



# SPACE CYBERSECURITY WEEKLY WATCH

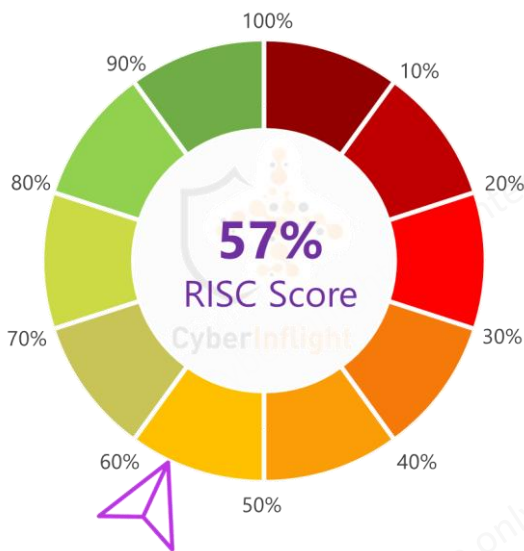
Week 19  
May 7 – 13, 2024

Timeframe : Weekly  
# of articles identified : 27  
Est. time to read : 45 minutes

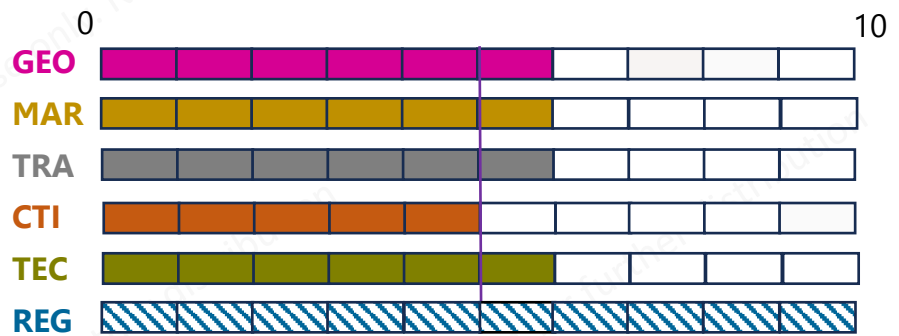
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

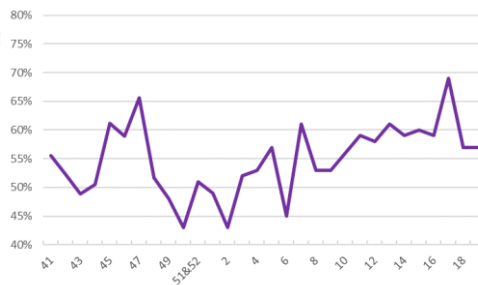
## Overview & RISC Score



Same than last week



### RISC Score Evolution



*This W19 shows the same RISC Score level as last week, showing a decrease from W17, being the highest week of the year. Despite this week, the level is quite constant and higher than last year at the same period.*

This week's RISC score is 57%. This week, our CEO, Florent Rizzo, was interviewed by La Tribune about the major challenges facing the space cybersecurity sector. In addition, the Lithuanian Foreign Minister declared Russia's jamming of GPS signals has marked a shift in its non-conventional attacks against the Baltic states. Russia is indeed moving towards a more physical domain in its attacks, affecting airplanes and the daily lives of people in the Baltic region. On the market front, Leonardo-led-consortium Indra is developing the first pan-European center for monitoring risks to digital infrastructure in real-time. This center for dynamic cyber risk management will monitor in real time the degree of threat to which digital infrastructures are exposed throughout the continent. In addition, cybersecurity has taken a step forward with a new course aimed at professionals working in Scotland's booming space sector. Space industry executives can now enroll in the 'executive space course' at Strathclyde University in Glasgow. On the technology front, Viavi Solutions announced the availability of SecurePNT 6200 with SecureTimeSM services, a resilient timing clock solution that delivers the most comprehensive assurance of PNT services used in critical infrastructure operations worldwide. Finally, Russian electronic warfare has created problems for some American-made precision weaponry in Ukraine. Moscow is telling the US what it needs solutions for to be ready for future fights.



# CYBERINFLIGHT'S NEWS



## The space industry is facing an escalation of cyber attacks due to geopolitical context

Since the outbreak of the war in Ukraine, the number of cyberattacks targeting space systems has grown significantly. Florent RIZZO, CyberInflight's CEO, has been interviewed by La Tribune, about the major challenges facing the sector, at a time when cybersecurity will be in the center of the future European Space Law. **#SpaceCybersecurity #Cyberattacks**  
**Link:** <https://toulouse.latribune.fr/entreprises/business/2024-05-06/le-spatial-fait-face-a-une-recrudescence-de-cyberattaques-liee-au-contexte-geopolitique-996702.html>



## GEOPOLITIC

### Space cooperation and South Asia's security dilemma

India's space program has been a key element of its foreign policy, and its growing capabilities and ambitions in the domain of space have become a major focus of its international relations. The country's space program has been a key element of its foreign policy, and its growing capabilities and ambitions in the domain of space have become a major focus of its international relations.

Space Security

**Link:** [https://www.csis.org/analysis/indias-space-program-and-its-implications-for-space-security](#)

### Taliban announced a representation of the Russian Federation to the airport due to joining of the OPI group

The Taliban government in Afghanistan has announced the appointment of a representative of the Russian Federation to the airport, following the group's decision to join the OPI group. This move is seen as a significant step towards normalizing relations with Russia and the international community.

**Link:** [https://www.csis.org/analysis/taliban-represents-russia-at-afghan-airport](#)

### China space program will bring world to a standstill in chilling plan to wipe out GPS and control the skies, warns US

The United States has issued a warning that China's space program could bring the world to a standstill. In a chilling plan, the country aims to wipe out GPS and control the skies, which could have catastrophic consequences for global navigation and communication systems.

**Link:** [https://www.csis.org/analysis/china-space-program-will-bring-world-to-standstill](#)



## GPS jamming represents shift in Russian attacks on Baltics

Lithuanian Foreign Minister Gabrielius Landsbergis declared Russia's jamming of GPS signals marks a shift in its non-conventional attacks against the Baltic states. "They are moving from the cyber domain, disinformation domain, towards a more physical one which affects airplanes, daily lives of people in our region", he said in a joint news conference with his new Latvian counterpart Baiba Braze in Vilnius. **#Lithuania #Russia**

**Link:** <https://www.lrt.lt/en/news-in-english/19/2270028/gps-jamming-represents-shift-in-russian-attacks-on-baltics-lithuanian-fm>

### Over 50 companies and government representatives attend US France comprehensive dialogue on space

Over 50 companies and government representatives attended the US France comprehensive dialogue on space, which focused on the challenges and opportunities in the space industry. The event highlighted the importance of international cooperation in space exploration and the development of space-based technologies.

**Link:** [https://www.csis.org/analysis/us-france-dialogue-on-space](#)





# MARKET & COMPETITION

## Indra equips the European Commission cyber risk management center with secure communications prepared to withstand future quantum computer attacks

A Leonardo-led-consortium, incorporating Indra, is developing the first pan-European center for monitoring risks to digital infrastructure in real-time. This center for dynamic cyber risk management will monitor in real time the degree of threat to which digital infrastructures are exposed throughout the continent, tracking the activity of criminal groups on the Internet, dark web and social networks, relying on different databases to extract intelligence. #Indra #EuropeanCommission

**Link:** <https://www.indracompany.com/en/noticia/indra-equips-european-commission-cyber-risk-management-center-secure-communications-prepared>

## ESA launches call for proposals for the development of a quantum communication network

The European Space Agency (ESA) has launched a call for proposals for the development of a quantum communication network. The network will be used to secure the communication of sensitive information between Earth and space.

**Link:** [https://www.esa.int/Enabling\\_Support/Space\\_Engineering\\_Technology/ESA\\_launches\\_call\\_for\\_proposals\\_for\\_the\\_development\\_of\\_a\\_quantum\\_communication\\_network](https://www.esa.int/Enabling_Support/Space_Engineering_Technology/ESA_launches_call_for_proposals_for_the_development_of_a_quantum_communication_network)

## ESA launches call for proposals for the development of a quantum communication network

The European Space Agency (ESA) has launched a call for proposals for the development of a quantum communication network. The network will be used to secure the communication of sensitive information between Earth and space.

**Link:** [https://www.esa.int/Enabling\\_Support/Space\\_Engineering\\_Technology/ESA\\_launches\\_call\\_for\\_proposals\\_for\\_the\\_development\\_of\\_a\\_quantum\\_communication\\_network](https://www.esa.int/Enabling_Support/Space_Engineering_Technology/ESA_launches_call_for_proposals_for_the_development_of_a_quantum_communication_network)



## Indra equips the European Commission cyber risk management center with secure communications prepared to withstand future quantum computer attacks

A Leonardo-led-consortium, incorporating Indra, is developing the first pan-European center for monitoring risks to digital infrastructure in real-time. This center for dynamic cyber risk management will monitor in real time the degree of threat to which digital infrastructures are exposed throughout the continent, tracking the activity of criminal groups on the Internet, dark web and social networks, relying on different databases to extract intelligence. #Indra #EuropeanCommission

**Link:** <https://www.indracompany.com/en/noticia/indra-equips-european-commission-cyber-risk-management-center-secure-communications-prepared>

## ESA launches call for proposals for the development of a quantum communication network

The European Space Agency (ESA) has launched a call for proposals for the development of a quantum communication network. The network will be used to secure the communication of sensitive information between Earth and space.

**Link:** [https://www.esa.int/Enabling\\_Support/Space\\_Engineering\\_Technology/ESA\\_launches\\_call\\_for\\_proposals\\_for\\_the\\_development\\_of\\_a\\_quantum\\_communication\\_network](https://www.esa.int/Enabling_Support/Space_Engineering_Technology/ESA_launches_call_for_proposals_for_the_development_of_a_quantum_communication_network)

## ESA launches call for proposals for the development of a quantum communication network

The European Space Agency (ESA) has launched a call for proposals for the development of a quantum communication network. The network will be used to secure the communication of sensitive information between Earth and space.

**Link:** [https://www.esa.int/Enabling\\_Support/Space\\_Engineering\\_Technology/ESA\\_launches\\_call\\_for\\_proposals\\_for\\_the\\_development\\_of\\_a\\_quantum\\_communication\\_network](https://www.esa.int/Enabling_Support/Space_Engineering_Technology/ESA_launches_call_for_proposals_for_the_development_of_a_quantum_communication_network)

## ESA launches call for proposals for the development of a quantum communication network

The European Space Agency (ESA) has launched a call for proposals for the development of a quantum communication network. The network will be used to secure the communication of sensitive information between Earth and space.

**Link:** [https://www.esa.int/Enabling\\_Support/Space\\_Engineering\\_Technology/ESA\\_launches\\_call\\_for\\_proposals\\_for\\_the\\_development\\_of\\_a\\_quantum\\_communication\\_network](https://www.esa.int/Enabling_Support/Space_Engineering_Technology/ESA_launches_call_for_proposals_for_the_development_of_a_quantum_communication_network)

## ESA launches call for proposals for the development of a quantum communication network

The European Space Agency (ESA) has launched a call for proposals for the development of a quantum communication network. The network will be used to secure the communication of sensitive information between Earth and space.

**Link:** [https://www.esa.int/Enabling\\_Support/Space\\_Engineering\\_Technology/ESA\\_launches\\_call\\_for\\_proposals\\_for\\_the\\_development\\_of\\_a\\_quantum\\_communication\\_network](https://www.esa.int/Enabling_Support/Space_Engineering_Technology/ESA_launches_call_for_proposals_for_the_development_of_a_quantum_communication_network)



# TRAINING & EDUCATION



## Cybersecurity enters final frontier with new Scottish course for space sector

Cybersecurity has entered the final frontier with a new course for professionals working in Scotland's growing space sector. Space industry executives are enrolling on the 'executive space course' at Strathclyde University in Glasgow – to understand the challenges of cybersecurity in space. **#Scotland #SpaceUniversity**

**Link:** <https://futurescot.com/cybersecurity-enters-final-frontier-with-new-scottish-course-for-space-sector/>

**Executive course at Strathclyde University**  
The new executive space course is designed for professionals working in the space sector. It covers the challenges of cybersecurity in space, including the risks of data breaches, cyberattacks, and the impact of space weather. The course is delivered by Strathclyde University in Glasgow, Scotland.

**Space industry executives**  
Space industry executives are enrolling on the 'executive space course' at Strathclyde University in Glasgow. The course is designed for professionals working in the space sector, providing them with the knowledge and skills needed to understand the challenges of cybersecurity in space.

**Strathclyde University**  
The course is delivered by Strathclyde University in Glasgow, Scotland. It is a new addition to their offerings, reflecting the growing importance of cybersecurity in the space sector.

**Space industry executives**  
Space industry executives are enrolling on the 'executive space course' at Strathclyde University in Glasgow. The course is designed for professionals working in the space sector, providing them with the knowledge and skills needed to understand the challenges of cybersecurity in space.

**Space industry executives**  
Space industry executives are enrolling on the 'executive space course' at Strathclyde University in Glasgow. The course is designed for professionals working in the space sector, providing them with the knowledge and skills needed to understand the challenges of cybersecurity in space.

**Space industry executives**  
Space industry executives are enrolling on the 'executive space course' at Strathclyde University in Glasgow. The course is designed for professionals working in the space sector, providing them with the knowledge and skills needed to understand the challenges of cybersecurity in space.







## TECHNOLOGY



### Stopping satellite attacks and spoofing

Viavi Solutions Inc. announced the availability of SecurePNT 6200 with SecureTimeSM services, a resilient timing clock solution that delivers the most comprehensive assurance of PNT services used in critical infrastructure operations worldwide. SecurePNT and SecureTime build on VIAVI's proven assured PNT solutions with the addition of the Fugro AtomiChron timing service, enabling intelligent zero-trust multisource assurance combining signals from GEO, LEO and MEO GPS and GNSS constellations. **#ViaviSolutions #SecurePNT**

**Link:** <https://www.communicationstoday.co.in/stopping-satellite-attacks-and-spoofing/>



## THREAT INTELLIGENCE

**Russian jamming of GPS spoofing shows multiple areas of the US with high probability of spoofing**

**Link:** [https://www.businessinsider.com/russian-jamming-gps-spoofing-us-2024-5](#)



**Russian jamming of GPS spoofing shows multiple areas of the US with high probability of spoofing**

Russian jamming of GPS spoofing shows multiple areas of the US with high probability of spoofing. The jamming is being done by the Russian military and is aimed at disrupting GPS signals in the US. This is a significant threat to the US and its allies. **#Russia #US**

**Link:** [https://www.businessinsider.com/russian-jamming-gps-spoofing-us-2024-5](#)



### Russia's jamming of American weapons in Ukraine is showing the US what it needs to be ready for in a future fight

Russian electronic warfare has created problems for some American-made precision weaponry in Ukraine, but Moscow is also showing its hand and telling the US what it needs solutions for to be ready for future fights. **#Russia #US**

**Link:** <https://www.businessinsider.com/russian-electronic-warfare-shows-us-needs-for-future-wars-2024-5>



**Russian jamming of GPS spoofing shows multiple areas of the US with high probability of spoofing**

Russian jamming of GPS spoofing shows multiple areas of the US with high probability of spoofing. The jamming is being done by the Russian military and is aimed at disrupting GPS signals in the US. This is a significant threat to the US and its allies. **#Russia #US**

**Link:** [https://www.businessinsider.com/russian-jamming-gps-spoofing-us-2024-5](#)



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](mailto:research@cyberinflight.com)