diploweb.com La revue géopolitique
ISSN : 2111-4307

Surveillance américaine sur l'Internet

Antécédents et conséquences

dimanche 19 janvier 2014,par Laurent BLOCH

Citer cet article / To cite this version :
Laurent BLOCH, **Surveillance américaine sur l'Internet**, *Diploweb.com : la revue géopolitique, 19 janvier 2014.*

Les dispositifs d'espionnage de la NSA ne datent pas d'hier. Par ailleurs, même si c'est avec moins de moyens, les autres pays en font autant. Qu'y a-t-il donc de nouveau avec les révélations de l'affaire Snowden ? Chercheur à l'IFAS, Laurent Bloch répond.

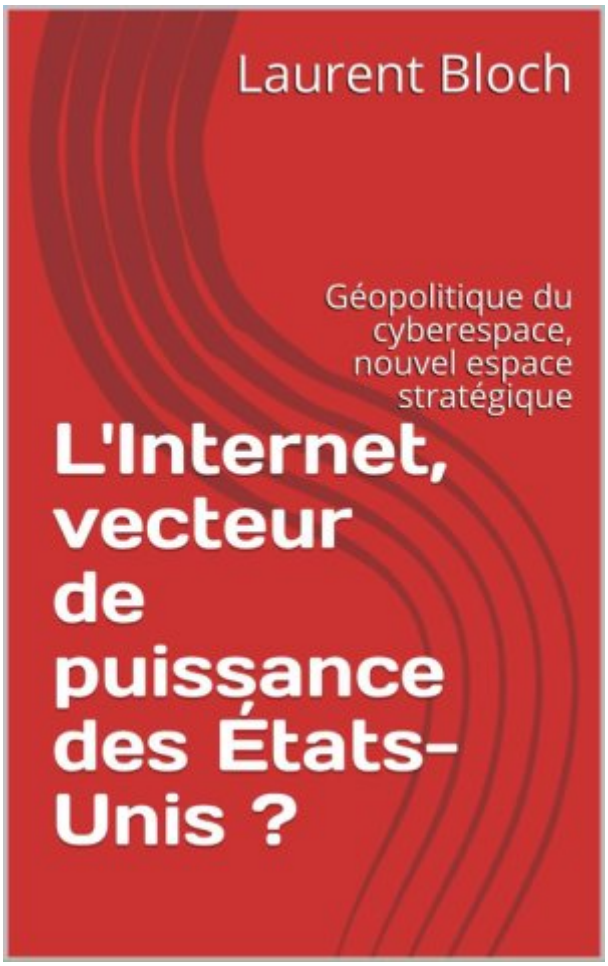
Ce que révèle Edward Snowden

La divulgation par Edward Snowden des documents qui prouvent l'ampleur des opérations de surveillance des communications sur Internet par la *National Security Agency* (NSA) n'en finit pas de propager ses ondes de choc et de susciter l'indignation, sincère ou simulée, comme le signale par exemple l'article d'Annegret Bendiek et Tim Ridout publié le 26 novembre 2013 sur le site du *German Marshall Fund*, *Restoring Trust in Internet Privacy and Data Security*. Les auteurs font le point sur le projet de résolution soumis à l'ONU par le Brésil et l'Allemagne, pays avec à leur tête des dames, Dilma Rousseff et Angela Merkel, dont les conversations téléphoniques ont été consciencieusement écoutées par la NSA, ce qui ajoute la muflerie à l'espionnage. Le texte de ce projet fait référence au Pacte international relatif aux droits civils et politiques, co-signé par les États-Unis, pour préconiser une extension à l'Internet des garanties de protection de la vie privée et des données personnelles dont les citoyens des pays démocratiques bénéficient dans le monde « hors-ligne ».

> Un tempo soigneusement étudié

La divulgation de ces documents par Snowden est effectuée selon un tempo soigneusement étudié, afin de laisser aux acteurs visés le temps d'essayer de se disculper, pour que la vague suivante de publications prouve encore mieux qu'ils avaient menti de façon éhontée. On peut penser au scandale de Panama et à la publication au compte-gouttes, par Édouard Drumont, des documents confidentiels de Reinach à la fin du XIX^{e} siècle en France. Il est à noter que l'ensemble des documents obtenus par Edward Snowden sont maintenant entre les mains de Glenn Greenwald et de Laura Poitras, qui en conduisent une exploitation commerciale.

Livre édité par Diploweb



Laurent Bloch, "L'Internet, vecteur de puissance des Etats-Unis ?", éd. Diploweb
Il importe d'avoir une vision d'ensemble de la géopolitique de l'Internet, intégrant notamment le rôle historique et central des Etats-Unis dans son développement. En effet, l'Internet est depuis plusieurs décennies un nouveau vecteur de puissance pour les Etats-Unis. Dès lors, rien d'étonnant que la Toile devienne le lieu d'une bataille. Format kindle et papier, sur Amazon.

Ces révélations de Snowden, notamment sur les projets PRISM et *Muscular* (ce dernier en collaboration avec les services britanniques du *Government Communications Headquarters* ou GCHQ), font suite à celles de *Wikileaks*, par exemple la publication par Bradley (Chelsea) Manning de vidéos particulièrement compromettantes sur les opérations américaines en Irak. En remontant plus loin dans le temps, on trouve que les mêmes acteurs, dans le cadre du traité secret *United Kingdom - United States Communications Intelligence Agreement* signé le 5 mars 1946, avaient mis en place dès le milieu des années 1970 le dispositif *Echelon*, destiné à capter les communications téléphoniques et les télécopies « intéressantes » un peu partout dans le monde. C'est en 1988 que le journaliste Duncan Campbell a révélé l'existence de ce système d'interception dans un article intitulé *Somebody's listening* (Quelqu'un écoute), publié dans le *New Statesman*.

De ce qui précède on déduit aisément que les dispositifs d'espionnage de la NSA ne datent pas

d'hier, que d'ailleurs, même si avec moins de moyens, les autres pays en font autant, et que donc ceux qui voulaient savoir ce qu'il en était, par exemple parce que c'était leur métier, savaient. Qu'y a-t-il donc de nouveau avec les révélations de l'affaire Snowden ?

Les faits révélés excèdent les hypothèses antérieures

Voilà **ce qui est nouveau dans le domaine des faits** :

. **l'ampleur du dispositif PRISM-*Muscular* n'était pas soupçonnée** : même les professionnels n'avaient pas envisagé l'archivage (pour une courte période de temps) de *toutes* les données échangées, et l'archivage à plus long terme de *toutes* les métadonnées relatives aux communications ;

. **les interceptions *Muscular*, directement sur les fibres optiques transocéaniques**, des données échangées en clair sur les réseaux privés de gros opérateurs tels que Google et Yahoo !, auraient fait figure de science-fiction si elles n'avaient pas été explicitées par le *Washington Post* du 30 octobre 2013 ;

. ces interceptions directes sur le réseau sont d'autant plus choquantes que, par ailleurs, au titre du programme PRISM, la NSA a obtenu **un accès ouvert en permanence sans formalités aux serveurs de Google, Yahoo !, Microsoft, Apple, Dropbox, Youtube, Facebook et AOL**, ce qu'en termes techniques on nomme une *interface de programmation* (*Application Program Interface*) ou API. D'ailleurs, les entreprises dont les réseaux ont été, à leur insu, l'objet des interceptions *Muscular*, ont manifesté un vif mécontentement à l'encontre de la NSA et du GCHQ. Certains experts ont estimé que ces révélations pourraient causer aux opérateurs incriminés une perte annuelle de 35 milliards de dollars à l'horizon 2016.

Retenons que la NSA (et le GCHQ) ont mené de front deux approches de l'espionnage du réseau : le projet **PRISM** en coopération avec les grands opérateurs américains, et **le projet *Muscular*** , non-coopératif. Un des intérêts principaux de *Muscular* est de se déployer hors du territoire américain, ce qui permet de contourner la législation *FISA (Foreign Intelligence Surveillance Act) Amendments Act* de 2008 qui limite l'écoute des communications des citoyens américains (il n'y a aucune restriction pour l'écoute des ressortissants étrangers).

Évaporation de la confiance

Mais ce qui résulte des faits évoqués ci-dessus dans le domaine des opinions et des institutions est sans doute plus important :

. un article du blog de Bruce Schneier (excellent comme d'habitude) intitulé *A Fraying of the Public/Private Surveillance Partnership* signale que l**a coopération entre la NSA et les grands opérateurs de l'Internet** énumérés ci-dessus, qui fonctionnait très bien tant qu'elle était secrète, y compris aux yeux des entreprises pour certains aspects mentionnés ci-dessus, **semble partir en quenouille depuis qu'elle s'étale sur la place publique** ;

. ces grandes entreprises américaines perçoivent que ces révélations risquent de détourner leur clientèle internationale vers des opérateurs d'autres pays, européens ou asiatiques ;

. en effet, le *Patriot Act* du 26 octobre 2001 ne laisse aucun doute sur le fait qu'une entreprise, quelle que soit sa nationalité, qui exerce son activité sur le territoire des États-Unis, est tenue de répondre positivement aux demandes d'accès aux données de ses clients qui lui seraient adressées par la NSA (ou une autre agence fédérale de sécurité) ;

. ainsi, de grands opérateurs tels que BT ou Orange, bien que britannique ou français, sont soumis au *Patriot Act* du fait de leur présence commerciale et technique aux États-Unis, au contraire par exemple d'OVH, dont les activités nord-américaines sont basées au Canada ;

. il est à noter que le *Patriot Act* réduit à néant les garanties de protection des données personnelles obtenues par la Commission européenne au titre d'un accord avec le Département du Commerce des États-Unis ratifié le 26 juillet 2000, qui a instauré un cadre juridique dénommé *Safe Harbor* (Sphère de sécurité).

Le 27 novembre 2013, l'Assemblée générale de l'ONU a adopté une résolution introduite par la France et intitulée Le droit à la vie privée à l'ère du numérique.

Notons que le même jour la Commission européenne a adopté un texte dans lequel il est clairement indiqué qu'elle continuera à travailler étroitement avec les services de renseignement américains pour des échanges de données personnelles, ce qui semble paradoxal. On pourra consulter à ce propos la réaction de la députée européenne Françoise Castex [1]. Contrairement aux vœux du Parlement européen, la Commission refuse notamment de réexaminer l'accord SWIFT, aux termes duquel sont transmises aux États-Unis de nombreuses données sur les transactions bancaires, officiellement pour permettre de repérer les flux financiers qui alimentent le terrorisme international. Et bien qu'elle reconnaisse que le cadre juridique *Safe Harbor* soit désormais, comme nous l'avons souligné ci-dessus, vide de toute substance, elle ne le remet pas en cause.

> Voir aussi l'étude de Laura Brincourt sur Diploweb.com : Le "Cloud Act", trois ans après : révélateur du besoin de définition de notre souveraineté dans l'espace numérique

Espionnage économique

Si la protection des données personnelles est remise en question, celle des **données des entreprises** ne l'est pas moins. De nombreux incidents attestent que les services de renseignement américains, au premier rang desquels la NSA, recherchent et obtiennent des informations économiques relatives à des entreprises ou à des administrations étrangères, et en font bénéficier leurs concurrents américains. On trouvera des exemples d'utilisation à ces fins des interceptions *Echelon* dans un article de Claude Delesse (négociations ALENA, GATT, concurrence entre Boeing et Airbus pour la vente d'avions à l'Arabie Saoudite en 1994, concurrence entre Raytheon Corporation et Thomson CSF en 1994 pour un système de surveillance de la forêt amazonienne). Cette activité dans le domaine économique est intitutionnalisée au sein de l'*Office of Executive Support* du Département du Commerce américain.

L'espionnage économique des communications téléphoniques au moyen du système *Echelon* s'est bien sûr prolongé avec PRISM, amplifié grâce aux possibilités techniques supérieures des systèmes informatiques. Même si aucun fait précis n'est encore apparu sur la place publique, les différents acteurs ont commencé à adapter leurs pratiques à cette menace. La *Cloud Security Alliance* a mené une enquête auprès de ses membres européens, qui montre que 10% d'entre eux renonceraient à des projets de contrats avec des opérateurs américains d'informatique en nuage *(Cloud Computing)* à la suite des révélation de Snowden. James Staten, analyste de *Forrester Research*, écrit que le chiffre (évoqué ci-dessus) de 35 milliards de dollars de pertes annuelles pour les fournisseurs du *Cloud* est une estimation trop faible, et il prédit un manque à gagner de 180 milliards de dollars.

Ces événements et leurs rebondissements pourraient (devraient ?) conduire à une remise en question du projet (en cours de négociation) de traité de coopération économique entre l'Union et les États-Unis, le *Transatlantic Trade and Investment Partnership*.

Topologie du cyberespionnage

Pour capter les données et les communications de tout le monde, la NSA n'a pas hésité à contraindre les grands opérateurs américains, qui maintenant s'en mordent les doigts, et à se brancher sur des fibres optiques transocéaniques avec la complicité du GCHQ britannique. Mais il faut bien dire que ces interceptions sont grandement facilitées pour un État (par exemple les États-Unis) sur le territoire duquel une grande partie du trafic mondial de l'Internet transite, sans qu'il soit besoin d'aller le chercher à l'autre bout de la planète.

Josh Karlin, Stephanie Forrest et Jennifer Rexford, dans leur article *Nation-State Routing : Censorship, Wiretapping, and BGP*, se sont penchés sur cette question. Ils ont élaboré un *indice de centralité* d'un pays dans l'Internet, qui correspond peu ou prou, si l'on considère le trajet d'un paquet de données entre deux points quelconques du réseau, à la probabilité que ce trajet passe par le territoire du pays considéré. Ils ont aussi construit un *indice de centralité forte (Strong Country Centrality)*, qui estime la difficulté qu'il y a à *éviter* de passer par le territoire d'un État pour aller d'un point à un autre dans le réseau : cet indice est construit comme la somme (divisée par le nombre de chemins) de variables qui vaudront 1 si le pays en question est un point de passage obligé entre les deux points par le chemin considéré, 0 sinon.

Un pays doté d'un indice de centralité élevé, et, *a fortiori*, d'un indice de centralité forte élevé, sera bien placé pour espionner les échanges entre d'autres pays, et en outre en bonne position pour échapper à l'espionnage. Inversement, les pays à faible indice seront plus facilement espionnés, et ne pourront guère espionner les autres.

Pour des raisons historiques et économiques, les États-Unis, qui ont créé l'Internet et ses principaux opérateurs commerciaux, que ce soit dans le domaine des publications ou dans celui des infrastructures, bénéficient du **privilège du premier entrant**, et leurs indices sont supérieurs à ceux de tous les autres pays. Voici les résultats des calculs de Josh Karlin, de Stephanie Forrest et de Jennifer Rexford (CC = *Country Centrality*, SCC = *Strong Country Centrality*) :

{{}}	**CC**	**SCC**

États-Unis	0,740695 (1)	0,546789 (1)
Grande Bretagne	0,294532 (2)	0,174171 (2)
Allemagne	0,250166 (3)	0,124409 (3)
France	0,139579 (4)	0,071325 (4)
Pays-Bas	0,128784 (5)	0,051139 (5)
Canada	0,104595 (6)	0,045357 (6)
Japon	0,072961 (7)	0,027095 (11)
Chine	0,069947 (8)	0,030595 (10)
Australie	0,066219 (9)	0,037885 (8)
Hongrie	0,064767 (10)	0,023094 (14)
Singapour	0,063522 (11)	0,043445 (7)
Italie	0,047068 (12)	0,027088 (12)
Espagne	0,043248 (13)	0,025370 (13)
Russie	0,043228 (14)	0,035191 (9)
Autriche	0,024632 (15)	0,010501 (17)
Suède	0,023350 (16)	0,009785 (19)
Afrique du Sud	0,019294 (17)	0,013778 (15)
Danemark	0,015684 (18)	0,008101 (21)
Serbie	0,014935 (19)	0,012312 (16)
Suisse	0,013302 (20)	0,003865 (35)

Ce tableau donne une idée de la présence d'un pays dans l'Internet, pondérée positivement par la situation géographique (cf. le bon rang de la Hongrie et de Singapour), et négativement par la propension à censurer les communications.

Nos auteurs donnent un tableau spécial consacré aux indices des pays connus pour leur censure systématique de l'Internet :

{{}}	**CC**	**SCC**
Chine	0,069947 (8)	0,030595 (10)
Vietnam	0,007087 (30)	0,003916 (34)
Corée du Sud	0,003548 (44)	0,001044 (54)
Arabie Saoudite	0,003286 (47)	0,001722 (49)
Émirats Arabes Unis	0,000839 (65)	0,000541 (63)
Pakistan	0,000274 (81)	0,000265 (74)
Iran	1,12e-05 (105)	9,48e-06 (101)
Yémen	1,06e-07 (131)	7,50e-08 (130)

Oman	2,64e-08 (138)	2,64e-08 (133)
Myanmar	0	0
Corée du Nord	0	0
Soudan	0	0
Syrie	0	0

Les indices égaux à 0 correspondent à des pays qui ne voient passer *aucun* trafic international.

Outils du cyberespionnage

> La NSA peut recueillir à peu près toutes les données qu'elle souhaite.

La divulgation du mode opératoire de projets tels que PRISM et *Muscular*, ainsi que de projets liés, tels *Upstream* [2], montre que la NSA peut recueillir à peu près toutes les données qu'elle souhaite. Ceci fait, se pose la question de savoir comment exploiter ces masses immenses de données.

Dans un article intitulé *L'imbécillité de l'intelligence*, Michel Volle examine d'un œil critique les méthodes de la NSA : un intertitre de son texte, « Tout observer, c'est ne rien comprendre », en résume l'idée générale.

Comme l'explique Michel Volle, les deux piliers du renseignement sont la collecte d'informations, et leur analyse. L'équilibre entre ces deux piliers doit être maintenu. L'informatique et les réseaux fournissent à la collecte des moyens extrêmement puissants. Les méthodes statistiques informatisées en font autant pour l'analyse, ce qui peut faire naître l'illusion d'une automatisation possible de l'ensemble du processus. **Le monde de la finance a déjà cédé à une illusion de ce type, avec les résultats que l'on sait**. Si la NSA y cède également, ce que ses pratiques révéles par Snowden suggèrent, les conséquences seront (sont ?) également catastrophiques, avec à la clé des erreurs judiciaires ou, pire, extra-judiciaires : quiconque aura téléphoné au mauvais moment, dans le mauvais pays, en parlant la mauvaise langue, pourra, par le jeu des corrélations calculées par le logiciel statistique, se retrouver rattaché à un réseau terroriste ou maffieux avec lequel il n'a rien à voir, et en subir les conséquences fort déplaisantes.

Il n'en reste pas moins que les perspectives ouvertes à l'espionnage des pays et des particuliers par les moyens informatiques et réticulaires contemporains sont d'une ampleur dont les dictateurs du XX^{e} siècle n'ont même pas rêvé, non plus que George Orwell.

Nouvelles révélations

Les lignes qui précèdent ont été écrites au début du mois de décembre 2013. Depuis cette date, de nouveaux documents ont été rendus publics par Edward Snowden, qui sapent encore un peu la confiance que l'on pouvait avoir dans les institutions et les entreprises de l'Internet,

surtout américaines.

Corruption des logiciels de RSA Security

Selon un article de Joseph Menn publié le 20 décembre à San Francisco par l'agence Reuters, la NSA aurait versé dix millions de dollars à l'entreprise *RSA Security*, spécialiste de solutions de sécurité pour les entreprises, afin que soient implantées dans certains de ses logiciels des « portes dérobées » destinées à permettre aux agents de la NSA de contourner les barrières de confidentialité qu'ils étaient censés établir.

RSA Security n'est pas n'importe quelle entreprise de logiciels de sécurité : fondée en 1982, depuis 2006 filiale d'*EMC*, géant du stockage de données et de l'informatique en nuage (il possède aussi *VMware*, à l'origine de certaines technologies décisives pour ces activités), cette entreprise doit le sigle qui la nomme aux initiales de ses fondateurs, Ronald Rivest, Adi Shamir et Leonard Adleman, inventeurs du système de cryptographie asymétrique à clé publique qui porte le même nom. Elle est (était ?) un leader du marché de la sécurité informatique, avec un prestige considérable. C'est un nouveau pan de l'« informatique de confiance » et de l'« Internet sûr » qui s'effondre. D'après les sources de Reuter, RSA a livré, de 2004 à 1013, son logiciel BSafe avec un générateur de nombres pseudo-aléatoires affaibli, de façon à permettre aux experts de la NSA un accès aux données chiffrées.

Dès le 14 novembre 2013, avant même la publication du scandale RSA, Bruce Schneier, qui avait été le premier à identifier les faiblesses cryptographiques de BSafe en 2007, écrivait sur son blog un article (signalé ci-dessus) pour signaler la grave perte de confiance qui résulte des révélations de Snowden.

Attaques contre Tor

Le 4 octobre 2013, Bruce Schneier avait également exposé dans un article publié par le *Guardian* les méthodes utilisées par la NSA pour contourner les dispositifs de sécurité mis en œuvre par le système Tor d'accès anonymisé à l'Internet. Tor *("The Onion Router")* achemine les données d'une session TCP selon un itinéraire imprévisible, au moyen de rebonds aléatoires sur des nœuds du réseau configurés de sorte qu'il soit impossible de remonter à l'adresse d'origine de la session. En effet, chaque nœud « connaît » son prédécesseur immédiat et son sucesseur, mais pas les autres relais, contrairement à ce qui se passe lors d'une session TCP ordinaire, où l'adresse d'origine figure dans tous les paquets de données. D'autre part, les données transmises sont chiffrées à chaque étape. La métaphore du « routage en oignon » fait référence à ces chiffrements successifs.

La possibilité offerte par Tor de naviguer anonymement sur l'Internet, et même d'y créer des sites Web ou d'autres services, en fait une cible prioritaire pour la NSA, dont les agents se sont attaqués au système d'installation des logiciels qui permettent d'utiliser Tor.

La première étape de l'attaque consiste à identifier les utilisateurs de Tor. Pour ce faire la NSA s'appuie sur ses capacités propres de surveillance de l'Internet, en collaboration avec les opérateurs dont elle s'est assurée la collaboration. La NSA a créé un fichier d'« empreintes digitales » caractéristiques de sessions TCP liées à Tor, qui permet de repérer les « suspects » sur le réseau.

Une fois constituée la base de données des « suspects » qui ont téléchargé les logiciels de Tor et qui génèrent des sessions Tor, il s'agit de s'attaquer aux navigateurs qu'ils emploient, principalement Firefox, en exploitant certaines de ses vulnérabilités. Pour ce faire la NSA procède à des attaques par interposition *("Man in the Middle")*, qui consistent à usurper le nom d'un site que la victime souhaite visiter afin de détourner ses communications vers un site contrôlé par l'attaquant, sur lequel pourront être menées des investigations frauduleuses, et à partir duquel le navigateur du visiteur pourra être infecté par des logiciels contrôlés par l'attaquant. La suite est du piratage de routine, enfin presque.

La simple liste des utilisateurs de Tor est déjà une arme efficace : ainsi, un étudiant du MIT qui avait essayé de faire chanter l'administration de l'université en la menaçant à travers Tor a pu être identifié et arrêté après simple consultation des « abonnés » Tor du campus.

Conclusion

Même les spécialistes de cyberdéfense les plus blasés ont pu être étonnés par les révélations d'Edward Snowden sur le cyberespionnage de la NSA. Les moyens mis en œuvre sont bien dans la tradition militaire américaine : ils misent plus sur la quantité que sur la subtilité. C'est une force, mais face à des adversaires retors, résolus et persévérants la réussite n'est pas garantie (rappelons-nous le Viêt Nam). En fait, des parades existent face à cette collecte massive de données, ainsi que des possibilités de désinformation. Et l'exploitation de renseignements obtenus de la sorte peut se révéler problématique.

L'arbre ne doit pas cacher la forêt : à côté des méthodes massives et brutales évoquées ci-dessus, existent des possibilités d'attaques ciblées ponctuelles, qui demandent plus de travail humain, mais qui peuvent avoir un rendement élevé. Le sabotage en masse d'une lignée de composants destinés à des routeurs de cœur de réseau, ou la corruption furtive et persistante du micro-code de l'ordinateur (ou du smartphone) d'un personnage important peut laisser espérer des résultats spectaculaires, avec peu de risque de détection.

Plus

Voir le site de l'Institut français d'analyse stratégique

P.-S.

Chercheur en cyberstratégie à l'Institut français d'analyse stratégique.

Notes

[1] Françoise Castex, députée européenne socialiste, particulièrement impliquée dans les

problématiques du cyberespace, de la protection des données personnelles et des nécessaires évolutions des règles de propriété intellectuelle, est menacée de se voir retirer l'investiture de son parti pour les prochaines élections européennes.

[2] *Muscular* est un projet particulier d'interception sur les réseaux privés de Google et de Yahoo !, en collaboration avec le GCHQ britannique, cependant qu'*Upstream* est un projet plus général qui vise l'interception sur fibres optiques en général.