UQÀM | CHAIRE RAOUL-DANDURAND EN ÉTUDES STRATÉGIQUES ET DIPLOMATIQUES

CHRONIQUES DES NOUVELLES CONFLICTUALITÉS

@Chris Karidis/Unsplash

Câbles sous-marins : de la Baltique à Taïwan, de profondes interrogations

Par Alexis Rapin

Alors que les incidents touchant des câbles internet sous-marins se multiplient, de plus en plus d'États se questionnent sur la résilience de leur connectivité à l'internet global. L'architecture particulière de ces autoroutes de l'information soulève des défis stratégiques encore souvent méconnus.

Le 7 octobre dernier, au moment même où le monde suit avec effroi la vague d'attaques fomentées par le Hamas dans le sud d'Israël, un autre événement inquiétant se déroule en silence dans les eaux froides de la mer Baltique. En l'espace d'une dizaine d'heures, un gazoduc et pas moins de trois câbles internet sous-marins sont subitement endommagés dans les profondeurs séparant la Finlande et l'Estonie. Le gazoduc Balticconnector enregistre une brutale chute de pression, forçant ses opérateurs à fermer les valves pour prévenir d'importantes fuites de gaz. L'un des câbles internet est complètement sectionné, les deux autres significativement endommagés. Dans les pays baltes, la suspicion s'installe rapidement. Alors qu'un dégât isolé peut relever de l'accident, quatre dommages quasi simultanés inspirent bien davantage un acte de sabotage.

Dans les jours qui suivent, les spéculations vont bon train. La Russie, toute proche des eaux concernées, est rapidement désignée comme suspecte potentielle. Le sabotage présumé, dit-on, viserait à punir la Finlande de sa récente entrée dans l'OTAN. Un constat vient toutefois ébranler cette hypothèse : on découvre que parmi les liaisons sous-marines endommagées figure un câble internet russe, opéré par Rostelecom, une compagnie d'État. Entre-temps, d'autres révélations viennent esquisser un scénario inattendu : c'est un navire marchand chinois, le NewNew Polar Bear, qui semble avoir endommagé les quatre infrastructures sous-marines en laissant traîner son ancre dans son sillage. Celle-ci est d'ailleurs repêchée au fond de l'eau par les autorités finlandaises une quinzaine de jours après l'incident.

Le mystère ne fait toutefois que s'épaissir depuis. Alors que le commanditaire ayant affrété la traversée baltique du NewNew Polar Bear s'avère difficile à identifier, le porte-conteneur vient d'entamer une traversée de l'Arctique, direction le Pacifique-Nord, loin de la juridiction des enquêteurs finlandais. Si les experts insistent que les dégâts causés par le navire chinois peuvent difficilement avoir été involontaires, personne ne sait pour l'heure qui exactement aurait ordonné un tel coup d'éclat ni pourquoi.

Un précédent taïwanais

De fait, les raisons qui motiveraient le gouvernement chinois à viser des infrastructures en mer Baltique apparaissent à première vue nébuleuses. Reste qu'un élément de contexte contribue à nourrir les suspicions : un incident passablement similaire à celui du NewNew Polar Bear a déjà été observé plus tôt en 2023. En février dernier, deux câbles internet sous-marins ont été sectionnés au large des îles Matsu, un petit archipel rattaché à Taïwan et situé très proche des côtes chinoises. Pendant près de 50 jours, les 13 000 résidants des Matsu ont dû composer avec une connectivité extrêmement limitée, péniblement assurée par des liaisons satellitaires ou à micro-ondes. Un navire marchand et un chalutier battant pavillon chinois sont suspectés d'avoir causé les ruptures, vraisemblablement en laissant traîner leur ancre ou filet trop près des câbles. Si les autorités de Taipei disent privilégier la thèse de l'accident, nombre d'observateurs sont prompts à y voir une action d'intimidation savamment orchestrée par Pékin.

Volontaire ou non, l'incident des Matsu est pris très au sérieux par les décideurs taïwanais. Alors que près de 95 % des échanges internet mondiaux sont assurés par les câbles internet sous-marins, l'île sinophone ne peut compter que sur 14 liaisons câblées pour maintenir une connexion digne de ce nom à l'internet global. Rompre ces liens paraît, pour une grande puissance comme la Chine, une entreprise aussi réalisable qu'elle serait cataclysmique pour une économie insulaire et connectée comme Taïwan. Un tel scénario, dans un éventuel

contexte de conflit armé, ne serait d'ailleurs pas sans précédent. L'une des premières actions entreprises par le Royaume-Uni en 1914 fut en effet de sectionner les câbles télégraphiques sous-marins reliant l'Allemagne à ses colonies d'outre-mer. Les Ottomans auraient même déployé la tactique plus tôt encore, en coupant un câble télégraphique reliant Odessa à Constantinople pendant la guerre russo-turque de 1877.

Faciles à saboter, plus ardus à réparer

Si les incidents du NewNew Polar Bear et des îles Matsu démontrent une chose, c'est que saboter des câbles sous-marins est hélas étonnement facile et à la portée d'une multiplicité d'acteurs. Nul besoin de sous-marins lourdement équipés ou de nageurs de combat surentraînés ; un navire marchand et son ancre peuvent suffire à endommager sérieusement une telle infrastructure. Comme l'explique Camille Morel, chercheuse en relations internationales à l'université Jean Moulin Lyon III, les câbles internet sous-marins sont essentiellement des tuyaux de quelques centimètres de diamètre, posés (parfois légèrement enterrés) au fond de l'eau, sans guère autre forme de protection que leur inaccessibilité naturelle et la difficulté de trouver leur position exacte. Si les points d'entrée terrestres des câbles sont souvent un peu mieux protégés par les acteurs concernés, l'immensité des distances à couvrir implique généralement que les liaisons ne sont que peu surveillées en haute mer.

En revanche, et c'est là où le bât blesse, réparer ces mêmes câbles s'avère une entreprise délicate. Nécessitant un matériel et un savoir-faire très spécifiques, la restauration de ces liaisons n'est actuellement assurée que par une poignée d'opérateurs privés à travers le monde, tels Global Marine, Subcom ou ASN Marine. En tout et pour tout, il n'existerait actuellement que 60 navires de pose et d'entretien de câbles sous-marins à travers le

@Ibrahim Rifath/Unsplash

monde, contre un total de 485 câbles maritimes déjà existants (avec quelque 70 autres en projet).

Pour Douglas R. Burnett, ancien officier de la marine américaine associé à l'Université Johns Hopkins, garantir la survivabilité des liaisons en contexte de conflit pourrait bien s'avérer un défi de taille :

> Les accords de maintenance des câbliers en temps de paix contiennent des clauses de force majeure qui les excusent en cas de guerre impliquant l'État contractant ou des grandes puissances. Même si les accords devaient être respectés, les procédures normales d'intervention des navires de réparation, telles que le principe coutumier de « premier arrivé, premier servi », seraient dépassées par une situation dans laquelle les belligérants endommageraient de nombreux câbles sous-marins et voudraient tous que leurs réparations soient effectuées en premier. Les câblodistributeurs seront par ailleurs réticents à naviguer dans des eaux contestées où ils pourraient bien constituer des cibles[1].

Pour toutes ces raisons, les États-Unis maintiennent depuis fin 2021 un programme de coopération visant à maintenir en permanence sous pavillon américain deux navires civils pouvant installer, entretenir et réparer des câbles sous-marins, contractuellement engagés à répondre en priorité aux contingences du gouvernement américain.

La géographie toujours têtue

La sécurité des câbles sous-marins soulève donc de profondes interrogations et de nombreux défis. Pour autant, on peut aussi se questionner sur les impacts réels à escompter d'éventuelles ruptures majeures de connexions internet sous-marines. De fait, en dépit de dégâts occasionnés à pas moins de trois câbles immergés dans la Baltique, aucun des pays reliés n'a pour l'heure signalé de baisse de connectivité significative au lendemain de l'incident du NewNew Polar Bear. Certes, des cas de dommages aux câbles ayant occasionné des perturbations majeures de l'accès à internet existent bel et bien, comme l'illustrent des précédents observés au Bangladesh en 2007 ou en Égypte en 2013. Néanmoins, le caractère décentralisé d'internet, l'existence de liaisons câblées terrestres et la redondance de certaines lignes maritimes suggèrent que de nombreux pays semblent actuellement jouir d'une résilience relative en termes de connectivité.

Le cas des îles Matsu, toutefois, démontre parallèlement que cette règle ne s'applique pas partout de manière égale. Les entités insulaires, comme Taïwan, s'avèrent évidemment plus vulnérables à une rupture des liaisons maritimes, de même que certaines régions continentales, mais géographiquement reculées. Au Canada, par exemple, les câbles sous-marins sont actuellement l'option privilégiée afin de connecter le Nunavik ou le Nunatsiavut au réseau internet câblé. Assurer la survivabilité de telles liaisons revêt alors une importance d'autant plus marquée pour les États concernés. Une occasion de plus (s'il en fallait une) de rappeler que le cyberespace, s'il semble avoir aboli les distances et les frontières, n'en reste pas moins intimement lié à la géographie et à ses contraintes.

Alexis Rapin est chercheur à l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand.

Pour en savoir plus sur la Chaire Raoul-Dandurand et ses travaux : https://dandurand.uqam.ca/

[1] Librement traduit par l'auteur.