JULY 2024

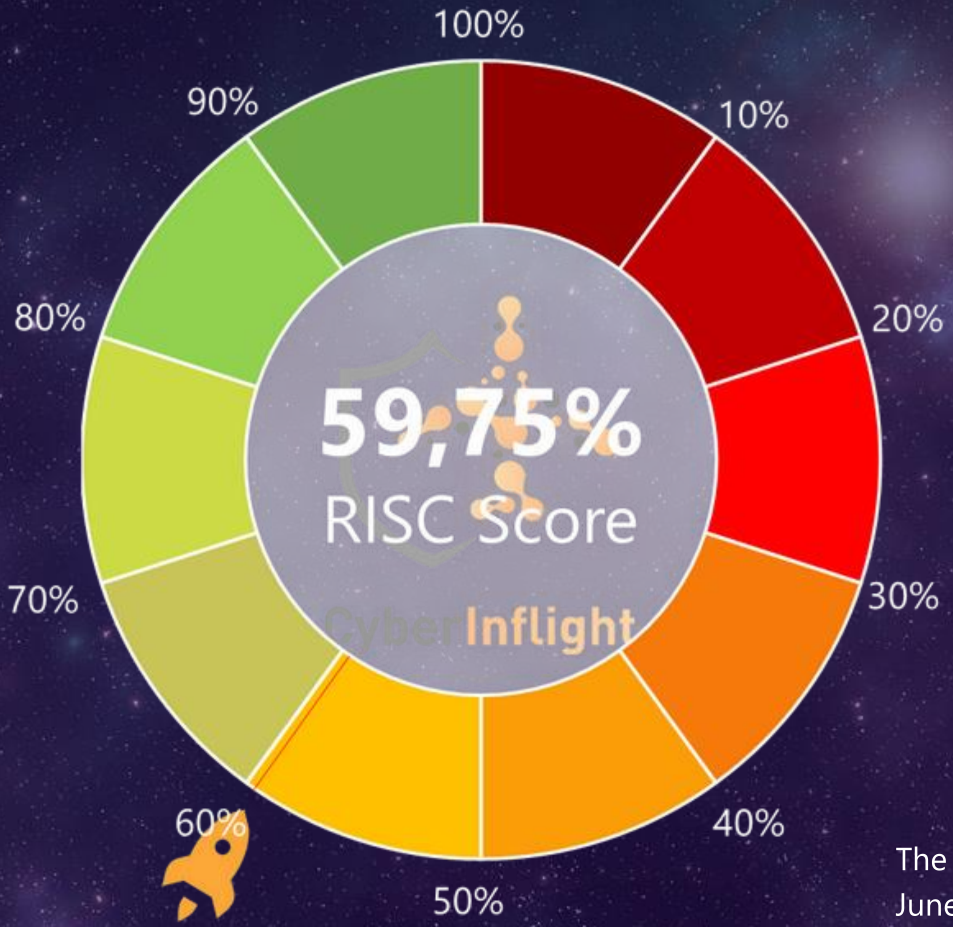
Space Cybersecurity Monthly Watch

Source: European Space Agency - Artist's view of a Galileo satellite

Monthly RISC Score & Highlights
Weekly Observations
Expert Analysis

July 2024 RISC Score

The Resilience Index for Space Cybersecurity (RISC) Score is a unique assessment of the space industry. It is an indicator that provides an overview and score of the space cybersecurity resilience for the week or month. To perform the calculation of the final weighted average, a score out of 10 is assigned to each news category based on the importance of the news identified. A weight is then assigned to each category: Market Intelligence (4), Threat Intelligence (5), Technology (2), Geopolitics (3), Regulation (3), Education & Training (1). We can see that the threat and market intelligence news have a greater impact on the score because CyberInflight has assigned them greater importance to space cybersecurity resilience.



The RISC Score was 56.75% in June, and it increased by 3 percentage points in July.

The rise of this RISC Score is due to several geopolitical and regulatory initiatives, as well as growth in the space cybersecurity market.

Monthly highlights - July 2024

Regarding the **intensification of international geopolitical tensions**, nations foresee growing risk of cyberattacks in the near future. Belligerents are developing both **defensive and offensive capabilities**, offensive capabilities aimed at **targeting space assets**. Such initiatives are in the context of **space warfare**, given that **space assets are now increasingly recognized as critical infrastructure**. Nations are **developing regulations and advanced technologies to bolster their preparedness for space-related threats**.

Nation after nation is becoming aware of the importance of the "secure by design" principle for space assets.

On July 11, a report that provides **recommendations for the USSF** was released on how it should **encourage the commercial sector to adopt robust cybersecurity strategies** that ensure **Space Mission Assurance**. The latter is designed to deter adversaries, mitigate risks from emerging space threats, and develop resilient space architectures.

The **Spacecraft Cybersecurity Act** was introduced on July 10. This legislation mandates **NASA incorporate cybersecurity measures into its acquisition process**, which means integrating essential cybersecurity requirements **from the initial stages of spacecraft manufacturing to their operational phases**.

NATO was planning to develop its first-ever **Commercial Space Strategy** during the 2024 NATO Summit in July. This strategy aims to **enhance space resilience** and accelerate the integration of new technologies from the **commercial space sector** into military operations for their effectiveness. Such an initiative testifies to the importance that NATO places on **space security in Europe**.

This month was also marked by the establishment of **strategic geopolitical alliances to ensure national space cybersecurity**. During the NATO Summit on its 75th anniversary, NATO expressed concerns about the fact that China is indeed becoming more ambitious and aggressive in space. NATO also showed apprehension about **China's deepening space cooperation with Russia**. This fact has prompted **Japan and NATO to strengthen their cooperation** to address new security threats transcending geographical boundaries, such as cyberattacks and conflicts in space. This cooperation also aims to improve **Japan and NATO's satellite resilience**.

On July 5, **Sweden** adopted a **defense and security space strategy to anticipate potential space threats** and to firm up its **posture in space** as a space actor.

In this Monthly Watch, **our expert** is going to develop the concept of **Space as a critical infrastructure**.

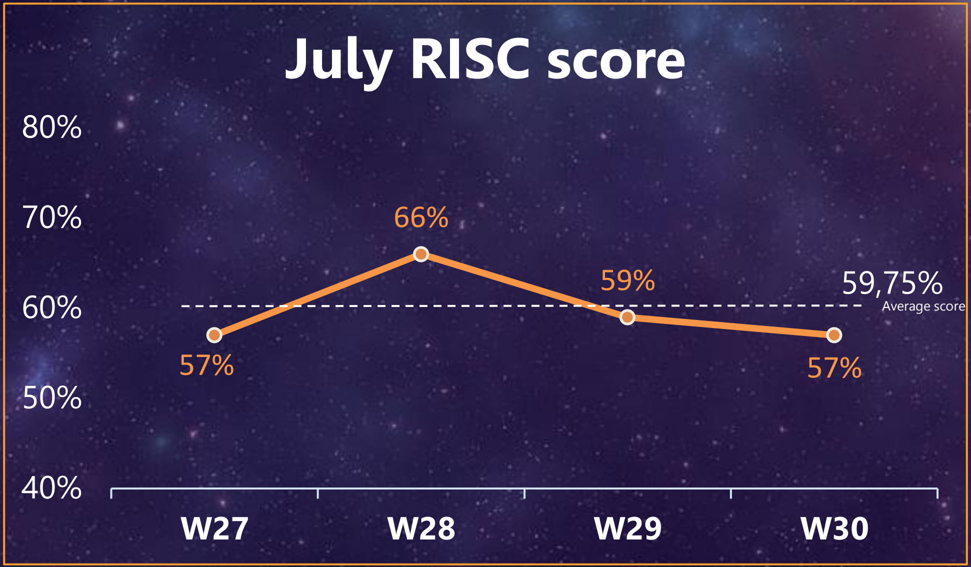
Weekly Observations

W27: 57%

Russian satellite LUCH 2, which is stalking other satellites, was on another move, approaching THOR 7, a Norwegian commercial geosynchronous satellite. This SIGINT satellite is able to map contact networks, geolocate satellite users, perform eavesdropping on data communications, jam, spoof and inspect vulnerabilities of other satellites to shut them down.

W28: 66%

Japan strengthens its cooperation with NATO to address new security threats that transcend geographic boundaries, such as cyberattacks and conflicts in space. This collaboration may involve enhancing the resilience of Japan and NATO's satellites to protect them against jamming and spoofing.



W29: 59%

The US prepares jammer devices to target Russian and Chinese satellites. These new ground-based jammers are designed to disrupt enemy satellites' ability to transmit information about US forces during a conflict, countering satellite communications that could support attacks.

W30: 57%

The Pentagon has released an updated Arctic strategy, warning that Russian's GPS jamming targets the US, Canada, and their allies. The strategy also mentioned that Russia's Arctic capabilities pose a significant threat to the US homeland, as well as to allies and partner territories.

W27: July 2 – 8, 2024
W29: July 16 – 22, 2024

W28: July 9 – 15, 2024
W30: July 23 – 29, 2024

Expert Analysis 1/2

Our societies' reliance on space has grown exponentially in recent years. As our dependence on space-based technologies intensifies, so does the need to protect these vital assets. This has led to an increasing emphasis on developing and enforcing regulations to ensure cybersecurity in space.

Throughout this year, numerous discussions have focused on space regulations, such as the European Union Space Law (EUSL) and the French Loi sur les Opérations Spatiales (LOS). These discussions have revitalized the conversation around designating space as critical infrastructure. Critical infrastructure refers to the systems, facilities, and assets vital for the functioning of society and the economy. **By officially recognizing space as critical infrastructure, governments and international bodies could prioritize the security and resilience of space-based assets**. This includes space systems and infrastructures. While communication satellites are already under protective measures, extending this categorization to all space systems would ensure comprehensive safeguarding against potential threats, including cyberattacks.

Various regional and national regulations and initiatives are emerging in response to the increasing awareness of the need for cyber protection in space. **Europe has taken a significant step forward by designating space as critical infrastructure under the NIS v2 directive**. The directive mandates that European Union member states incorporate these new regulations into their national laws by October 17, 2024. Some countries, such as **Belgium, Croatia, and Hungary, have already complied with this directive.** Regarding national initiatives, governments are recognizing the critical nature of space infrastructure.

> By officially recognizing space as critical infrastructure, governments and international bodies could prioritize the security and resilience of space-based assets.

Expert Analysis 2/2

For instance, **France has categorized space as a critical infrastructure since 2006, while Australia and the UK have made similar designations in 2021 and 2022**. The UK government has further demonstrated its commitment by announcing the introduction of the Cyber Security and Resilience Bill into Parliament this summer. It will adopt the provisions of NIS v2 and implement them into national law, even after the country exits from the European Union.

The **conversation about recognizing space as critical infrastructure is gaining momentum in the United States**, with the government issuing guidance emphasizing the need for a strong cyber defense posture for all space systems. At **the center of these discussions is the bipartisan Space Infrastructure Act**, first introduced in June 2021. This proposed legislation aims to formally recognize space systems as critical infrastructure, ensuring they receive the necessary protection and resources to defend against evolving threats. The National Security Council is evaluating critical infrastructure under Presidential Policy Directive 21 (PPD-21) and considering potential updates, while a joint government-private sector working group led by CISA called "Space Systems Critical Infrastructure Working Group" has also been established. The Space Information Sharing and Analysis Center (ISAC) advocates for space to be designated as critical infrastructure, while the Aerospace Industries Association (AIA) argues that current protections for commercial satellites are insufficient and expresses reservations about such a designation.

The categorization of space as critical infrastructure is open to debate, but it is important to acknowledge that potential belligerents may argue in favor of this designation to protect their activities in space. After careful consideration, it becomes evident that space systems serve as the critical infrastructure of all other essential infrastructures.

Héloïse Do Nascimento Cardoso,
Market Analyst at CyberInflight

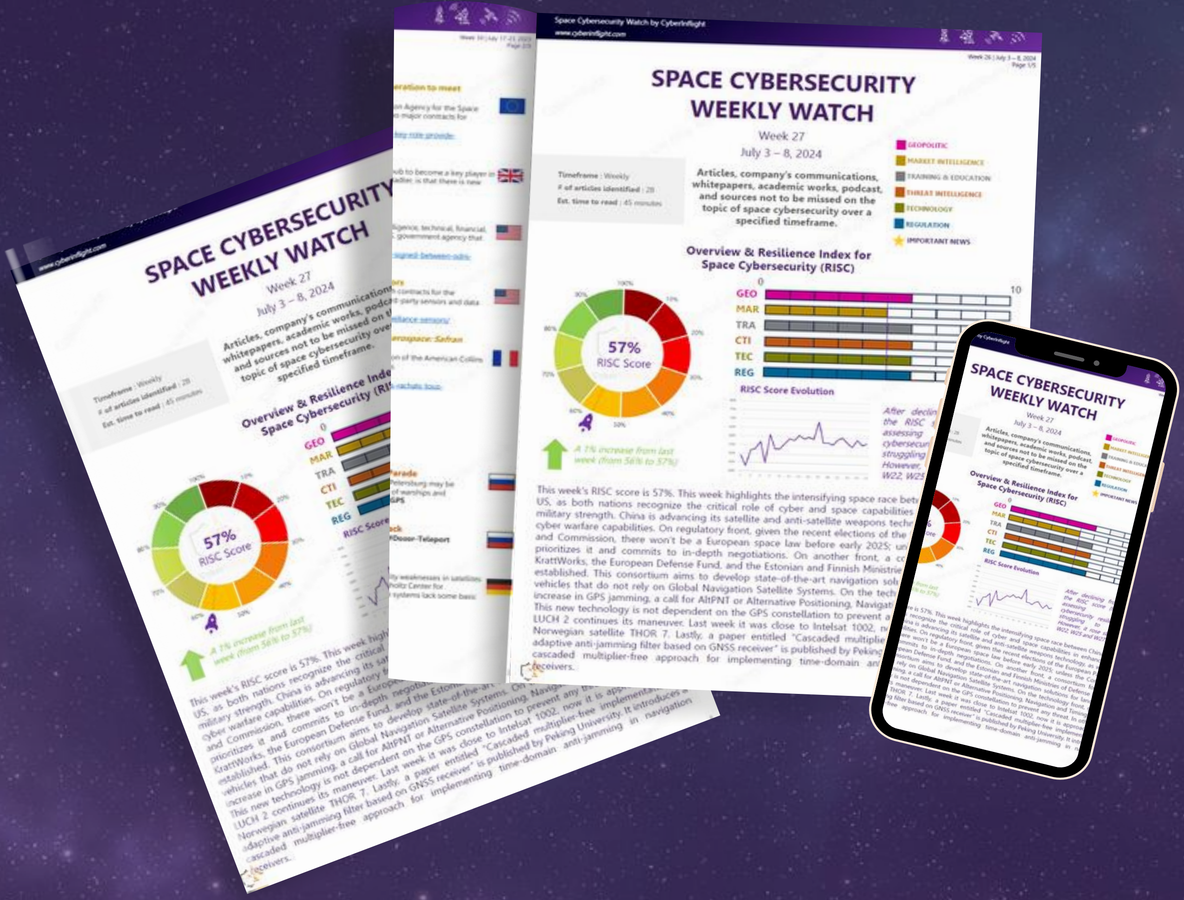
> The categorization of space as critical infrastructure is open to debate, but it is important to acknowledge that potential belligerents may argue in favor of this designation to protect their activities in space.

CyberInflight is an independent company at the heart of the Space Cybersecurity ecosystem. Discover our unique products.

The only Research Report entirely dedicated to the sector

Get our latest Space Cybersecurity Market Intelligence Report, Edition 2024

Stay updated every week with the dedicated watch on Space Cybersecurity!



Space Cybersecurity Watch by CyberInflight
www.cyberinflight.com

Week 26 | July 3 – 8, 2024
Page 1/5

SPACE CYBERSECURITY WEEKLY WATCH

Week 27
July 3 – 8, 2024

Timeframe : Weekly
# of articles identified : 28
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 & Resilience Index for Space Cybersecurity (RISC)

A 1% increase from last week (from 56% to 57%)

After declin
the RISC
assessing
cybersecur
struggling
However,
W22, W25

This week's RISC score is 57%. This week highlights the intensifying space race betw
US, as both nations recognize the critical role of cyber and space capabilities
military strength. China is advancing its satellite and anti-satellite weapons techn
cyber warfare capabilities. On regulatory front, given the recent elections of the
and Commission, there won't be a European space law before early 2025; un
prioritizes it and commits to in-depth negotiations. On another front, a co
KrattWorks, the European Defense Fund, and the Estonian and Finnish Ministrie
established. This consortium aims to develop state-of-the-art navigation solu
vehicles that do not rely on Global Navigation Satellite Systems. On the tech
increase in GPS jamming, a call for AltPNT or Alternative Positioning, Navigat
This new technology is not dependent on the GPS constellation to prevent a
LUCH 2 continues its maneuver. Last week it was close to Intelsat 1002, n
Norwegian satellite THOR 7. Lastly, a paper entitled "Cascaded multiplie
adaptive anti-jamming filter based on GNSS receiver" is published by Peking
cascaded multiplier-free approach for implementing time-domain an
receivers.

Get access to the full version now !

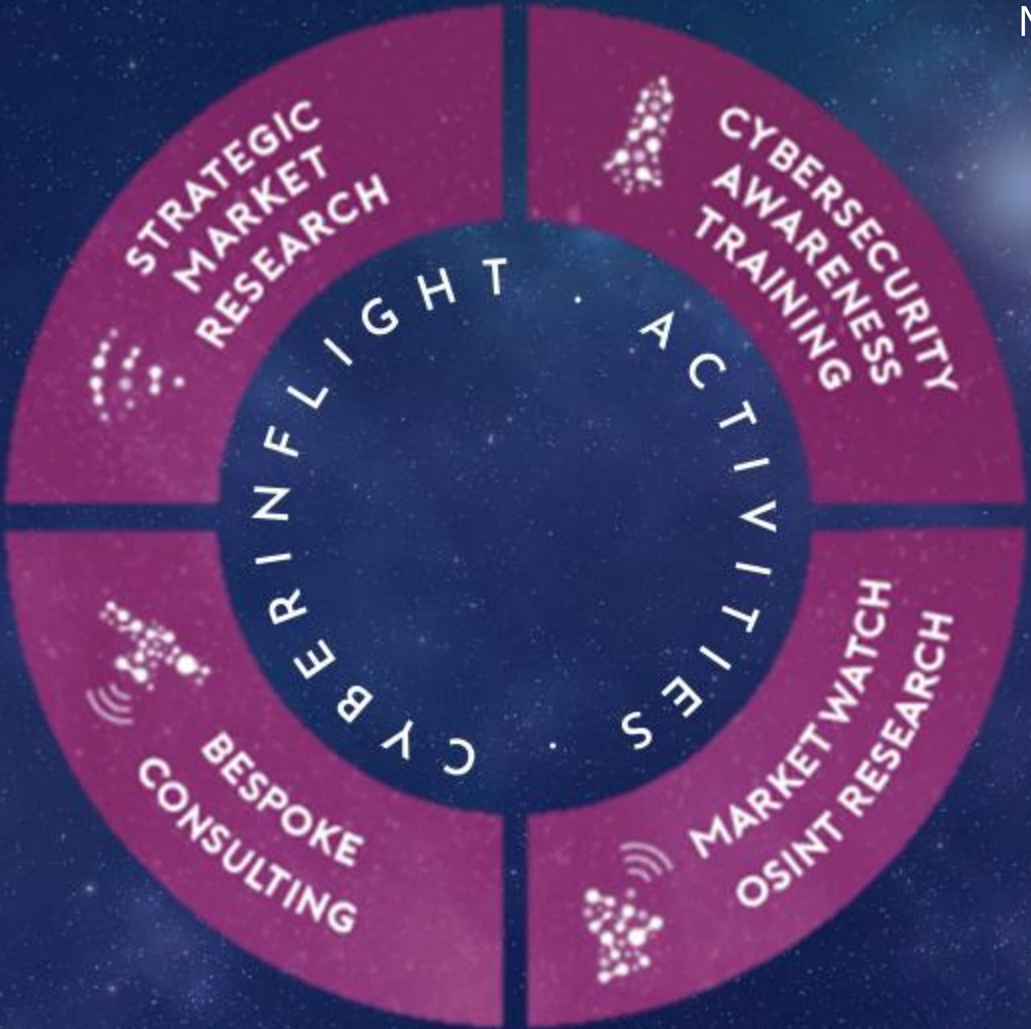
The watch can be customized to your needs, you can order yours!

To register or for more information, reach out to research@cyberinflight.com

CYBERINFLIGHT

CyberInflight

SPACE CYBERSECURITY
MARKET INTELLIGENCE



CYBERINFLIGHT · ACTIVITIES ·

STRATEGIC MARKET RESEARCH

CYBERSECURITY AWARENESS TRAINING

MARKET WATCH OSINT RESEARCH

BESPOKE CONSULTING

SPACE ISAC
PROUD MEMBER

RAISE THE
CYBERSECURITY
AWARENESS
OF THE SPACE
INDUSTRY

cyberinflight.com