

SPACE CYBERSECURITY WEEKLY WATCH

Week 44

October 28 - November 3, 2025

Timeframe: Weekly

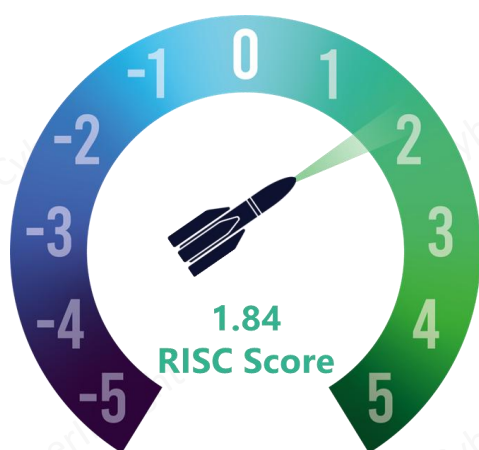
of articles identified: 45

Est. time to read: 90 minutes

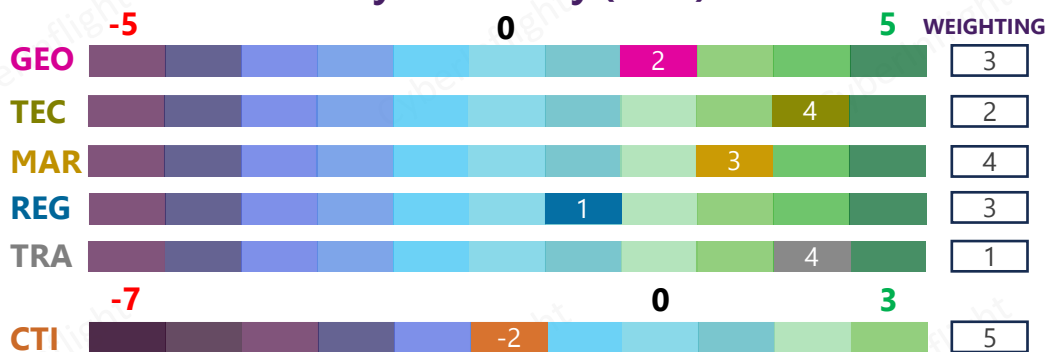
Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

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

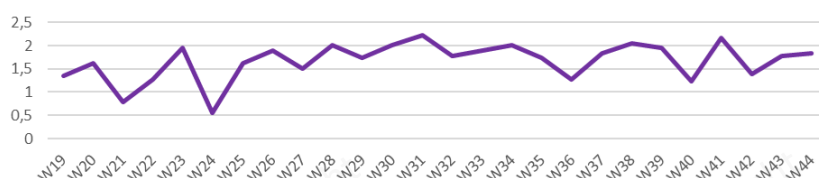
RISC Score Assessment



Overview & Resilience Index for Space Cybersecurity (RISC)



RISC Score evolution in 2025



↑ The RISC score for this watch is 1.84, a slight increase from last week due to improvements in the technology and training & education sections.

This week, the European Space Agency (ESA) unveiled details of its €1.2bn European Resilience from Space (ERS) program, presented in Brussels. The initiative aims to create an integrated network of Earth observation, navigation, and secure communications satellites to support defense, crisis management, and critical infrastructure resilience. Meanwhile, on the regulatory front, Professor Matthew Warren of the Royal Melbourne Institute of Technology highlighted the urgent need for a unified Australian framework to secure the nation's space infrastructure. From a technological standpoint, cybersecurity specialist Anvil Secure and space logistics firm D-Orbit have jointly unveiled a comprehensive white paper that addresses the application of cybersecurity measures throughout the lifecycle of satellite missions. The guide recommends specific mitigations, including encryption of radio communications, thorough validation of hosted payloads, and robust firmware protection from build through orbital deployment. On the market front, Leonardo will lead a new European initiative to develop a platform for assessing quantum-secure communications, following the award of a multi-year contract from the European Space Agency. The work brings together a consortium including Thales Alenia Space, Telespazio Belgium, ThinkQuantum, and DamoTech. Turning to threat intelligence, a US Space Force general says it's 'concerning' just how fast China is closing the gap on the space tech that backs modern armies. The training & education section focuses on a podcast with Kristiina Omri, Vice President of Special Programs at CybExer Technologies, and Aare Reintam, the company's COO. Recorded in Tallinn, on the eve of the Software Defined Space Conference, the conversation explores how Estonia, in collaboration with the ESA, is helping shape the future of space cybersecurity through the creation of the world's first Space Cyber Range.

GEOPOLITICS

Germany's 2025 New Defense Budget will expand NATO air, space, and long-range strike power

Germany's 2025 New Defense Budget will expand NATO air, space, and long-range strike power. The budget will increase the number of German fighter jets from 330 to 350, with a focus on the Eurofighter Typhoon. It will also increase the number of German long-range strike aircraft from 18 to 24, with a focus on the Airbus A400M military helicopter. The budget will also increase the number of German space satellites from 10 to 15, with a focus on the Galileo navigation system. The budget will also increase the number of German cyber defense units from 10 to 15, with a focus on the National Cyber and Information Security Agency (BSI).

Source: [The Guardian](#)



1.2 miliardi di Euro per il progetto ERS, con cui l'ESA vorrebbe rendere l'Europa più autonoma nello spazio (Trad.: €1.2bn for the ESA's ERS project to strengthen Europe's autonomy and resilience in space)

The European Space Agency (ESA) has unveiled details of its €1.2bn European Resilience from Space (ERS) program, presented in Brussels. ERS aims to create an integrated network of Earth observation, navigation, and secure communications satellites to support defense, crisis management, and critical infrastructure resilience. The program includes a €250m Low Earth Orbit PNT constellation to reinforce Galileo against cyber and signal interference and a €200m secure communications segment evolving from IRIS². #ESA #ERS

Sources: [Astrospace](#), [ESA](#)



Low Earth Orbit, high stakes: Pakistan must claim its place in the satellite internet race

Low Earth Orbit, high stakes: Pakistan must claim its place in the satellite internet race. The article discusses the importance of satellite internet for Pakistan, particularly in rural areas. It mentions that Pakistan is currently not a member of the International Telecommunication Union (ITU) and that this is a major obstacle to its participation in the satellite internet race. The article also mentions that Pakistan is currently not a member of the Organization for the Prohibition of Chemical Weapons (OPCW) and that this is a major obstacle to its participation in the satellite internet race.

Source: [The Guardian](#)



Comply or collapse: why President Trump's battle shows the American depends on securing operational technology

Comply or collapse: why President Trump's battle shows the American depends on securing operational technology. The article discusses the importance of operational technology (OT) for the United States, particularly in the context of the ongoing trade war with China. It mentions that the United States is currently not a member of the World Trade Organization (WTO) and that this is a major obstacle to its participation in the trade war. The article also mentions that the United States is currently not a member of the Organization for the Prohibition of Chemical Weapons (OPCW) and that this is a major obstacle to its participation in the trade war.

Source: [The Guardian](#)



REGULATION



Australian cyber security standards and space

Professor Matthew Warren of RMIT University highlights the urgent need for a unified Australian framework to secure the nation's space infrastructure, now defined as part of its critical infrastructure. While Australia currently relies on general cybersecurity laws, the article argues for specific space-focused standards, drawing on lessons from international models such as the U.S. NIST CSF 2.0, NASA-STD-1006, and CISA guidance. It also references the upcoming IEEE P3536 space system cybersecurity design standard. #Framework #Opinion

Source: [Space and Defense](#)



Integrating the mission: The quest for AI regulation in space and satellite operations

Integrating the mission: The quest for AI regulation in space and satellite operations. The article discusses the importance of AI regulation in space and satellite operations. It mentions that the United States is currently not a member of the International Telecommunication Union (ITU) and that this is a major obstacle to its participation in the satellite internet race. The article also mentions that the United States is currently not a member of the Organization for the Prohibition of Chemical Weapons (OPCW) and that this is a major obstacle to its participation in the satellite internet race.

Source: [The Guardian](#)

TECHNOLOGY

Implementing quantum-safe transport during mobile for critical infrastructure

Implementing quantum-safe transport during mobile for critical infrastructure. The article discusses the importance of quantum-safe transport for critical infrastructure. It mentions that the United States is currently not a member of the International Telecommunication Union (ITU) and that this is a major obstacle to its participation in the satellite internet race. The article also mentions that the United States is currently not a member of the Organization for the Prohibition of Chemical Weapons (OPCW) and that this is a major obstacle to its participation in the satellite internet race.

Source: [The Guardian](#)



TECHNOLOGY



Anvil Secure and D-Orbit outline steps to advance satellite cybersecurity across mission operations

Cybersecurity specialist Anvil Secure and the space logistics firm D-Orbit have jointly unveiled a comprehensive white paper addressing the application of cybersecurity measures throughout the lifecycle of satellite missions. The new publication centers on D-Orbit's ION Satellite Carrier, describing operational stages and providing strategic direction for manufacturers of small satellites. The guide recommends specific mitigations including encryption of radio communications, thorough validation of hosted payloads, and robust firmware protection from build through orbital deployment. **#Resilience #WhitePaper**

Source: [SpaceWar](#)



Software introduces new alternative PDR step to address GNSS disruptions

Software introduced by D-Orbit's ION Satellite Carrier, a comprehensive cybersecurity solution designed to reduce the risk of GNSS disruption, is now being tested on a small satellite. The software introduces a new step in the PDR (Payload Readiness Review) process, focusing on the validation of the software's ability to handle GNSS disruptions. This step involves a thorough review of the software's ability to maintain operations in the event of a GNSS outage, ensuring that the satellite can continue to function and transmit data. The software also includes a robust firmware protection mechanism, ensuring that the satellite's firmware is secure and cannot be tampered with during deployment or operation.



Postlander provides rapid, resilient autonomy in navigation

Postlander, a software solution developed by D-Orbit's ION Satellite Carrier, is designed to provide rapid, resilient autonomy in navigation. The software is designed to handle GNSS disruptions and provide a fallback navigation system. It uses a combination of inertial navigation and other sensors to maintain accurate position and velocity data. The software is designed to be highly resilient, ensuring that the satellite can continue to operate even in the event of a GNSS outage. The software also includes a robust firmware protection mechanism, ensuring that the satellite's firmware is secure and cannot be tampered with during deployment or operation.



Caldero supports precision GNSS antenna portfolio

Caldero, a software solution developed by D-Orbit's ION Satellite Carrier, is designed to support precision GNSS antenna portfolio. The software is designed to handle GNSS disruptions and provide a fallback navigation system. It uses a combination of inertial navigation and other sensors to maintain accurate position and velocity data. The software is designed to be highly resilient, ensuring that the satellite can continue to operate even in the event of a GNSS outage. The software also includes a robust firmware protection mechanism, ensuring that the satellite's firmware is secure and cannot be tampered with during deployment or operation.



AI navigation platform provides to boost satellite network capability

AI navigation platform, a software solution developed by D-Orbit's ION Satellite Carrier, is designed to boost satellite network capability. The platform uses artificial intelligence to optimize satellite network operations. It can predict satellite positions and velocities, allowing for more efficient network management. The platform also includes a robust firmware protection mechanism, ensuring that the satellite's firmware is secure and cannot be tampered with during deployment or operation.



Modeling data center for GNSS, and GNSS PDR based autonomous driving

Modeling data center for GNSS, and GNSS PDR based autonomous driving, a software solution developed by D-Orbit's ION Satellite Carrier, is designed to provide a comprehensive view of satellite network operations. The software uses modeling to predict satellite positions and velocities, allowing for more efficient network management. The software also includes a robust firmware protection mechanism, ensuring that the satellite's firmware is secure and cannot be tampered with during deployment or operation.



Native protocols with next phase of operations time transfer project back by ESA

Native protocols with next phase of operations time transfer project back by ESA, a software solution developed by D-Orbit's ION Satellite Carrier, is designed to provide a comprehensive view of satellite network operations. The software uses native protocols to transfer time data between satellites and ground stations. The software also includes a robust firmware protection mechanism, ensuring that the satellite's firmware is secure and cannot be tampered with during deployment or operation.



Implementing secured PDR for static and dynamic applications

Implementing secured PDR for static and dynamic applications, a software solution developed by D-Orbit's ION Satellite Carrier, is designed to provide a comprehensive view of satellite network operations. The software uses secured PDR to ensure that the satellite's firmware is secure and cannot be tampered with during deployment or operation.



MARKET & COMPETITION



ESA backs Leonardo-led program to test quantum-secure space communications

Leonardo will lead a new European initiative to develop a platform for assessing quantum-secure communications, following the award of a multi-year contract from the European Space Agency. The work brings together a consortium including Thales Alenia Space, Telespazio Belgium, ThinkQuantum, and DamoTech. The contract covers the creation of a Quantum Security Validation Platform, an architecture intended to test emerging quantum and post-quantum technologies for space systems. **#ESA #Contract**

Source: [Orbital Today](#)



ESA and Airbus partner to deliver autonomous multi-orbit network infrastructure

ESA and Airbus have signed a multi-year contract to develop a platform for assessing quantum-secure communications, following the award of a multi-year contract from the European Space Agency. The work brings together a consortium including Thales Alenia Space, Telespazio Belgium, ThinkQuantum, and DamoTech. The contract covers the creation of a Quantum Security Validation Platform, an architecture intended to test emerging quantum and post-quantum technologies for space systems. **#ESA #Contract**



ESA and Airbus partner to deliver autonomous multi-orbit network infrastructure

ESA and Airbus have signed a multi-year contract to develop a platform for assessing quantum-secure communications, following the award of a multi-year contract from the European Space Agency. The work brings together a consortium including Thales Alenia Space, Telespazio Belgium, ThinkQuantum, and DamoTech. The contract covers the creation of a Quantum Security Validation Platform, an architecture intended to test emerging quantum and post-quantum technologies for space systems. **#ESA #Contract**



ESA and Airbus partner to deliver autonomous multi-orbit network infrastructure

ESA and Airbus have signed a multi-year contract to develop a platform for assessing quantum-secure communications, following the award of a multi-year contract from the European Space Agency. The work brings together a consortium including Thales Alenia Space, Telespazio Belgium, ThinkQuantum, and DamoTech. The contract covers the creation of a Quantum Security Validation Platform, an architecture intended to test emerging quantum and post-quantum technologies for space systems. **#ESA #Contract**



ESA and Airbus partner to deliver autonomous multi-orbit network infrastructure

ESA and Airbus have signed a multi-year contract to develop a platform for assessing quantum-secure communications, following the award of a multi-year contract from the European Space Agency. The work brings together a consortium including Thales Alenia Space, Telespazio Belgium, ThinkQuantum, and DamoTech. The contract covers the creation of a Quantum Security Validation Platform, an architecture intended to test emerging quantum and post-quantum technologies for space systems. **#ESA #Contract**



ESA and Airbus partner to deliver autonomous multi-orbit network infrastructure

ESA and Airbus have signed a multi-year contract to develop a platform for assessing quantum-secure communications, following the award of a multi-year contract from the European Space Agency. The work brings together a consortium including Thales Alenia Space, Telespazio Belgium, ThinkQuantum, and DamoTech. The contract covers the creation of a Quantum Security Validation Platform, an architecture intended to test emerging quantum and post-quantum technologies for space systems. **#ESA #Contract**



ESA and Airbus partner to deliver autonomous multi-orbit network infrastructure

ESA and Airbus have signed a multi-year contract to develop a platform for assessing quantum-secure communications, following the award of a multi-year contract from the European Space Agency. The work brings together a consortium including Thales Alenia Space, Telespazio Belgium, ThinkQuantum, and DamoTech. The contract covers the creation of a Quantum Security Validation Platform, an architecture intended to test emerging quantum and post-quantum technologies for space systems. **#ESA #Contract**



ESA and Airbus partner to deliver autonomous multi-orbit network infrastructure

ESA and Airbus have signed a multi-year contract to develop a platform for assessing quantum-secure communications, following the award of a multi-year contract from the European Space Agency. The work brings together a consortium including Thales Alenia Space, Telespazio Belgium, ThinkQuantum, and DamoTech. The contract covers the creation of a Quantum Security Validation Platform, an architecture intended to test emerging quantum and post-quantum technologies for space systems. **#ESA #Contract**



MARKET & COMPETITION

France to develop ANTHOS, Europe's largest low-orbit space surveillance system for the French National Space Agency

France has selected a contract to develop ANTHOS, Europe's largest low-orbit space surveillance system, for the French National Space Agency (CNES). The system will consist of a constellation of satellites in low Earth orbit (LEO) that will monitor and track objects in space, including satellites and debris. The system will be developed by a consortium of French and European companies, including CNES, Airbus, and Thales. The system is expected to be operational by 2030.



Source: [European Space Agency](#)

ESA to space cybersecurity for satellites

The European Space Agency (ESA) is launching a new initiative to enhance the cybersecurity of its satellites. The initiative will focus on developing and implementing cybersecurity measures for the agency's satellites, including the use of secure communication protocols and the implementation of robust security architectures. The initiative is expected to be completed by 2025.



Source: [Space News](#)

Space sector's cybersecurity differences pay more or pay later

Cybersecurity for space has been an afterthought in the commercial space industry, but that mindset is starting to shift as satellite operators grow more concerned about the threat of cyberattacks and the potential impact of such attacks on their operations. The industry is now beginning to invest in cybersecurity measures, but the question remains whether this investment will pay off in the long run or if it will be a costly mistake.

Source: [Space News](#)

THREAT INTELLIGENCE

Chinese espionage planes reveal a secret of China's spy satellites

Chinese espionage planes have revealed a secret of China's spy satellites: they are capable of intercepting and decoding signals from satellites in orbit. This capability is a significant threat to the security of satellite communications and could have major implications for the global space industry. The revelation comes from a report by the Wall Street Journal.



Source: [Wall Street Journal](#)



US Space Force general says it's 'concerning' just how fast China is closing the gap on the space tech that backs modern armies

According to Brig. Gen. Brian Sidari, the deputy chief of space operations for intelligence with the US Space Force, China is rapidly catching up on the space-based capabilities that enable modern armies to fight effectively. Beijing has spent years investing in its space operations, and a recent reorganization of the military branch that oversaw space, along with other strategic domains like cyberspace and information warfare, suggested an interest in a more streamlined approach to space-related missions. **#China #SpaceWarfare**



Source: [Business Insider](#)

The geopolitics of Starlink in Bangladesh

As Starlink enters Bangladesh, questions of high-speed internet for remote areas, digital divide with lack of infrastructure, cyber espionage and data sovereignty, and growing regional tensions, and other factors make this a difficult and complex issue for the country. The Bangladesh government is currently evaluating the potential benefits and risks of the service.



Source: [The Business Insider](#)

Indonesian developer says SpaceX is 90% to 95% LEO satellite

Indonesian developer says SpaceX is 90% to 95% LEO satellite. The developer claims that SpaceX's Starlink satellites are designed to operate in low Earth orbit (LEO) and are capable of providing high-speed internet to users on the ground. The claim is based on the developer's analysis of the satellite's performance and capabilities.



Source: [The Business Insider](#)

Starlink's 100,000 users to begin receiving broadband in limited Ukraine

Starlink's 100,000 users to begin receiving broadband in limited Ukraine. The service is expected to provide high-speed internet to users in Ukraine, which is currently facing a severe internet outage. The service is being provided by SpaceX, which has a partnership with the Ukrainian government.



Source: [The Business Insider](#)

THREAT INTELLIGENCE

Southwestern expands global espionage campaign to target aerospace and space sectors

Southwestern, an intelligence firm based in Taiwan, has been actively expanding its global espionage campaign, targeting the aerospace and space sectors. The firm has been identified as a key player in a series of cyberattacks against major aerospace and space companies, including Lockheed Martin, Boeing, and SpaceX. The attacks have resulted in the theft of sensitive information, including design plans, source code, and other proprietary data. Southwestern's activities have been linked to the Chinese government, which has been accused of supporting the firm's operations. The firm's activities have raised concerns about the security of aerospace and space systems, and the potential for espionage to compromise national security.

Source: [Southwestern](#)



Heightened techniques to mitigate the effect of GPS jamming and spoofing

According to the U.S. Department of Defense, GPS spoofing and jamming have become a significant threat to the U.S. military and its allies. The department has announced a series of new techniques to mitigate the effect of GPS jamming and spoofing, including the use of anti-jamming and anti-spoofing technologies. The department has also announced a series of new policies to protect the U.S. military and its allies from GPS spoofing and jamming. The department has also announced a series of new programs to train military personnel in the use of anti-jamming and anti-spoofing technologies.

Source: [DoD News](#)



Cybersecurity and domestic operations are being compromised within the realm of China: Cybersecurity in the space domain a brief critical overview of the risks

The article analyzes the use of space-based cyber warfare and the risks it poses to the U.S. military and its allies. The article highlights the use of space-based cyber warfare to target the U.S. military and its allies, and the potential for espionage to compromise national security. The article also discusses the use of space-based cyber warfare to target the U.S. economy and its allies, and the potential for espionage to compromise national security. The article concludes that the use of space-based cyber warfare is a significant threat to the U.S. military and its allies, and that the U.S. must take steps to protect itself from this threat.

Source: [U.S. Space Force](#)

Military report says China's escalating cyber tactics, worse of typhoon cyber threats to U.S. critical infrastructure

A new report from the U.S. House of Representatives says that China's escalating cyber tactics pose a significant threat to the U.S. military and its allies. The report says that China has been using a variety of cyber tactics to target the U.S. military and its allies, including the use of spyware, malware, and other cyber weapons. The report also says that China has been using cyber tactics to target the U.S. economy and its allies, and that this poses a significant threat to the U.S. economy and its allies. The report concludes that the U.S. must take steps to protect itself from China's escalating cyber tactics.

Source: [House Report](#)



TRAINING & EDUCATION

U.S. to launch Space Cybersecurity Foundation 2025

The U.S. House of Representatives has announced the launch of the Space Cybersecurity Foundation 2025. The foundation is a non-profit organization that will focus on promoting space cybersecurity research, education, and training. The foundation will also focus on promoting space cybersecurity policy and advocacy. The foundation will be led by a board of directors, and will have a staff of professionals. The foundation will also have a number of advisory committees. The foundation will be a key player in the space cybersecurity community.

Source: [House News Service](#)



Cybersecurity in outer space a growing concern

In the context of increasing risks from space-based cyber warfare, the U.S. House of Representatives has announced a series of new programs to train military personnel in the use of anti-jamming and anti-spoofing technologies. The programs will focus on the use of anti-jamming and anti-spoofing technologies to protect the U.S. military and its allies from GPS spoofing and jamming. The programs will also focus on the use of anti-jamming and anti-spoofing technologies to protect the U.S. economy and its allies from GPS spoofing and jamming. The programs will be a key part of the U.S. military's efforts to protect itself from space-based cyber warfare.

Source: [House Report](#)



Model for robust cybersecurity capabilities described using intelligent learning

The U.S. House of Representatives has announced a series of new programs to train military personnel in the use of anti-jamming and anti-spoofing technologies. The programs will focus on the use of anti-jamming and anti-spoofing technologies to protect the U.S. military and its allies from GPS spoofing and jamming. The programs will also focus on the use of anti-jamming and anti-spoofing technologies to protect the U.S. economy and its allies from GPS spoofing and jamming. The programs will be a key part of the U.S. military's efforts to protect itself from space-based cyber warfare.

Source: [House Report](#)



Is space the final frontier of espionage?

The U.S. House of Representatives has announced a series of new programs to train military personnel in the use of anti-jamming and anti-spoofing technologies. The programs will focus on the use of anti-jamming and anti-spoofing technologies to protect the U.S. military and its allies from GPS spoofing and jamming. The programs will also focus on the use of anti-jamming and anti-spoofing technologies to protect the U.S. economy and its allies from GPS spoofing and jamming. The programs will be a key part of the U.S. military's efforts to protect itself from space-based cyber warfare.

Source: [House Report](#)



TRAINING & EDUCATION

ESA opens applications for the 19th edition of the Leadership Skills in Spacecraft Communications Training Course

The European Space Agency is looking for 20 motivated engineering students to take part in the 19th edition of the Leadership Skills in Spacecraft Communications Training Course. The course, co-organised with the European Space Agency and the European Space Agency, will be held from 19 to 21 October 2025 at the Training and Learning Facility, located within the European Space Agency and Education Centre (ESA-ETC) in ESRP, Belgium. [Read More](#)



ESA opens applications for the 19th and 20th editions of the Leadership Skills in Spacecraft Communications Training Course

The European Space Agency is looking for 20 motivated engineering students to take part in the 19th and 20th editions of the Leadership Skills in Spacecraft Communications Training Course. The course, co-organised with the European Space Agency and the European Space Agency, will be held from 19 to 21 October 2025 at the Training and Learning Facility, located within the European Space Agency and Education Centre (ESA-ETC) in ESRP, Belgium. [Read More](#)



ESA opens applications for the 19th and 20th editions of the Leadership Skills in Spacecraft Communications Training Course

The European Space Agency is looking for 20 motivated engineering students to take part in the 19th and 20th editions of the Leadership Skills in Spacecraft Communications Training Course. The course, co-organised with the European Space Agency and the European Space Agency, will be held from 19 to 21 October 2025 at the Training and Learning Facility, located within the European Space Agency and Education Centre (ESA-ETC) in ESRP, Belgium. [Read More](#)



ESA opens applications for the 19th and 20th editions of the Leadership Skills in Spacecraft Communications Training Course

The European Space Agency is looking for 20 motivated engineering students to take part in the 19th and 20th editions of the Leadership Skills in Spacecraft Communications Training Course. The course, co-organised with the European Space Agency and the European Space Agency, will be held from 19 to 21 October 2025 at the Training and Learning Facility, located within the European Space Agency and Education Centre (ESA-ETC) in ESRP, Belgium. [Read More](#)



ESA opens applications for the 19th and 20th editions of the Leadership Skills in Spacecraft Communications Training Course

The European Space Agency is looking for 20 motivated engineering students to take part in the 19th and 20th editions of the Leadership Skills in Spacecraft Communications Training Course. The course, co-organised with the European Space Agency and the European Space Agency, will be held from 19 to 21 October 2025 at the Training and Learning Facility, located within the European Space Agency and Education Centre (ESA-ETC) in ESRP, Belgium. [Read More](#)



3473: CybExer technologies on building the world's first space cyber range

What does cybersecurity look like beyond Earth's atmosphere? That's the question at the heart of this conversation with Kristiina Omri, Vice President of Special Programs at CybExer Technologies, and Aare Reintam, the company's COO. Recorded in Tallinn, on the eve of the Software Defined Space Conference, the conversation explores how Estonia, in collaboration with the European Space Agency, is helping shape the future of space cybersecurity through the creation of the world's first Space Cyber Range. [#Estonia #Podcast](#)



Source: [Tech Talks Networks](#)

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