

# SPACE CYBERSECURITY WEEKLY WATCH

Week 24

June 10 - 16, 2025

Timeframe: Weekly

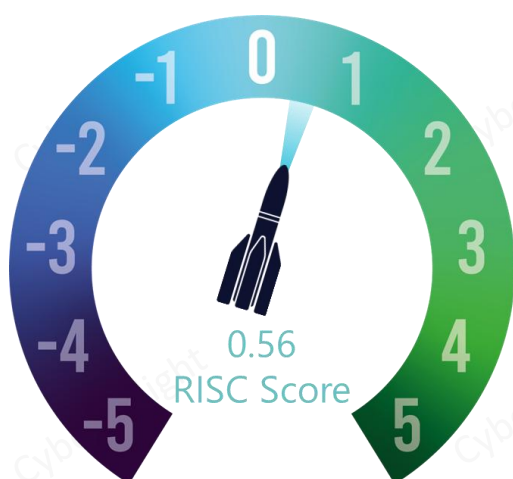
# of articles identified: 33

Est. time to read: 70 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**

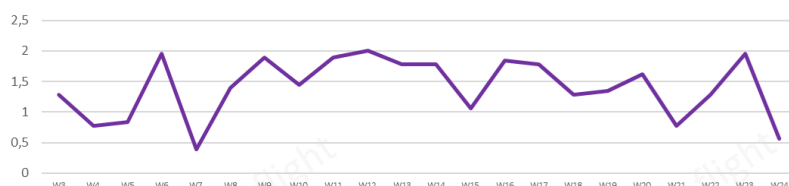
## RISC Score Assessment



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



## RISC Score evolution in 2025



The RISC score for this watch is 0.56, a significant decrease from last week. This difference is due to many threats and negative geopolitics news.

Last week, CyberInflight participated in the annual EU Space ISAC plenary meeting in Madrid. It marked a key moment for advancing cooperation and information-sharing across the space community. This week, geopolitics news includes a call by thirteen European Union member states to the European Commission to respond to interference with GNSS in EU countries. The interference originates in Russia and Belarus and is a result of the ongoing war with Ukraine. Since 2022, jamming and spoofing have been observed in the airspace of the Baltic Sea Region, posing a threat to various modes of transport. Regarding regulation, sustaining select efforts to change the nation's cybersecurity by amending Executive Order 13694 and Executive Order 14144 has been made. President Trump updated some of the major touchstones of Biden's cyber policy legacy written at the beginning of January 2025, while keeping a few others. On the technological front, Kymeta cracks the code for dual-band satellite connectivity. On the market side, the Paris Air Show has started, and some objectives have already been discussed, such as meeting the challenges of technological warfare with European entrepreneurs. Regarding threats, despite no "smoking gun", the most critical threat is the loss of an Airbus satellite sold to Azerbaijan due to an unknown reason. It's important to note that news about satellites suffering cyberattacks is very rare. Lastly, a paper aims to analyze the responsible entities for space cybersecurity governance in the UK, the USA, Germany, and the European Union, and compare existing policies and guidelines against current threats.



## CYBERINFLIGHT'S NEWS



### CyberInflight participated in the annual EU Space ISAC plenary meeting in Madrid

The annual EU Space ISAC plenary meeting was hosted in Madrid. The plenary, co-chaired by the European Commission's Directorate-General for Defense Industry and Space (EU DEFIS) and the EUSPA - EU Agency for the Space Program, marks a key moment for advancing cooperation and information-sharing across the space community.

#SpaceISAC #BoardMeeting

**Link:** <https://www.linkedin.com/feed/update/urn:li:activity:7338867234926219265/?actorCompanyId=30108787>



## GEOPOLITICS



### 13 EU member states demand action on GNSS interference

Thirteen member states of the European Union have called on the European Commission to respond to interference with GNSS in EU countries. The interference originates in Russia and Belarus, as a result of the ongoing war with Ukraine.

#GNSS #Interferences

**Link:** <https://www.gpsworld.com/13-eu-member-states-demand-action-on-gnss-interference/>



## REGULATION



### Sustaining select efforts to strengthen the nation's cybersecurity and amending executive order 13694 and Executive Order 14144

President Trump took a red pen to much of the Biden administration's cyber legacy in a little-noticed move on Friday, June 6. Under an executive order signed, Trump updated some of the major touchstones of Biden's cyber policy legacy written at the beginning of January 2025-- while keeping a few others. #Trump #Cyber

**Link:** <https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/>





## TECHNOLOGY

### ★ Kymeta cracks the code for dual-band satellite connectivity

A new satellite antenna from US-based Kymeta can connect to Ku- and Ka-band networks at the same time, highlighting a technical first that could reshape how military platforms stay connected in the field. **#Connectivity #Band**

**Link:** <https://nextgendefense.com/kymeta-dual-band-satellite/>



## MARKET & COMPETITION

### Space Force's new satellite antenna

Space Force's new satellite antenna is designed to connect to multiple satellite networks at the same time, highlighting a technical first that could reshape how military platforms stay connected in the field. **#Connectivity #Band**

**Link:** <https://nextgendefense.com/kymeta-dual-band-satellite/>



### US Space Force's new satellite antenna

Space Force's new satellite antenna is designed to connect to multiple satellite networks at the same time, highlighting a technical first that could reshape how military platforms stay connected in the field. **#Connectivity #Band**

**Link:** <https://nextgendefense.com/kymeta-dual-band-satellite/>



### Space Force's new satellite antenna

Space Force's new satellite antenna is designed to connect to multiple satellite networks at the same time, highlighting a technical first that could reshape how military platforms stay connected in the field. **#Connectivity #Band**

**Link:** <https://nextgendefense.com/kymeta-dual-band-satellite/>



### Space Force's new satellite antenna

Space Force's new satellite antenna is designed to connect to multiple satellite networks at the same time, highlighting a technical first that could reshape how military platforms stay connected in the field. **#Connectivity #Band**

**Link:** <https://nextgendefense.com/kymeta-dual-band-satellite/>



### Space Force's new satellite antenna

Space Force's new satellite antenna is designed to connect to multiple satellite networks at the same time, highlighting a technical first that could reshape how military platforms stay connected in the field. **#Connectivity #Band**

**Link:** <https://nextgendefense.com/kymeta-dual-band-satellite/>



### ★ Salon du Bourget : répondre aux défis de la guerre technologique avec les entrepreneurs européens (Trad: Paris Air Show: meeting the challenges of technological warfare with European entrepreneurs)

Europe is at a strategic turning point, where security is no longer limited to land borders, but extends into orbit. Faced with hybrid threats and accelerating global technological competition, the European Union must reinforce its industrial autonomy and support entrepreneurial innovation to defend its sovereignty. **#PAS25 #Security**

**Link:** <https://www.maddyness.com/2025/06/16/salon-du-bourget-repondre-aux-defis-de-la-guerre-technologique-avec-les-entrepreneurs-europeens/>



### Salon du Bourget : répondre aux défis de la guerre technologique avec les entrepreneurs européens (Trad: Paris Air Show: meeting the challenges of technological warfare with European entrepreneurs)

Europe is at a strategic turning point, where security is no longer limited to land borders, but extends into orbit. Faced with hybrid threats and accelerating global technological competition, the European Union must reinforce its industrial autonomy and support entrepreneurial innovation to defend its sovereignty. **#PAS25 #Security**

**Link:** <https://www.maddyness.com/2025/06/16/salon-du-bourget-repondre-aux-defis-de-la-guerre-technologique-avec-les-entrepreneurs-europeens/>



### US Space Force's new satellite antenna

Space Force's new satellite antenna is designed to connect to multiple satellite networks at the same time, highlighting a technical first that could reshape how military platforms stay connected in the field. **#Connectivity #Band**

**Link:** <https://nextgendefense.com/kymeta-dual-band-satellite/>





These terms are defined as follows: **cybercrime** is a crime involving the use of computers or networks to commit a crime; **cyberstalking** is a crime involving the use of computers or networks to stalk a person; **cybersex** is a crime involving the use of computers or networks to engage in sexual activity; **cyberterrorism** is a crime involving the use of computers or networks to threaten or harm a person or a group of people; **cyberwar** is a crime involving the use of computers or networks to attack a country or a group of countries.



## THREAT INTELLIGENCE

bioRxiv preprint doi: <https://doi.org/10.1101/2019.05.20.256400>; this version posted May 20, 2019. 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.

Source: reported in a 1998 survey of students, staff, parents, or governing body (with consent) in the past year – with increase from the 1998/99 academic year (see <http://www.dh.gov.uk>)



The secret antenna, Airbus and China 2/2 - Just weeks after France detected a Chinese intelligence operation near its critical space sites, an Airbus satellite suddenly stopped working. **#Airbus #Satellite**

**Link:** <https://www.intelligenceonline.com/surveillance--interception/2025/06/12/the-mysterious-loss-of-an-airbus-satellite-sold-to-azerbaijan.110464569-eve>



© CyberIntel

**Source:** <http://china.ustrade.state.gov/docs/default-source/press-releases/2014/04/20140423china.pdf>



The final step before the model is fitted is to standardize the predictors. This is done by subtracting the mean of each predictor from its values and then dividing by the standard deviation of the predictor. This is done for each predictor in the model. The reason for this is that the model coefficients are interpreted in terms of standard deviations. If the predictors are not standardized, the coefficients will be in different units and it will be difficult to compare them. By standardizing the predictors, the coefficients will be in the same units and it will be easier to compare them. The standardization is done using the `scale()` function in R. The `scale()` function takes a matrix of predictors and returns a matrix of standardized predictors. The `scale()` function also returns the mean and standard deviation of each predictor. The mean and standard deviation of each predictor are stored in the `attr` attribute of the matrix. The `scale()` function is used to standardize the predictors in the model. The standardized predictors are then used to fit the model. The model coefficients are interpreted in terms of standard deviations. The `scale()` function is used to standardize the predictors in the model. The standardized predictors are then used to fit the model. The model coefficients are interpreted in terms of standard deviations.



For more information on other subscription-based tools to make 2016's small-business owner's goals, log onto [www.entrepreneur.com](http://www.entrepreneur.com). **#SmallBiz2016 #Entrepreneur**



Not for sale. This journal is the central point for the management, distribution of updates in networks with our software and our systems. **© 2000 IBM**



## TRAINING & EDUCATION

© 2006 The Authors  
Journal compilation © 2006 Blackwell Publishing Ltd





## TRAINING & EDUCATION

**US Space Conference 2025** will be a two-day event for experts, solutions, and opportunities in space. The conference will be held on 10-11 July 2025 at the Sheraton Hotel, bringing together global space leaders, policymakers, researchers, and innovators to explore the future space for security. [#USSpaceConf2025](#)



**Link:** [https://www.uscspacemission.com/conference/2025-to-lead-a-revolution-space-for-peace-security-and-innovative](#)

**Is space electromagnetic warfare considered cyber warfare?** Cyberwarfare in space  
The paper explores the technology, capabilities, and impact of electromagnetic warfare and cyber warfare in space. It discusses the role of space in cyberwarfare, the challenges of cyberwarfare in space, and the need for a new model of cyberwarfare in space. [#CyberWarfareInSpace](#)

**Link:** [https://www.uscspacemission.com/conference/2025-to-lead-a-revolution-space-for-peace-security-and-innovative](#)

**Executive Interview: Space system designs, RF signal abuse, NATO in space**  
High-capability radio frequency (RF) components are in demand for various military space systems, as is the use of commercial infrastructure to host both civil and military space systems. How does NATO use NATO for space and high-frequency components of finding threats? [#NATOinSpace](#)



**Link:** [https://www.uscspacemission.com/conference/2025-to-lead-a-revolution-space-for-peace-security-and-innovative](#)

**Space management for cyberwarfare mitigation in NATO NATO satellite networks with processing**  
In this paper, space management and processing design are investigated in NATO NATO satellite networks to mitigate cyberwarfare threats and improve satellite services in NATO NATO satellite systems. [#NATOinSpace](#)



**Link:** [https://www.uscspacemission.com/conference/2025-to-lead-a-revolution-space-for-peace-security-and-innovative](#)

**OSINT 2025: Cyber resilience framework for space communication systems**  
This paper explores the framework of OSINT 2025, which is a framework for space communication systems. [#OSINT2025](#)



**Link:** [https://www.uscspacemission.com/conference/2025-to-lead-a-revolution-space-for-peace-security-and-innovative](#)

**Formal Faults-based methods: What more operations for and processing satellite communication**

This paper presents a formal method-based approach to satellite communication. It discusses the challenges of satellite communication and the need for a new model of satellite communication. [#FormalFaultsBasedMethods](#)



**Link:** [https://www.uscspacemission.com/conference/2025-to-lead-a-revolution-space-for-peace-security-and-innovative](#)



### Space cybersecurity governance: assessing policies and frameworks in view of the future European space legislation

This paper aims to analyze the responsible entities for space cybersecurity governance in the UK, the USA, Germany, and the European Union and compare existing policies and guidelines against current threats. [#Paper #Regulation](#)



**Link:** <https://academic.oup.com/cybersecurity/article/11/1/tyaf013/8162738?login=false>

**OSINT 2025: Cyber resilience framework for space communication systems**  
This paper explores the framework of OSINT 2025, which is a framework for space communication systems. [#OSINT2025](#)



**Link:** [https://www.uscspacemission.com/conference/2025-to-lead-a-revolution-space-for-peace-security-and-innovative](#)

*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)*