AUGUST 2024

Space Cybersecurity Monthly Watch

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

Monthly RISC Score & Highlights
Weekly Observations
Expert Analysis

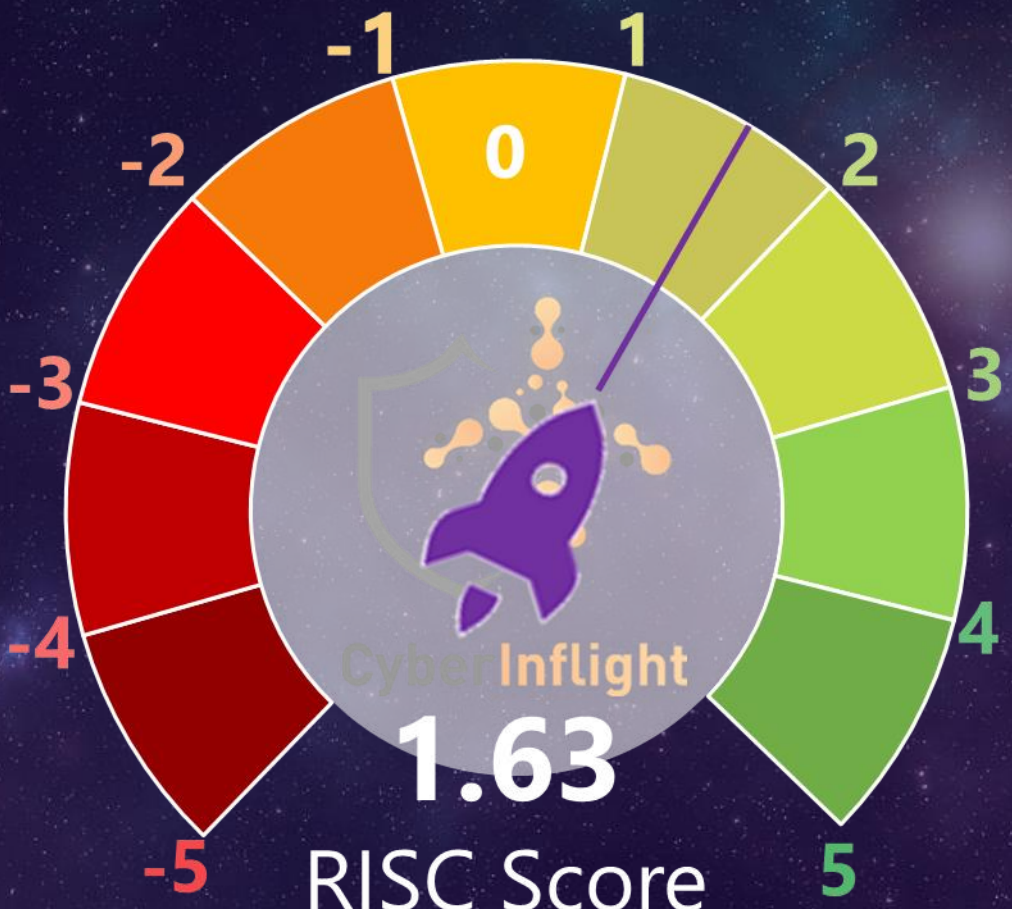
CyberInflight

AUGUST 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.

We have improved the score calculation with a new formula in order to enhance our process! 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 59.75% in July, and it was an increased of 3% compared to June.

The RISC Score can fluctuate for different reasons, such as geopolitical tensions, advancements in satellite technology, and emerging cybersecurity threats.

Monthly Highlights - August 2024

In recent geopolitical developments, several countries, such as the UK, South Korea, Japan, and India, have made **significant efforts to enhance their space defense and surveillance capabilities**. The UK hosted its first space wargame, "Space Warrior," while South Korea prepared for the launch of a new spy satellite. Japan and India also strengthened their cybersecurity partnership, reflecting the increasing regional cooperation in response to shared threats. Tensions were evident in Ukraine's destruction of a Russian gas platform used for GPS interference, **highlighting the growing role of space-based and electronic warfare in global conflicts**. Iran opened a state-of-the-art electronic warfare center, further emphasizing the importance of electronic warfare worldwide.

Technological innovations were another key theme this month, with **breakthroughs in quantum communication and satellite technology.** OneNav's L5 signals showcased resistance to jamming, and Chinese researchers achieved a milestone in secure communications with space-to-ground quantum key distribution (QKD) via a lightweight quantum satellite. These advancements signal a future where secure, resilient communications will be crucial to maintaining both national security and commercial interests. The rise of satellite-enabled Industrial Internet of Things (IIoT) connectivity also demonstrated the growing importance of satellite technology in optimizing Supervisory Control and Data Acquisition (SCADA) systems, especially in remote regions.

Market developments were driven by strategic collaborations and significant contracts. **Intelsat's partnership with Levira, and the UK Ministry of Defence's engagement with Atheras Analytics for military satellite communications analysis**, reflect the increasing commercial interest in space technologies. Additionally, the UK's investment of £20m (i.e., $26.1m) in a state-of-the-art anti-jamming test facility highlights the rising importance of safeguarding critical infrastructure against electronic warfare. These developments underscore the expanding demand for advanced security solutions in the space sector.

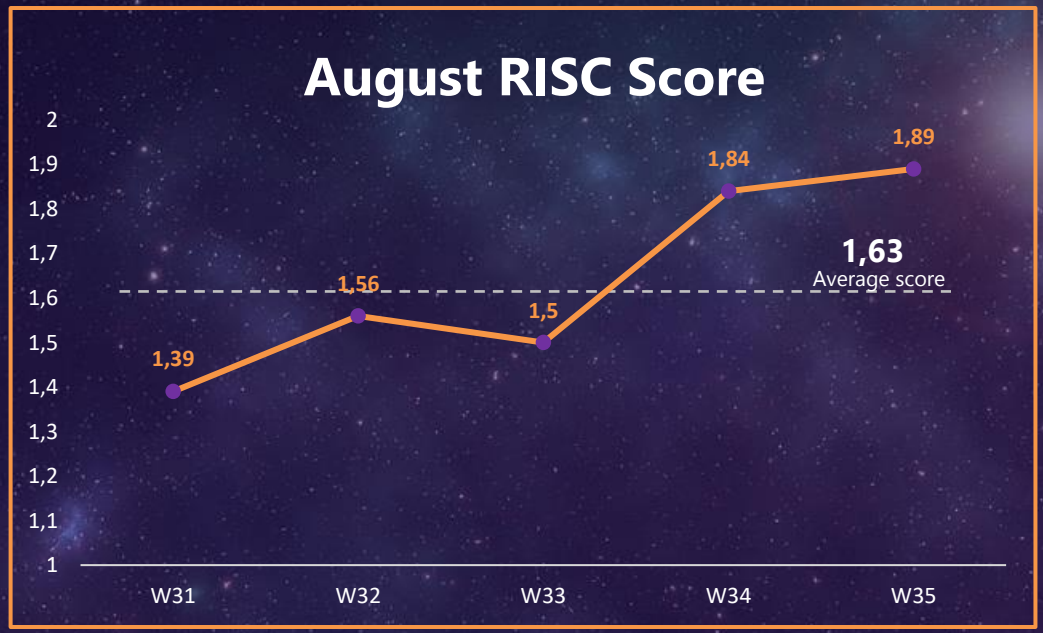
On the regulatory and threat intelligence front, the month saw the introduction of key legislation and reports. In the US, **the Spacecraft Cybersecurity Act was introduced in Congress**, while the **EU moved toward the enforcement of the NIS2 and DORA regulations**, which aim to strengthen cybersecurity in critical infrastructure sectors. At the same time, a report from Thales revealed an **alarming rise in ransomware attacks on critical infrastructure**, emphasizing the need for enhanced defenses. Concerns over spoofing attacks on global navigation satellite systems (GNSS) also grew, with Ukraine's response to Russian GPS interference highlighting the ongoing risks of cyber-threats in space-based operations.

In this Monthly Watch, **our expert** will examine **Quantum technologies as a new strategy for space superiority.**

Weekly Observations

W31
RISC Score: 1,39

oneNav has announced that its L5 signals are immune to jamming, representing a significant advancement in satellite navigation technology. This breakthrough promises greater reliability for critical applications, particularly in environments where signal interference can pose serious risks.



W32
RISC Score: 1,56

A team of researchers has developed a technology capable of storing information within a cloud of atoms. Researchers from NASA's and Infleqtion, produced the first quantum memory of the Star and Striped Space Agency. This technology is NASA's first step towards creating a large-scale quantum network that can lead to safer spatial communications and possibly new scientific discoveries.

W33
RISC Score: 1,50

The National Institute of Standards & Technology officially released the long-awaited final versions of three new post-quantum encryption algorithms, with additional, more specialized algorithms on the way. They are all designed to defend against future hacks carried out by quantum computers, an unproven but rapidly developing threat that could quickly crack the kinds of encryption used almost universally today, including those used in the most sensitive Pentagon systems.

W34
RISC Score: 1,84

Chinese researchers have successfully demonstrated space-to-ground communications using a lightweight quantum satellite, advancing Quantum Key Distribution (QKD) technology. This innovation is a significant leap in secure communications, potentially revolutionizing global cybersecurity

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.

W31: July 30 – August 5, 2024
W32: August 6 – 12, 2024
W33: August 13 – 19, 2024
W34: August 20 – 26, 2024
W35: August 27 – September 2, 2024

Expert Analysis 1/2

The space domain is competitive and progressively militarized. Leading players want proactive engagement in space to operate fully in this domain. **Actors increasingly turn to new technologies, such as quantum and post-quantum cryptography (PQC), to stabilize their position and protect their space assets.** These include traditional actors such as the United States or Europe, emerging nation-states such as China or India, and young New Space companies.

On the market side, August was a good month for quantum investments. First, SBQuantum, a Canadian company founded in 2017, was contracted by the European Space Agency (ESA) and the Canadian Space Agency (CSA) to provide its hardware. ESA plans to evaluate SBQuantum's quantum diamond magnetometer technology's reliability and accuracy in space and how it could be deployed on a satellite. Moreover, in Edinburgh, Scotland, Heriot-Watt University has broken ground on a new £2.5m (i.e., $3.2m) Optical Ground Station facility to demonstrate and test secure quantum communications over satellites. It is part of the Quantum Communications Hub project funded by the UK's National Quantum Technologies Program. The facility is expected to be operational by the end of fall 2024. Therefore, **when it comes to emerging and evolving technology such as quantum, private and academic players are a cornerstone to achieving and maintaining space superiority for nation-states.**

When it comes to emerging and evolving technology such as quantum, private and academic players are a cornerstone to achieving and maintaining space superiority for nation-states.

Another interesting trend that the market and academia have witnessed recently is the **development of quantum technologies along lightweight satellites or nanosatellites**. For instance, the research nano-satellite QUBE, funded by the German Federal Ministry of Education and Research (BMBF), was successfully launched into orbit on August 16. It has started its operations to test recently developed quantum communication technologies. This is a first for a nanosatellite.

Expert Analysis 2/2

In parallel with this launch, Chinese researchers have successfully demonstrated space-to-ground communications using a lightweight quantum satellite, advancing Quantum Key Distribution (QKD) technology. This innovation also represents a significant leap forward in secure communications.

New players are also entering the fray and can tilt the balance of superiority in space. For example, the Indian Space Research Organization (ISRO) has announced plans to launch a satellite with ultra-secure quantum communications capabilities based on quantum cryptography or QKD. The agency has not yet announced a launch date. While it is expected that it may be difficult for a country like India to develop such capabilities, and it may take about ten years to build QKD as a standard, this nation-state is paving the way, **changing the face of the space race.**

Along with these growing investments and players, quantum comes with challenges. At the August meeting of the U.S. President's National Security Telecommunications Advisory Committee (NSTAC), National Cyber Director Harry Coker said that the threat of quantum computing is "not just on the horizon [...] Most actors are already using a 'store now and break later' [framework] to decrypt it once they have quantum capability." NSTAC believes several actors investing in quantum computing are doing so to gain a strategic advantage over the United States.

To protect against this threat, PQC is also an area of study and investment, as evidenced by the recent publication of three NIST PQC standard algorithms, and is expected to **gain further momentum in the marketplace and academia in the coming months and years.**

Valentine Crepineau
Market Analyst at CyberInflight

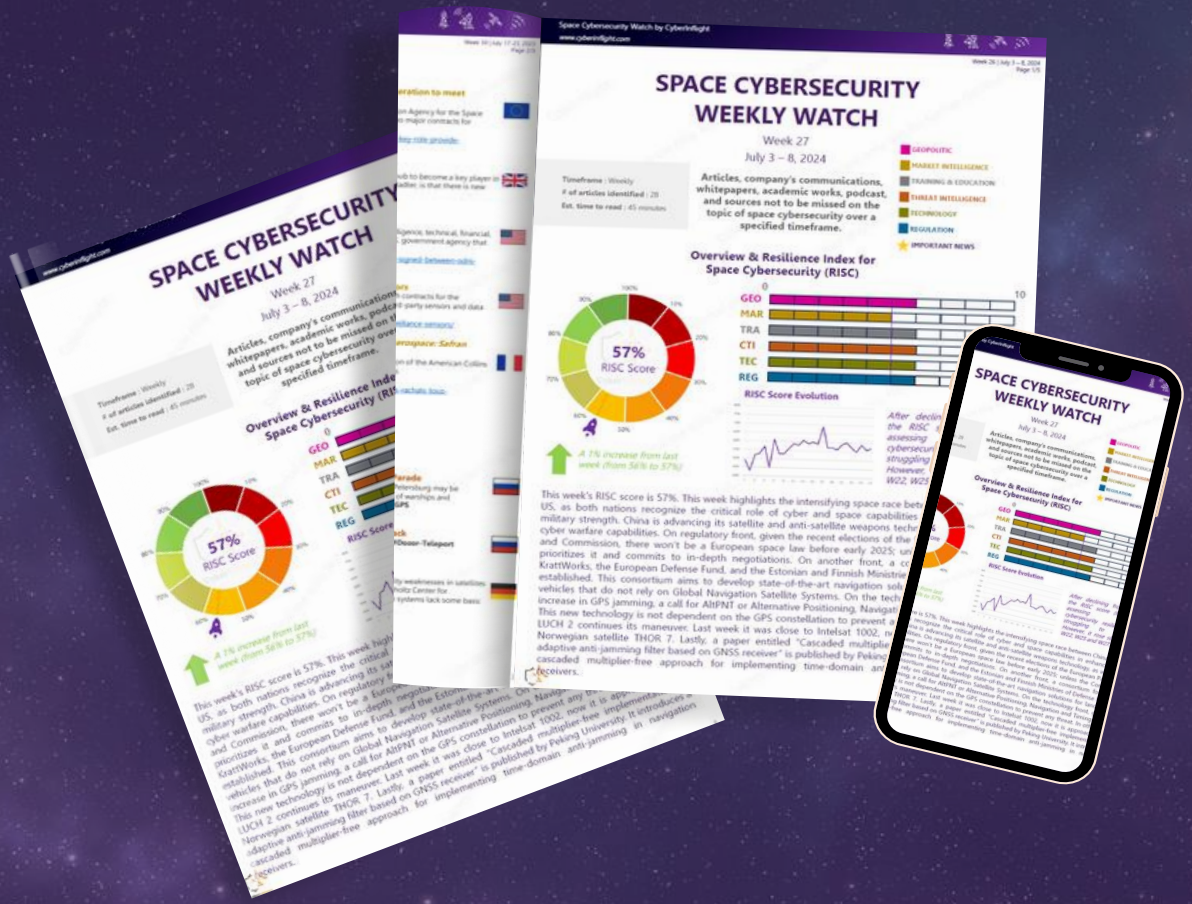
New players are also entering the fray and can tilt the balance of superiority in space.

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!



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

SPACE ISAC
PROUD MEMBER

RAISE THE CYBERSECURITY AWARENESS OF THE SPACE INDUSTRY

cyberinflight.com