



SPACE CYBERSECURITY WEEKLY WATCH

Week 37

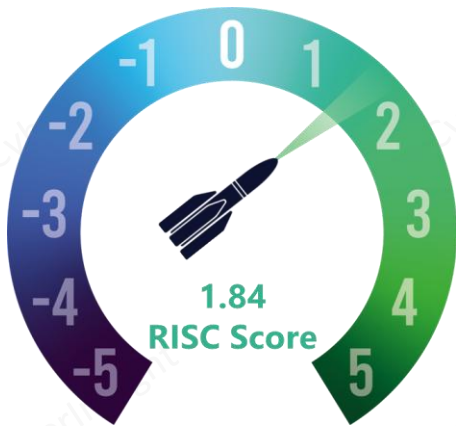
September 9 - 15, 2025

Timeframe: Weekly
of articles identified: 43
Est. time to read: 90 minutes

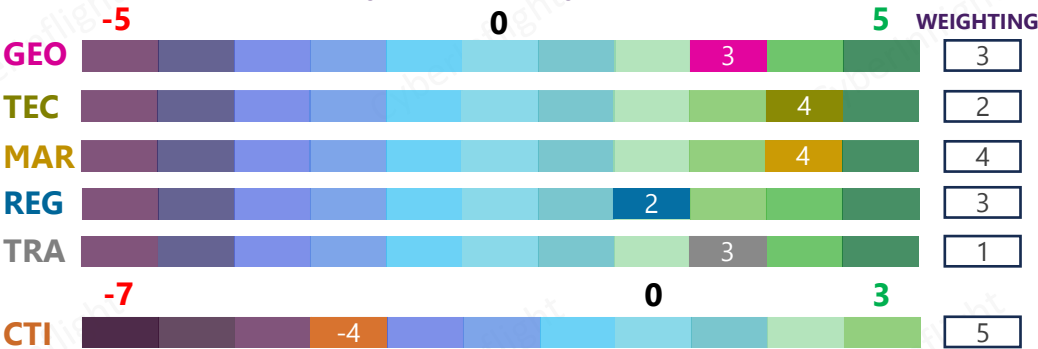
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

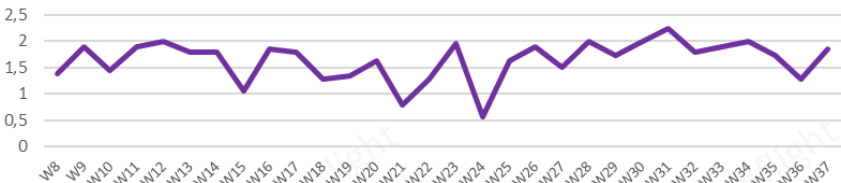
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



↑ The RISC score for this watch is 1.84. This increase from last week is attributed to a strong emphasis on technology and market developments.

This week, the General Assembly on Defense, Space and Cybersecurity event occurred in Esrin, the ESA's Earth Observation Center. On this occasion, Josef Aschbacher urgently called to strengthen Europe's space defense capabilities. He highlighted the alarming disparity between Europe and space powers such as the United States and China. On the regulation front, the Aerospace Corporation has released Space Attack Research and Tactic Analysis (SPARTA) v3.1, adding space segment guidance for NIST (National Institute of Standards and Technology) controls. On the technological front, the US Space Force contractors are building an AI-powered tool to detect cyberattacks on satellites by directly monitoring the behavior and telemetry outputs of satellite systems in orbit. Meanwhile, on the market front, Elon Musk's SpaceX is set to acquire wireless spectrum licenses from EchoStar for approximately \$17bn. The companies have also agreed to a partnership that will allow EchoStar's Boost Mobile subscribers to access Starlink's direct-to-cell service, thereby extending satellite connectivity to areas without coverage. On the threat side, military leaders at DSEI 2025, a major international defense and security exhibition held in London from 9 to 12 September 2025, stressed the need for closer industry-defense collaboration to accelerate innovation and strengthen capabilities against hybrid space-cyber threats. The training and education section focuses on a paper discussing open-source satellite communication protocols and explores the security vulnerabilities within them. It highlights SpaceCAN, a modified version of the well-known CAN Bus protocol used in the automotive industry.

GEOPOLITICS

2025 marks Chinese national's first space program and rising U.S.-China rivalry and espionage fears

With two decades separating the two nations with each other from one another in the program due to security and intelligence needs. The article, which the authors state is a security document, also highlights the growing space race between the U.S. and China. The article, published by Bloomberg News, was authored by John and James Doherty, senior editors at Bloomberg News.

Sources: [Bloomberg Intelligence](#)



U.S. and EU strengthen space cooperation at 15th U.S.-EU space dialogue

The United States and the European Union have strengthened their cooperation in space, defense, and security efforts from the 15th U.S.-EU space dialogue, which took place in Washington, D.C. The dialogue, which is the largest annual gathering of space officials from the U.S. and EU, was held at the State Department. The dialogue, which is the largest annual gathering of space officials from the U.S. and EU, was held at the State Department.

Sources: [U.S. Department of State, Politico](#)



Space Force considers adding 'warrior' to command's name

The Space Force is considering adding 'warrior' to its command's name to reflect its role in space operations, according to a report from the Wall Street Journal. The report, which is based on sources familiar with the matter, says that the Space Force is considering adding 'warrior' to its name to reflect its role in space operations, according to a report from the Wall Street Journal.

Sources: [Wall Street Journal](#)



Israel offers space cybersecurity cooperation to South Korea's MSS

The Israeli government is offering to provide security assistance to South Korea's Ministry of Security (MSS) in exchange for intelligence and security cooperation. The offer, which is part of a broader effort to strengthen ties between the two countries, was made by the Israeli government.

Sources: [Reuters](#)



ESA Director General's opening remarks at the General Assembly on Defense, Space & Cybersecurity

Josef Aschbacher made an urgent call to strengthen Europe's space defense capabilities during his opening speech at the General Assembly on Defense, Space and Cybersecurity event held at Esrin, the ESA's Earth Observation Center. Faced with the growing threat from international actors and recent incidents in space, he warned: "Europe is not just lagging behind; we are not even playing the same game." Aschbacher highlighted the alarming disparity between Europe and powers such as the United States and China. #ESA #Resilience

Sources: [ESA](#), [InfoEspace](#), [Decode39](#)



REGULATION



SPARTA v3.1 expands space cybersecurity with updated controls, new techniques, and research contributions

The Aerospace Corporation has released Space Attack Research and Tactic Analysis (SPARTA) v3.1, adding space segment guidance for NIST (National Institute of Standards and Technology) controls, a new user guide, mappings to MITRE's EMB3D, and techniques contributed by researchers. The update also incorporates the DEF CON 33 presentation 'Hacking Space to Defend It: Generating IoBs with SPARTA,' along with some general bug fixes and aesthetic updates to the GUI to enhance usability. #SPARTAv3.1 #Update

Sources: [Medium Aerospace Corporation](#), [Industrial Cyber](#)



TECHNOLOGY

2025 year's 'most significant space event' is a 'disruptible' test

The year's most significant space event is a 'disruptible' test, according to a report from the Wall Street Journal. The report, which is based on sources familiar with the matter, says that the test is a 'disruptible' test, according to a report from the Wall Street Journal.

Sources: [Wall Street Journal](#)



TECHNOLOGY

How Airbus' SIMBA helps monitor GPS spoofing

The German satellite navigation manufacturer Airbus has announced the new SIMBA system is designed to detect and prevent GPS spoofing attacks. The system is based on a multi-sensor approach that combines GPS data with other data sources such as inertial sensors, barometric pressure, and other sensors to detect and prevent spoofing attacks. The system is designed to be integrated into a variety of applications, including navigation, timing, and location-based services. [#SIMBA #GPS #Spoofing](#)

Source: [Airbus](#)



ESA's Galileo Navigation System Receives First Navigation Data from Galileo-10 GPS satellite in Europe

ESA's Galileo Navigation System has received the first navigation data from Galileo-10, a GPS satellite in Europe. The Galileo-10 satellite is the first of a new generation of Galileo satellites that will provide improved accuracy and reliability for navigation services. The satellite is expected to be launched in the near future. [#Galileo #GPS #Navigation](#)

Source: [ESA](#)



Breakthrough in semiconductor technology sets new efficiency record for broadband satellite communications

High throughput satellite (HTS) technology has achieved a new efficiency record for broadband satellite communications. The new record was set by a HTS satellite that achieved a throughput of 1.2 Gbps. This is a significant improvement over previous records and demonstrates the potential for HTS technology to provide high-speed, low-latency satellite communications. [#HTS #Satellite #Communications](#)

Source: [ESA](#)



ESA and NASA partner to research high bandwidth HTS communications

ESA and NASA have partnered to research high bandwidth HTS communications. The partnership will focus on developing new HTS technologies and applications that will enable high-speed, low-latency satellite communications. The partnership is expected to lead to a variety of new HTS applications, including high-speed data transfer, remote sensing, and navigation. [#ESA #NASA #HTS](#)

Source: [ESA](#)



★ Space Force building tools to detect cyberattacks on satellites

US Space Force contractors are building an AI-powered tool to detect cyberattacks on satellites by directly monitoring the behavior and telemetry outputs of satellite systems in orbit. The Cyber Resilience On-Orbit tool will be available as a software program but could be implemented in hardware and installed on satellites, said Dick Wilkinson, cofounder and chief technology officer of Proof Labs, an Albuquerque, N.M., start up. CROO should be available next year, he said at a gathering organized by the non-profit Aerospace Corp. and the Space ISAC. [#USSF #CROO](#)

Source: [Air & Space Forces](#)



France unveils SIMBA, a satellite navigation system to combat the quantum threat for global defense and government

France has unveiled SIMBA, a satellite navigation system designed to combat the quantum threat for global defense and government. The system is based on a multi-sensor approach that combines GPS data with other data sources such as inertial sensors, barometric pressure, and other sensors to detect and prevent spoofing attacks. The system is designed to be integrated into a variety of applications, including navigation, timing, and location-based services. [#SIMBA #GPS #Spoofing](#)

Source: [France](#)



AI revolutionizes space navigation, satellites, and quantum functions

AI is revolutionizing space navigation, satellites, and quantum functions. AI is being used to develop new satellite navigation systems, to improve satellite navigation accuracy, and to develop new quantum functions. AI is also being used to develop new satellite navigation systems, to improve satellite navigation accuracy, and to develop new quantum functions. [#AI #Satellite #Navigation](#)

Source: [AI](#)



Quantum navigation moves from lab to flight deck as GPS spoofing hits industrial scale

Quantum navigation is moving from the laboratory to the flight deck as GPS spoofing hits industrial scale. Quantum navigation is a new technology that uses quantum mechanics to provide accurate navigation data. It is expected to be used in a variety of applications, including navigation, timing, and location-based services. [#Quantum #Navigation](#)

Source: [AI](#)



MARKET & COMPETITION

Advanced navigation expands across U.S. and Europe to meet ongoing demand for PNT technology
Advanced Navigation, a global leader in secure positioning, navigation, and timing (PNT) technologies and solutions, has announced its expansion to establish PNT centers of excellence (COEs) across the U.S. and Europe beginning with the U.S. PNT COE.



Source: [TechCrunch](#)

France Space Space leads 30 states to develop demonstration for GNSS with European and French agencies
European Space Agency and other 30 states, and French Space Space, have been selected by the French Space Agency (CNES) as part of a joint project to develop all the projects under the French 2025 program to lead an international demonstration of the French Space Space's connectivity network (CNES).



Source: [SpaceNews](#)

Germany announces Nordic cybersecurity cooperation to strengthen Europe's defense

Germany announced a new strategic alliance to boost its defense cyber defense capability and a growing Nordic force to get the job done. The alliance includes the new defense force, to get the job done, the alliance joins defense and cybersecurity efforts of new members during the summer. **Magdalena Madsen**



Source: [Defense News](#), [Defense News](#)

France joining British cyber efforts to meet market with emerging satellites

France joining British has a second effort to boost its defense cyber defense capability, efforts defined by the French and British defense forces. The French cyber defense capabilities are currently in government and industry, with plans for more cyber systems by 2025. It is a joint effort to boost cyber defense in space and defense. **Magdalena Madsen**



Source: [BBC](#)

European Technology gets investment from Russia's Edge and Intelligence Capital

European Technology, a provider of intelligence and defense technology, has announced a strategic partnership with Russia's Edge and Intelligence Capital, a provider of intelligence and defense technology. The partnership is a strategic partnership between the two companies, which will focus on the development of new technologies and the expansion of the company's global reach. **Magdalena Madsen**



Source: [CyberInflight](#)

France Aerospace and SME Systems to enhance Deep Strike Capability with anti-jamming GPS

France Aerospace has signed a contract with SME Systems to integrate anti-jamming GPS systems. The agreement is a strategic partnership between the two companies, which will focus on the development of new technologies and the expansion of the company's global reach. **Magdalena Madsen**



Source: [Defense News](#)

British partners with Russia for next generation defense connectivity

British, a British technology company specializing in satellite communications, is partnering with Russia Space Networks to provide a secure next generation connectivity network with the necessary security and performance to support British operations and defense forces. Russia has now been up and running at the end of the project. **Magdalena Madsen**



Source: [TechCrunch](#)

High Arctic does to space - Arctic, Canada and France, Canada does to - space force - High Arctic in the space industry Arctic, Canada and France under the 'space force'

Arctic, Canada, and France, which are aligned on the principle of a three-way consultation in the space sector including territories, will meet next week in high-level negotiations in the situation of their space activities. Specifically, the three major space groups, which aim to merge their activities into a single entity, will meet next week in the situation of their space activities. France Space Space, Canada, Arctic Space Space, Arctic Intelligence and Arctic Space Space. **Magdalena Madsen**



Source: [TechCrunch](#)

MARKET & COMPETITION

Mobile network 4G LTE is lighter than 5G for space-based communications

Mobile network 4G LTE is lighter than 5G for space-based communications. The report of 4G LTE network is lighter than 5G network, and it is more suitable for space-based communications. The report also mentions that 4G LTE network is more suitable for space-based communications than 5G network. The report also mentions that 4G LTE network is more suitable for space-based communications than 5G network.

Source: [TechCrunch](#)



5G network is more suitable for space-based communications

5G network is more suitable for space-based communications. The report of 5G network is more suitable for space-based communications than 4G LTE network. The report also mentions that 5G network is more suitable for space-based communications than 4G LTE network. The report also mentions that 5G network is more suitable for space-based communications than 4G LTE network.

Source: [TechCrunch](#)



5G network is more suitable for space-based communications

5G network is more suitable for space-based communications. The report of 5G network is more suitable for space-based communications than 4G LTE network. The report also mentions that 5G network is more suitable for space-based communications than 4G LTE network. The report also mentions that 5G network is more suitable for space-based communications than 4G LTE network.

Source: [TechCrunch](#)



Mobile communication infrastructure: A strategic investment in geopolitical resilience and secure mission execution

Mobile communication infrastructure: A strategic investment in geopolitical resilience and secure mission execution. The report of mobile communication infrastructure is a strategic investment in geopolitical resilience and secure mission execution. The report also mentions that mobile communication infrastructure is a strategic investment in geopolitical resilience and secure mission execution. The report also mentions that mobile communication infrastructure is a strategic investment in geopolitical resilience and secure mission execution.

Source: [TechCrunch](#)

★ SpaceX buys wireless spectrum from EchoStar in \$17bn deal

Elon Musk's SpaceX said it will buy wireless spectrum licenses from EchoStar (SATS.O), opens new tab for its Starlink satellite network for about \$17bn, a major deal crucial to expanding Starlink's nascent 5G connectivity business. The companies also agreed to a deal that will enable EchoStar's Boost Mobile subscribers to access Starlink direct-to-cell service to extend satellite service to areas without service. **#Starlink #Contract**

Source: [CNBC](#)



THREAT INTELLIGENCE

Mobile network 4G LTE is lighter than 5G for space-based communications

Mobile network 4G LTE is lighter than 5G for space-based communications. The report of 4G LTE network is lighter than 5G network, and it is more suitable for space-based communications. The report also mentions that 4G LTE network is more suitable for space-based communications than 5G network. The report also mentions that 4G LTE network is more suitable for space-based communications than 5G network.

Source: [TechCrunch](#)



★ DSEI Takeaways: Space and cyber and the invisible front line

The advance of space and cyber technologies is creating "an invisible front line" in the warfighting domain. Military leaders at DSEI stressed the need for agility, favoring faster 80% solutions over lengthy, rigid programs. The piece also underscores closer industry-defense collaboration to accelerate innovation and strengthen capabilities against hybrid space-cyber threats. **#DSEI #FrontLine**

Source: [Via Satellite](#)





TRAINING & EDUCATION



TRAINING & EDUCATION

Researchers at Space Cybersecurity Watch and its affiliate, CyberInflight, present a new satellite vulnerability research report by Victor, with a focus on the competitive space domain, and the identification of security threats. The report identifies the vulnerability of the Space Cyber Protocol (SCP) and the Space Controller Area Network (SpaceCAN) protocols. The report aims to use the SCP vulnerability research to the other satellite protocols. The report also aims to use the SCP vulnerability research to the other satellite protocols and use the research to identify and subsequently make corrections. [Read the report](#)



Space and satellite security is a complex and multi-faceted issue. It is a challenge that is becoming increasingly important as the space domain becomes more competitive. The report identifies the vulnerability of the Space Cyber Protocol (SCP) and the Space Controller Area Network (SpaceCAN) protocols. The report aims to use the SCP vulnerability research to the other satellite protocols. The report also aims to use the SCP vulnerability research to the other satellite protocols and use the research to identify and subsequently make corrections. [Read the report](#)



Researchers at Space Cybersecurity Watch and its affiliate, CyberInflight, present a new satellite vulnerability research report by Victor, with a focus on the competitive space domain, and the identification of security threats. The report identifies the vulnerability of the Space Cyber Protocol (SCP) and the Space Controller Area Network (SpaceCAN) protocols. The report aims to use the SCP vulnerability research to the other satellite protocols. The report also aims to use the SCP vulnerability research to the other satellite protocols and use the research to identify and subsequently make corrections. [Read the report](#)



Space and satellite security is a complex and multi-faceted issue. It is a challenge that is becoming increasingly important as the space domain becomes more competitive. The report identifies the vulnerability of the Space Cyber Protocol (SCP) and the Space Controller Area Network (SpaceCAN) protocols. The report aims to use the SCP vulnerability research to the other satellite protocols. The report also aims to use the SCP vulnerability research to the other satellite protocols and use the research to identify and subsequently make corrections. [Read the report](#)



Unveiling security vulnerabilities in open-source satellite communication protocols

Security researcher Vic Huang shares his research on satellite communication protocols that are open source and discovers security vulnerabilities in them. Among protocols that are in focus - CubeSat Space Protocol (CSP) and Space Controller Area Network (SpaceCAN). SpaceCAN is a fork of the famous CAN Bus protocol used in the automotive industry. It has been used in satellites since at least 2003, which means that a large number of satellites orbiting our planet may have CAN Bus in them. **#SpaceCAN #Paper**



Source: [Eerie Glow](#)

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