dimanche 25 août 2013

Les câbles sous-marins, clé de voûte de la cybersurveillance

Maxime Vaudano

Pour se figurer l'espionnage des télécommunications, la première image qui vient à l'esprit est celle de "grandes oreilles" interceptant à la volée les signaux satellite parcourant le monde. Popularisée par la guerre froide et son décorum, cette représentation est pourtant depuis longtemps dépassée.

Depuis les années 1990, l'écrasante majorité des télécommunications mondiales emprunte en effet les quelques 250 câbles sous-marins qui sillonnent le globe de long en large. "Dans un monde où chaque milliseconde compte, l'aller-retour vers les satellites représente une perte de temps inutile", explique Benjamin Bayart, spécialiste des télécommunications et porte-parole du fournisseur d'accès à Internet associatif FDN. À tel point que 99 % du trafic intercontinental, Internet comme téléphone, transite aujourd'hui sous les océans, selon Tim Stronge, vice-président du centre de recherche Telegeography.

Un basculement confirmé par les révélations de l'ex-consultant du renseignement américain Edward Snowden sur la cybersurveillance exercée par les États-Unis et leurs partenaires. Si l'Agence de sécurité nationale américaine (NSA) parvient à espionner la quasi-totalité de nos communications, ce n'est ni grâce aux satellites, ni même grâce au programme Prism, qui lui donnerait accès aux serveurs des Facebook, Microsoft et autres Google – ce que ces entreprises démentent catégoriquement. C'est en s'attaquant directement au "backbone", la colonne vertébrale de l'Internet.

Les plages britanniques, pivots du réseau mondial

Connectez-vous à un site hébergé aux États-Unis ou envoyez un e-mail au Brésil, et soyez certain que les paquets d'informations qui transporteront votre requête passeront à un moment ou à un autre par l'un de ces "tuyaux" de l'Internet, propriétés de géants comme Vodafone, Verizon ou Orange.

Représentation géographique schématique d'une connexion au site de la Maison Blanche depuis Paris, avec l'outil Visual Trace Route.

Or, la configuration du réseau fait du Royaume-Uni une plaque tournante des télécommunications mondiales. Sur son territoire, en contact avec 49 des 265 câbles sous-marins en service dans le monde, transite la quasi-totalité des échanges Europe-Amérique. Sans compter que les voies impénétrables de l'Internet peuvent parfois relier la France à la Russie en passant l'Atlantique... Peu étonnant, donc, que la NSA ait chargé son allié britannique d'espionner ces très riches tuyaux qui émergent dans l'une des 71 stations britanniques d'atterrissage des câbles.

Le réseau des câbles sous-marins

>>cliquez pour voir la carte en plus grand

Le programme "Tempora", mis au jour le 21 juin par The Guardian, autorise l'agence de renseignement électronique britannique, le GHCQ, à surveiller l'ensemble des communications transitant par les câbles de sept grands opérateurs télécom mondiaux, parmi lesquels British Telecom, Verizon, Vodafone ou Level 3. Comme le montre (en rouge) la carte ci-dessus, les alliés américains et britanniques ont donc théoriquement accès à près du quart du réseau mondial avec ce seul programme.

Un matériel disponible sur le marché

Si, comme le rappelle le site spécialisé PCPro [en anglais], l'espionnage pirate des câbles sous-marins ne présente pas d'insurmontables difficultés, les services secrets britanniques n'ont pas eu à se donner cette peine. Grâce à une disposition obscure d'une loi datant de 2000, les opérateurs télécom sollicités par le gouvernement britannique sont forcés de coopérer à la

surveillance – et empêchés d'en parler publiquement.

Reste à installer dans les stations d'atterrissage des câbles un système de "tapping", qui permet de copier l'intégralité des données en circulation sur les fibres optiques, de façon quasiment indétectable. Le matériel décrit par Edward Snowden semble correspondre en tous points à celui que fournit l'entreprise américaine Glimmerglass, comme le remarque l'organisme de recherche CorpWatch. Présenté comme une "solution de lutte contre le cybercrime et le cyberterrorisme", le "CyberSweep" serait capable de récupérer les métadonnées, voire le contenu des emails, chats et conservations Facebook, comme l'indique un document promotionnel révélé par Wikileaks.

Ce type de matériel serait installé dans les grands nœuds du réseau Internet, comme la station d'atterrissage de Bude, sur la côte occidentale du Royaume-Uni, utilisée selon Edward Snowden comme "laboratoire" du GCHQ pendant trois ans. Accueillant pas moins de 6 câbles, Bude disposerait, selon les estimations de Teleography, d'une bande passante supérieure à 7 téraoctets par seconde, soit un peu moins de 10 % du trafic international.

Pour ne rien gâcher, elle est située à quelques jets de pierre d'une station d'interception du GHCQ. Autrefois spécialisée dans la surveillance des signaux satellites, celle-ci a pu être remise au goût du jour à l'aide de la "subvention" de 15,5 millions de livres (17,8 millions d'euros) que lui a accordée la NSA pour son "réaménagement", selon un autre document révélé par Edward Snowden.

Impossible de le vérifier, puisque l'accès au complexe où atterrissent les câbles est interdit, comme l'a constaté Andrew Blum, auteur de *Tubes. A Journey to the Center of the Internet : "En deux ans d'enquête, c'est l'un des rares lieux du réseau auxquels je n'ai pas eu l'autorisation d'accéder."* Même Orange (ex-France Telecom), copropriétaire d'un des câbles passant par Bude, explique *qu'aucun opérateur ne peut savoir ce qui se passe dans ces stations*.

Les câbles, enjeu géopolitique

Pour les agences de renseignement, la méthode du *"tapping"* revêt une importance déterminante. Elle est largement complémentaire de programmes comme Prism, cantonnés aux données que vous déposez "volontairement" sur les serveurs des géants du Web. Schématiquement, à défaut de vous forcer à vous arrêter à toutes les aires d'autoroute pour ouvrir discrètement votre coffre (vos données), la NSA et le GCHQ flashent tous les dix kilomètres l'ensemble des plaques d'immatriculation circulant sur l'autoroute, pour reconstituer a posteriori votre trajet – des *métadonnées* qui en disent déjà assez long sur vous.

On comprend donc pourquoi les gouvernements s'intéressent d'aussi près aux câbles sous-marins intercontinentaux. Le savoir-faire du français Alcatel Submarine Networks (ASN), l'une des rares entreprises mondiales à maîtriser leur fabrication, a été qualifié en janvier dernier de "stratégique" par la ministre de l'économie numérique, Fleur Pellerin.

Aux États-Unis, l'administration a tout bonnement mis sur pied une *"team telecom"* chargée de s'assurer que les principaux câbles de l'Atlantique et du Pacifique restent sous contrôle américain, comme le racontait en juillet The Washington Post. En début d'année, leur lobbying a notamment permis de faire capoter le déploiement d'un nouveau câble transatlantique, fabriqué par le chinois Huawei. Jugée trop proche du gouvernement chinois, l'entreprise risquait, selon les Américains, d'espionner ce nouveau câble New York-Londres pour le compte de Pékin.

Maxime Vaudano, le 23/08/2013- Le Monde.fr

1- **Le chiffrement HTTPS, une protection suffisante pour les données ?**

Théoriquement, la plupart des informations sensibles qui circulent sur le réseau sont chiffrées grâce à la méthode HTTPS, qui empêche aux yeux indiscrets de consulter le contenu de ce qu'ils ont intercepté. C'est notamment le cas des transactions par carte bancaire, ou de Gmail et Facebook, où le HTTPS est activé par défaut. Les espions peuvent néanmoins consulter les métadonnées des communications, comme par exemple l'adresse du site visité.
La présence de ce garde-fou est signalée dans les barres d'adresse des

navigateurs par l'ajout d'un "s" après le traditionnel "http", et certains mini-programmes permettent d'en systématiser l'utilisation. Toutefois, rien n'empêche théoriquement les sites que vous visitez de fournir directement à la NSA la clé de chiffrement, pour lui permettre de décoder facilement vos communications. C'est notamment ce qu'aurait fait Microsoft pour sa messagerie en ligne Outlook, selon The Guardian.

Enfin, comme l'explique Benjamin Bayart, *"les grandes puissances de calcul dont on dispose aujourd'hui peuvent venir à bout du chiffrement HTTPS en un temps limité, de l'ordre de quelques semaines, en essayant une à une toutes les combinaisons possibles"*.

2- **Note NDÉ :** Source du logo de l'article : http://www.telegeography.com/page_attachments/products/website/telecom...

http://www.lemonde.fr/technologies/article/2013/08/23/les-cables-sous-...
http://www.lemonde.fr/technologies/article/2013/08/23/les-cables-sous-marins-cle-de-voute-de-la-cybersurveillance_3465101_651865.html

http://www.legrandsoir.info/les-cables-sous-marins-cle-de-voute-de-la-cybersurveillance.html