

# SPACE CYBERSECURITY WEEKLY WATCH

Week 29  
July 15 - 21, 2025

Timeframe: Weekly  
# of articles identified: 32  
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**

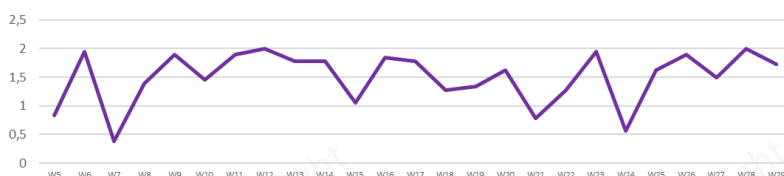
## RISC Score Assessment



## Overview & Resilience Index for Space Cybersecurity (RISC)



## RISC Score evolution in 2025



↓ The RISC score for this watch is 1.73, a decrease from last week. This difference is due to a tense geopolitical landscape and increased threats.

This week, the European Council decided to impose restrictive measures on Russia following the GNSS signal disruptions in several European countries that have been linked to electronic warfare activities from Kaliningrad, including jamming and spoofing of GNSS signals. In response, European commercial satellites that Russia believes are aiding Ukraine are now a legitimate target for signal jamming for Russia. Russia's Digital Development and Communications Ministry informed the International Telecommunication Union (ITU) and Radio Regulations Board (RRB) that Moscow will target commercial and broadcast satellites that support Ukraine's military. On the regulatory front, the "space operator" notion designed by the EU Space Act continued to be analyzed and explained to respond to interrogations. On the market front, France's Direction Générale de l'Armement (DGA) announced that it had ordered cyber simulators from Airbus Defence & Space and French cybersecurity specialist Neverhack. The two service providers will develop, build, and maintain several dedicated platforms and provide training and education services. On the technology front, L3Harris recently demonstrated a cutting-edge PNT solution for the USSF Space Systems Command that is adaptable to different platforms, is fully reprogrammable on-orbit, and is scalable to support additional signals and increased power to address evolving threats. Lastly, from June 30 to July 4, the second edition of the Space Cybersecurity Training Course brought together 30 brilliant bachelor's and master's students from 18 countries at ESA's ESEC-Galaxia Training and Learning Facility in Belgium.





In response to the call from 113 countries earlier in the month, the European Council decided to impose restrictive measures. GNSS signal disruptions in several European countries have been linked to electronic warfare activities from Kaliningrad, including jamming and spoofing of GNSS signals. These activities primarily affected the Baltic States and disrupted civil aviation. **#EU #Sanctions**



**Indulged to launch negotiations on security, defence partnership with EU**



**US and Vietnam conduct advanced cybersecurity training to strengthen resilience of critical infrastructure**



China's ministry of state security urges crackdown on sports espionage



## REGULATION

From conformity to resilience: A practical guide to ISO 27001, ISO 9001, and ISO 14001 compliance for small operations



Across 118 articles and 10 annexes, the draft Act addresses authorization and registration for space activities, governance by Member States, technical rules, and more. As explored below, the scope of the draft Act is less than certain. However, the generally proposed process for authorization of space operators may be identified. **#EUSpaceAct #Operator**



**Link:** <https://www.gtlaw.com/en/insights/2025/7/the-eu-space-act-scope-and-european-space-operator-authorization>



## MARKET & COMPETITION



### France : le ministère des Armées commande des simulateurs cyber à Airbus et Neverhack (Trad: France: Ministry of Armed Forces orders cyber simulators from Airbus and Neverhack)

On July 10, 2025, France's Direction Générale de l'Armement (DGA) announced that it had ordered cyber simulators from Airbus Defence & Space and French cybersecurity specialist Neverhack. Until 2033, the two service providers will develop, build and maintain several dedicated platforms, as well as providing training and education services. The contract is worth up to €250m. #DGA #ADS

**Link:** <https://incyber.org/article/france-ministere-armees-commande-simulateurs-cyber-airbus-neverhack/>





## THREAT INTELLIGENCE

### U.S. and U.K. agencies have not coordinated in penetrating critical infrastructure

U.S. and U.K. agencies have not coordinated in penetrating critical infrastructure, according to a report by the U.S. House of Representatives. The report states that the U.S. and U.K. have not coordinated in penetrating critical infrastructure, which is a major concern for the U.S. House of Representatives.

**Link:** [https://www.washingtonpost.com/news/energy-environment/wp/2025/07/15/u-s-and-u-k-agencies-have-not-coordinated-in-penetrating-critical-infrastructure/](#)



### European agencies have been leading group to break up

European agencies have been leading group to break up, according to a report by the U.S. House of Representatives. The report states that the U.S. and U.K. have not coordinated in penetrating critical infrastructure, which is a major concern for the U.S. House of Representatives.

**Link:** [https://www.washingtonpost.com/news/energy-environment/wp/2025/07/15/u-s-and-u-k-agencies-have-not-coordinated-in-penetrating-critical-infrastructure/](#)



### Russia says European satellites aiding Ukraine are legitimate targets for signal jamming

European commercial satellites that Russia believes are aiding Ukraine are a legitimate target for signal jamming, Russia has told international regulators. Russia's Digital Development and Communications Ministry informed the International Telecommunication Union (ITU) and Radio Regulations Board (RRB) that Moscow will target commercial and broadcast satellites it believes aid Ukraine's military. **#Russia #Jamming**

**Link:** <https://kyivindependent.com/russia-says-european-satellites-aiding-ukraine-are-legitimate-targets-for-signal-jamming/>



### A commercial is reported to have for Media Broadcast Satellite (MBS)

The commercial MBS is reported to have launched a commercial effort in the United States. The MBS is a commercial effort in the United States, which is a major concern for the U.S. House of Representatives.

**Link:** [https://www.washingtonpost.com/news/energy-environment/wp/2025/07/15/u-s-and-u-k-agencies-have-not-coordinated-in-penetrating-critical-infrastructure/](#)



### Spending to space - 2025 gains new momentum in U.S. space budget global missile action

The U.S. House of Representatives has passed a bill to increase spending on space. The bill is a major concern for the U.S. House of Representatives, which is a major concern for the U.S. House of Representatives.

**Link:** [https://www.washingtonpost.com/news/energy-environment/wp/2025/07/15/u-s-and-u-k-agencies-have-not-coordinated-in-penetrating-critical-infrastructure/](#)



### U.S. and U.K. agencies have not coordinated in penetrating critical infrastructure

U.S. and U.K. agencies have not coordinated in penetrating critical infrastructure, according to a report by the U.S. House of Representatives. The report states that the U.S. and U.K. have not coordinated in penetrating critical infrastructure, which is a major concern for the U.S. House of Representatives.

**Link:** [https://www.washingtonpost.com/news/energy-environment/wp/2025/07/15/u-s-and-u-k-agencies-have-not-coordinated-in-penetrating-critical-infrastructure/](#)



## TECHNOLOGY

### U.S. and U.K. agencies have not coordinated in penetrating critical infrastructure

U.S. and U.K. agencies have not coordinated in penetrating critical infrastructure, according to a report by the U.S. House of Representatives. The report states that the U.S. and U.K. have not coordinated in penetrating critical infrastructure, which is a major concern for the U.S. House of Representatives.

**Link:** [https://www.washingtonpost.com/news/energy-environment/wp/2025/07/15/u-s-and-u-k-agencies-have-not-coordinated-in-penetrating-critical-infrastructure/](#)



### L3Harris has the future of PNT ready now

L3Harris recently demonstrated a cutting-edge Positioning, Navigation, and Timing (PNT) solution for the US Space Force's (USSF) Space Systems Command that is adaptable to different platforms, is fully reprogrammable on-orbit, and is scalable to support additional signals and increased power to address evolving threats. **#PNT #USSF**

**Link:** <https://news.satnews.com/2025/07/17/l3harris-has-the-future-of-pnt-ready-now/>



### Space Telecommunications Inc. launches worldwide-based proof of location system to enable tracking

Space Telecommunications Inc. has launched a worldwide-based proof of location system to enable tracking. The system is a major concern for the U.S. House of Representatives, which is a major concern for the U.S. House of Representatives.

**Link:** [https://www.washingtonpost.com/news/energy-environment/wp/2025/07/15/u-s-and-u-k-agencies-have-not-coordinated-in-penetrating-critical-infrastructure/](#)



## TECHNOLOGY

### Enhancing 5G/6G security resilience for 5G security

The integration of 5G and 6G networks is transforming the capabilities of mobile networks and applications, with multiple sectors, such as manufacturing, healthcare, and transportation, relying on 5G/6G networks with varying degrees of criticality. The growing dependence on 5G/6G is, however, accompanied by a corresponding increase in the risk associated with the use of the network infrastructure. The article reviews the growth in security and privacy risks in 5G/6G infrastructure and assesses the efforts of the industry to develop protected and secured 5G/6G networks.

**Keywords:** 5G/6G security

**Link:** [https://www.cyberinflight.com/5g-6g-security-resilience-for-5g-security](#)

## TRAINING & EDUCATION

### CyberInflight to enter space to address security and cyber risks in shaping legal norms

The article reviews the challenges of space being increasingly vulnerable to cyberattacks, various policy legal measures, such as the UN Outer Space Treaty, the UN Space Security Treaty, and a draft Space Security Bill and discusses the space industry, national governments, and non-governmental organizations' efforts to address space security.

**Keywords:** Space security

**Link:** [https://www.cyberinflight.com/cyberinflight-to-enter-space-to-address-security-and-cyber-risks-in-shaping-legal-norms](#)

Space cybersecurity involves building frameworks, including information, and communication, and cyber threat space infrastructure, including satellite and ground-based systems, to detect, prevent, and respond to cyber threats. The article reviews a framework for characterizing the types of space cybersecurity threats. The framework includes 7 categories for characterizing the space assets, threat assets, and threats that a system of space assets. **Keywords:** Space security

**Link:** [https://www.cyberinflight.com/space-cybersecurity-framework](#)

### 5G/6G space security protocol

The article reviews the challenges of space being increasingly vulnerable to cyberattacks, various policy legal measures, such as the UN Outer Space Treaty, the UN Space Security Treaty, and a draft Space Security Bill and discusses the space industry, national governments, and non-governmental organizations' efforts to address space security.

**Link:** [https://www.cyberinflight.com/5g-6g-space-security-protocol](#)

### ★ Discover the ESA academy space cybersecurity training course

From 30 June to 4 July, the second edition of the Space Cybersecurity Training Course brought together 30 brilliant bachelor's and master's students from 18 countries at ESA's ESEC-Galaxia Training and Learning Facility in Belgium.

**#ESAAcademy #TrainingCourse**

**Link:** [https://www.linkedin.com/posts/esaeduacademy\\_esacademy-activity-7350457327960965120-Gi0Q?utm\\_source=share&utm\\_medium=member\\_desktop&rcm=ACoAAC6ww1MBDUN4xAUPfCv581dgYy1A-7vIm60](https://www.linkedin.com/posts/esaeduacademy_esacademy-activity-7350457327960965120-Gi0Q?utm_source=share&utm_medium=member_desktop&rcm=ACoAAC6ww1MBDUN4xAUPfCv581dgYy1A-7vIm60)

An analysis of the 5G/6G security building blocks at 5G/6G with the 5G/6G security framework and the 5G/6G security framework.

The article is part of a series of articles on the subject of the 5G/6G security building blocks at 5G/6G with the 5G/6G security framework and the 5G/6G security framework.

**Link:** [https://www.cyberinflight.com/5g-6g-security-building-blocks-at-5g-6g-with-the-5g-6g-security-framework-and-the-5g-6g-security-framework](#)

CyberInflight provides an online cybersecurity course for the space industry, covering the challenges of space being increasingly vulnerable to cyberattacks, various policy legal measures, such as the UN Outer Space Treaty, the UN Space Security Treaty, and a draft Space Security Bill and discusses the space industry, national governments, and non-governmental organizations' efforts to address space security.

The article reviews the challenges of space being increasingly vulnerable to cyberattacks, various policy legal measures, such as the UN Outer Space Treaty, the UN Space Security Treaty, and a draft Space Security Bill and discusses the space industry, national governments, and non-governmental organizations' efforts to address space security.

**Link:** [https://www.cyberinflight.com/cyberinflight-provides-an-online-cybersecurity-course-for-the-space-industry](#)






# TRAINING & EDUCATION

University of Surrey launches Space Institute to drive the UK's space security issues and tackle significant global challenges

The Institute will focus on the development of the space sector's resilience, which includes the ability to identify, detect, understand, and respond to cyber threats. It will also work to build the highly skilled workforce needed to support the UK's space sector and to ensure the UK's space sector is resilient to cyber threats.

For more information, visit [www.surrey.ac.uk/space-institute](#)



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)