STRATÉGIE MARITIME – LE RÉSEAU MONDIAL DE CÂBLES SOUS-MARINS : UNE TOILE DANS LA *TOILE*

Camille Morel

Comité d'études de Défense Nationale | « Revue Défense Nationale »

2015/9 N° 784 | pages 117 à 120

ISSN 2105-7508

Article disponible en ligne à l'adresse :

https://www.cairn.info/revue-defense-nationale-2015-9-page-117.htm

STRATÉGIE MARITIME

Le réseau mondial de câbles sous-marins : une toile dans la *Toile*

Nos sociétés ultra-connectées sont aujourd'hui dépendantes d'un réseau de câbles sous-marins qui parcourt le globe, véritable colonne vertébrale du trafic de communications internationales. Contrairement aux idées reçues – notamment sur la place des satellites – les câbles sous-marins représentent en effet 99 % des flux intercontinentaux. Les câbles de cuivre ont servi le télégraphe et le téléphone, la fibre optique garantit désormais le transport continu et massif des données *Internet*. Les individus – dans leurs usages privés – comme les entreprises et les administrations – à des fins de gestion – y recourent de plus en plus massivement sous l'effet, notamment, du *Cloud Computing* [1].

Cette liaison des câbles sous-marins avec la *Toile* les associe désormais au cyberespace, ce qui rend ces infrastructures particulièrement critiques. L'affaire Snowden, en révélant un captage intensif d'informations à partir des infrastructures sous-marines, a souligné mieux qu'un long discours, l'enjeu stratégique des câbles sous-marins.

À l'heure où les États se dotent de services de cybersécurité, leur vulnérabilité doit être prise en compte par l'ensemble des acteurs : les câbles sous-marins sont, et seront, encore davantage à l'avenir une cible de guerre, un outil d'espionnage ainsi qu'un enjeu économique. Ils pourraient également devenir un instrument de terrorisme…

(1) Le *Cloud Computing*, ou informatique en nuage, est un modèle d'accès mettant à disposition un certain nombre de services (capacité de stockage en ligne, transmission de données...).

Une cible de guerre

L'intérêt stratégique des câbles sous-marins de télécommunication a été identifié par les États dès leur naissance, en 1852 : en témoignent les opérations sur les réseaux et infrastructures ennemies en temps de guerre. Car, au-delà d'un outil de puissance diplomatique permettant d'obtenir un pouvoir sur les négociations [2] et sur les colonies, leur emploi lors des conflits s'inscrit dans une stratégie militaire classique. L'objectif consiste, pour chacun des belligérants, à conserver son réseau de communication intact tout en attaquant celui de l'adversaire pour l'endommager, voire le neutraliser. D'ailleurs, le droit international reconnaît officiellement aux belligérants une liberté d'action sur les câbles sous-marins en temps de guerre [3].

La première action de guerre contre les câbles sous-marins a lieu en 1898, lors du conflit hispano-américain. L'objectif pour les États-Unis était d'isoler la métropole ennemie de ses colonies, ce qu'ils atteindront grâce à plusieurs coupures de câbles sous-marins alimentant Cuba et les Philippines, et en se réappropriant la plupart d'entre eux. La clause présente dans le Traité de Versailles, menant à l'administration par les alliés des câbles allemands à la fin de la Première Guerre mondiale, démontre l'importance symbolique accordée par les belligérants à ces systèmes. Le réseau *Sound Surveillance System* (*SOSUS*), installé en partie sur les câbles sous-marins par les Américains au cours de la guerre froide [4] pour espionner l'activité des sous-marins soviétiques en Atlantique, s'inscrit dans une logique d'instrumentalisation des câbles sous-marins en temps de crise.

(2) Voir les cas de coupures britanniques lors de grandes négociations internationales. O. Wachs : « Les câbles sous-marins considérés comme arme de guerre », *Revue maritime*, novembre 1899, p. 423-431, p. 424.

(3) V. Holland : « Des câbles sous-marins en temps de guerre », *Journal de droit international privé*, 1898, Clunet, p. 648-652.

(4) On compte 22 installations en 1974.

Les câbles étant dorénavant au service d'*Internet*, ils constituent plus que jamais une cible de premier ordre, permettant indirectement l'atteinte de sites ou de cœurs névralgiques menaçant les États comme l'ensemble du système international. Ils doivent donc être pris en compte comme des composants essentiels du cyberconflit, en défense comme en attaque.

Ces différents exemples montrent la pertinence actuelle et future de l'outil matériel câblier en dehors même des aspects stratégiques d'écoutes, élément pourtant non négligeable...

Le câble comme outil d'espionnage

Le risque immatériel actuel qui pèse sur les câbles sous-marins est celui d'espionnage par captage direct d'informations. Si cette technique de renseignement n'est pas nouvelle, son actualité a pris une autre teinte avec les différentes révélations de l'affaire Snowden. La mise à jour des programmes *Tempora* ou *Upstream* a permis une prise de conscience : chacun s'est aperçu de la transparence de ses données et surtout de l'accessibilité de celles-ci. Mais les gouvernements avaient dès l'origine compris le potentiel de ces infrastructures comme source de renseignement et se sont efforcés de lancer des écoutes, en matière civile comme militaire. Des programmes majeurs ont notamment été mis en place par les Anglo-Saxons en temps de paix (*Echelon*).

Le renseignement tiré des câbles sous-marins est un atout considérable aujourd'hui, avec l'accès à une information massive en continu, faite de la donnée la plus *lambda* à celle plus rare et stratégique. Ce foisonnement permet une récupération à grande échelle de renseignements clefs pour les États. Le stockage de données dans le *Cloud*, employé par les administrations, les industriels ou les individus, facilite certes l'accès et la préservation de l'information collectée, mais devient surtout un enjeu en termes de connaissance et d'information au service de l'intérêt national. Chacun tente ainsi d'espionner les autres : la presse a récemment révélé plusieurs affaires de ce type avec pour protagonistes les États-Unis, la France [5] ou encore la Nouvelle-Zélande [6]. Car l'espionnage, dans notre ère globale, s'effectue aussi bien sur des terrains classiques que dans le cadre de la guerre économique.

Un enjeu économique

Les conséquences d'un dysfonctionnement momentané des câbles pourraient se révéler dramatiques pour le système économique mondial. Les transactions financières s'effectuant aujourd'hui par cette voie, toute rupture significative de câble engendrerait un ralentissement de l'activité boursière, puis, par effet cumulé, une potentielle crise économique régionale voire mondiale. De manière concrète, les risques associés à la perte de connectivité à *Internet* sont tout aussi importants : les chaînes de production et les services internationalisés s'en trouveraient interrompus. L'activité administrative, comme industrielle, serait paralysée et la perte financière considérable. Une telle situation pourrait entraîner un isolement forcé du pays victime au regard du reste de l'économie. Les deux coupures de câble successives de 2008, en Méditerranée, ont entraîné une perte de connectivité importante à la fois en Égypte (70 % des connexions *Internet* du pays ont été affectées) et dans l'ensemble de la péninsule Arabique, jusqu'à l'Inde (le pays a perdu 40 à 50 % de sa capacité réseau) [7].

(5) Vincent Jauvert : « Comment la France écoute (aussi) le monde », *L'Obs*, juillet 2015 (http://tempsreel.nouvelobs.com/).

(6) « La Nouvelle-Zélande espionne les îles françaises du Pacifique », *Le Monde.fr*, mars 2015 (www.lemonde.fr/).

(7) Laurent Checola et Olivier Dumons : « Qui tire les câbles du cyberespace ? », *Le Monde Magazine*, mars 2009 (www.lemonde.fr/).

Enfin, la question de l'entrée en jeu de grands groupes parmi les acteurs principaux du marché câblier complexifie également la donne économique. Aujourd'hui, détenu par un petit nombre de *carriers*, le marché est étroitement stable et contrôlé. Mais l'enjeu que représente une transmission efficace des données à l'heure d'une activité continue sur la *Toile* pour les géants de l'*Internet* comme *Google*, *Facebook* ou *Microsoft*, les encourage à se tourner vers ce secteur pour investir dans un réseau indépendant. Cette entrée en lice modifierait à leur profit les rapports établis jusqu'alors.

Si la déstabilisation de l'équilibre international peut être engendrée par une rupture de câble, il importe de rester vigilant en cas de menace terroriste.

Un terreau terroriste ?

Des dégradations malveillantes peuvent être réalisées sur les câbles sous-marins pour des raisons militaires, économiques, privées ou encore politiques. Aujourd'hui se fait jour un nouveau phénomène : celui du pillage de câbles sous-marins à des fins économiques, *a priori* privées. Au large du Vietnam, des pêcheurs locaux ont ainsi volé une section de câble en 2007, tentant de tirer profit du matériel dérobé. Une série de coupures de câbles intercontinentaux atterrissant en Californie a eu lieu en juin 2015, perturbant le réseau de San Francisco jusqu'à Seattle. Soupçonnant une action coordonnée, le *FBI* vient d'ouvrir une enquête sur ces mystérieuses ruptures. Principale crainte : des intentions terroristes, qui, bien qu'encore jamais réalisées à ce jour, apparaissent aujourd'hui crédibles.

Les menaces pourraient peser aussi bien sur les câbles en haute mer que sur les zones d'atterrissement ainsi que sur tous les centres névralgiques aujourd'hui indispensables pour relier les différents continents. Le canal de Suez en est un bon exemple. Il concentre une forte densité de câbles dans un contexte peu sécurisé (peu de profondeur) et soulève la problématique sécuritaire de l'*Egyptian Bypass*.

Cette anticipation est d'autant plus importante que la prise en compte par le droit de ce type d'actes terroristes n'est pas satisfaisante. Pourtant, après les voies aériennes – détournement d'avions – et les voies terrestres – attaque au sein des infrastructures ferroviaires – la voie maritime, par ses infrastructures câblières sous-marines, pourrait tout autant devenir une cible du terrorisme...

Conclusion

En dehors des aspects purement stratégiques, et des enjeux économiques et terroristes qui s'y associent, les câbles sous-marins sont désormais intimement liés aux notions d'accès à l'information et à l'idée de transparence. Leur rôle est primordial dans l'ouverture des sociétés au monde. Pourtant, plusieurs événements récents semblent corroborer l'hypothèse selon laquelle le câble sous-marin peut aussi apparaître comme un outil limitatif des libertés publiques, à la disposition notamment des régimes autoritaires : le cas syrien est révélateur d'un tel emploi liberticide. Plusieurs coupures d'*Internet* dans le pays, en novembre 2012 et mai 2013, laissent en effet supposer une action délibérée de l'État sur le système câblier pour contrôler le flux d'informations et l'accès à *Internet* de sa population [8].

La question du contrôle des données relatives aux citoyens, et donc la préservation de la liberté privée, est un autre défi posé par les câbles sous-marins. L'affaire de la *Team Telecom* – cellule spéciale américaine mise en place pour obtenir un contrôle quasi-total des points d'accès aux zones d'atterrissement –

(8) Dominique Boullier : « *Internet* est maritime : les enjeux des câbles sous-marins », *Revue Internationale et Stratégique*, 2014/3, n° 95, p. 149-158, p. 155.

est l'illustration de l'emploi fait, par les services de sécurité nationaux, des câbles sous-marins à des fins de récoltes massives d'informations sur les individus. La mainmise des entreprises privées du secteur – comme *Google* – sur les câbles sous-marins pose le même défi éthique, autorisant indirectement leur ingérence complète dans les données transportées.

Les câbles sous-marins représentent donc un véritable défi au regard des libertés publiques et le seront davantage dans les années à venir, dans la mesure où ils sont intimement reliés aux régimes politiques des États, aux intérêts économiques ainsi qu'à la cyberstratégie.

Camille Morel

ASP - Chargée d'études au CESM

BIBLIOGRAPHIE COMPLÉMENTAIRE

Douglas R. Burnett, Mick P. Green : « *Security of international submarine cable infrastructure: time to rethink?* », *Legal Challenges In Maritime Security*, Leiden, 2008, p. 557-583.

Centre d'études stratégiques de la Marine : *Abysses, Études Marines*, Paris, juin 2015, n° 8, p. 54.

Tara Davenport : « *Submarine communication cables and law of the sea* », *Ocean Development and International Law*, 2012, vol. 43, p. 201-242.

Claude Delesse : Echelon *et le renseignement électronique américain* ; Éditions Ouest-France, collection Espionnage, 2012, 176 pages.

Michel Voelckel : « Des mots sous la mer : à propos de la convention de Paris du 14 mars 1884 pour la protection des câbles sous-marins », *Annuaire du droit de la mer*, Pedone, Paris, 2012, p. 269-276.