On the edge of the Arctic Circle, where Greenland's ice-scoured landscape stretches toward the horizon, Europe is quietly building infrastructure for a new kind of security threat. It's not missiles or submarines, it's hackers in space.

In Kangerlussuaq, a former US military airbase turned research hub, a small Lithuanian startup called Astrolight is constructing a ground station unlike most of the satellite dishes dotting the planet. Instead of radio waves, it will use lasers to beam massive amounts of data from orbit to Earth; faster, harder to intercept, and far more secure than traditional satellite links.

Backed by the European Space Agency, the project is one piece of a much larger push underway across Europe: an effort to harden satellite communications against cyberattacks, espionage, and interference as space becomes an increasingly contested domain.

For decades, satellites were treated by policymakers as neutral infrastructure, technical utilities that quietly powered GPS navigation, weather forecasting, TV broadcasts, and internet backhaul. That perception shattered in February 2022, when a cyberattack on the Viasat satellite network knocked out communications across parts of Europe at the exact moment Russia launched its invasion of Ukraine.

The message was clear: space systems are no longer just civilian tools. They are strategic assets and prime targets.

When space became a cyber battlefield

Since that attack, interference with satellite systems has surged. Governments now warn openly about electronic jamming, cyber intrusions, and hostile maneuvers by rival spacecraft. Earlier this year, European officials flagged growing concern over Russian and Chinese satellites conducting close-proximity operations — effectively spying — near European assets

in orbit.

The European Commission has gone so far as to describe space as “more contested” than ever, citing a rise in cyberattacks targeting both satellites and the ground stations that control them. In response, EU governments are racing to reduce dependence on foreign technology and strengthen resilience through new regulations, including the upcoming European Space Act, and investments in critical infrastructure.

That urgency is especially visible in the Arctic.

A single point of failure

Today, roughly 80 percent of Europe’s satellite data traffic funnels through one location: Svalbard, a remote Norwegian archipelago situated deep inside the Arctic Circle. The site hosts Europe’s primary Arctic ground station and supports major navigation and Earth-observation programs.

It’s also geopolitically sensitive. Svalbard lies close to Russian territory, sees regular foreign activity, and relies on a single undersea fiber-optic cable to connect its ground station to the global internet. That cable has already been damaged multiple times — accidentally, at least officially.

“If that cable goes down, intentionally or not, you lose access to a huge portion of Europe’s satellite intelligence,” Astrolight CEO Laurynas Mačiulis explains. “That’s a critical vulnerability.”

The Greenland ground station is designed as a backup — a geographically separate node capable of receiving encrypted data via laser links that are far harder to jam or intercept than radio frequencies. Laser communications also offer dramatically higher data rates, a growing

necessity as satellites generate ever-larger volumes of imagery and sensor data.

In practical terms, it's redundancy. In security terms, it's resilience.

The Starlink problem

Europe's anxiety about space security isn't limited to hacking. It's also about control.

The war in Ukraine demonstrated just how vital satellite connectivity has become on the modern battlefield — and how dependent that connectivity can be on private companies. Elon Musk's Starlink constellation has played a critical role in keeping Ukrainian forces online, but its availability has occasionally hinged on Musk's personal decisions.

That uncertainty has rattled European policymakers.

The EU's answer is IRIS², a multibillion-euro secure satellite communications constellation announced in 2022. Designed to operate in low and medium Earth orbit, IRIS² aims to provide encrypted, government-grade connectivity for military, emergency services, and critical infrastructure — without relying on non-European providers.

Officials say the system will feature end-to-end encryption and security certification by national authorities, making intercepted signals effectively useless to adversaries.

The catch? IRIS² won't be operational until the latter part of the decade.

Until then, Europe remains dependent on a mix of commercial systems, legacy infrastructure, and stopgap solutions — a risky position in a rapidly escalating technological arms race.

Who defends space?

Even as Europe invests billions in satellites and ground stations, a quieter challenge looms: figuring out who's actually responsible for defending them.

Unlike traditional military domains, space and cyber defense structures are relatively new. Many countries now operate space commands or cyber commands — but coordination between them is often murky. Mandates overlap. Responsibilities blur. Incident response can become fragmented.

Cybersecurity experts warn that maturity, not just money, is now the limiting factor.

Space systems also don't fit neatly into existing cybersecurity frameworks. Most security firms don't treat "space" as its own sector. Instead, satellites are lumped into categories like telecommunications, environmental services, or media — leaving operators without tailored threat models or specialized tools.

And what works on Earth doesn't always work in orbit.

Satellites can't be patched easily. They have limited computing power. Latency, radiation, and physical inaccessibility all change the rules. A cyberattack that might be contained on a terrestrial network can become catastrophic in space, where recovery options are minimal.

"You can't just take a cybersecurity solution designed for laptops and deploy it on a satellite," one researcher notes. "The environment is fundamentally different."

Securing the final frontier

From laser-linked ground stations in Greenland to sovereign satellite constellations still years from launch, Europe is learning — sometimes uncomfortably — that space security is no longer optional.

Satellites underpin everything from Google Maps directions to financial transactions, disaster response, and military coordination. As space fills with more hardware, more actors, and more geopolitical tension, the risks multiply.

The Arctic outpost rising in Greenland is a small piece of that puzzle — but it reflects a broader shift in thinking. Space is no longer just about exploration or connectivity. It’s about defense, redundancy, and trust.

And in an era where data can decide wars, Europe doesn’t want to leave that trust floating unprotected above the Earth.