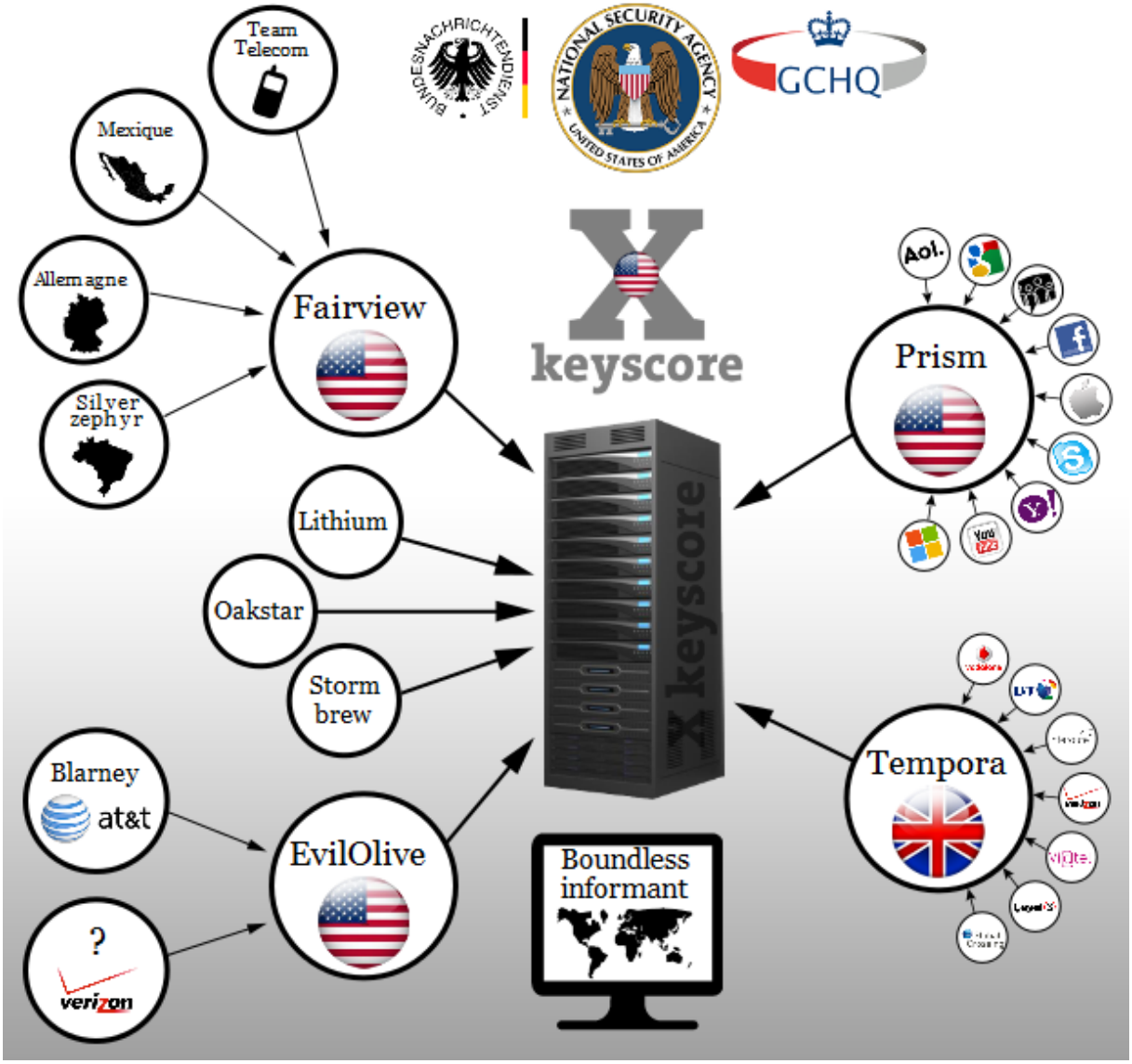
Plongée dans la "pieuvre" de la cybersurveillance de la NSA

Le Monde.fr | 27.08.2013 à 15h59 | Par Maxime Vaudano

Au fil des révélations, les documents de l'ancien consultant de la NSA Edward Snowden dressent le portrait complexe de l'écosystème de la cybersurveillance américaine, piloté par la toute-puissance Agence de sécurité nationale (NSA). Deux méthodes sont utilisées pour collecter les informations : l'accès direct aux serveurs des grandes entreprises du net ("back door") et la surveillance directe des infrastructures où transitent quotidiennement les communications ("upstream").



Légende :

L'Agence de sécurité américaine (NSA)

La plus grande agence de renseignement américaine, créée en 1952, est chargée de surveiller les communications électroniques et de prévenir les menaces extérieures contre les Etats-Unis. A ce titre, elle n'est a priori pas censée surveiller les communications des Américains.

L'unité "Special Source Operations" de la NSA, présentée par Edward Snowden comme le "joyau de la couronne", est à l'origine de l'ensemble des programmes présentés dans cette infographie – à l'exception notable de Tempora, piloté par le GCHQ, son proche allié britannique.

Qui contrôle la NSA ? Le Foreign Intelligence Surveillance Act (FISA) de 1978 a mis en place la Foreign Intelligence Surveillance Court (FISC) pour contrôler les activités de surveillance. Pour toute écoute, la NSA est censée obtenir un mandat de la FISC, qui doit en retour vérifier que l'agence n'outrepasse pas la loi. Toutefois, son président a reconnu dans une interview au *Washington Post* ne pas disposer des moyens suffisants pour exercer sa mission de contrôle.

Qui a accès aux données ? 850 000 employées et contractuels de la NSA possèdent l'accréditation top secret, ce qui pourrait théoriquement leur donner accès à au moins une partie des données collectées par l'agence. Le journaliste Glen Greenwald a ainsi assuré que "même les analystes NSA du bas de l'échelle" avaient la possibilité d'accéder aux données privées.

Parmi les clients de choix des programmes de la NSA figurent également le FBI (sécurité intérieure), la CIA (renseignement extérieur) et le ministère de la justice américain. Les autres agences de renseignement fédérales, spécialisées par exemple dans la lutte contre les drogues ou les cyberattaques, peuvent également formuler des demandes pour accéder à ces informations. Mais elles se plaignent depuis plusieurs années du fort taux de refus qu'on leur oppose, et de la mainmise des grandes agences sur ces données, selon le *New York Times*.

Le Government Communications Headquarters

Créée après la première guerre mondiale, cette agence spécialisée dans le renseignement électronique est l'équivalent britannique de la NSA. Très proche de sa grande sœur américaine, elle reçoit de sa part une importante subvention annuelle.

Responsable de la mise en œuvre du programme Tempora, le GCHQ pourrait en contrepartie accéder à une partie des données de la NSA. Selon *The Guardian*, 60 % du renseignement britannique vient en effet de la NSA. *Der Spiegel* a également rapporté que des agents du GCHQ avaient formé leurs homologues allemands du BND à l'utilisation du logiciel XKeyScore, ce qui laisse penser qu'ils y ont accès.

Enfin, des documents fournis par Edward Snowden montrent que le GCHQ a accès aux données collectées par le programme PRISM depuis juin 2010.

La réponse du GCHQ : l'agence s'est contentée d'assurer qu'elle se conformait à la loi.

Le Bundesnachrichtendienst (BND)

L'agence de renseignement extérieure allemande est un partenaire de la NSA, alors même que l'Allemagne est l'une de ses cibles prioritaires.

D'après *Der Spiegel*, le BND utilise le logiciel XKeyScore "à petite échelle" depuis 2007, dans la base de la NSA située à Griesheim, sur le territoire allemand. Le BfV, l'agence de renseignement intérieur, a également utilisé le logiciel "afin d'augmenter ses capacités de support de la NSA dans des actions antiterroristes conjointes".

La réponse du BND : l'agence a assuré n'avoir "aucune information" sur la collecte de données personnelles de citoyens allemands en Allemagne par la NSA, et a refusé de commenter l'utilisation de XKeyScore.

XKeyScore

Cet acronyme au nom barbare désigne ce qui apparaît comme l'outil central du système de renseignement américain, permettant d"examiner "quasiment tout ce que fait un individu sur Internet". C'est vraisemblablement le système que les analystes de la NSA utilisent le plus souvent pour leurs recherches.

A en juger par les documents publiés par *The Guardian*, XKeyScore s'apparente à un véritable Google pour espions, alimenté par les données des différents programmes de

surveillance liés à la NSA. Celles-ci sont conservées trois à cinq jours, et jusqu'à plusieurs années pour les plus importantes. D'après *Der Spiegel*, des fonctionnalités importées du monde du jeu vidéo ont été implémentées dans le logiciel, comme les "points d'expérience" ou le "déblocage de missions".
La force de ce système réside dans le croisement puissant des différentes bases de données, et la possibilité de rechercher rétrospectivement des informations sur un individu qui n'était nullement suspect au moment où l'on a collecté ses données.
Selon les documents, 700 serveurs répartis dans 150 sites de par le monde ont accès à XKeyScore :
Le journaliste Marc Ambider, co-auteur d'un livre sur la sécurité nationale américaine, a expliqué sur son blog que deux autres sources de données étaient compilées dans XKeyScore :

- Les écoutes d'ambassades et de gouvernements étrangers mises en place par le Special Collection Service, une unité spéciale conjointe de la CIA et de la NSA
- Les renseignements collectés par les interceptions sur les satellites étrangers

* Précision : si les diapositives mises en ligne par *The Guardian* montrent que XKeyScore est capable de lire le contenu des courriels et des messages privés Facebook, la généralisation depuis 2010 de la technologie de chiffrement HTTPS rend aujourd'hui cette collecte théoriquement impossible. Selon toute vraisemblance, seules les métadonnées des communications (expéditeur, destinataire, date) sont aujourd'hui collectées – à moins de consacrer plusieurs semaines de calcul à briser la protection pour "ouvrir" le contenu des communications.

Fairview

Fairview est un "programme parapluie" destiné à "contrôler Internet", selon Thomas Drake, un ancien haut responsable de la NSA. Il regrouperait divers programmes américains de surveillance, dont le point commun est la portée internationale :

- Des partenariats avec l'Allemagne et le Mexique pour espionner les communications sur leur territoire
- Le programme Silverzephyr, qui intercepte les communications au Brésil
- Plusieurs programmes d'interception dans les autres pays d'Amérique Latine (Colombie, Venezuela, Brésil, Mexique, Argentine, Aquateur, Panama, Costa Rica, Nicaragua, Honduras, Paraguay, Chili, Pérou et Salvador)
- Des partenariats conclus avec des opérateurs télécoms mondiaux, permettant à la NSA de surveiller leurs câbles sous-marins

Prism

Prism est le premier programme de surveillance électronique à avoir été mis au jour par *The Guardian* et *The Washington Post*, les 6 et 7 juin. Il s'agit d'une série de partenariats conclus progressivement par la NSA depuis décembre 2007 avec plusieurs géants du net : Microsoft, Yahoo, Google, Facebook, PalTalk, Youtube, Skype, AOL et Apple.
Selon les documents rendus publics par Edward Snowden, la NSA et le GCHQ disposent d'un accès direct à leurs serveurs, surnommé « back door » (porte de derrière) : elles peuvent donc se servir à leur guise dans les données (messages, photos, courriels, chats…), sans intervention des entreprises en question. Dispensée de demander une ordonnance de justice pour chaque collecte, la NSA peut théoriquement transférer en masse sur ses propres serveurs toutes les données liées à des personnes dont elle peut penser « raisonnablement » qu'elles sont à l'étranger – en temps réel ou dans les archives.

Le 12 juin, *The Guardian* nous apprend que Microsoft a fourni à la NSA la clé de chiffrement de sa messagerie en ligne Outlook, pour lui permettre de contourner son propre système de protection des données de ses utilisateurs. Microsoft a également aidé la NSA et le FBI à accéder aux données de son service de stockage de fichiers SkyDrive, et facilité l'interception d'appels passés sur sa plateforme Skype.
Le 23 août, une nouvelle information publiée par le quotidien confirme l'existence de ce programme : la NSA a remboursé aux neuf entreprises des frais engagés pour mettre leurs systèmes aux nouvelles normes imposées par la FISC. Il s'agit notamment de pouvoir séparer plus efficacement les données des Américains et des non-Américains.
Réponse des Etats-Unis : le programme est légal, puisqu'il a été autorisé par la FISC. En outre, aucune donnée de citoyen américain n'est examinée. La suite des révélations prouvera que de nombreux Américains sont en réalité surveillés « par inadvertance », et que leurs données sont conservées.
Réponse des 9 entreprises : elles démentent en bloc toute connaissance d'un accès direct à leurs serveurs. Selon elles, les seules données transmises à la NSA le sont au cas par cas, sur le fondement d'ordonnances judiciaires émises dans le cadre de la loi FISA (Foreign Intelligence Surveillance Act). Soit à peine quelques milliers de requêtes par an.

Tempora

Ce programme piloté par le GCHQ existe depuis 2011. Il s'agit d'un « partenariat contraint » avec sept compagnies mondiales de télécom, dont les noms ont été révélés par le *Süddeutsche* : British Telecom, Vodafone Cable, Verizon Business, Global Crossing, Level 3, Viatel et Interoute.
Celles-ci doivent donner à l'agence de renseignement britannique un accès "illimité" à leurs câbles de fibre optique, où transite l'essentiel du trafic Internet et téléphonique mondial. On ignore encore si cela concerne uniquement le territoire britannique, ou l'ensemble des câbles que possèdent ces entreprises dans le monde.
En plaçant des systèmes de "tapping" sur plus de 200 câbles, le GCHQ aurait quoiqu'il en soit accès à au moins 21 pétaoctets de données de toutes sortes par jour.
Les données sont stockées trois jours, et les métadonnées trente jours. Si, au minimum, 250 analystes de la NSA ont pu accéder à ces données, *The Guardian* suggère que l'ensemble des 850 000 accrédités de l'agence américaine peut également y avoir accès.
Le GCHQ abattrait le "sale boulot" d'interception des communications à la place de sa grande sœur américaine, en contrepartie d'une subvention de 100 millions de livres (117 millions d'euros) sur trois ans.

Boundless Informant

Evoqué pour la première fois le 8 juin par *The Guardian*, Boundless Informant ne collecte aucune information. Il s'agit d'un outil d'analyse, qui se contente de visualiser en temps réel sur une carte le nombre d'informations recueillies sur chaque pays.
On apprend grâce aux documents révélés par Edward Snowden qu'en mars 2013, les pays les plus surveillés étaient :

1. L'Iran (14 milliards de données collectées)
2. Le Pakistan (13,5)
3. La Jordanie (12,7)
4. L'Egypte (7,6)
5. L'Inde (6,3)

Au total, 97 milliards de données ont été collectées en un mois, unité qui désignerait, selon *The Guardian*, un courriel ou un coup de téléphone. D'après la légende de la carte, la France

semble se situer dans la moyenne basse sur l'échelle de la surveillance américaine, bien que les documents ne fournissent aucun chiffre précis.
L'existence de Boundless Informant montre que, contrairement à ce qu'avaient prétendu ses responsables, la NSA est tout à fait capable de savoir d'où viennent les données qu'elle collecte. Elle peut ainsi savoir combien d'Américains sont surveillés, et donc combien de fois elle a outrepassé la loi qui l'en empêche.
Réponse de la NSA : l'agence maintient qu'elle est incapable de déterminer "avec certitude" l'origine et l'identité des personnes qu'elle surveille. Elle refuse donc de divulguer le nombre de communications américaines qui ont été espionnées.

EvilOlive

Ce programme, vraisemblablement lancé à la fin 2012, s'attache à collecter la quasi-intégralité des métadonnées des communications circulant dans les réseaux des grands opérateurs télécoms américains. A en croire *The Guardian*, il permettrait de capter "plus de 75% du trafic Internet passant dans ses filtres", et d'archiver pour des années les données jugées intéressantes.
Selon un rapport top-secret de 2009 publié par le quotidien, les "filtres" en question seraient des sondes placées dans plusieurs nœuds stratégiques du réseau américain (fibres optiques, passerelles IP et câbles sous-marins) grâce à des partenariats avec les opérateurs télécoms, permettant à la NSA de récupérer et d'archiver les données en masse. Contrairement au programme britannique Tempora, ces partenariats fonctionneraient sur la base du volontariat. Légalement, ils seraient basés sur des autorisations délivrées tous les trois mois par la FISC.
Au moins trois opérateurs américains collaboreraient ainsi avec la NSA. Parmi eux, plusieurs sources concordantes désignent AT&T et Verizon, les deux leaders américains des télécoms.
EvilOlive serait en réalité le prolongement de plusieurs programmes de collecte de métadonnées initiés depuis octobre 2001 avec les opérateurs télécoms américains. Regroupés sous le nom de code Stellar Wind, ils auraient été arrêtés fin 2011, après que la FISC eut jugé ses méthodes anticonstitutionnelles. Consacrés aussi bien aux données Internet que téléphoniques, ils étaient initialement limités aux communications impliquant au moins un interlocuteur étranger. Mais plusieurs réformes ont permis de collecter des données américano-américaines en toute légalité depuis octobre 2007.
Réponse de l'administration américaine : en se contentant de collecter les métadonnées (date de la communication, destinataire…), la NSA ne viole pas la vie privée des Américains.
Note : Les documents d'Edward Snowden font également référence à un programme baptisé ShellTrumpet, visiblement complémentaire d'EvilOlive et en place depuis cinq ans. Peu d'information ont filtré sur ce programme, mis à part le fait qu'il a dépassé en décembre 2012 le cap de mille milliards de données collectées. Deux autres programmes de collectes de métadonnées, baptisés MoonLightPath et Spinneret, devaient être lancés en septembre 2013.

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

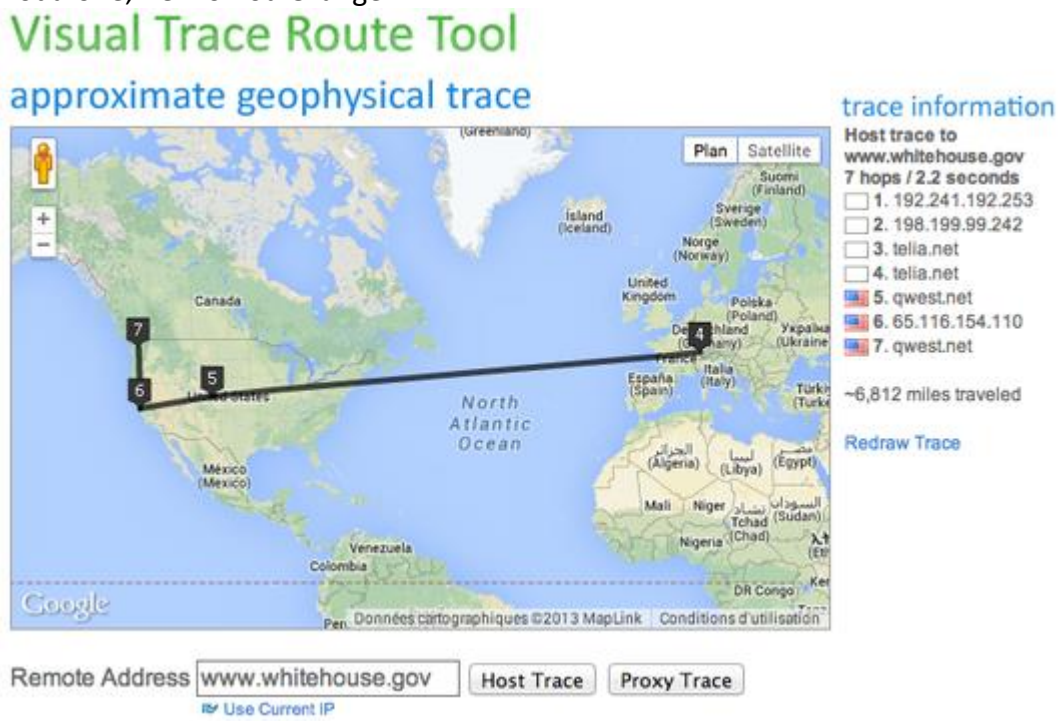
Le Monde.fr | 23.08.2013 à 09h36 • Mis à jour le 23.08.2013 à 16h39 | Par Maxime Vaudano

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 empruntent en effet les quelque 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. A 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 Etats-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 Etats-Unis ou envoyez un email 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.



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 cables sous-marins

En rouge : cables possédés (en partie) par l'un des 7 "partenaires d'interception" du GHCQ
Données : Telegeography

En vert : autres cables

» 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 satellite, 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 Télécom), co-propriétaire 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 Etats-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 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"*.