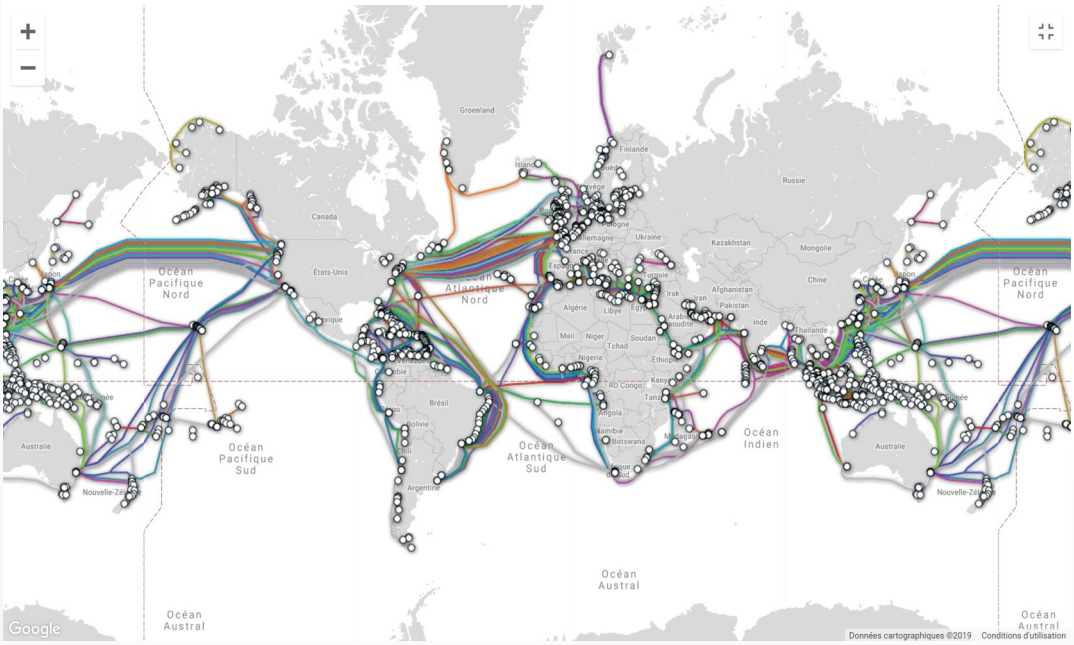
BRENNUS 4.0

LETTRE D'INFORMATION DU CENTRE DE DOCTRINE ET D'ENSEIGNEMENT DU COMMANDEMENT

Mars 2020

Câbles sous-marins : entre vulnérabilité et enjeu stratégique

Par le commandant Hélène Gorbéna, officier stagiaire de l'EMSST



(source : www.submarinecablemap.com – carte des câbles sous-marins au 30 décembre 2018)

Depuis les attaques informatiques majeures qui ont marqué les esprits, (*Soldat de Bronze* en Estonie en 2007, *Stuxnet* en Iran, découvert en 2010, ou encore *Wannacry* qui a touché près de 200 000 entités à travers le monde en 2016), la cybersécurité est aujourd'hui un sujet de préoccupation croissante. L'augmentation significative d'attaques, majoritairement liées au monde de la cybercriminalité mais également aux États, est observée. Ainsi, de nombreuses solutions de protection, d'anticipation de la menace, de détection, d'anti-virus ou autres anti-spywares sont proposées par des sociétés qui se bousculent pour occuper une place sur ce marché prometteur. Cependant, la protection logicielle est incomplète sans protection physique. Il existe en effet plusieurs façons de voler, modifier voire supprimer des données, dès lors que l'attaquant dispose d'un accès physique au support de ces données. De même, il est vain de protéger des systèmes, si l'espion se place en amont des dispositifs de protection pour intercepter les données. Le chiffrement qui, seul, peut compliquer voire empêcher l'exploitation des données, les sécurise momentanément, jusqu'à ce que les algorithmes employés soient cassés, ce qui n'est qu'une question de temps et de puissance de calcul. Or, non seulement les flux sont encore trop peu chiffrés, mais ils transitent par des câbles sous-marins qui sont une partie de l'architecture physique de l'Internet et permettent à un attaquant d'accéder, non sans difficulté logistique, aux flux de données mondiaux, en amont de tous les systèmes de protection logicielle. Ils présentent donc des vulnérabilités qu'il est important de connaître afin de tenter de se prémunir de leur altération, voire de leur exploitation à des fins malveillantes. Au-delà de ces faiblesses, ils représentent un enjeu de puissance pour les États soucieux de préserver leur souveraineté.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES ARMÉES
Armée de Terre

SI VIS PACEM PARA BELLUM

Le monde entier connecté par les fonds marins

Les câbles sous-marins tapissent le fond des mers et des océans depuis le XIXe siècle et sont encore méconnus du grand public. Or, contrairement à une idée encore assez répandue, seul 1% du trafic d'Internet transite par les réseaux satellitaires. Les 99% des flux de données restants passent par ces câbles. Depuis la pose du premier câble télégraphique entre la France et l'Angleterre en 1851, leur nombre a augmenté de façon exponentielle. Le site « submarinecablemap.com » recense plus de 430 câbles en 2018 qui transportent données et/ou énergie au moyen de différentes technologies, la fibre optique étant aujourd'hui massivement utilisée pour les télécommunications. Les câbles combinent, en effet, de nombreux avantages comparativement aux satellites : des coûts bien moindre, permettant de proposer des tarifs compétitifs, des débits et qualités de transmission élevés, une durée de vie importante[2]. Il faut toutefois reconnaître quelques désagréments à ce réseau sous-marin. Si sa localisation rend difficile son accès à des fins malveillantes, il en est de même pour la pose et surtout l'entretien. En effet, ces opérations sont réalisées par des navires câbliers, majoritairement privés. Le marché du câble sous-marin est tenu par quelques grands groupes. Entre autres la société française Nexans, dont la filiale norvégienne est spécialiste de la fabrication du câble sous -marin. Le groupe Orange Marine détient 15% du marché avec 6 navires câbliers opérant à travers le monde et 450 000km de câbles posés. Ce dernier fait principalement face à la concurrence des Etats-Unis (Subcom), de la Grande Bretagne (Global Marine Systems Limited) du Japon (NEC) et, dans une moindre mesure, de la Chine (Huawei). Orange Marine s'est notamment lancée, en coopération avec PCCW global, division de l'agence de télécommunications de Hong Kong, dans un projet de câble de 12 000 km appelé PEACE, qui tracera en 2020 la route la plus courte entre la Chine et l'Europe, via le Pakistan, le Kenya, Djibouti et l'Egypte[3].

La pose et l'entretien d'un câble sont des opérations complexes. Le câble est tout d'abord embarqué sur le câblier, enroulé dans des cuves et préalablement équipé des répéteurs de signal qui sont disposés tous les 50 à 100km et assureront le maintien de la force du signal. Selon le type de fond et la fréquentation du site, le câble pourra être simplement posé ou bien ensouillé dans une tranchée creusée par une charrue équipant les câbliers. Cette technique, qui permet une meilleure protection du câble, rend leur entretien plus complexe. Lorsqu'il faut réparer ou changer une portion de câble endommagé, une fois le câble concerné repéré, le câblier utilise, par fond faible, un système de grappin pour tenter de le remonter. Lorsque le fond est trop important ou que le câble est ensouillé, la mise en œuvre d'un engin submersible s'avère nécessaire. Là encore se développe un marché qui offre des perspectives tout aussi intéressantes qu'inquiétantes. Enfin, lorsque le câble rejoint la terre, il le fait via un point d'atterrissement. Généralement, le câble passe sous une plage et aboutit dans une chambre de câblage, le plus souvent semi-enterrée, où se fait le raccordement au réseau terrestre[4]. Ces sites sont peu connus mais également peu protégés. Les câbles disposent donc de vulnérabilités intrinsèques qu'il convient de détailler.

(source : http://la-story.over-blog.com/2018/11/cable.html)

Des vulnérabilités critiques

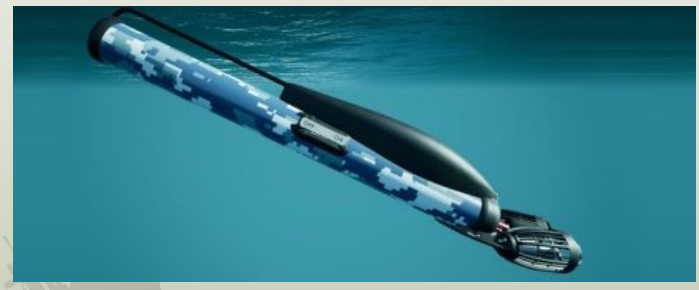
En juillet 2018, le gouvernement japonais a mis à jour sa stratégie de cybersécurité, appelant au renforcement de la protection de l'infrastructure physique de l'accès à Internet, notamment celle des câbles sous-marins. La dépendance d'un pays insulaire comme le Japon à cette infrastructure est extrême. Elle a été rendue encore plus évidente à la suite du tremblement de terre et au tsunami de 2011 qui ont endommagé un grand nombre de câbles, nécessitant notamment le report du trafic de l'Est du pays vers l'Ouest[5]. Le fond marin lui-même est donc l'une des premières faiblesses des câbles, les éruptions volcaniques ou tremblements de terre sous-marins n'étant pas rares. Les morsures de requins, apparemment anecdotiques, contribuent également, mais moins significativement que les activités de pêche (pose de filets ou ancrages), à endommager régulièrement les câbles[6]. Pour coûteuses que soient ces menaces naturelles ou fortuites – elles représentent l'immense majorité des problèmes décelés -, elles ne sont pas les plus préoccupantes. En effet, les câbles peuvent être convoités par des pirates intéressés par la revente du câble lui-même. Ainsi, en 2007, au Vietnam, 500km de câbles ont été dérobés, causant une coupure de l'Internet au niveau national. Le sabotage est également une cause de dégradation récurrente, notamment en Afrique. Le Gabon a ainsi été coupé

du monde pendant 4 jours en 2015 à la suite de la coupure volontaire du câble Sat3 reliant la côte Ouest de l'Afrique à l'Europe. Au-delà des câbles, les parties émergées du réseau peuvent être la cible d'attaque. Ainsi, fait encore rarissime aujourd'hui, un navire câblier a fait l'objet d'un assaut de la part de la piraterie locale alors qu'il posait du câble en mer Rouge en 2015. Par ailleurs, les points d'atterrissement sont un autre point de vulnérabilité majeure, par leur nombre limité et leur faible niveau de protection physique. Enfin, l'espionnage, par l'intermédiaire des fonds marins, n'est pas un phénomène nouveau. Déjà en 1971, les Etats-Unis avaient notamment pu collecter du renseignement en « écoutant » le câble servant aux communications de la flotte soviétique dans le Pacifique, dans le cadre de l'opération Ivy Bell[7]. Il faut également rappeler les manœuvres préoccupantes du bâtiment de recherche océanographique (ou en tout cas déclaré comme tel) russe *Yantar* à proximité des câbles sous-marins, relevées en 2015. Tout ceci fait ressurgir des images dignes de la Guerre Froide. Ainsi donc, dans le contexte multipolaire dans lequel nous nous trouvons aujourd'hui, entre dépendance économique exponentielle aux flux de données, menaces terroristes et attaques informationnelles, les risques qui pèsent sur l'infrastructure de l'Internet sont croissants, les câbles sous-marins et les données qui y transitent représentent des enjeux de puissance pour les États.

(source : https://www.marinetraffic.com/fr/ais/details/ships/shipid:1215053/vessel:YANTAR)

Enjeu de puissance et quête de souveraineté numérique

À la suite des révélations d'Edward Snowden à l'occasion de l'ouverture du sommet « NET mundial » en 2014, la présidente du Brésil Dilma Roussef a appelé à un changement de gouvernance de l'Internet afin de sortir de la tutelle des États-Unis. Elle a concrétisé par la suite cette volonté en signant un accord de coopération avec l'Union Européenne comprenant notamment la mise en place d'un câble sous-marin direct entre le Brésil et l'Europe[8]. Il s'agit d'un projet parmi de nombreux autres qui tendent à garantir, à des États inquiets de l'omniprésence des États-Unis dans toutes les instances de gestion et de décision, une maîtrise plus importante de leurs flux de données. Cette problématique s'impose aux États dont l'accès à Internet est garanti par une faible variété de câbles. C'est le cas de nombreux pays africains ou encore du Liban[9]. Les moyens de pression et les capacités d'écoute qui en découlent conduisent les États à rechercher la diversification de leurs moyens d'accès à Internet. En France, le problème se pose de façon différente, car si la métropole dispose de plusieurs points d'atterrissement et d'arrivée de câbles, elle est confrontée, au travers de sa Zone Économique Exclusive de 11 millions de km² (la deuxième en superficie après celle des États-Unis) et de ses départements, territoires et collectivités d'Outre-Mer, à une diversité de situations, d'interconnexions et de partenariats importante. En conséquence, la France doit s'intéresser à la quasi-totalité des « routes » des câbles pour assurer à ses citoyens d'Outre-Mer, l'accès à l'Internet. On peut également imaginer que la protection de ces câbles se jouera sous la mer au moyen, entre autres, de drones sous-marins. De nombreux industriels se sont lancés dans la course au développement de ce type d'engins. Thalès et Aquabotix travaillent ainsi sur un projet commun de drone sous-marin multi-fonctions[11]. Enfin, si les câbles suivent aujourd'hui les mêmes routes que les câbles télégraphiques d'il y a 100 ans, car les détroits par lesquels passe le trafic maritime commercial n'ont pas changé, le réchauffement climatique et la fonte des glaces sont en passe d'ouvrir de nouvelles voies plus courtes mais également moins vulnérables aux risques naturels et accidentels. C'est un sujet qui intéresse, entre autres, la Russie car elle est aujourd'hui fortement dépendante des câbles terrestres qui transitent par d'autres États, ou encore la Chine, qui est aussi en recherche de voies alternatives au même titre que son projet de « Route de la Soie numérique ».



(Source : https://subseaworldnews.com/2018/12/21/thales-and-aquabotix-team-up-on-subsea-drones/)

Perspectives

En 2017, le satellite Russe Louch-Olymp s'est approché de façon très suspecte du satellite franco-italien de communications sécurisées Athena-Fidus. Révélé en septembre 2018 par la ministre des Armées Florence Parly, qui a alors nommément accusé la Russie de tentative d'espionnage[12], cet évènement montre que même les vecteurs de communication supposés inaccessibles sont aujourd'hui visés. Au-delà de la protection de l'infrastructure, c'est bien la protection des données sensibles qui est au cœur des préoccupations. La complémentarité des mesures de protection est donc à rechercher, notamment par la généralisation du chiffrement. En France, la loi n°2004-575 du 21 juin 2004 autorise l'utilisation des moyens de cryptologie[13]. Tout citoyen peut donc librement chiffrer ses données en utilisant des logiciels de chiffrement, des disques et supports amovibles ou des fichiers qui deviennent simples d'emploi, gratuits et accessibles à tous. De plus, il existe des protocoles qui chiffrent les données lorsqu'elles circulent sur les réseaux (IPSec, TLS) ou lorsque la requête web quitte le navigateur (HTTPS). Ces méthodes de chiffrement des communications sont encore méconnues et trop peu utilisées par le grand public, ce qui rend les flux vulnérables à l'interception. De plus, dans ce domaine comme dans celui des câbles ou des satellites, pour les États il est tentant de développer leurs propres algorithmes afin de s'assurer de l'absence de « *backdoors* » (ou portes dérobées), potentiellement insérées dans le code par des agences de renseignement[14]. C'est également ce qui conduit certains pays à se lancer dans le développement d'un « *cloud* souverain » afin de garantir le stockage des données de leurs citoyens sur leur propre sol. La Russie construit ainsi d'immenses *data-centers* en Sibérie[15]. Enfin, l'étude d'une stratégie de routage des paquets de données[16] qui garantirait, par exemple, que les données en provenance et à destination d'un même pays ne transitent pas par un autre pays, est également une piste étudiée par certains États.

(Source : http://www.comptoir-hardware.com/actus/software-pilotes/36829-des-backdoors-a-gogo-sur-les-routeurs-cisco-.html)

Pour conclure, il ressort que les câbles sous-marins sont un sujet essentiel car les vulnérabilités sont nombreuses et les menaces concrètes. Ils représentent un enjeu critique, les États étant fortement dépendants du bon fonctionnement des réseaux et de l'intégrité des données qui y circulent. Ils sont donc une composante physique qu'il est essentiel de surveiller et de protéger afin d'en limiter les vulnérabilités. À la lumière des luttes d'influence qui se jouent dans le cyberespace, la protection des données sensibles et la souveraineté numérique sont également des enjeux majeurs dont les câbles sous-marins ne représentent qu'un volet.

———————

[1] Louis Pétiniaud, *Cartographier l'affaire Snowden*, Hérodote N°152-153, 2014

[2] http://www.cablesm.fr/2009_C_10-01_cle2c7389.pdf

[3] https://subseaworldnews.com/2018/12/21/pccw-global-and-orange-to-land-peace-cable-in-france/.

[4] http://ifmer.org/assets/documents/files/documents_ifm/Les-cables-sous-marins-et-les-navires-cabliers.pdf

[5] Motohiro Tsuschya - https://www.asiaglobalonline.hku.hk/undersea-cables-cyberspace-stability-security/

[6] Camille Morel, *Menace sous les mers : les vulnérabilités du système câblier mondial*, Hérodote N°163, 2016

[7] http://www.opex360.com/2015/10/27/que-font-les-navires-russes-pres-des-cables-marins-utilises-pour-les-telecommunications/

[8] Frédérick Douzet, *La géopolitique pour comprendre le cyberespace*, 2014

[9] Jérémy Robine et Kavé Salamatian, *Peut-on penser une cybergéographie ?,* Hérodote N°152-153, 2014

[10] http://www.opex360.com/2018/12/11/comment-la-marine-nationale-surveille-les-cables-sous-marins-de-

communication/

[11] https://subseaworldnews.com/2018/12/21/thales-and-aquabotix-team-up-on-subsea-drones/

[12] https://www.lemonde.fr/international/article/2018/09/07paris-revele-une-tentative-d-espionnage-russe-sur-un-satellite-franco-italien-en-2017_5351908_3210.html

[13] Myriam Quéméner, *Le droit face à la disruption numérique*, Gualino, 2018

[14] https://www.lemondeinformatique.fr/actualites/lire-la-securite-absolue-n-existe-pas-retour-sur-7-backdoors-63787.html

[15] Frédérick Douzet, Kévin Limonier, Jérémy Robine, Kavé Salamatian, Rémi Géraud, Romain Campigotto, *Les nouveaux territoires stratégiques du cyberespace : le cas de la Russie,* Stratégique N°117, 2017

[16] http://reseaux.blog.lemonde.fr/2012/11/04/routage-enjeu-cyberstrategie/