JUNE 2024

Space Cybersecurity Monthly Watch

Monthly Highlights & RISC Score
Main Weekly Observations
Experts Analysis

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

CyberInflight

www.cyberinflight.com

Monthly Highlights

Nations around the world have a significant **dependence on space systems**, and that dependence is only growing. It is a modern battlefield that **provides an opportunity for geopolitical adversaries to attack**.

In June, the **International Telecommunications Union (ITU)** reviewed several complaints from Ukraine and European countries about Russian satellite interferences. The UK also complains about Russian GPS jamming on UK military flights. Additionally, the **International Civil Aviation Organization (ICAO)** condemns North Korean missile tests and GPS jamming of aircraft at Incheon Airport.
According to what we observed during the month, Russia is trying to disrupt NATO's communications systems, access military data, and **test the readiness of its geopolitical adversaries**.

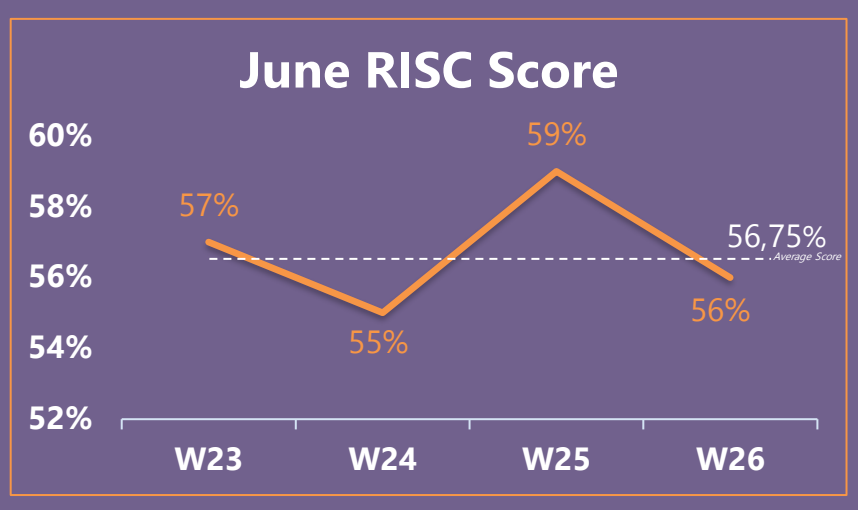
Recognizing this modern space warfare, **some countries have taken initiatives this month to improve space cybersecurity**. **North Korea has** established a satellite cybersecurity body to enhance satellite cybersecurity and protect satellites from design to operation. The **Space ISAC and the Australian Cyber Collaboration Centre** have signed a Memorandum of Understanding to share information and use advanced tools, capabilities, and expertise from both organizations to address critical challenges and drive growth in the space cyber sector. Additionally, the US Space Force Commercial Space Strategy was developed to reinforce US national security and the country's competitive advantage in space. **US Space Command** is also **actively rehearsing a response** to potential attacks on its space assets.

This month, Spacecom observes that **Russia, China, North Korea, and Iran may be forming an "axis"** as they increasingly cooperate in space, which sounds a bit like Operation Olympic Defender. In June, the event "**Les Assises du NewSpace**" was held, highlighting the complex reality of the space sector, which requires constant updating and improvement of technology **to maintain France's position in space**. Reflecting on our observations during the month, the **global market for military GNSS anti-jamming and anti-spoofing solutions has expanded**. Also, this month, we can see entities such as Safran Federal, SandboxAQ, and Air Force Research Laboratory **developing cutting-edge technologies to improve navigation accuracy and reliability** even in GPS-denied or compromised environments.
In this Monthly watch, CyberInflight enlightens you on the latest news about **Luch 2**.

Main Weekly Observations

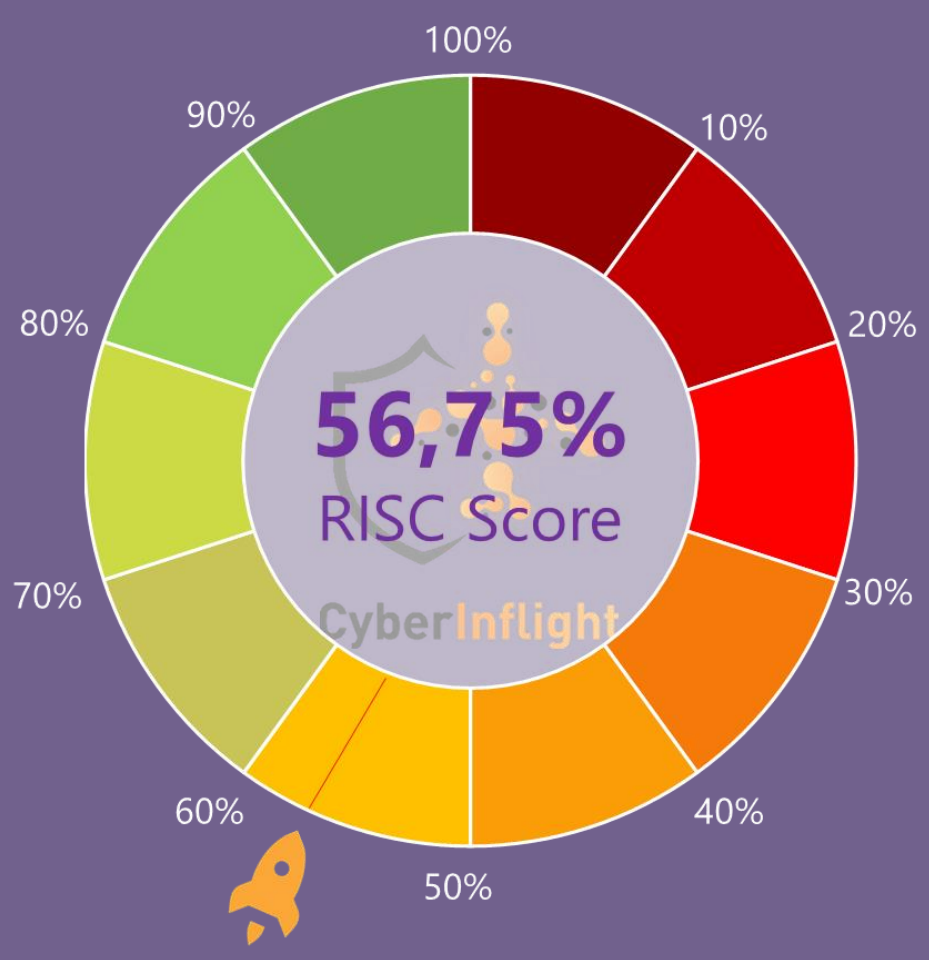
W23: June 4 – 10, 2024
W24: June 11 – 17, 2024
W25: June 18 – 24, 2024
W26: June 25 – July 1, 2024

W23: In **South Korea**, a satellite cybersecurity body has been established by National Intelligence Service (NIS) to strengthen satellite cybersecurity and to protect satellites during their entire lifespan, from design to operation. The NIS will collaborate with Korean entities and other organizations to protect Korean space assets from cyber threats.
W24: The **US Space Force** intends to fly more GPS satellites to complement the 31 GPS satellites now in orbit to protect the GPS system from signal jamming. The House Appropriations Defense Subcommittee questions the effectiveness of this strategy for GPS resilience, saying the plan focuses only on satellites without considering the resilience of other space assets.



W25: AQNav was released by **SandboxAQ**, a technology designed for navigation when GPS systems are jammed or unavailable. The combination of AI algorithms, powerful quantum sensors, and Earth's crustal magnetic field in AQNav makes it resistant to interference.
W26: The **US Space Command** is gearing up for a possible Russian satellite attack in light of the "co-planar" spacecraft that Russia has positioned to monitor US satellites.

June RISC Score



In May, the RISC Score was 58%. There was a decrease of 1,25 percentage points in June.

LUCH-OLYMP: A RUSSIAN APPROACH TO INFORMATION WARFARE IN SPACE

In recent months, the Russian satellite Luch-Olymp K2 has been in the news for its various maneuvers in geostationary orbit. Luch-Olymp K2 - or Luch-5X, as it is officially known - was launched into orbit by a Proton rocket from Baikonur, Kazakhstan, on March 12-13, 2023. It was a discreet lift-off, with no picture released of the arrival at the launch site or of the launch itself.

The Russian news described K2 as a geostationary relay. Still, it was soon suspected that it would replace another satellite called Luch-Olymp K in its electronic intelligence (SIGINT) and secure communications listening missions. The latter's known or suspected capabilities included the **ability to intercept and analyze uplink and downlink signals from satellites in geostationary orbit and locate user terminals on the ground** based on the analysis of these signals.

Moreover, according to former Commandement de l'Espace (French Space Force) commander Michel Friedling, **Luch-Olymp K collected data that was then fed into the Tobol electronic warfare complex database.** This use for military intelligence seems to have continued with the upgraded satellite version.

Furthermore, Luch-Olymp K2 has undergone several improvements over its predecessor. Several reports seem to attest to its ability to imitate and reproduce the signal emitted by a telecommunication satellite. In other words, **K2 could usurp the legitimate signal intended for the user segment.** Since the beginning of the war in Ukraine, **Luch-Olymp K and K2 have approached many satellites covering Europe**. Between March 13th and 15th, 2022, Luch-Olymp K approached Intelsat 39 to less than 5km, breaking the 10km security limit. Then, in early October 2023, K2 placed itself at an unusually close distance from the European Eutelsat 3B and 9B communications satellites, rekindling fears of eavesdropping or jamming. Even more recently, between April and July 2024, K2 approached ASTRA 4A at around 45km.

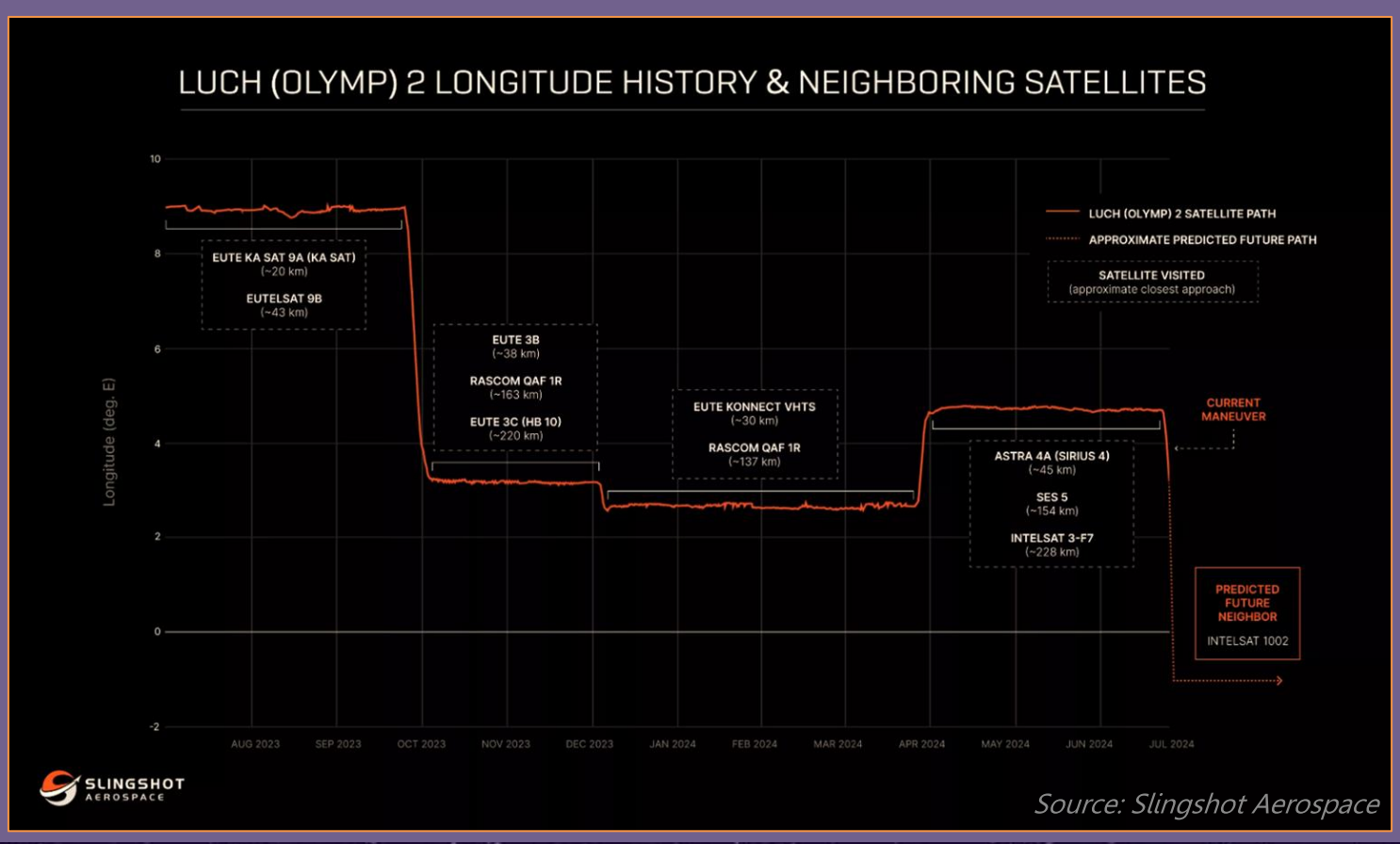
> It cannot be ruled out that Russian intelligence services are using these approaches to prepare cyberattacks or more conventional military actions.

Its future neighbor is estimated to be the American Intelsat 1002 satellite. Audrey Schaffer, CEO of the American company Slingshot Aerospace, explained that while K2 kept a distance greater than 10km from those satellites, it does not mean that it does not potentially pose a security threat. According to experts, it cannot be ruled out that Russian intelligence services are using these approaches to prepare cyberattacks or more conventional military actions.

Indeed, these capabilities and actions in space bear witness to the Russian vision of information warfare. Like the Chinese, **the Russians do not distinguish between so-called cyber activities and those involving signal manipulation (such as Electronic Warfare)**. With the Luch-Olymp satellite series, both activities are integrated into a single whole.

Luch-Olymp also highlights **Russia's tendency to specialize in signal segment operations**, whether defensive or offensive. On the offensive side, organizations such as ROSTEC, KRET, KB Arsenal, and numerous research institutes develop and manufacture ground and space-based electronic warfare equipment. This ecosystem is primarily inherited from the USSR's industrial base. At the same time, the Russian authorities, aware of the risks posed to the signals segment, want to protect communications, which is a significant concern for them, especially in this geopolitical context.

Valentine Crepineau & Matthias Popoff
Market Analysts at CyberInflight

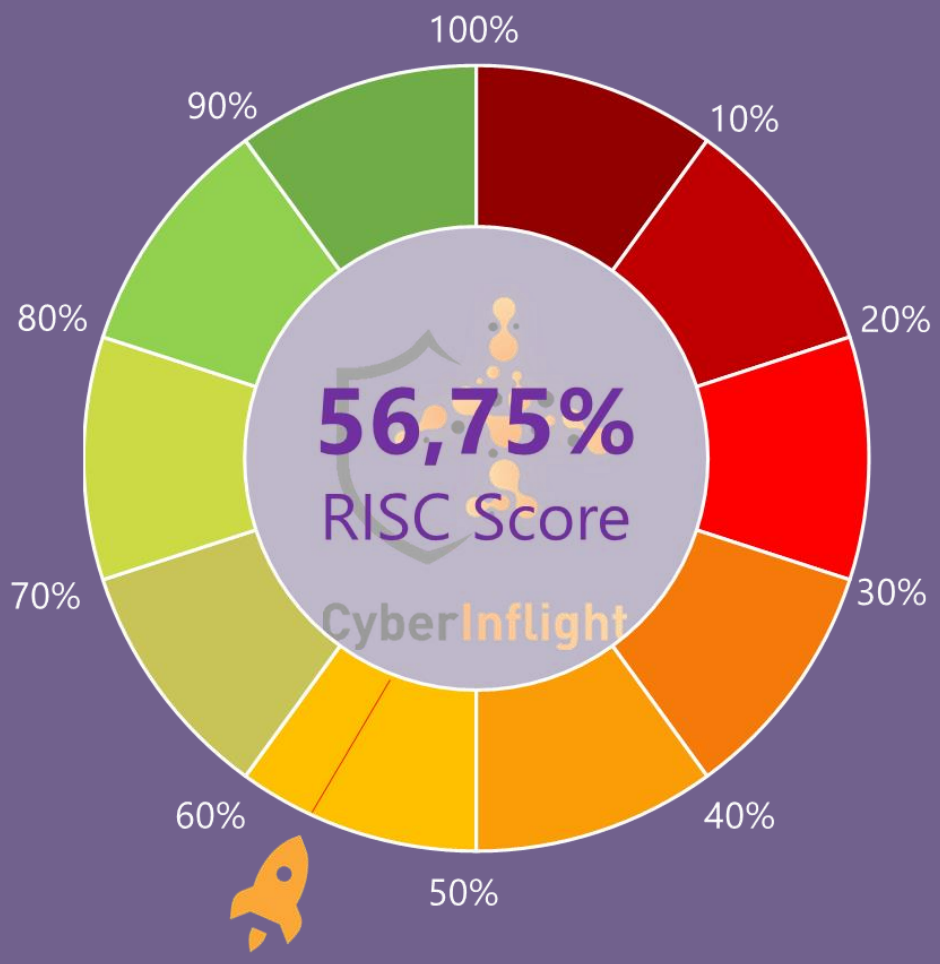


Source: Slingshot Aerospace

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

Get our latest Space Cybersecurity Report – 2024

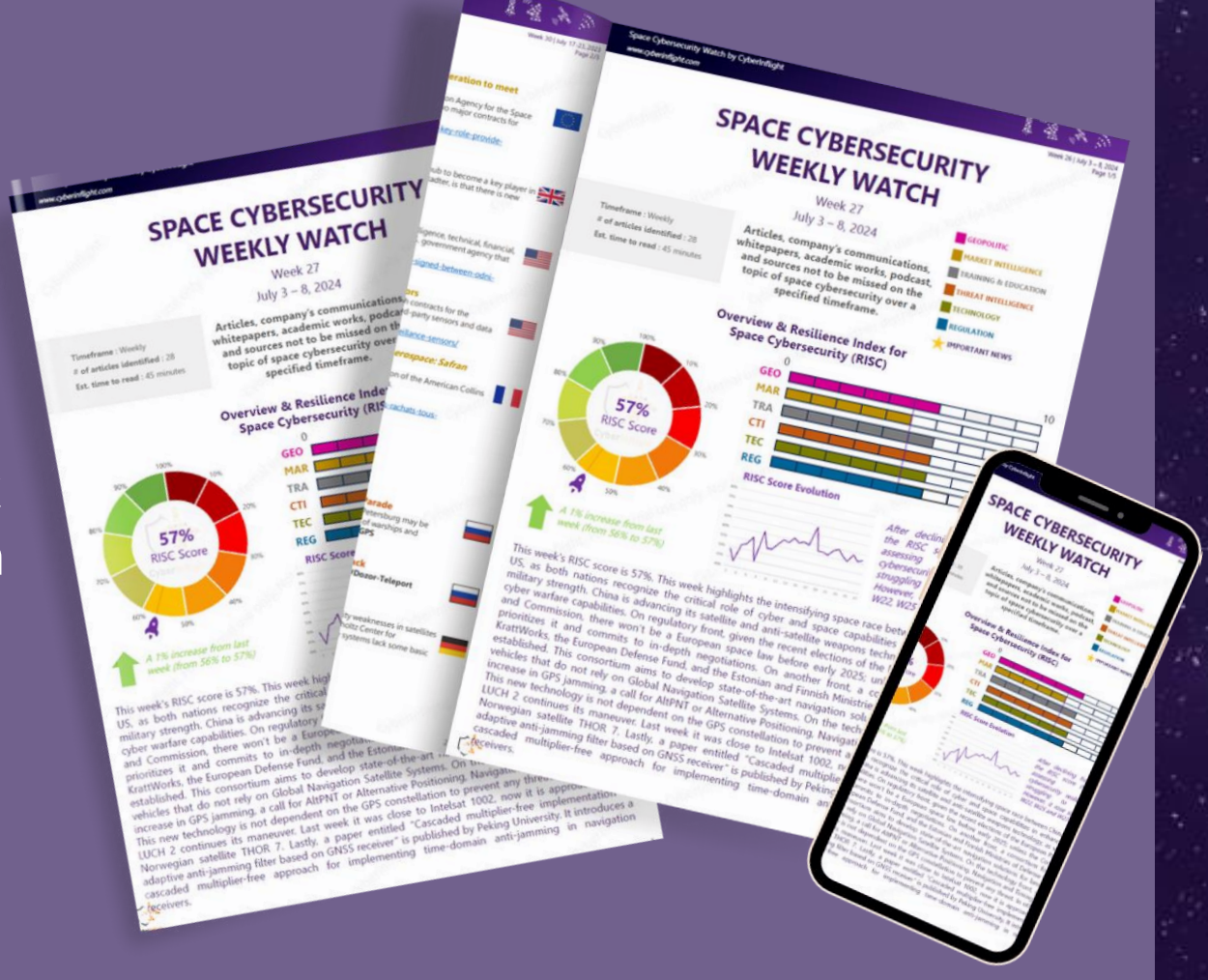
The only Research Report entirely dedicated to the sector



Keep an eye on the weekly RISC Score evolution !

Based on a broad range of calculation criteria, Resilience Index for Space Cybersecurity (RISC) Score is a unique assessment of the space industry

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. Order your customized watch.

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

CyberInflight

CYBERINFLIGHT

SPACE CYBERSECURITY MARKET INTELLIGENCE

RAISE THE CYBERSECURITY AWARENESS OF THE SPACE INDUSTRY

cyberinflight.com

SPACE ISAC PROUD MEMBER