Space: the New Cyber Frontier of All Dangers — Exposing the Vulnerability of Satellite Communications

- October 23, 2025

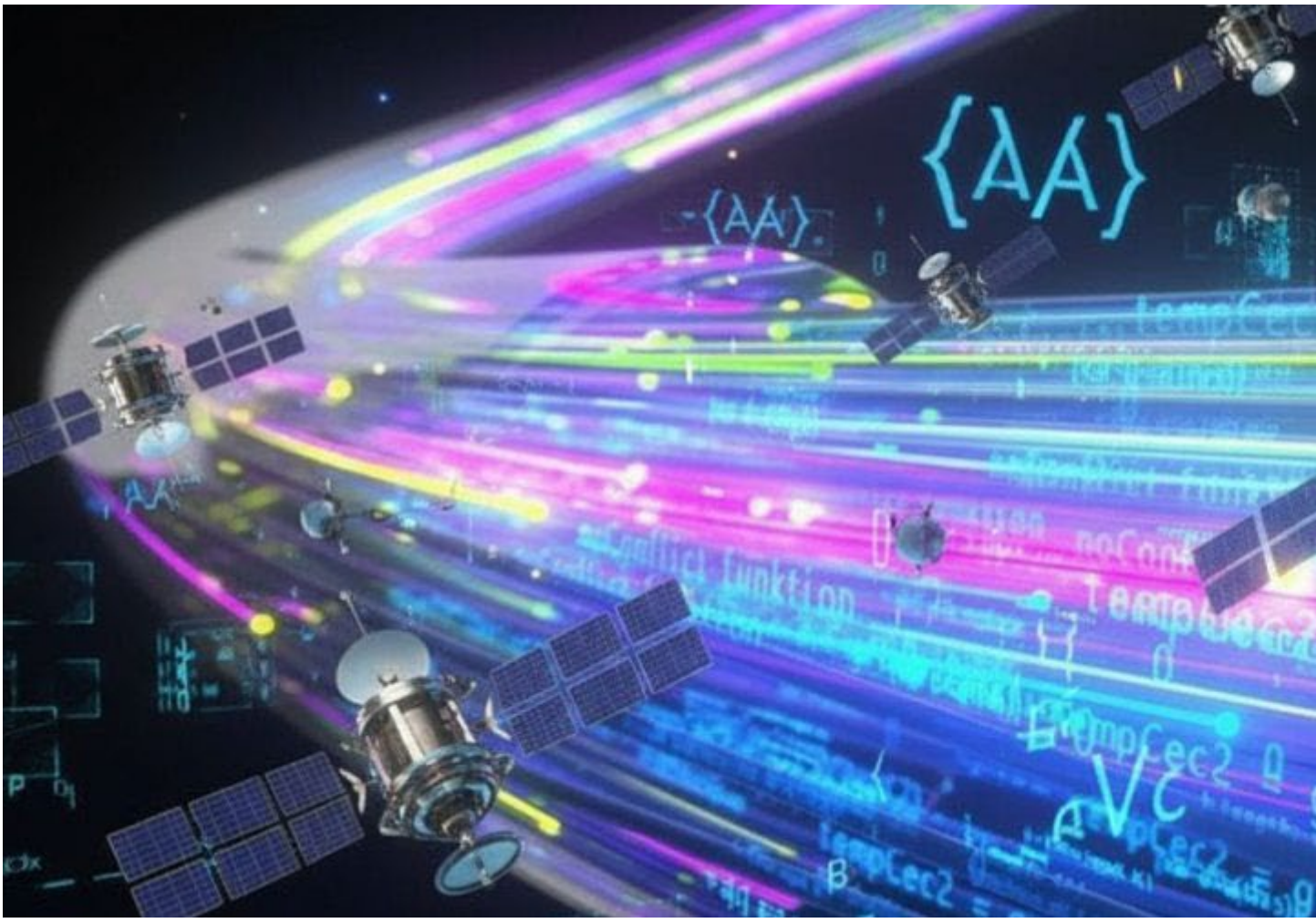

Illustration © AI-generated variation based on an image published at: https://www.diplomacy.edu/blog/dive-deep-into-protecting-submarine-cables/
(Photo link: [https://diplo-media.s3.eu-central-

1.amazonaws.com/2023/02/algorithm-streams-over-the-optical-fiber-3d-illustration-stockpack-istock-1030×579.jpg](https://diplo-media.s3.eu-central-1.amazonaws.com/2023/02/algorithm-streams-over-the-optical-fiber-3d-illustration-stockpack-istock-1030×579.jpg))

The leakage or destruction of data—whether through negligence or targeted attack on its transmission channels—is not a new issue. Nations have long sought to protect their infrastructure in this regard. The first international agreements aiming to protect undersea telegraph cables from intentional damage date back to the late 19th century, with the International Convention signed in Paris in 1884 (1), implemented in the United States through the "Submarine Cable Act", enacted four years later (2).

As transmission methods have evolved over decades and centuries, so too have countermeasures, in an endless race toward the next technological breakthrough offering the best possible safeguards. **Space** has now become the latest domain where solutions are still being explored—or, quite literally, *decoded*.

Before examining the specific issue of satellite data leakage, it is useful to compare the different transmission domains and assess their relative weight "as of today," along with their respective vulnerabilities.

A Comparative approach of Data Flow and Strategic Value By Domains

When discussing vulnerability in the era of hybrid threats and the so-called "grey zone," one can reason in terms of massive flows of data—perhaps not strategic in themselves but capable of paralyzing a nation—or in terms of data sensitivity from a defense and security standpoint.

A first step is to gauge the relative volumes of these transmissions while distinguishing regional traffic from global flows. At the global level, local traffic—whether intra-continental or domestic—is largely carried through land infrastructures: fiber optics, xDSL, coaxial cables, 4G/5G, Wi-Fi, and CDNs. In this sector, figures indicate a land dominance ranging between 70 and 95% of global traffic. Analysts caution however that this broad range should be taken as an order of

magnitude, given the difficulty of precisely separating local from international traffic and the diversity of measurement metrics (3).

Next come the maritime domain – or should we say the submarine domain -, which account for an estimated 5 to 25% of total global traffic (4), and the aerospace domain, representing between 1 and 3%.

By contrast, if we focus on intercontinental traffic, the numbers differ sharply: 90 to 99%*of intercontinental links run through submarine cables (5), 0 to 5% through land routes, and 0 to 2% via satellite (with only about 1% of global internet traffic relying on satellites (6)).

Although satellites still represent a small fraction of the global market compared to other domains, it is worth noting that this market is growing rapidly in niche market segments—remote areas (rural, maritime, aerial) and security or defense sectors (as a key enabler of multi-domain operations). Some projections estimate a compound annual growth rate (CAGR) of 13.9% over the next five years, reaching $22.6 billion by 2030, as satellite communications increasingly provide “an earth interface for voice, video, and data accessible from any point on the planet” (7).

While most data today travels through terrestrial and undersea channels, the next sovereignty battle over information is being fought in space—a low-volume yet highly vulnerable domain.

Just as undersea cables once became openly critical infrastructure, satellites are now a new source of unprecedented vulnerabilities—though with an inverse relationship between the volume they carry and their current exposure risk.

Space: An “Inverted Vulnerability”

Space is no longer a sanctuary. Long considered a safe haven, it is now becoming the new battleground of cyberspace. A joint study by the University of California San Diego(UC San Diego)) and the University of Maryland, recently reported by Wired and Euronews (8), revealed a systemic weakness: nearly half of all signals transmitted by geostationary satellites still travel unencrypted, whereas fiber traffic is almost always encrypted. In other words, with only a few percentage points of total global traffic, the satellite sector concentrates a disproportionate share of interception and data-leak risks.

By comparison, tapping undersea fiber is technically far more difficult than intercepting radio signals, as fibers are shielded and require physical or technical access to the cable. Yet interception remains possible—as shown by historical examples: for instance, during the Cold War, the U.S. Navy deployed listening devices on Soviet cables in the Sea of Okhotsk (a clandestine operation known as Ivy Bells Operation (9)), while some nations today deploy reconnaissance or cable-laying vessels to locate access or vulnerability points, such as the Russian ship Yantar, operated by the GUGI (Main Directorate for Deep-Sea Research), and recently suspected of espionage in European waters (10).

Cables are also subject to attacks targeting landing stations or network management infrastructures. Any flaw in remote management systems or access control can be exploited, while sabotage may be used to cut critical flows or pursue denial strategies (11).

Numerous similar incidents have made national authorities more aware of their dependency on underwater cable infrastructure and prompted them to strengthen audits, redundancy, and resilience measures.

Amid the solutions being implemented, one can highlight the following:
– Physical reinforcement (burying cables in sensitive coastal zones, adding shielding) (12);
– Redundancy (route diversification (13));
– Enhanced surveillance of at-risk routes (14);
– Proactive maintenance to ensure equipment reliability (15);
– Hardened encryption, with the promising development of quantum-based encryption, such as hybrid quantum key distribution (QKD) systems for optical submarine communications (16).

Cette transition semble inéluctable, en ce sens qu'il faut dorénavant intégrer à long terme des solutions résistantes aux ordinateurs quantiques, qui peuvent casser certaines cryptographies actuelles.

The same trend now applies to satellite data, once thought to be relatively immune from such risks.

Since 2023, ENISA, ANSSI, and ESA have been promoting common standards— quantum-safe encryption, network segmentation, and

hardened VSAT terminals —and working toward a European Space Cybersecurity Framework.

On January 30, 2025, the European Commission and European Space Agency launched the EuroQCI initiative, described by the EU as follows: ” The EuroQCI initiative aims to develop secure communication networks that will be quantum-safe—e.g., using quantum-safe cryptography—thus protecting them from quantum and classical attacks across the EU and its overseas territories. These networks will combine terrestrial fiber-optic and satellite communication links.(17)

The discovery by the U.S. researchers from the Universities of California and Maryland serves as a healthy wake-up call: with a few hundred Euros ($800 to be precise) worth of equipment, one can intercept unencrypted signals from geostationary satellites.

Between 2022 and 2025, these researchers intercepted:

• T-Mobile client calls and SMS (over 2,700 numbers in nine hours);

• U.S. and Mexican military data, including helicopter positions and maintenance logs;

. Corporate exchanges** (Walmart Mexico, banks, oil companies, power grids);

• Unencrypted in-flight Wi-Fi streams from commercial aircraft.

Following publication of the study, T-Mobile encrypted its satellite transmissions within weeks. AT&T announced corrections to misconfigured satellite links in certain zones. However, such fixes remain limited to the cases exposed by the researchers.

Many operators or critical infrastructures have not publicly reported remediation—or may not yet have implemented visible changes.

Technologically, various encryption solutions already exist. For instance, L3Harris’s MCU-110C provides uplink and downlink encryption with Over The Air (OTAR) rekeying capabilities (8). Other providers such as Viasat offer end-to-end encryption securing not only satellites but the entire space system (19).

These technologies are mature or maturing, which proves that equipment is less the issue than the challenge to mass-scale deploy them across existing infrastructures.

According to some forecasts, the encrypted satellite telemetry upgrade market, valued at $1.53 billion in 2024, is projected to grow at about 10.2% CAGR through 2033 – driven by rising demand not only from defense and satellite operators but also from the commercial sector (20).

As cybersecurity “best practices” become standard—much like buying car insurance— encryption is increasingly viewed as a basic requirement rather than an optional safeguard.

Yet several obstacles still hinder widespread implementation:
– Lack of backward compatibility for older satellites;
– Increased cost and complexity for operators (encryption can reduce transmission capacity);
– And more generally – as is the case for everything space-related -, the absence of a harmonized international regulatory framework for space cybersecurity.

The findings from UC San Diego and Maryland echo other high-profile events—the KA-SAT network attack during Russia’s invasion of Ukraine in 2022, and the early-2000s interception of U.S. military drone feeds in Iraq and Afghanistan by insurgents capturing unencrypted satellite links (21) are among them.

Together, they starkly expose the fragility of orbital cybersecurit —a domain where the race between sword and shield seems endless.

By Murielle Delaporte

Notes and sources:

(1) « Protection des câbles sous-marins. Convention internationale du 14 mars 1884. Texte des lois rendues dans les divers États en vue de la mise en vigueur de cette convention » (Gallica-BNF, https://gallica.bnf.fr/ark:/12148/bd6t510067117/f5.item.texteImage

(2) See the digital version of the Act kept at the Washington DC-based Library of Congress, https://www.loc.gov/resource/uscode.uscode1934-001047002/ ; https://tile.loc.gov/storage-services/service/ll/llsl/llsl-c17/llsl-c17.pdf

(3) https://blog.cloudflare.com/radar-2024-year-in-review/

(4) https://blog.telegeography.com/2023-mythbusting-part-3

(5) https://www2.telegeography.com/hubfs/LP-Assets/Ebooks/state-of-the-network-2024.pdf ; to go further, see for instance the following CSIS report: https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

(6) https://superfactful.com/2025/08/06/satellites-handle-a-very-small-amount-of-global-internet-traffic/

(7) Quote taken from: https://www.grandviewresearch.com/industry-analysis/satellite-internet-market-report; on this issue, see the reports of the UN digital agency (ITU pour « International Telecommunications Union »),such as for instance: https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-internet-traffic/

(8) https://satcom.sysnet.ucsd.edu/ ; this study has been in particular the focus of the following publications:
Greenberg, Andy, et Matt Burgess. “Satellites Are Leaking the World’s Secrets: Calls, Texts, Military and Corporate Data.” WIRED, October 14, 2025. https://www.wired.com/story/satellites-are-leaking-the-worlds-secrets-calls-texts-military-and-corporate-data/ ; Desmarais, Anna. “Military Data, Texts, and Internet History: Scientists Intercept Unprotected Data from Satellites.” Euronews, October 14, 2025. https://www.euronews.com/next/2025/10/14/military-data-texts-and-internet-history-scientists-intercept-unprotected-data-from-satell

(9) See on this issue for example the article by Matthew Carle, published in Military.com in 2017 and entitled “The Mission Behind Operation Ivy Bells and How It Was Discovered”, https://www.military.com/history/operation-ivy-bells.html

(10) The Russian spy ship stalking Europe’s subsea cables, Financial Times, 25 septembre 2025, https://www.ft.com/content/0b351091-3f82-4f2f-bef2-a52a35f009f2 ; see also:: Avioutskii, Viatcheslav. “Ce bateau russe qui s’en prend aux câbles sous-marins européens.” Atlantico, 29 septembre 2025. https://atlantico.fr/article/decryptage/ce-bateau-

russe-qui-sen-prend-aux-cables-sous-marins-europeens-yantar-flotte-russe-sanctions-guerre-hybride-viatcheslav-avioutskii.

(11) See for instance: Van Soest, H., & Fine, H. (2024, March 11). Vital Yet Vulnerable: Undersea Infrastructure Needs Better Protection. RAND Corporation, https://www.rand.org/pubs/commentary/2024/03/vital-yet-vulnerable-undersea-infrastructure-needs.html

(12) https://www.diplomacy.edu/blog/dive-deep-into-protecting-submarine-cables

(13) Burnett, D. R. 2021. “Submarine Cable Security and International Law.” International Law Studies 97: 55–80. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2992&context=ils

(14) Sherman, Justin. Cyber Defense Across the Ocean Floor : The Geopolitics of Submarine Cable Security. Atlantic Council – Scowcroft Center for Strategy and Security, 13 septembre 2021. https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/

(15) According to the International Cable Protection Committee (ICPC), there are about 150 to 200 maintenance issues a year which trigger an average of 3 repair a week. See: ICPC Viewpoint, Charting Submarine Cables Is Critical for Maritime Safety and Infrastructure Protection, 2025, https://www.iscpc.org/publications/icpc-viewpoints/charting-submarine-cables-is-critical-for-maritime-safety-and-infrastructure-protection/

(16) Liñares, Javier, Xoán Prieto-Blanco, Andrés Vázquez-Martínez, and Emilio F. Mateo. “Multichannel Hybrid Quantum Cryptography for Submarine Optical Communications.” arXiv preprint arXiv:2508.10521, August 14, 2025. https://doi.org/10.48550/arXiv.2508.10521

(17) This quote comes from: European Commission et European Space Agency. Commission and European Space Agency Sign EuroQCI Implementation Agreement. Digital Strategy – European Commission, January 20th, 2025. https://digital-strategy.ec.europa.eu/en/news/commission-and-european-space-agency-sign-euroqci-implementation-agreement

(18) https://www.l3harris.com/all-capabilities/secure-satellite-communications-encryption-unit-mcu-110c

(19) https://www.viasat.com/government/security/encryption/space/

(20) https://dataintelo.com/report/satellite-telemetry-encryption-upgrades-market

(21) https://www.wired.com/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach/