

# SPACE CYBERSECURITY WEEKLY WATCH

Week 35

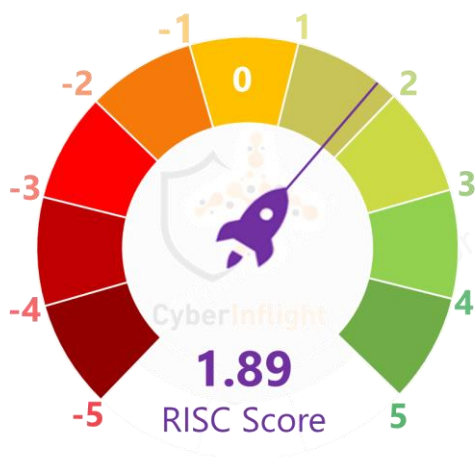
August 27 – September 2, 2024

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

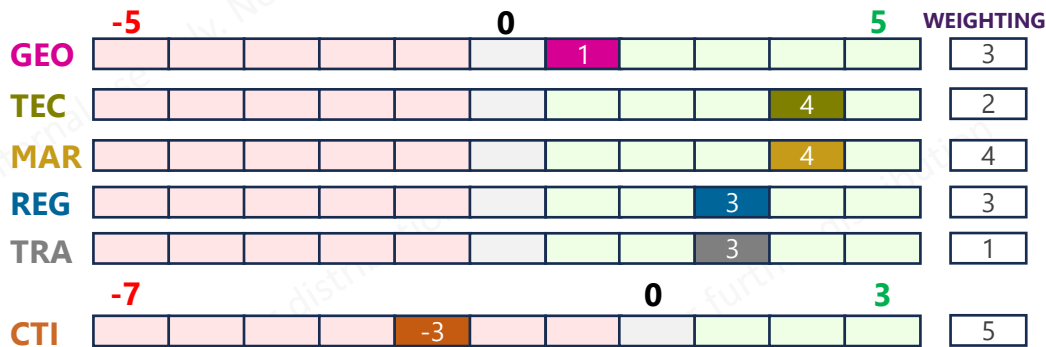
- **GEOPOLITICS**
- **TECHNOLOGY**
- **MARKET INTELLIGENCE**
- **REGULATION**
- **TRAINING & EDUCATION**
- **THREAT INTELLIGENCE**
- ★ **IMPORTANT NEWS**

Timeframe : Weekly  
# of articles identified : 29  
Est. time to read : 30 minutes

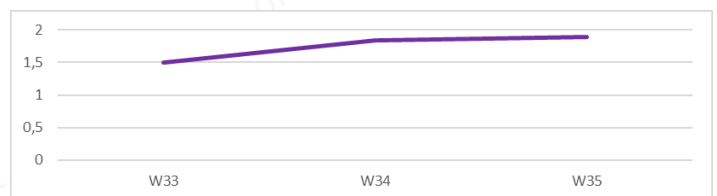
## RISC Score Assessment



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



## RISC Score Evolution



↑ This week's RISC score is 1.89, a slight increase from last week, mainly due to new contracts awarded and recent technological progress.

On the geopolitical front, Monday, September 2, SpaceX's Falcon 9 will launch the third batch of satellites for a reconnaissance satellite constellation built by SpaceX and Northrop Grumman for the National Reconnaissance Office to provide imaging and other reconnaissance capabilities. The satellite's structure follows the NRO's new concept of space architecture by using many smaller satellites to create constellations that will insure resistance from attacks. On the technological side, Thales Alenia Space has revealed the results of their ASCEND feasibility study on the development of space-based data centers. The study explores the potential for deploying data centers in space to enhance data processing and storage capabilities. On the market front, Atheras Analytics has been selected by the UK Ministry of Defence to conduct Ka-band propagation analysis for the proposed Skynet 6 ground station sites. This analysis is vital for ensuring the efficiency and reliability of the UK's next-generation military satellite communications. On the regulatory front, a paper examining the importance of international cooperation in establishing an effective legal framework to address cyber threats against satellites has been published by Hasanuddin University (Indonesia). On the Threat Intel side, a group of Iranian cyber actors acts as access brokers for ransomware gangs and collaborates with affiliates to target the US and its allies, exploiting vulnerabilities across different sectors. The group's focus spans across multiple critical US industries, including defense and space. Lastly, NASA's Independent Verification & Validation (IV&V) program has initiated a cybersecurity educational outreach program aimed at fostering cybersecurity awareness and skills among students. This initiative is part of NASA's efforts to strengthen cybersecurity capabilities in the space industry.



# GEO POLITICS



## SpaceX plans NROL-113 launch of reconnaissance satellites for secret government mission

Monday, September 2, SpaceX's Falcon 9 will launch the third batch of satellites for a reconnaissance satellite constellation built by SpaceX and Northrop Grumman for the National Reconnaissance Office to provide imaging and other reconnaissance capabilities. The satellite's structure follows the NRO's new concept of space architecture by using many smaller satellites to create constellations that will insure resistance from attacks. **#SpaceX #SIGINT**



**Link:** <https://news.satnews.com/2024/08/28/spacex-plans-nrol-113-launch-of-reconnaissance-satellites-for-secret-government-mission/>

## La France a proposé des 'garnisons spatiales'



# TECHNOLOGY

## Space Technologies introduces upgraded satellite models with enhanced capabilities



Space Technologies has unveiled its upgraded satellite models, designed to meet the growing demand for high-resolution imaging and other reconnaissance capabilities. The new models offer enhanced performance, improved capabilities, addressing the growing need of satellite operators to meet diverse and complex mission requirements. **#SpaceTech #Satellite**

**Link:** <https://www.spacetechnologies.com/en/newsroom/2024/08/28/space-technologies-introduces-upgraded-satellite-models-with-enhanced-capabilities>

## Space Force & Northrop Grumman establish joint lab in US for space domain awareness



The US Space Force is collaborating with Northrop Grumman to establish a joint lab in the US to enhance space domain awareness. The lab will focus on the detection and tracking of space objects, contributing to global security and defense. **#SpaceForce #NorthropGrumman**

**Link:** <https://www.spaceforce.mil/Newsroom/2024/08/28/space-force-and-northrop-grumman-establish-joint-lab-in-us-for-space-domain-awareness>

## US leaders urged to prioritize GPS and PNT for national security



US leaders are urged to prioritize GPS and PNT for national security. The report highlights the critical role of these technologies in various sectors, including defense, transportation, and agriculture. **#GPS #PNT #NationalSecurity**

**Link:** <https://www.defense.gov/Newsroom/2024/08/28/us-leaders-urged-to-prioritize-gps-and-pnt-for-national-security>



## Thales Alenia Space completes ASCEND feasibility study on space data centers

Thales Alenia Space has revealed the results of their ASCEND feasibility study on the development of space-based data centers. The study explores the potential for deploying data centers in space to enhance data processing and storage capabilities, catering to the growing demands of the digital age. **#SpaceDataCenters #Thales**



**Link:** <https://spacewatchafrica.com/thales-alenia-space-reveals-results-of-ascend-feasibility-study-on-space-data-centers-3/c>

## Building Space Operations Business Models for Next-Gen Satellites



Building Space Operations Business Models for Next-Gen Satellites. The report discusses the challenges and opportunities in developing sustainable business models for next-generation satellite operations. **#SpaceOperations #BusinessModels**

**Link:** <https://www.spaceoperations.com/en/newsroom/2024/08/28/building-space-operations-business-models-for-next-gen-satellites>

## US University launches quantum secure communications lab



A US university has launched a quantum secure communications lab. The lab will focus on developing and testing quantum communication systems to enhance data security. **#QuantumSecure #Communications**

**Link:** <https://www.quantumsecure.com/en/newsroom/2024/08/28/us-university-launches-quantum-secure-communications-lab>

## Space.com, Space.com: US leaders urge for quantum cryptography research



Space.com, Space.com: US leaders urge for quantum cryptography research. The report emphasizes the importance of investing in quantum cryptography research to secure future communications. **#QuantumCryptography #Research**

**Link:** <https://www.space.com/en/newsroom/2024/08/28/space-com-space-com-us-leaders-urge-for-quantum-cryptography-research>



# MARKET & COMPETITION



## Atheras Analytics chosen by UK MoD for Ka-Band propagation analysis for Skynet 6

Atheras Analytics has been selected by the UK Ministry of Defence to conduct Ka-band propagation analysis for the proposed Skynet 6 ground station sites. This analysis is vital for ensuring the efficiency and reliability of the UK's next-generation military satellite communications. **#UKDefence #SatelliteData**

**Link:** <https://www.satcom.digital/news/atheras-analytics-selected-by-uk-mod-to-provide-ka-band-propagation-analysis-for-proposed-skynet-6-ground-station-sites>





## REGULATION

### Enhancing EU cybersecurity by addressing the risks from the 5G2G standard

The European Union (EU) has taken a significant step towards enhancing its cybersecurity capabilities by addressing the risks from the 5G2G standard. This initiative is part of the EU's broader strategy to strengthen its digital resilience and protect critical infrastructure from cyber threats.

### 5G2G standard: addressing the risks from the 5G2G standard

### A research agenda for cybersecurity law and policy

This research agenda explores the challenges and opportunities in cybersecurity law and policy, focusing on the integration of international law and geopolitical strategy. It highlights the need for a comprehensive approach to address the evolving cyber threat landscape.

### 5G2G standard: addressing the risks from the 5G2G standard

For more information, visit the link below.

### Satellite cybersecurity: integration of international law and geopolitical strategy

This article examines the importance of international cooperation in establishing an effective legal framework to address cyber threats against satellites. In this context, collaboration among nations is essential to develop global cybersecurity standards capable of protecting critical infrastructure from attacks that could disrupt international stability. This study emphasizes that the synergy between international law and geopolitical strategy can create a safer and more resilient environment for satellite operations in the future. **#Cooperation #CriticalInfra**

**Link:** [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4918410](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4918410)



## TRAINING & EDUCATION

### NASA IV&V launches cybersecurity educational outreach program

NASA's Independent Verification & Validation (IV&V) program has initiated a cybersecurity educational outreach program aimed at fostering cybersecurity awareness and skills among students. This initiative is part of NASA's efforts to strengthen cybersecurity capabilities in the space industry. **#CybersecurityEducation #NASATraining**

**Link:** <https://theycyberexpress.com/nasa-ivv-cybersecurity-educational-outreach/>



### 5G2G standard: addressing the risks from the 5G2G standard

The 5G2G standard is a significant milestone in the evolution of mobile networks, offering enhanced performance and capacity. However, it also introduces new cybersecurity challenges, particularly related to the increased attack surface and the potential for data interception and manipulation.

### 5G2G standard: addressing the risks from the 5G2G standard

For more information, visit the link below.

For more information, visit the link below.

### 5G2G standard: addressing the risks from the 5G2G standard

The 5G2G standard is a significant milestone in the evolution of mobile networks, offering enhanced performance and capacity. However, it also introduces new cybersecurity challenges, particularly related to the increased attack surface and the potential for data interception and manipulation.

### 5G2G standard: addressing the risks from the 5G2G standard

For more information, visit the link below.

### 5G2G standard: addressing the risks from the 5G2G standard

The 5G2G standard is a significant milestone in the evolution of mobile networks, offering enhanced performance and capacity. However, it also introduces new cybersecurity challenges, particularly related to the increased attack surface and the potential for data interception and manipulation.

### 5G2G standard: addressing the risks from the 5G2G standard

For more information, visit the link below.

### 5G2G standard: addressing the risks from the 5G2G standard

The 5G2G standard is a significant milestone in the evolution of mobile networks, offering enhanced performance and capacity. However, it also introduces new cybersecurity challenges, particularly related to the increased attack surface and the potential for data interception and manipulation.

### 5G2G standard: addressing the risks from the 5G2G standard

For more information, visit the link below.





# THREAT INTELLIGENCE



## Iranian state hackers act as access brokers for ransomware gangs, target US and allies' critical infrastructure

A shadowy group of Iranian cyber actors is acting as access brokers for ransomware gangs and collaborating with affiliates to target the U.S. and its allies, exploiting vulnerabilities across different sectors. The FBI, CISA, and the Department of Defense Cyber Crime Center (DC3) warned that these actors, believed to be state-sponsored, are focusing aggressively on access brokering and enabling ransomware attacks. The group's focus spans across multiple critical US industries, including education, finance, healthcare, and defense, as well as government entities. **#Iran #CriticalInfra**

**Link:** <https://thecyberexpress.com/iranian-access-brokers-for-ransomware/>



*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)*