L’espace, nouveau front cyber de tous les dangers : la vulnérabilité des communications satellitaires exposée

- octobre 23, 2025

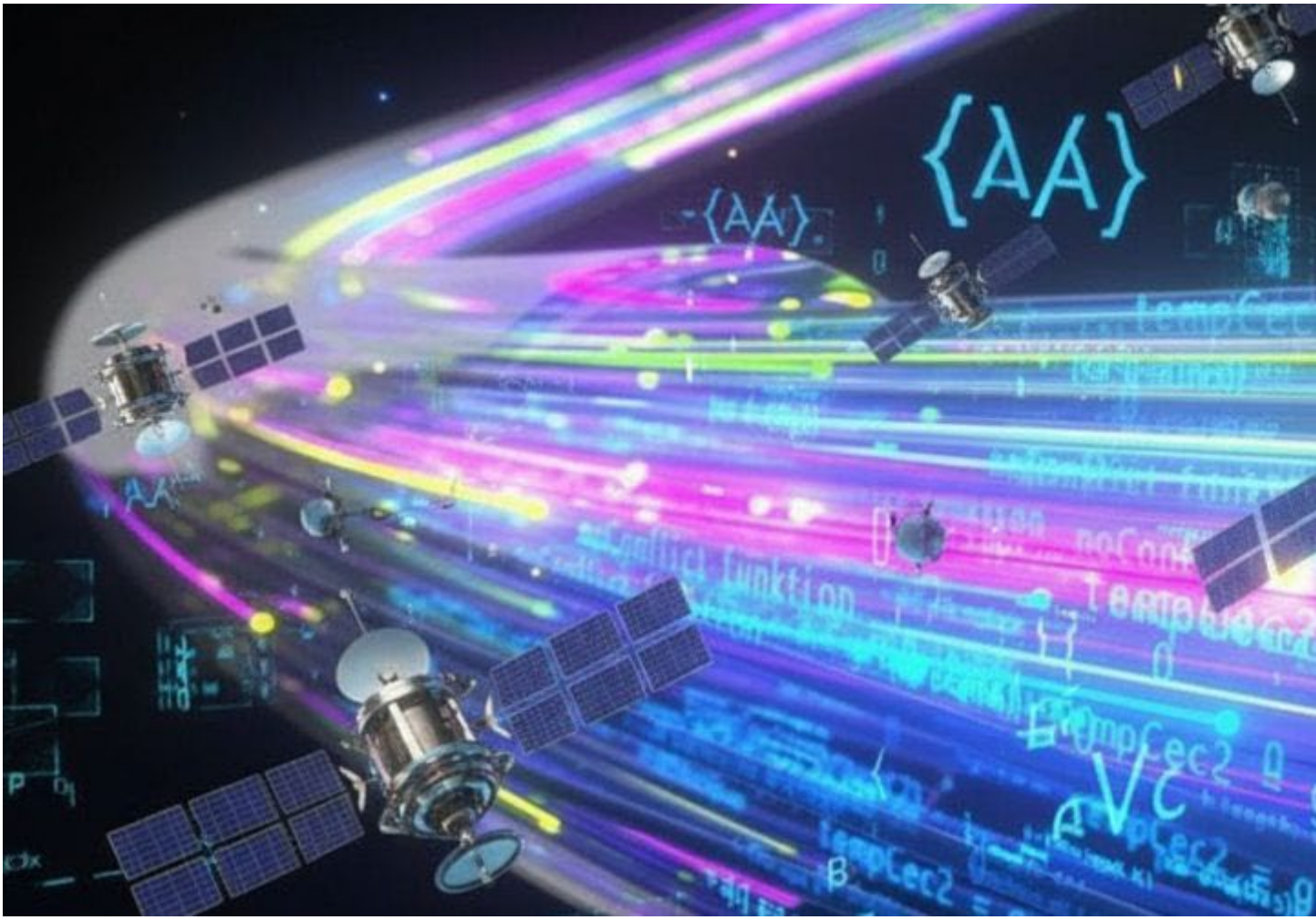

Illustration © variation générée par IA sur la base de l’illustration publiée dans : https://www.diplomacy.edu/blog/dive-deep-into-

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

La fuite ou destruction de données par négligence ou attaque ciblée sur leur mode de transmission n'est pas une problématique nouvelle, tandis que les nations se sont toujours essayées à protéger leurs infrastructures en ce sens. C'est ainsi par exemple que les premiers accords internationaux cherchant à protéger les câbles télégraphiques sous-marins contre les perturbations intentionnelles remontent à la fin du XIXème siècle avec la Convention internationale signée en 1884 à Paris (1), laquelle fut mise en œuvre aux Etats-Unis au travers du « Submarine Cable Act » signé quatre ans plus tard (2).

Les modes de transmission évoluant au fil des ans et des siècles, les parades ne cessent elles non plus de s'inscrire dans une quête sans fin vers la dernière prouesse technologique offrant la meilleure garantie possible en la matière. L'espace est aujourd'hui le dernier domaine où les solutions sont en cours de défrichage, voire – sans mauvais jeu de mot – de déchiffrage.

Avant de faire un tour d'horizon de cette problématique de la fuite de données satellitaires, il a paru intéressant de comparer les divers modes de transmissions par milieux en essayant d'en mesurer le poids respectif « au jour d'aujourd'hui » et leur vulnérabilité respective.

Les enjeux par milieu : volume et stratégicité de la donnée

Quand on parle de vulnérabilité à l'heure de l'hybridité de la menace et de la fameuse « zone grise », on peut raisonner en termes de volumes de données pas nécessairement stratégiques en elles-mêmes, mais susceptibles de paralyser le fonctionnement d'un pays, ou en termes de données sensibles d'un point de vue de la défense et de la sécurité dudit pays.

Si l'on essaie donc en un premier temps d'avoir un aperçu des volumes en question, il faut également distinguer les flux régionaux des flux globaux. Au niveau global, le trafic « local » qu'il soit intra-continent ou intra-pays pèse fortement au travers de l'utilisation de la fibre terrestre, xDSL, câble coax, 4G/5G, Wi-Fi, CDN, etc. Dans ce secteur, les chiffres

indiquent une domination terrestre avec une fourchette estimée entre 70 et 95% du trafic mondial. D'après les analyses disponibles, cette large fourchette doit être considérée comme un ordre de grandeur, car elle reflète justement la difficulté de mesurer avec précision ce qui relève du trafic local et ce qui relève de l'international, sans compter les différences entre métriques utilisées (3).

Viennent ensuite le milieu marin – ou plus exactement sous-marin – estimé entre 5 et 25 % du trafic mondial total (4), et le milieu aérospatial qui se situe entre 1 et 3% de ce dernier.

A noter que si l'on raisonne en revanche en termes de trafic intercontinental, les chiffres (considérés plus solides que les précédents) diffèrent drastiquement avec 90 à 99% de liaisons intercontinentales passant par câbles sous-marins (5), de 0 à 5% transitant par itinéraires terrestres et entre 0 et 2% pour la part satellitaire (seulement 1% du trafic internet mondial dépend des satellites (6)).

Si les satellites ne représentent donc encore qu'une petite part du marché mondial par rapport aux autres milieux, il convient de souligner que ce marché croît très vite dans les zones de niche qu'il concerne : zones difficiles d'accès – rurales, maritimes ou aériennes – et/ou secteurs de la sécurité (secours) et de la défense bien-sûr (en tant que facilitateur notamment du concept multi-domaine). Les prévisions relatives à la taille du marché mondial de l'internet parlent d'un taux de croissance lissée (ou taux de croissance annuel composé / CAGR) de 13,9% dans les cinq ans qui viennent (22,6 milliards de dollars en 2030), les communications par satellite offrant de façon croissante une option en matière d'« interface terrestre pour la voix, la vidéo et les données, accessible depuis n'importe quel point de la planète » (7).

Si la donnée transite aujourd'hui majoritairement par des canaux terrestres et sous-marins, c'est désormais dans l'espace que se joue ainsi la prochaine bataille de la souveraineté informationnelle : un milieu à faible volumétrie, mais à haut potentiel de vulnérabilité.

Comme hier les câbles sous-marins, les satellites sont désormais devenus des infrastructures critiques sources de vulnérabilités inédites, mais avec un rapport inverse entre volume transporté et risque d'exposition.

Espace : une « vulnérabilité inversée »

L’espace n’est plus un sanctuaire. Longtemps perçu comme un relais sûr, il est en passe de devenir le nouveau champ de bataille du cyberespace. Une étude conjointe des universités de Californie (UC San Diego) et du Maryland, relayée dans la presse notamment par WIRED et Euronews (8), vient de révéler une faille systémique : près de la moitié des signaux émis par des satellites géostationnaires transiteraient encore sans chiffrement, alors que ceux transmis via la fibre le sont systématiquement. En d’autres termes, avec seulement quelques pourcentages du trafic mondial à son actif, le secteur satellitaire concentre une part disproportionnée des risques de fuite et d’interception.

A titre comparatif, en ce qui concerne la vulnérabilité sous-marine, l’écoute passive du cœur de la fibre est techniquement plus difficile que celle des signaux radio, car les fibres sont confinées et nécessitent un accès physique ou technique au câble. Il n’en reste pas moins que l’interception demeure possible comme en témoignent plusieurs exemples passés : pendant la Guerre froide, les États-Unis avaient posé des dispositifs d’écoute sur des câbles de communications soviétiques dans la mer d’Okhotsk (opération clandestine connue sous le nom d’Ivy Bells (9)), tandis que certaines puissances positionnent leurs navires de reconnaissance ou de câblage, de façon à identifier des points d’accès ou de vulnérabilité (tels par exemple le navire russe Yantar issu d’une unité du ministère russe de la Défense appelée GUGI, acronyme de « Direction principale des recherches en eaux profondes » récemment soupçonné d’espionnage dans les eaux européennes (10)).

Les câbles sont aussi sujets à des attaques au niveau des stations d’atterrissage ou des infrastructures de gestion du réseau. Toute faille dans les systèmes de gestion à distance ou dans les contrôles d’accès est susceptible d’être bien-sûr exploitée, tandis que le sabotage de câbles est un moyen de couper l’accès à des flux critiques ou d’appuyer une stratégie de déni (11).

De nombreux événements de ce type ont alerté les autorités publiques quant à la dépendance du monde au réseau sous-marin, et ont amené les opérateurs et États à renforcer les audits, la redondance et la résilience.

Parmi les solutions mises en œuvre, on peut citer des mesures de renforcement physique (enterrement des câbles en zone côtière ou sensible ; renforcement de leur protection avec blindage supplémentaire) (12), de redondance (diversification des routes (13)), de surveillance accrue des tracés à risques (14), mais aussi de l’état des

équipements devant engendrer une maintenance particulièrement proactive (15). Un chiffrage renforcé y compris via des développements récents de cryptographie quantique appliquée aux câbles sous-marins fait également partie des solutions prometteuses : par exemple une approche hybride de cryptographie quantique (QKD) est proposée pour les communications optiques sous-marines (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.

La tendance est dorénavant la même en ce qui concerne la protection des données satellitaires que l'on pensait encore récemment relativement sanctuarisées.

Depuis 2023, l'ENISA, l'ANSSI, et l'ESA promeuvent ainsi la mise en œuvre de normes communes -chiffrement *quantum-safe*, segmentation réseau, durcissement des terminaux VSAT – et la création d'un *Space Cybersecurity Framework* européen.

Le 30 janvier dernier, la Commission européenne et l'Agence spatiale européenne lançait ainsi par exemple l'initiative EuroQCI décrite par l'UE comme suit :
« L'initiative EuroQCI vise à développer des réseaux de communication sécurisés, résistants aux attaques quantiques – par exemple grâce à l'utilisation de la cryptographie dite quantum-safe (à l'épreuve du quantique) -, afin de les protéger contre les attaques tant quantiques que classiques, sur l'ensemble du territoire de l'Union européenne et de ses territoires d'outre-mer. Ces réseaux combineront des liaisons terrestres en fibre optique et des communications par satellite. » (17)

La découverte de l'équipe de chercheurs des Universités de Californie à San Diego et du Maryland joue ainsi un rôle d'alerte salutaire, en démontrant qu'avec quelques centaines d'Euros (environ 800 dollars), il est possible de capter des communications satellitaires non chiffrées émises par des satellites géostationnaires.

Entre 2022 et 2025, les interceptions des chercheurs ont de fait concerné :

• les appels et SMS de clients T-Mobile (plus de 2 700 numéros identifiés en neuf heures) ;

• des données militaires américaines et mexicaines, incluant notamment les positions et registres de maintenance d'hélicoptères ;

• divers échanges entre industriels (Walmart Mexico, banques, compagnies pétrolières, réseaux électriques) ;

• des flux Wi-Fi d'avions commerciaux captés sans cryptage.

Suite à la publication de l'étude, T-Mobile a annoncé avoir chiffré ses transmissions satellitaires en quelques semaines. AT&T a aussi déclaré avoir corrigé un problème de configurations satellitaires non chiffrées dans certaines zones et remis ses liens en sécurité. Toutefois, ces réactions restent pour l'instant limitées aux cas révélés par les chercheurs.

Beaucoup d'opérateurs ou d'infrastructures critiques n'ont en effet pas rendu publiques leurs corrections, ou n'ont pas encore procédé à des changements visibles.

Au niveau technologique, différentes solutions existent cependant déjà : des modules cryptographiques spatiaux existent depuis déjà plusieurs années. Par exemple, le MCU-110C de L3Harris fournit le chiffrement pour les liaisons montantes et descendantes, avec des capacités de rechargement de clés OTAR (*Over The Air*) (18). D'autres industriels, tels Viasat par exemple, propose des solutions de chiffrement de bout en bout pour sécuriser non seulement les satellites, mais l'ensemble du système spatial (19).

Ces solutions techniques sont déjà mûres ou en voie de maturation, ce qui montre que l'outillage ne manque pas, mais que le défi réside davantage dans leur déploiement à très grande échelle sur des infrastructures existantes.

A noter que le marché des mises à niveau de télémétrie satellitaire chiffrée est estimé à 1,53 milliard de dollars en 2024, et devrait croître à un taux annuel d'environ 10,2 % jusqu'en 2033. Une croissance reflètant une demande accrue non seulement des acteurs de la défense ou des opérateurs satellitaires classiques, mais aussi du secteur commercial, en vue du renforcement de la sécurité des liaisons spatiales (20). Tout comme les « bonnes pratiques » en matière de cyber sécurité commencent à se généraliser comme l'on prend une assurance pour sa voiture, la sécurisation par chiffrement est de plus en plus considérée comme une exigence de base et non plus seulement une option.

Malgré ces progrès, plusieurs obstacles ralentissent une mise en œuvre généralisée, parmi lesquels la question de la rétro-compatibilité sur des satellites plus anciens non reconfigurables, un surcoût et une complexité difficiles à suivre pour nombre d'opérateurs dans la mesure où le chiffrement peut réduire la capacité de transmission, et, de façon générale, comme pour tout ce qui a trait au domaine spatial, l'absence de cadre normatif international harmonisé.

Les conclusions de l'étude des Universités de Californie et du Maryland font écho à d'autres évènements – attaque du réseau KA-SAT lors de l'invasion de l'Ukraine en 2022, compromission au début des années 2000 de flux drones des forces armées américaines en Irak et Afghanistan par des insurgés capables de capter les transmissions satellitaires entre drones et stations de contrôle(21) -, et agissent comme un révélateur brutal des fragilités de la cybersécurité orbitale.

Un domaine où la course entre l'épée et le bouclier semble infinie…

Par Murielle Delaporte

Notes et références :

(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) accessible en version numerique via le lien suivant : https://gallica.bnf.fr/ark:/12148/bd6t510067117/f5.item.texteImage

(2) Voir sur ce sujet les textes originaux localisés à la bibliothèque du Congrès à Washington et accessibles en version numérique notamment via ces liens : 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 ; pour aller plus loin, voir par exemple le rapport

de CSIS : 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) Citation issue de : https://www.grandviewresearch.com/industry-analysis/satellite-internet-market-report ; voir sur ce sujet les rapports de l'agence numérique de l'ONU (ITU pour « International Telecommunications Union »), tels que par exemple : https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-internet-traffic/

(8) https://satcom.sysnet.ucsd.edu/, étude reprise notamment dans : 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/ et 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) Voir par exemple sur ce sujet, l'article de Matthew Carle, publié dans Military.com en 2017 sous le titre « The Mission Behind Operation Ivy Bells and How It Was Discovered » accessible via ce lien : https://www.military.com/history/operation-ivy-bells.html

(10) The Russian spy ship stalking Europe's subsea cables, Financial Times, 25 septembre 2025, consulté en octobre 2025, https://www.ft.com/content/0b351091-3f82-4f2f-bef2-a52a35f009f2 ; voir également : 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) Voir par exemple sur ce sujet : 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) D’après l’International Cable Protection Committee (ICPC), il y aurait 150 à 200 problèmes de maintenance par an nécessitant environ trois réparations de câbles par semaine. Voir : 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) Cette citation est traduite de l’anglais ; la citation exacte est la suivante : « EuroQCI aims to develop secure communication networks that will be quantum safe e.g. using Quantum-safe cryptography, thus making it safe against quantum and classical attacks across the whole of the EU and its overseas territories. They will combine terrestrial fibre optic and satellite communication networks. »
Elle est issue de : European Commission et European Space Agency. Commission and European Space Agency Sign EuroQCI Implementation Agreement. Digital Strategy – European Commission, 20 janvier 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/