

(Source : Mondialisation.ca)



De nouveaux documents fournis par Edward Snowden, l'ex-agent de la *National Security Agency* (NSA), et présentés dans un article du *Guardian* révèlent **le partenariat étroit entre les services de renseignement européens et la NSA dans la surveillance de masse d'Internet et des communications téléphoniques au cours des cinq dernières années.** Ils donnent un aperçu de la manière dont un système d'espionnage paneuropéen a émergé, dirigé contre l'ensemble de la population européenne et de la population mondiale.

Les programmes révélés par le *Guardian* montrent pourquoi les gouvernements européens ont minimisé les premières révélations sur l'espionnage d'Internet de la part des agences de renseignements américaines et britanniques en juin. Une crise diplomatique majeure a néanmoins éclaté il y a deux semaines quand il est apparu que les États-Unis espionnaient également la chancelière allemande Angela Merkel.

Le directeur des services de renseignements américains James Clapper a admis en toute candeur que les services de renseignements surveillaient des milliers de politiciens dans les gouvernements et les partis d'opposition des pays « alliés. »

Dans ce scandale international grandissant au sujet de la NSA, **les gouvernements européens n'agissent aucunement pour défendre les droits démocratiques. Tout en ayant des objections à la surveillance massive de leurs propres communications par la NSA, ils travaillent avec celle-ci pour espionner le trafic Internet mondial et créer à leur propre usage les infrastructures de surveillance dont auraient besoin**

des états policiers en Europe.

Les documents publiés par le *Guardian* montrent que les services de renseignements Français, Espagnols, Suédois, Hollandais et Allemands coopèrent dans le cadre d'un système de surveillance paneuropéen comparable au réseau de surveillance mondial de la NSA. **Ces agences se branchent directement sur les câbles en fibre optique et développent des relations secrètes avec les compagnies de télécommunications nationales,** comme la NSA l'a fait avec Google et Facebook.

Au cœur de ce réseau d'espionnage, il y a le *Government Communications Headquarters* (GCHQ) britannique. L'agence de renseignement du Royaume-Uni occupe une situation privilégiée en raison de sa position géographique à l'entrée des câbles transatlantiques qui relient les États-Unis et l'Europe, de ses liens particuliers avec la NSA, et de son contexte législatif très favorable à l'espionnage créé par les décisions de gouvernement travaillistes et conservateurs successifs.

En 2008, le système « Tempora » a été développé par le GCHQ, il surveille systématiquement toutes les communications entrantes et sortantes par son accès aux câbles en fibre optique par lesquels passe tout le trafic Internet du Royaume-Uni. Les documents qui ont été révélés montrent que près de 600 millions d'appels sont surveillés chaque jour en se branchant sur plus de 200 câbles en fibre optique;

La même année, les responsables du GCHQ ont exprimé leur admiration pour le Service des renseignements fédéraux allemand (BND) quant à ses capacités technologiques, et déclaré qu'ils avaient « un énorme potentiel technologique et un bon accès au cœur de l'Internet – ils voient déjà certains porteurs [terme qui désigne les câbles en fibre optique] fonctionner à 40 Go/s et 100 Go/s. » Go/s (Gigaoctets par secondes) indique la vitesse de transfert des données.

Les responsables britanniques admireraient le BND parce qu'ils n'ont pas pu surveiller autant de câbles que leurs homologues allemands. En 2012, ils n'étaient toujours capables que de surveiller les câbles à 10 Go/s et cherchaient un moyen de développer la capacité de se brancher sur les nouveaux câbles à 100 Go/s.

L'agence de renseignement du Royaume-Uni a aidé le BND à contourner les lois allemandes qui limitent sa capacité à utiliser cette technologie. L'article du *Guardian* rapporte : « Nous avons aidé le BND (ainsi que le SIS [sécurité extérieure anglaise] et la sécurité intérieure) à

argumenter en faveur d'une réforme ou d'une réinterprétation des lois très restrictives sur les interceptions de communications en Allemagne. »

Le GCHQ loue également la Direction générale de la sécurité extérieure (DGSE) française et les relations qu'elle a établi avec une compagnie de télécommunications qu'elle ne nomme pas. « La DGSE est un partenaire très motivé, techniquement compétent, qui a fait preuve d'une grande volonté de s'engager sur les questions d'adresses IP [Internet Protocol], et de travailler avec le GCHQ sur une base de « coopération et de partage. »

Les services de renseignements britanniques ont également entraîné des techniciens de la DGSE. Le document affirme, « Nous avons pris contact avec le principal partenaire de la DGSE dans l'industrie, qui a quelques approches innovatrices dans certains défis relatifs à Internet, qui augmentent le potentiel pour le GCHQ d'utiliser cette compagnie dans le secteur du développement des protocoles. » En 2009, les deux agences ont collaboré pour briser des méthodes de cryptage sur le réseau.

LE GCHQ a également collaboré avec le Centre espagnol des renseignements nationaux (CNI), qui pratique une surveillance de masse d'Internet grâce à ses liens avec une compagnie de télécommunications britannique qui n'est pas nommée, leur donnant « de fraîches opportunités et montrant certains résultats surprenants. » D'après la loi espagnole, la capture en masse des communications de manière indiscriminée est illégale.

Le CNI, comme le GCHQ, occupe également une position stratégique pour intercepter et surveiller les appels. Le câble transatlantique Columbus III qui relie la Sicile et la Floride passe par la ville de Conil dans la province de Cadix, il est utilisé par des millions de gens chaque jour.

L'article dit, « le partenaire commercial a fourni au CNI certains équipements tout en nous maintenant informés, ce qui nous a permis d'inviter le CNI à des discussions concentrées sur la question des IP cet automne [2008]. » Il a conclu que le GCHQ « a trouvé un homologue très capable dans le CNI, en particulier sur le terrain des Opérations secrètes sur Internet. »

La même année, le GCHQ a applaudi la nouvelle loi passée par le Parlement suédois qui permet à l'Organisme de défense radio national (*Försvarets Radioanstalt* - FRA) de surveiller tous les emails et appels téléphoniques qui entrent, sortent ou ne font que passer par la Suède. La nouvelle loi, qui ressemble au programme d'écoutes du gouvernement Bush mis en place en 2001 n'exige pas qu'un mandat soit obtenu pour pratiquer cette surveillance.

(Lire en anglais : [Swedish government adopts invasive wire-tapping measures](#)).

« Le GCHQ a déjà fourni beaucoup de conseils sur ces questions et nous attendons de pouvoir aider le FRA encore plus une fois qu'ils auront développé un plan pour faire avancer ce travail, » affirme ce rapport.

Le GCHQ maintient également des relations étroites avec les deux agences de renseignements hollandaises, mais « les Hollandais ont certains problèmes législatifs sur lesquels ils doivent travailler avant que leur environnement législatif leur permette d'opérer comme le fait le GCHQ. Nous donnons des conseils juridiques à des avocats hollandais sur la manière dont nous avons réglé certaines de ces questions. »

Toutes les agences de renseignements européennes sont complices de l'espionnage de la NSA, elles fournissent à l'agence américaine de grandes quantités de métadonnées - l'origine des appels, à qui ils sont passés, l'heure et la durée des appels, ainsi que les lieux depuis lesquels ils sont passés.

L'expert en terrorisme Jean-Charles Brisard a déclaré à *El Pais*, « les Européens ont des capacités qui sont très proches de celles des Américains pour intercepter, mais d'un autre côté, ils n'ont pas les mêmes ressources pour traiter cette information. C'est pourquoi ils transmettent ces données brutes pour qu'elles soient décryptées. »

Alejandro Lopez

Article original, [WSWS](#), paru le 4 novembre 2013

Partager cet article :

[Facebook](#)
[Twitter](#)
[Google+](#)
[Pinterest](#)

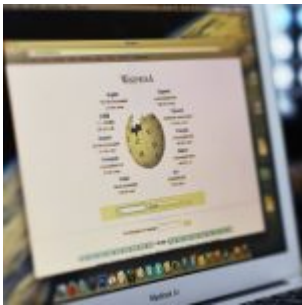
À lire également :



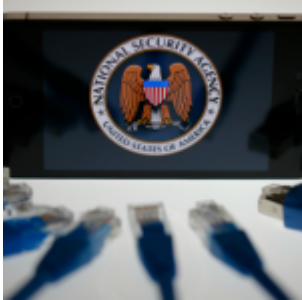
Plus ça change, plus c'est pareil : la NSA aurait écouté les conversations
de 35 chefs d'État



En bref : NSA = 5 000 000 000 données de géolocalisation par jour



Surveillance massive : Wikipedia porte plainte contre la NSA



Comment la NSA utilise les données des téléphones pour relier les
personnes entre elles