

SPACE CYBERSECURITY WEEKLY WATCH

Week 43

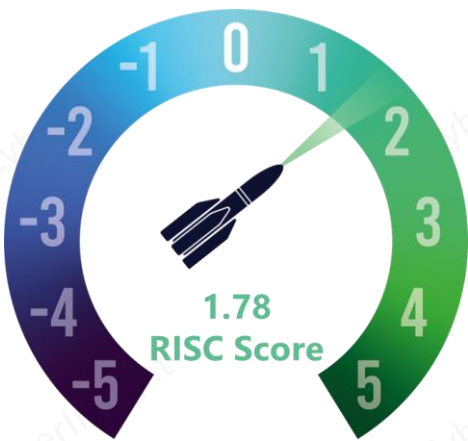
October 21- 27, 2025

Timeframe: Weekly
of articles identified: 37
Est. time to read: 75 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.

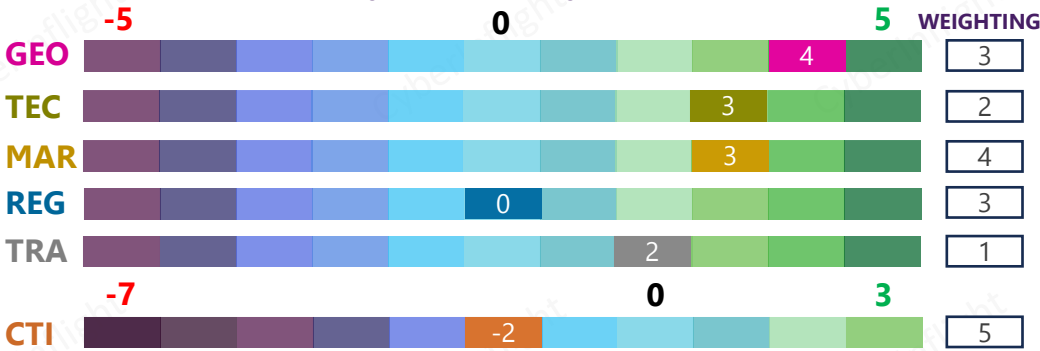
- GEOPOLITICS
- TECHNOLOGY
- MARKET & COMPETITION
- REGULATION
- TRAINING & EDUCATION
- THREAT INTELLIGENCE
- ★ IMPORTANT NEWS

RISC Score Assessment

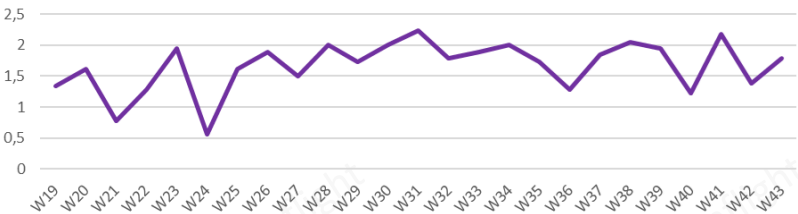


The RISC score for this watch is 1.78, an increase from last week. This change is due to a slight improvement on the threat intelligence front while the geopolitical situation remains stable, with several significant developments.

Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



This week, the geopolitical front focuses on Ukraine, where the parliament has approved a bill to establish a Cyber Force that will consolidate the country’s offensive and defensive military cyber capabilities under a unified command. This development comes as Ukraine simultaneously advances its plan to create a Space Force by the end of 2025. On the regulatory side, China has been selected to host the 2027 World Radiocommunication Conference (WRC-27) in Shanghai. The decision raises concerns from a U.S. perspective regarding China’s growing influence over global telecommunications governance. In the field of technology, Hamburg is emerging as a key hub in Germany’s national quantum computing strategy, led by the German Aerospace Center’s (DLR) Quantum Computing Initiative. 5 quantum computers are being built at DLR’s innovation center in Lokstedt, with projects focused on applications in mobility, artificial intelligence, materials science, and cybersecurity. On the market front, Airbus, Leonardo, and Thales have signed a memorandum of understanding (MoU) to combine their space activities within a new company. This new European space player aims to multiply the strike force of the 3 companies by combining their satellite production activities and related services. On the threat intelligence side, while the U.S. Space Force frequently discusses nation-state cyber-threats, commercial satellite operators are primarily targeted by low-level, financially motivated cyberattacks. According to Joel Francis from Space ISAC, “the most common attack type we see is phishing,” highlighting the persistent yet underestimated nature of these everyday threats in the space sector. The training section highlights the Italian team mHACKERoni, led by 24-year-old Lorenzo Leonardini, which won the 2025 European Cybersecurity Challenge organized by ENISA in Warsaw. His team had previously gained attention for successfully taking control of a satellite in orbit during the U.S. Department of Defense’s “Hack-A-Sat” competition in 2023.



Confronted with escalating cyber and space threats, Kyiv is now working to create centralized structures dedicated to defending Ukraine from future multi-domain attacks. On October 9, Ukraine's parliament approved a bill to establish a Cyber Force, which would unite its offensive and defensive military cyber capabilities under a single command. This legislation comes alongside Ukraine's parallel effort to create a Space Force by the end of 2025. **#Ukraine #SpaceWarfare**



©1996-2001 Intel®. Intel® is a registered trademark or trademark of Intel Corporation or its subsidiaries in the United States and other countries. All other trademarks are the property of their respective owners.

While participating in a major space mission, the launch of the ISS in 1998, the other half of us in the first week of November 2000. The Indian Space Research Organisation (ISRO) mission highlights India's rising space capability, and is the first of its kind in the world. The mission is a major step in the development of the Indian Space and Air Force (ISAF) and is a major step in the development of the Indian Space and Air Force (ISAF) and is a major step in the development of the Indian Space and Air Force (ISAF).



India's NSRF to establish strategic satellite station in the Chagos Archipelago

© 2015 National Technical Research Organization (NTRO) is a nonprofit organization to establish a highly qualified human resources, scientific generation and collection facility in the Chicago metropolitan area, including a research center in the United States. NTRO has entered a new agreement with the government of Ethiopia to establish a scientific training and research center in the Chicago metropolitan area, according to reports by the American Press and the State of New York.



The Arctic, outer space and influence-building: China and Russia join forces to expand in new strategic frontiers

Spain's geographical competition with the West is rapidly expanding into new domains. Being able to do things in addition, including water space and cyberspace, to those areas formerly more accessible, being is expanding to what you possess there as the road to becoming a global power. And it is not doing so alone. Russia has become a key partner for Chinese ambitions in space and the West, as Europe and other Western nations have pulled back from competition with Beijing. www.nytimes.com/2009/03/22/world/asia/22china.html



Source: Adapted from "Internet: A Rising Western Technological Power," in *Internet under the Sun*, edited by William J. Bennett, 1996. Reprinted by permission of the author. Copyright 1996 by William J. Bennett. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage or retrieval system, without prior written permission from the publisher.



United Republic to donate North-south corridor corridor to Ukraine

[illegible]

China's push for satellite cooperation in the Middle East

[illegible]

REGULATION



China will host the 2027 World Radiocommunication Conference (WRC-27) in Shanghai, giving it a strategic advantage in shaping global spectrum policy. The decision by the ITU marks a significant geopolitical win for Beijing, influencing future regulations affecting radar, wireless systems, and the expanding space economy. The move raises concerns about information security and China's growing influence over global telecommunications governance, prompting calls for a renewed U.S. commitment to spectrum diplomacy. **#WRC-27 #Opinion**



TECHNOLOGY

Advanced Navigation expands NATO capabilities with 6th satellite

Advanced Navigation, a global 3D Advanced Positioning, Navigation and Timing (APNT) and autonomous system, has been selected as the core of NATO's next generation navigation system. The system will provide integrated services, including 3D positioning, timing and navigation, to support NATO's mission. The system will be used by NATO's 28 member states, as well as other NATO allies and partners. The system will be used by NATO's 28 member states, as well as other NATO allies and partners. The system will be used by NATO's 28 member states, as well as other NATO allies and partners.

Source: [Advanced Navigation](#)



Lockheed Martin targets 2028 space interceptor test for U.S. National Space program

Lockheed Martin has a 2028 space interceptor test for the U.S. National Space program. The test will be conducted in 2028, and will involve the use of the company's new space interceptor. The test will be conducted in 2028, and will involve the use of the company's new space interceptor. The test will be conducted in 2028, and will involve the use of the company's new space interceptor.

Source: [Lockheed Martin](#)



Microsoft's infrastructure upgrade can be delivered long-term value

Microsoft is investing in infrastructure with an infrastructure upgrade aimed at strengthening its ability and growth. The company is investing in infrastructure with an infrastructure upgrade aimed at strengthening its ability and growth. The company is investing in infrastructure with an infrastructure upgrade aimed at strengthening its ability and growth.

Source: [Microsoft](#)



Adrian Iordache leading first Italian 6G/6G+ demonstration for 6thGigaparts testing solution

Adrian Iordache is leading the first Italian 6G/6G+ demonstration for 6thGigaparts testing solution. The demonstration will be conducted in 2025, and will involve the use of the company's new 6G/6G+ technology. The demonstration will be conducted in 2025, and will involve the use of the company's new 6G/6G+ technology.

Source: [Adrian Iordache](#)



Hamburg positions itself at the core of a national quantum effort

Hamburg is emerging as a key hub in Germany's national quantum computing strategy, led by the German Aerospace Center's (DLR) Quantum Computing Initiative. Five quantum computers are being built at DLR's innovation center in Lokstedt, with projects focused on applications in mobility, artificial intelligence, materials science, and cybersecurity. Early demonstrator systems are already operational, with larger, more complex quantum computers expected by 2027.

#Quantum #DLR

Source: [The Quantum Insider](#)



Safe Systems offers integrated air and ground 6G/6G+ interference monitoring

Safe Systems has developed a new 6G/6G+ interference monitoring system. The system will be used by NATO's 28 member states, as well as other NATO allies and partners. The system will be used by NATO's 28 member states, as well as other NATO allies and partners.

Source: [Safe Systems](#)



Adrian Iordache leads 6G/6G+ demonstration, completing Spain's most advanced secure space program

Adrian Iordache is leading the 6G/6G+ demonstration, completing Spain's most advanced secure space program. The demonstration will be conducted in 2025, and will involve the use of the company's new 6G/6G+ technology. The demonstration will be conducted in 2025, and will involve the use of the company's new 6G/6G+ technology.

Source: [Adrian Iordache](#)



The challenges to building resilient and reliable new terrestrial networks

New terrestrial networks offer a great way to improve the way we live and work. The new terrestrial networks offer a great way to improve the way we live and work. The new terrestrial networks offer a great way to improve the way we live and work.

Source: [The Challenges](#)

MARKET & COMPETITION

ESA awarded 100M€ by ESA-ESA Programme for 2025-2026

The European Space Agency (ESA) has awarded a 100M€ contract to the European Space Agency (ESA) for the 2025-2026 period. The contract is for the development and testing of the ESA-ESA Programme for 2025-2026. The contract is for the development and testing of the ESA-ESA Programme for 2025-2026. The contract is for the development and testing of the ESA-ESA Programme for 2025-2026.

Source: [ESA](#)



ESA awards 100M€ for 2025-2026

The European Space Agency (ESA) has awarded a 100M€ contract to the European Space Agency (ESA) for the 2025-2026 period. The contract is for the development and testing of the ESA-ESA Programme for 2025-2026. The contract is for the development and testing of the ESA-ESA Programme for 2025-2026. The contract is for the development and testing of the ESA-ESA Programme for 2025-2026.

Source: [ESA](#)



U.S. DoD awards contract for 2025-2026 to protect against GPS disruption

The U.S. Department of Defense (DoD) has awarded a contract for 2025-2026 to protect against GPS disruption. The contract is for the development and testing of the GPS disruption protection system. The contract is for the development and testing of the GPS disruption protection system. The contract is for the development and testing of the GPS disruption protection system.

Source: [DoD](#)



As space weapons proliferate, space satellites are getting new armor

As space weapons proliferate, space satellites are getting new armor. The new armor is designed to protect satellites from space weapons. The new armor is designed to protect satellites from space weapons. The new armor is designed to protect satellites from space weapons.

Source: [Space.com](#)



Airbus, Leonardo et Thales signent un protocole d'accord (MoU) afin de créer un acteur spatial européen de premier plan (*Trad.: Airbus, Leonardo, and Thales sign a memorandum of understanding (MoU) to create a leading European space player*)

Airbus, Leonardo, and Thales have signed a memorandum of understanding (MoU) to combine their space activities within a new company. This new European space player aims to multiply the strike force of the three companies by combining their satellite production activities and related services. The new company could be operational in 2027, subject to the necessary regulatory approvals and the fulfillment of the condition's precedent to the closing of the transaction.

#NewCompany #MoU

Source: [Thales](#)



Space Force plans 100M€ for 2025-2026

The Space Force has awarded a 100M€ contract for 2025-2026. The contract is for the development and testing of the Space Force Programme for 2025-2026. The contract is for the development and testing of the Space Force Programme for 2025-2026. The contract is for the development and testing of the Space Force Programme for 2025-2026.

Source: [Space.com](#)



ESA and ESA-ESA merge to accelerate global satellite launch to deliver connectivity

ESA and ESA-ESA have merged to accelerate global satellite launch to deliver connectivity. The merger is designed to accelerate global satellite launch to deliver connectivity. The merger is designed to accelerate global satellite launch to deliver connectivity. The merger is designed to accelerate global satellite launch to deliver connectivity.

Source: [ESA](#)



ESA-ESA merge to accelerate global satellite launch to deliver connectivity

ESA-ESA has merged to accelerate global satellite launch to deliver connectivity. The merger is designed to accelerate global satellite launch to deliver connectivity. The merger is designed to accelerate global satellite launch to deliver connectivity. The merger is designed to accelerate global satellite launch to deliver connectivity.

Source: [ESA](#)





When discussing cyber-threats, the Space Force often emphasizes nation-state attacks. However, satellite companies face daily low-level cyberattacks, primarily motivated by financial gain. “The most common attack type we see is phishing,” said Joel Francis from Space ISAC. With automated mass emailing tools, even unskilled hackers can launch wide-ranging phishing campaigns. As Francis noted, these attacks are generally broad and utilize commoditized techniques rather than being highly targeted or custom-crafted. **#SpaceThreat #Awareness**



What are the key components of a successful digital marketing strategy?



Copyright © 2010 John Wiley & Sons, Ltd.



There is already considerable evidence that ongoing cyber warfare could extend to space. Reports indicate concerns that hackers might target space satellites, including the GPS infrastructure system critical to the transportation law. A recent analysis by RAND suggests that defense and intelligence agencies are investigating possible operational threats, considering whether incidents should be due to technical failure or external threats.



The wireless network has enabled communications from across a central group of cables and electronic devices. It enables the network devices and other users depend on network devices (WLAN) and also help for operations and maintenance, making them more useful for planning, monitoring, and supply chain management.

The authors agree that there is no direct responsibility for a cyber attack on the wireless grid. The group does not think there will be the effect of the typical construction. The group has been made public, but the distribution of the attack may not be as simple. **Report 2010**



TRAINING & EDUCATION

© 2006 CyberTrust. All rights reserved. CyberTrust is a registered trademark of CyberTrust. All other trademarks are the property of their respective owners.



bioRxiv preprint doi: <https://doi.org/10.1101/000000>; this version posted March 1, 2016. The copyright holder for this preprint (which was not certified by peer review) is the author/funder, who has granted bioRxiv a license to display the preprint in perpetuity. It is made available under aCC-BY-NC-ND 4.0 International license.



TRAINING & EDUCATION

Efficient, dynamic, multipath spatial routing against eavesdropping in space-ground integrated networks

The paper presents a novel routing scheme based on dynamic routing (DR) in space-ground integrated networks. The DR is defined to search for the most secure routing paths. The scheme of DR is to select the most secure routing paths by searching routing paths. [IEEE Page](#)



Cooperative multi-robot navigation with programming-based spatial sampling for robust adaptive trajectory

This work presents an efficient, robust adaptive trajectory planning technique to address multi-robot navigation and the corresponding multi-robot coordination problem. In particular, the scheme of adaptive trajectory planning is proposed with spatial sampling to select the optimal paths of the working space in a dynamic environment. [IEEE Page](#)



Reconfigurable antenna-enhanced beamforming signal enhancement and interference suppression

Reconfigurable beamforming with beam steering antenna array can be used to effectively enhance signal and suppress interference due to significant variations in antenna steering gain over different steering angles. To reach this goal, an intelligent antenna array is proposed to enhance the antenna steering gain by reconfiguring the antenna array. The proposed antenna array is based on the reconfigurable antenna array. [IEEE Page](#)



Energy-efficient for efficient and fast 5G communication with enhanced antennas, beam forming and AI

This paper presents a novel method to reduce the energy consumption and enhance the efficiency of 5G communication system. The proposed method is based on the reconfigurable antenna array, beam forming and AI. The proposed method is based on the reconfigurable antenna array, beam forming and AI. [IEEE Page](#)



Lorenzo Leonardini: l'hacker che ha dirottato un satellite e vinto la gara europea per la sicurezza informatica (Trad.: Lorenzo Leonardini: the hacker who hijacked a satellite and won the European cybersecurity competition)

The Italian team mHACKERoni, led by 24-year-old Lorenzo Leonardini, won the 2025 European Cybersecurity Challenge organized by ENISA in Warsaw. His team had previously gained attention for successfully taking control of a satellite in orbit during the U.S. Department of Defense's "Hack-A-Sat" competition in 2023. In an interview, he emphasized the importance of developing secure coding practices and improving legacy systems' resilience.



#ENISA #EuropeanCybersecurityChallenge

Source: [Open Online](#)

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