SPACE CYBERSECURITY WEEKLY WATCH

Week 38

September 16 - 22, 2025

Timeframe: Weekly

# of articles identified: 53

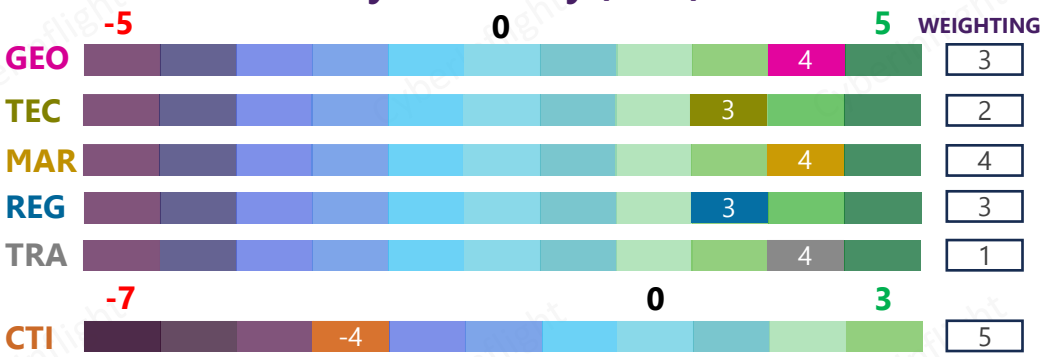
Est. time to read: 95 minutes

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

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025

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.

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

[redacted]

[redacted]

[redacted]

[redacted]

★ **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*

[redacted]

[redacted]

[redacted]

TECHNOLOGY

SES tests optical ground links

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**

Source: *Mobile World Live*

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

MARKET & COMPETITION

[redacted]

[redacted]

[redacted]

MARKET & COMPETITION

[redacted]

[redacted]

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*

[redacted]

[redacted]

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*

[redacted]

[redacted]

[redacted]

MARKET & COMPETITION

THREAT INTELLIGENCE

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

Cybersecurity reported an alleged sale of a classified technical report from the United States Space Force. #USSF #UnitedStates

Source: Cybersecurity

Alleged data breach of Malaysia Space Agency (MYSA)

Cybersecurity has reported an alleged data breach at the Malaysia Space Agency (MYSA). #MYSA #DataBreach

Source: Cybersecurity

Iranian state-APT targets telcos, satellite companies

A recent cyber espionage campaign attributed to an Iranian state-sponsored Advanced Persistent Threat (APT) group has been targeting telecommunications and satellite companies through a sophisticated social engineering campaign on professional networking sites. The operation has successfully compromised dozens of devices across multiple international organizations, highlighting a significant threat to critical infrastructure. #EspionageAPT

Sources: DarkReading, The Hacker News

Ransomware and cyber kill chains: Complex threats in the digital and cyberspace

With the acceleration of technological development and the increasing reliance on outer space, unprecedented security challenges have emerged. Cyberattacks are now extended to critical infrastructures and space systems themselves. Two key theaters are highlighted: Ransomware and the Cybersecurity Kill Chain model. #Ransomware #Governance

Source: LinkedIn

TRAINING & EDUCATION

Testing GNSS receivers against jamming and spoofing attacks

Testing how GNSS devices react to threats has become more and more important. The main test objective is to verify that these detection and mitigation techniques work as expected and that the GNSS receiver reacts properly and as expected in response to such attacks. #GNSS #Paper

Source: GPS World

Adaptive switching strategy of an aerial drone's GNSS antennas with metallic shielding for GNSS anti-jamming

This paper presents a simple and cost-effective anti-jamming method for global navigation satellite system (GNSS) antennas of an aerial drone. The drone has three GNSS antennas, such that two antennas stand at distinct heights inside a metallic shielding structure, and one antenna exists outside the shielding structure. #GNSS #Paper

Source: MDPI

EMC level guidelines for in-system interference with GPS receivers

Electronic systems and components that are placed near GPS receivers can easily cause disruptive electromagnetic interference. In this paper, EMC level guidelines are presented for electronics that are intended to be placed near to GPS receivers, as often happens in automotive and other applications. #GPS #Paper

Source: Cornell University

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

This study investigates radio frequency interference (RFI) at a Canadian test site using three collocated commercial off-the-shelf (COTS) GNSS detection and monitors. The analysis focuses on the frequency, type, and severity of interference events, as well as their impact on GNSS performance. #RFI #Paper

Source: Springer Nature

GNSS jamming and spoofing monitoring using low-cost COTS receivers

This paper presents a methodology for detecting and classifying RF events using low-cost commercial off-the-shelf (COTS) GNSS receivers. #GNSS #Paper

Source: Cornell University

Deep temporal graph networks for real-time correction of GNSS jamming-induced deviations

This paper advances jamming mitigation as dynamic graph regression and introducing a resilient, centric deep temporal graph network that predicts, and then corrects, the receiver's horizontal deviation in real time. #Jamming #Paper

Source: Papers

TRAINING & EDUCATION

[redacted]

[redacted]

[redacted]

CYSAT is finally coming to Toulouse, as part of the CBC

CYSAT will take place as a satellite event during the CBC in Toulouse, on November 27. The entire morning will be dedicated to panels, keynotes, and an interactive workshop session, bringing together leading experts in space, cybersecurity, and innovation. This half-day conference (in French) will bring together the NATO Space Centre of Excellence, Thales Alenia Space, Airbus, Look Up, CyberInflight, CNES, and CYSEC. **#CYSAT #Conference**

Sources: *CYSAT*, *CYSAT*

[redacted]

[redacted]

[redacted]

[redacted]