the size of the proposed facility. [Space Media](#)

Source: [Space Media](#)

Publication of the NATO Summit 1 'Security' Compendium 2024-2025

The NATO Summit 1 'Security' Compendium 2024-2025 is a report to announce the publication of the NATO Summit 1 'Security' Compendium 2024-2025. The report is a key document for NATO members, detailing the security situation in the North Atlantic region. [NATO Media](#)

Source: [NATO Media](#)



THREAT INTELLIGENCE

As North Korea's jamming threat grows, South's Air Force up its electronic warfare game

As North Korea's jamming threat grows, South's Air Force up its electronic warfare game. North Korea's jamming threat is growing, and South's Air Force is upping its electronic warfare game. [South Korea Media](#)

Source: [South Korea Media](#)



World war II to what? Space warfare capabilities as Russia and China build space weapons

World war II to what? Space warfare capabilities as Russia and China build space weapons. Military officials from both sides say space is no longer a neutral environment but an operational battlefield. [Russia Media](#)

Source: [Russia Media](#)



Chinese and U.S. satellites play a key role in the space, a new era of espionage starts

Chinese and U.S. satellites play a key role in the space, a new era of espionage starts. Chinese and U.S. satellites are playing a key role in the space, a new era of espionage starts. [China Media](#)

Source: [China Media](#)



Ground-based GPS jamming over northern Australia: Experts call for Europe-wide adoption of jamming-resistant technology

Ground-based GPS jamming over northern Australia: Experts call for Europe-wide adoption of jamming-resistant technology. Experts call for Europe-wide adoption of jamming-resistant technology. [Australia Media](#)

Source: [Australia Media](#)



French military leader warns of increased 'hostile' activity in space

In his first interview with international media since taking the helm of French Space Command last month, Major General Vincent Chusseau told reporters that the conflict in Ukraine has transformed space into a "fully-fledged operational domain". He said Russia has escalated attempts to jam satellites, blind them with lasers and launch cyberattacks since its full-scale invasion of Ukraine in 2022. [Russia](#) [SpaceWarfare](#)

Sources: [Reuters](#), [Daily Mail](#)



THREAT INTELLIGENCE

Alleged sale of classified technical report from United States Space Force

The source has reported an alleged sale of a classified technical report from the United States Space Force. [MSSM Headlines](#)

Source: [classified](#)



Alleged data breach of Malaysia Space Agency (MPSA)

The source has reported an alleged data breach of the Malaysia Space Agency (MPSA). [MSSM Headlines](#)

Source: [classified](#)



Iranian state RPT targets various satellite companies

The source has reported a cyber attack attributed to an Iranian state-sponsored threat RPT group. The group is targeting various satellite companies through cyber espionage, cyber sabotage, and cyber warfare. The source has reported that the group is targeting various satellite companies through cyber espionage, cyber sabotage, and cyber warfare. The source has reported that the group is targeting various satellite companies through cyber espionage, cyber sabotage, and cyber warfare. [MSSM Headlines](#)

Source: [classified](#), [in media](#), [in media](#)



Recommendations and cyber risk status: Complex threats in the digital and cyberspace

With the acceleration of technological development and the increasing reliance on cyber space, cyber threats are becoming more complex and sophisticated. The source has reported that the cyber threat landscape is becoming more complex and sophisticated. The source has reported that the cyber threat landscape is becoming more complex and sophisticated. [MSSM Headlines](#)

Source: [classified](#)

TRAINING & EDUCATION

Training UHFV residents against jamming and spoofing attacks

The source has reported that the UHFV residents are being trained against jamming and spoofing attacks. The source has reported that the UHFV residents are being trained against jamming and spoofing attacks. The source has reported that the UHFV residents are being trained against jamming and spoofing attacks. [MSSM Headlines](#)

Source: [classified](#)



Adaptive jamming strategy of an aerial drone's UHFV antennas with variable shielding for UHFV anti-jamming

The source provides a simple and cost-effective anti-jamming method for aerial navigation satellite system (GNSS) receivers of an aerial drone. The drone has three UHFV antennas, each with a different shielding structure. The source provides a simple and cost-effective anti-jamming method for aerial navigation satellite system (GNSS) receivers of an aerial drone. The drone has three UHFV antennas, each with a different shielding structure. [MSSM Headlines](#)

Source: [classified](#)



UHFV band level guidelines for system interference with UHFV antennas

The source provides a simple and cost-effective anti-jamming method for aerial navigation satellite system (GNSS) receivers of an aerial drone. The drone has three UHFV antennas, each with a different shielding structure. The source provides a simple and cost-effective anti-jamming method for aerial navigation satellite system (GNSS) receivers of an aerial drone. The drone has three UHFV antennas, each with a different shielding structure. [MSSM Headlines](#)

Source: [classified](#)



Analysis of UHFV radio frequency interference and impacts on UHFV receiver parameter

The source investigates radio frequency interference (RFI) as a candidate for the early detection and mitigation of UHFV receiver parameter. The source investigates radio frequency interference (RFI) as a candidate for the early detection and mitigation of UHFV receiver parameter. The source investigates radio frequency interference (RFI) as a candidate for the early detection and mitigation of UHFV receiver parameter. [MSSM Headlines](#)

Source: [classified](#)



UHFV jamming and spoofing monitoring using low-cost UHFV receivers

The source provides a methodology for detecting and monitoring UHFV signals using low-cost commercial off-the-shelf (COTS) UHFV receivers. The source provides a methodology for detecting and monitoring UHFV signals using low-cost commercial off-the-shelf (COTS) UHFV receivers. The source provides a methodology for detecting and monitoring UHFV signals using low-cost commercial off-the-shelf (COTS) UHFV receivers. [MSSM Headlines](#)

Source: [classified](#)



Using temporal graph networks for real-time detection of UHFV jamming-induced deviations

The source proposes a methodology for detecting and monitoring UHFV signals using low-cost commercial off-the-shelf (COTS) UHFV receivers. The source proposes a methodology for detecting and monitoring UHFV signals using low-cost commercial off-the-shelf (COTS) UHFV receivers. The source proposes a methodology for detecting and monitoring UHFV signals using low-cost commercial off-the-shelf (COTS) UHFV receivers. [MSSM Headlines](#)

Source: [classified](#)





Sources: *CYSAT*, *CYSAT*



Contact us at: research@cyberinflight.com

