SEPTEMBER 2024

Space Cybersecurity Monthly Watch

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

Monthly RISC Score & Highlights
Weekly Observations
Expert Analysis

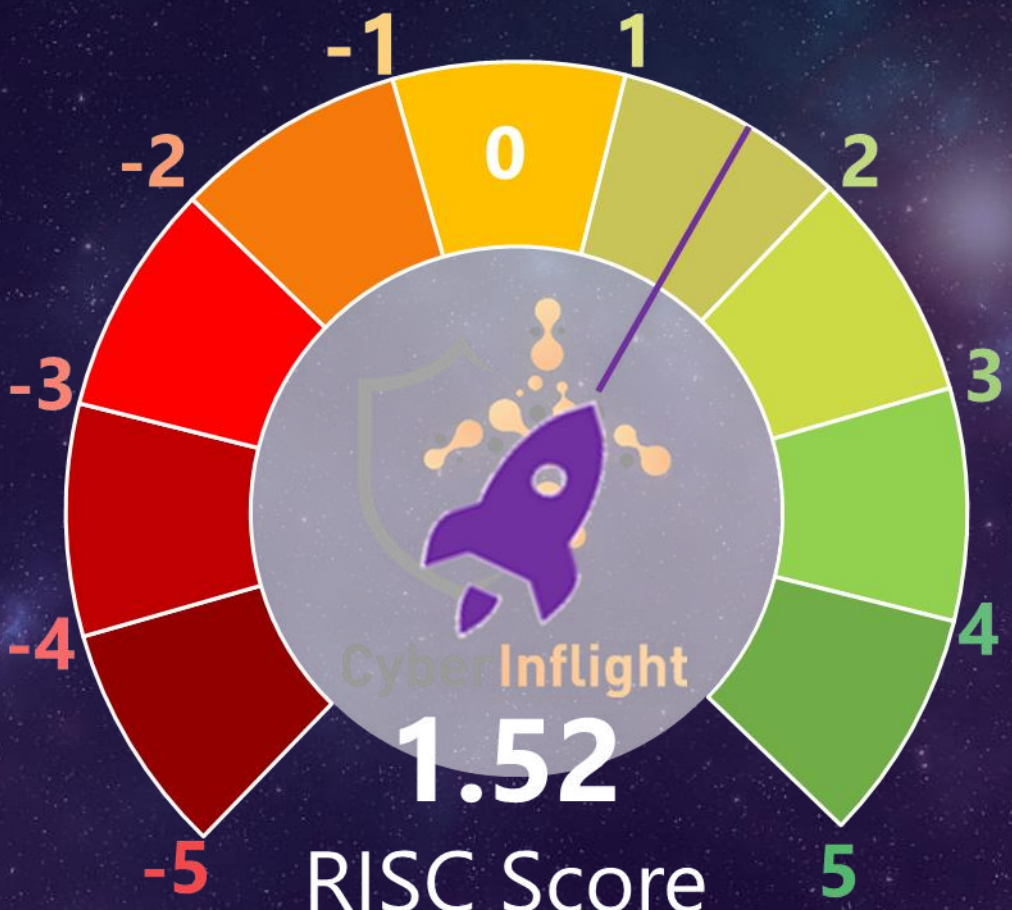
CyberInflight

SEPTEMBER 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 from a range of -7 to 5 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 1.63 in August, which decreased in September (-0.11 points). The score can fluctuate for different reasons, such as geopolitical tensions, technological advancements, and rising cybersecurity threats.

Monthly Highlights - September 2024

On the market front, an important trend in September was **improving military SATCOM resilience**. Airbus's completion of acquiring INFODAS, a German cybersecurity company, is a striking example. Airbus acquired INFODAS to bolster its portfolio and strengthen its position in providing secure communications for European military alliances. On the other side of the Atlantic, the US Department of Defense is also investing in securing military communications, as shown in the recent partnership of Intelligent Waves and SpiderOak. This partnership will focus on enabling safe communications for the US military in contested environments and is part of a broader effort to enhance defense capabilities through more secure and reliable communication systems.

This goes hand-in-hand with a **strong geopolitical focus on space superiority and security**. Several countries are pushing in this direction, as shown in the report released by the US Space Operations Command (SPOC), highlighting the increasing competition among global powers for space dominance and how SPOC plans to ensure that the US maintains its leadership in this domain. In Europe, the recent improvements in the IRIS2 program and OSNMA technology for the Galileo constellation also show the EU's will to protect its sovereignty and space superiority. Lastly, India's DRDO (Defence Research and Development Organization) Chief made a statement in which he emphasized the central role of space in future warfare and the need for India's defense sector to keep ramping up its space technologies and capabilities.

On the technological side, **PNT and GNSS resilience** were at the heart of several discussions and exercises. The Scottish military conducted a GPS-blocking exercise, and Norway armies led a JammerTest exercise to train troops operating in GPS-contested environments. On top of that, PNT systems resilience was the focal point of the IPSEC 2024 conference. Discussions concerned how PNT resilience underpins key sectors such as defense, telecommunications, and energy. Attendees explored innovations in PNT security technologies and shared insights into mitigating the growing threats to these essential systems from cyberattacks and disruptions.

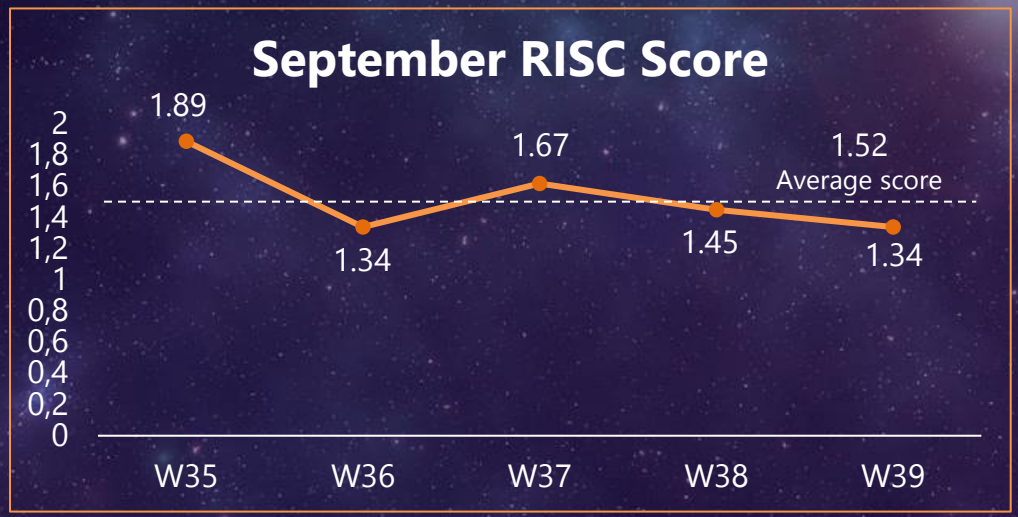
On the threat and regulation sides, different types of actors work toward **addressing cyber-threats through international cooperation**. UK, US, and Canada, for instance, have entered into a trilateral agreement to jointly address the increasing cyber-threats posed to critical national infrastructures. The initiative also focuses on intelligence sharing and strengthening military ties through the application of emerging technologies. Parallelly, Mitsubishi Heavy Industries (MHI) has officially joined the US Space Information Sharing and Analysis Center (ISAC). MHI and other members of the Space ISAC will share intelligence, collaborate on threat assessments, and improve collective resilience against cyber-threats targeting the space domain.

In the next pages, a CyberInflight Expert will analyze in more detail **collaboration and cooperation in Europe**.

Weekly Observations

W35
RISC Score: 1.89

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.



W36
RISC Score: 1.34

The European Union Agency for the Space Programme (EUSPA) has completed the testing of the Galileo Open Service Navigation Message Authentication (OSNMA) and is now gearing up for its operational launch. The testing activities were concluded in early June 2024 with the execution of cryptographic keychain renewal and revocation processes. The program is now preparing the forthcoming OSNMA Initial Service declaration.

W37
RISC Score: 1.62

Xenesis announced on Sept. 11 that it has secured a follow-up contract with the US Space Development Agency (SDA) to develop optical communication terminals for satellites. This 12-month project will take the optical terminals from a preliminary design stage to a conceptual design review with a TRL Level 5/6 in preparation for commercialization. These terminals will play a key role in the Proliferated Warfighter Space Architecture (PWSA), enhancing data transmission capabilities in military satellite networks.

W38
RISC Score: 1.45

US Space Operations Command (SPOC) has released a detailed report highlighting the growing geopolitical challenges in space. The report discusses the increasing competition among global powers for space dominance, particularly in the context of military and strategic operations. The report also outlines SPOC's future plans to ensure that the US maintains its leadership in space, with a strong focus on collaboration with international allies.

W39
RISC Score: 1.34

Mitsubishi Heavy Industries (MHI) has officially joined the Space Information Sharing and Analysis Center (ISAC) to enhance its cybersecurity posture for space systems. By becoming part of Space ISAC, MHI aims to share intelligence, collaborate on threat assessments, and improve resilience against cyber threats targeting space infrastructure.

W35: August 27 – September 2, 2024
W36: September 3 – 9, 2024
W37: September 10 – 16, 2024
W38: September 17 – 23, 2024
W39: September 24 – 30, 2024

Expert Analysis 1/2

Several stakeholders worldwide have been working toward addressing cyber-threats against space assets and infrastructure through **regional or international cooperation**. The EU has seen a similar regional dynamic for some time, notably through its **EU Space Strategy for Security and Defence**, which was identified in 2022. This strategy suggests action to strengthen the **EU's resilience and robustness** of space infrastructure and systems, emphasizing the need for **cooperation and collaboration** between Member States.

Through the impulsion of this strategy, the **EU Space Information Sharing Centre (ISAC)** was recently created by EUSPA and the European Commission, a striking example of the desire for more cooperation. The Space ISAC mainly aims to **raise awareness and develop the expertise of its members** in order to **enhance the overall security, resilience, and robustness** of the EU space sector. It was founded by **12 founding members** (CyberInflight, Airbus, GMV, Infodas, Leonardo, Priamos, OHB, Osmium, Prométhée, Satlantis, Thales Alenia Space and Tecnobit-Oesia Group) and was recently joined by 10 others members from the industry, and 3 new public partners (German Aerospace Center – DLR, European Space Agency – ESA, and the European Organisation for the Exploitation of Meteorological Satellites – EUMETSAT). This **membership-driven initiative** engages several actors from the industry, public institutions, and academia and aims to be a **network-based information-sharing platform.**

> As an EU initiative, the Space ISAC contributes to regional cooperation and helps further integrate the EU internal market.

As an EU initiative, the Space ISAC contributes to regional cooperation and helps further integrate **the EU internal market.**

Alongside the Space ISAC, the EU is developing several cyber frameworks promoting a **common European approach** to cybersecurity and space cybersecurity. The **NIS Directive**, published in July 2016, provided measures to reinforce security in cyberspace through establishing competent national authorities and improving cooperation between Member States. Then, the **NIS2 Directive** extended the initial scope of the framework to space and aimed to **further strengthen cooperation** between Member States, especially in regard to cybersecurity crisis management.

Expert Analysis 2/2

This cooperation is mainly seen through the **EU CyCLONe (Cyber Crisis Liaison Organisation Network)**, pushed by NIS2, which brings together European cybersecurity agencies.

Moreover, as the EU Space Strategy for Security and Defence recommended, a **European Space Law (EUSL)** is ongoing. Based on 3 key pillars, safety, resilience, and sustainability, the EUSL will be a new framework promoting a **common approach** and **collaboration** between Member States. Indeed, the EUSL aims to **unify European frameworks and laws** to avoid fragmentation in order to achieve a single European market and encourage actors of various nationalities to work together. This is set in a specific internal context of **increasing fragmentation**. Indeed, this fragmentation can be due to the multiplicity of EU players, each with particular tasks and competencies, and the multiplication of national laws and guidelines (11 EU Member States have adopted their own national space law), which has led the EU to consider a common framework to improve consistency between all actors. This is why the EU also emphasizes a **single market** moment through this law.

Moreover, the EU Space Strategy for Security and Defence promotes partnerships and collaboration on a **multinational stage** (among other things, by emitting norms, principles, and rules). The strategy calls for developing space security dialogues with third countries (notably the US, but not only), as well as **organizations** such as NATO.

To conclude, the EU has been **investing in and strengthening cooperation** between its Member States and with external third countries through different drivers, such as **regulation aspects** and **membership-driven initiatives**. This trend is **likely to be further emphasized** in the coming months and years, especially in a rising external geopolitical tensions context.

Valentine Crepineau
Market Analyst at CyberInflight

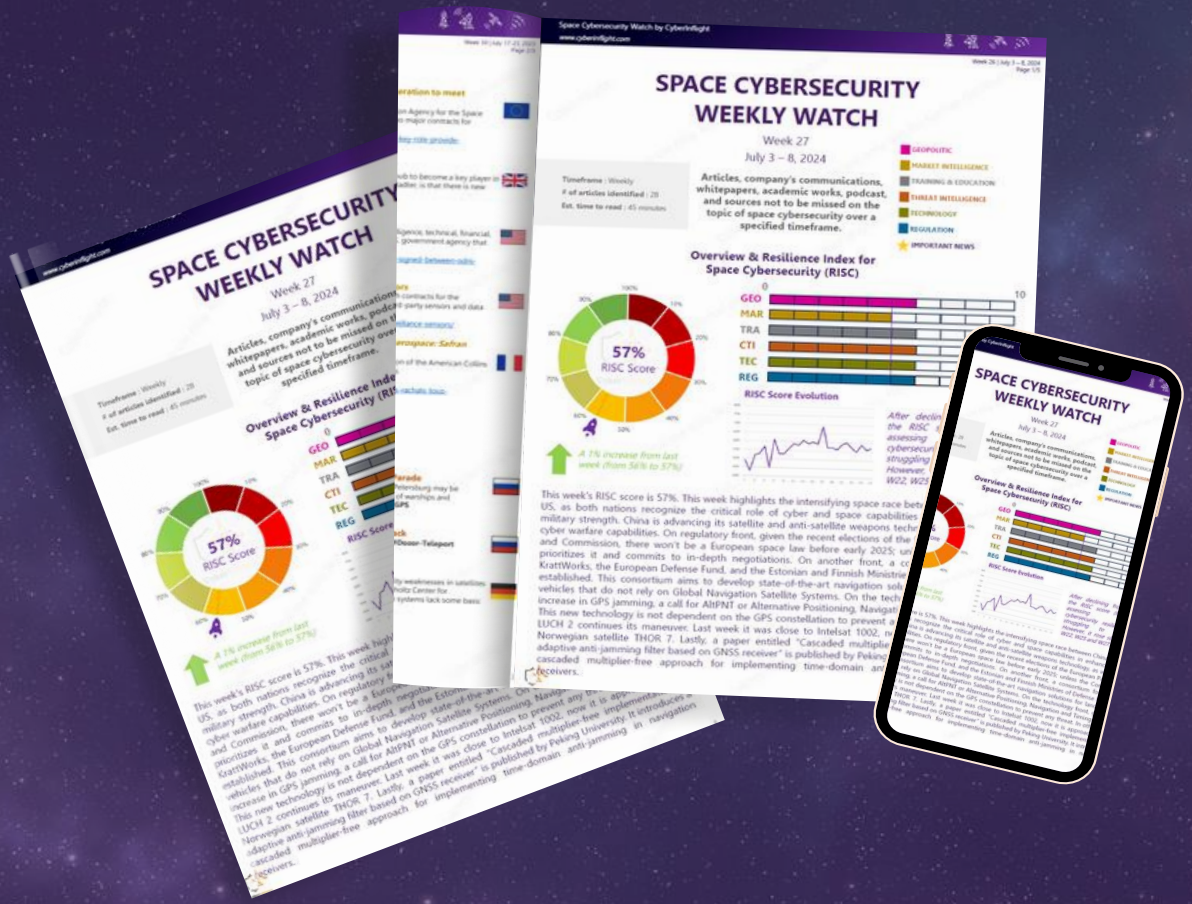
> The EUSL aims to unify European frameworks and laws to avoid fragmentation in order to achieve a single European market and encourage actors of various nationalities to work together.

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!



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

SPACE CYBERSECURITY
MARKET INTELLIGENCE

Raise the cybersecurity awareness of the space industry

cyberinflight.com

SPACE ISAC
PROUD MEMBER