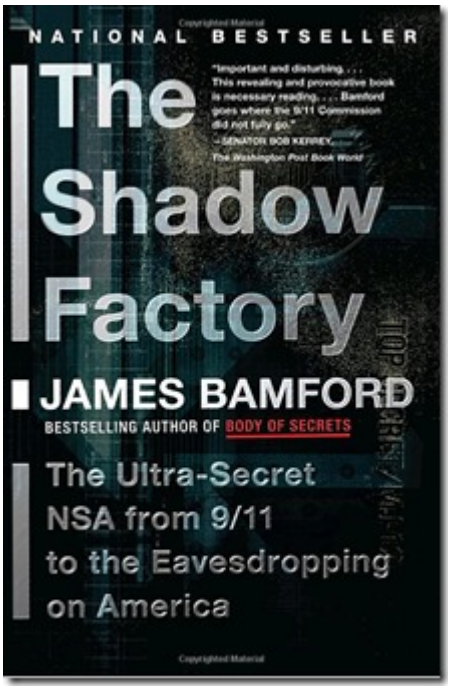
Opinions Libres
le blog d'Olivier Ezratty

Big brother nous surveillait déjà

Il n'y avait pas de quoi être bien surpris des révélations concernant le programme de surveillance PRISM de la NSA. Nous allons ici relativiser cette découverte avec ce qui se pratique dans bien d'autres pays dont la France. Et aussi voir où cela pourrait nous mener.

Vieilles interceptions

La NSA intercepte les communications électromagnétiques depuis des décennies. Elle a même été créée spécialement pour rationnaliser cette mission en 1952, en pleine guerre froide. Elle le faisait sur les communications téléphoniques, notamment satellitaires, via le programme Echelon. Elle avait mis en place au milieu des années 2000 un programme d'interception des communications Internet très bien documenté dans l'excellent "**The shadow factory**". Ce livre est le troisième écrit par le journaliste James Bamford sur la NSA, après "The puzzle palace" (1982) et "Body of secrets" (2001). Paru en 2008, il explique comment, en marge de la loi américaine, la NSA a installé après 9/11 des "salles noires" dans les nœuds de réseaux optiques des grands opérateurs télécoms américains (les Regional Bell Operating Companies ou RBOC) tels que AT&T ou Verizon.



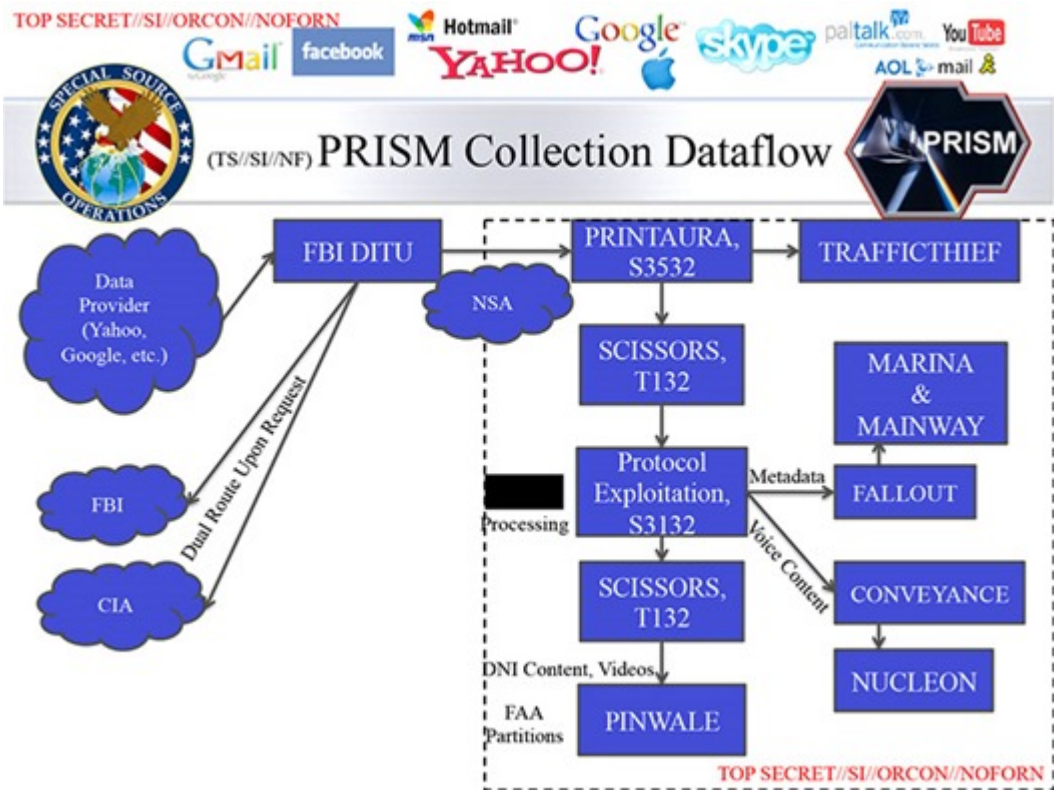
Ces salles répliquent les signaux transitant dans les fibres optiques. Ces signaux sont ensuite filtrés localement par des serveurs dédiés. Ne sont conservées que les trames IP provenant d'endroits ou sujets à surveiller, tels que ceux qui sont issus des pays dits à risques pour la sécurité des USA. Iran, Yémen, Syrie, etc. Le résultat du filtrage est alors envoyé dans l'un des centres d'analyse de ces données de la NSA, dont le siège situé à Fort

Meade près de Washington DC (*ci-dessous*). Ce système permet de savoir qui cause avec qui, qui consulte quoi, et éventuellement, de quoi il s'agit.

En parallèle, la NSA termine la construction d'un énorme data center à **Bluffdale dans l'Utah**. Il est censé stocker toutes les données d'interception.

PRISM complète ce dispositif qui avait déjà quelques années d'existence avec, semble-t-il, des serveurs installés chez les opérateurs de services Internet : Google, Yahoo, Microsoft et plein d'autres. Ces serveurs permettraient de fouiller non plus simplement dans les flux de données circulant sur Internet via les RBOC, mais aussi dans les stocks de données, situés dans les serveurs des pure players Internet.

Les **derniers slides** de la présentation dévoilée par Edward Snowden expliquent cela très bien. Ils montrent d'ailleurs que c'est l'ensemble de la communauté du renseignement US est impliquée dans PRISM et pas seulement la NSA. Le FBI est en effet l'organisation qui gère le lien avec les services Internet tandis que la NSA continue de filtrer les communications Internet au niveau des RBOC.



En résumé : sauf à être très fortement cryptées, nos communications Internet qui ont de grandes chances de transiter par les USA sont potentiellement interceptées par la NSA et le FBI. De là à ce que vous faites les

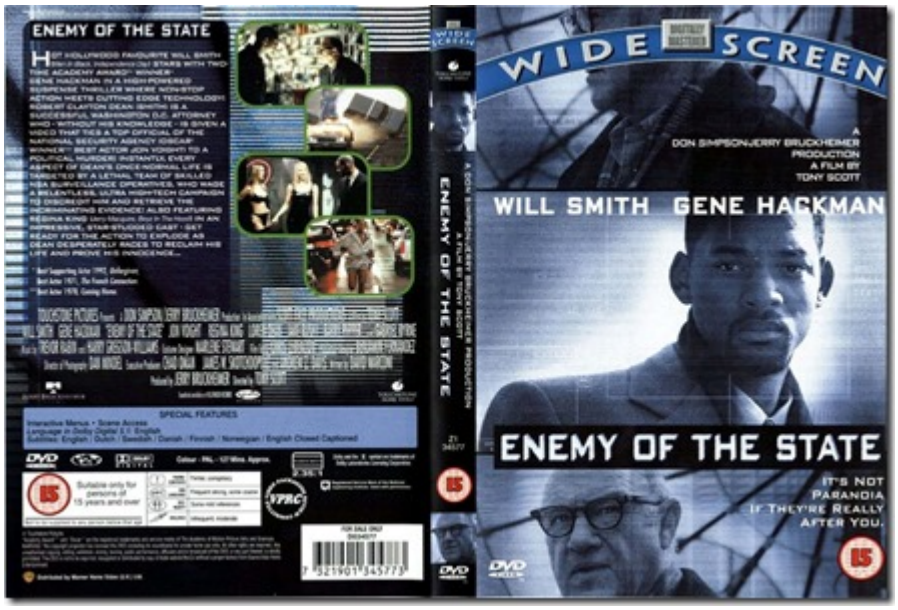
intéresse, cela dépend évidemment de vos activités ! Vos données seront examinées si vous faites partie de la centaine et quelques de milliers de cibles de la NSA.

Les infrastructures de la NSA sont évidemment intéressantes au niveau de leur architecture technique. L'agence a toujours été à la pointe dans deux domaines clés : le décryptage des données chiffrées, à l'aide de supercalculateurs avec une forte consommation de Cray en leur temps, maintenant probablement remplacés par des architectures plus distribuées et de l'autre, l'usage de technologies de télécommunication ultra-rapides. En effet, les données interceptées représentent des volumes très importants à faire circuler. La NSA est donc le premier client au monde d'infrastructures de télécommunications à base de fibres optiques à ultra-haut débit comme celles que nous avions explorées dans mon **premier article sur Alcatel-Lucent**.

Aussi ironique que cela puisse paraitre, dans "The shadow factory", James Bamford indique que la vision big brotherienne du film "Ennemi d'Etat" (Ennemy of the State) sorti en 1998 n'avait rien à voir avec la réalité. A l'époque, la NSA savait bien intercepter les communications téléphoniques mais était complètement à la rue pour ce qui concernait celles qui transitaient sur Internet, et notamment la VOIP. Il faut dire qu'à l'époque, l'Internet grand public n'avait que quatre petites années d'existence ! On peut dater l'arrivée du web grand public à l'émergence de Netscape Navigator fin 1994 !

"Ennemi d'Etat" présentait une vision prospective ne collant pas du tout à la réalité au moment de sa réalisation. 15 ans après, cette vision est devenue réalité. C'est le lot commun des films de science fiction d'Hollywood qui présentent des scénarios technologiques futuristiques qui inspirent ensuite les chercheurs, entrepreneurs et les états !

Mais même aujourd'hui, avec tous les moyens dont ils disposent, les services de renseignement américain et autres ont bien du mal à prévenir des opérations terroristes ou autres, surtout lorsqu'elles sont déclenchées par des individus isolés et communiquant peu.



Dernière révélation en date de l'affaire PRISM : la NSA espionnerait les ambassades européennes ou diverses missions à l'ONU, y compris de pays "amis". Là-dessus, rien de nouveau sous le soleil : l'espionnage est vieux comme le monde et celui des ambassades étrangères a démarré bien avant l'avènement du numérique ! Seuls les moyens ont évolué. Il est moins utile d'installer des micros dans les murs comme du temps de la guerre froide ! Quoique… ! En fait, avec des lasers, on peut écouter à distance une communication dans une pièce en visant une fenêtre. Mais les ambassades bien équipées disposent en général de salles isolées, sans fenêtres, et construites dans des cages de Faraday étanches aux ondes électromagnétiques. Et si vous visitez une

ambassade des USA, on vous videra de la tête aux pieds de tout objet numérique, clés USB comprises ! C'est l'un des rares endroits que je connaisse où de telles précautions d'usages soient de rigueur.

A un moment, certains commentateurs se sont étonnés que la NSA n'espionne pas Twitter. Et pour cause… la majeure partie des données qui y circulent sont publiques. Ne restent plus qu'à récupérer les Direct Message qui ne le sont pas. Cela ne devrait pas être trop difficile de le faire sans même passer par les serveurs de Twitter !

Et en France ?

Ca n'a pas loupé, la révélation du programme PRISM a gêné les USA et obligé les autres gouvernements à réclamer des explications. Explications que leurs services spéciaux ont déjà largement en main quand ils ne collaborent pas déjà ensembles et exploitent des données captées par leurs systèmes respectifs, notamment dans la traque de terroristes potentiels.

Mais pour le théâtre de la politique, les chefs d'Etats doivent jouer les vierges effarouchées ! Ce sont surtout les organisations de défense des citoyens ou de la vie privée qui se sont le plus rebiffées. La Quadrature du Net **défend ainsi le sort d'Edward Snowden**, l'employé américain de Booz & Allen à l'origine des fuites sur PRISM. Sa difficulté récente à trouver un pays d'asile témoigne de l'embarras des pays occidentaux face à l'allié américain !

On a même vu des articles presse expliquant aux Internautes comment éviter de voir leurs communications Internet espionnées par la NSA. Jusqu'à recommander **d'arrêter d'utiliser Google ou Facebook**.

Là-dessus, les journalistes ont un peu enquêté du côté français en se disant à juste titre que les pratiques de la NSA ne devaient pas relever de l'exception. Et on s'est rappelé de l'existence de programmes similaires en Europe et notamment en France. Cf "**Frencheleon, la DGSE est en première division**", "**Révélations sur le big brother français**" ou "**La DGSE écoute le monde (et les français) depuis 30 ans**".

Les différences entre les pratiques de la DGSE et de la NSA ? Elles se situent au niveau des moyens, bien plus importants aux USA (x10 à x20) et dans l'arsenal juridique qui encadre – ou pas – ces systèmes d'écoute. Aux USA, il s'agit de la loi FISA (Foreign Intelligence Surveillance Act) qui permet de surveiller les étrangers, et théoriquement pas les citoyens des USA (cf l'excellent **fiche Wikipedia** sur PRISM). En France, les lois concernées sont multiples et disparates, et on trouve diverses dispositions dans la LCEN et la LOPPSI 2.

Les similitudes : des moyens techniques voisins et une mutualisation des systèmes d'écoute par l'ensemble des organisations du renseignement français (DCRI, DGSE, DRM, Douanes, etc). Ces grandes oreilles sont opérées par la Direction Technique de la DGSE qui représenterait plus de la la moitié de ses effectifs, soit environ 2000 personnes. La France n'a pas l'avantage des USA d'avoir ses grosses artères Internet connectées au reste du monde. Mais tout de même, les nôtres sont reliées aux pays avoisinants et à ceux de la méditerranée et qui plus est nous sommes présents dans diverses régions du monde via nos DOM/TOM. Mais l'histoire ne dit pas encore si la DGSE intercepte en temps réel les communications des opérateurs télécoms comme la NSA le fait dans les centres des Baby Bells "RBOC".

Quid des relations entre les services français et les acteurs du numérique ? Là-aussi, elles existent et ce, depuis des années. Les grands acteurs sont tenus à diverses obligations que nous allons ici rappeler.

- Les **opérateurs télécoms** français mettent en place des écoutes ciblées par dizaines de milliers chaque année. Elles sont lancées sur commissions rogatoires de la justice. Il y a plusieurs personnes en charge de les lancer chez chacun des grands opérateurs. Cela concerne les menaces terroristes (via demandes de la DCRI) mais aussi la grande délinquance et toutes sortes d'enquêtes judiciaires en cours. Ces interceptions concernent l'ensemble des communications transitant via les opérateurs : téléphonie fixe et mobile, VOIP,

transits Internet, sites visités. Elles donnent lieu à un **versement d'une compensation** du Ministère de la Justice.

- Diverses lois régissent la manière dont les utilisateurs cryptent leurs données numériques. La LCEN (Loi sur la Confiance dans l'Economie Numérique) de 2004 permet ce cryptage mais **impose de fournir** aux autorités, notamment judiciaires, toutes les clés de cryptage utilisées. Leur taille n'est plus limitée. La LOPPSI 2 votée en 2011 (loi d'orientation et de programmation pour la performance de la sécurité intérieure) autorise la police sous contrôle judiciaire d'utiliser tout moyen pour s'introduire dans les ordinateurs de personnes suspectées de crimes graves, de trafic d'armes et de stupéfiants, de blanchissement d'argent ou d'aide à l'immigration illégale. Evidemment… sans le consentement des propriétaires des ordinateurs en question !

- Les dispositions sur la sécurité informatique relatives au cryptage des données et des liaisons sont gérées par **l'ANSSI**, l'Agence Nationale de la Sécurité des Systèmes d'Information. Cette agence, anciennement DCSSI, dépend du Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN, anciennement SGDN). Elle soumet la mise sur le marché français et l'exportation de logiciels de cryptage à une demande préalable.

- D'un point de vue pratique, ces contrôles imposent aux éditeurs de logiciels de fournir à l'ANSSI les moyens techniques de décoder les fichiers encryptés par ces logiciels. Cela concerne notamment les usuels formats Office lorsque l'on y adjoint un mot de passe (une protection très très légère). Cette capacité permet ainsi à la Police Judiciaire, entre autres organes dépendant de l'Etat, de décrypter certaines des données récupérées sur des disques durs saisis auprès de personnes suspectes de délits.

- L'ANSSI dispose même des codes sources des systèmes d'exploitation propriétaires tels que ceux de Windows pour les examiner à volonté et ce depuis près de 10 ans. L'histoire ne dit pas si l'ANSSI dispose de ceux de l'intégralité de MacOS. D'un point de vue pratique, cela met Windows presque sur un pieds d'égalité par rapport à Linux dont le code est open source (mais pas celui de toutes les applications que l'on exploite dessus). Presque car le nombre de personnes qui sont à même d'examiner le code source de Windows est probablement bien inférieur à ceux qui décortiquent celui de Linux.

- L'ANSSI est mise au courant par les grands éditeurs, dont Microsoft, des vulnérabilités concernant leurs logiciels, et avant le marché. Cela leur donne à la fois de l'avance pour se protéger, mais aussi pour exploiter ces failles. Les agences de renseignement n'ont pas besoin de mythiques portes dérobées dédiées ! Il leur suffit d'exploiter les nombreuses failles identifiées, le plus en amont possible. Les ordinateurs de la "base installée", y compris de délinquants, ne sont pas toujours suffisamment protégés et les dernières

mises à jour n'y sont pas toujours installées régulièrement. C'est aussi le cas de nombreux ordinateurs d'entreprises pouvant être la cible d'activités de renseignement économique, notamment dans les PME industrielles.

Face à cet arsenal, les délinquants de tout poil peuvent évidemment éviter de voir leurs communications déchiffrées. Ils peuvent soit cacher leurs messages dans des contenus anodins, comme avec les techniques de stéganographie qui servent à planquer des messages dans des images. Soit, il peuvent crypter fortement leurs données avec des clés qui ne sont pas fournies à l'Etat français. Ils peuvent aussi utiliser un tunnel VPN fortement crypté pour les communications de machine à machine. C'est là qu'interviennent les spécialistes du déchiffrement de la DGSE, très gourmande en mathématiciens de haut vol.

Comme l'a écrit Eric Schmidt dans son dernier livre "**The New Digital Age: Reshaping the Future of People, Nations and Business**", se cacher sur Internet deviendra suspect. C'est d'ailleurs l'un des facteurs qui a permis de retrouver Ben Laden à Abbottabad en 2011. Sa grande maison n'était pas connectée à Internet et n'émettait aucune onde électromagnétique ! Ce vide était louche. A contrario, l'usage de VPNs et de données fortement cryptées, pas faciles à casser pour les grandes clés, sont tout aussi louches. Dans ce cas, les services de renseignement s'intéresseront aux informations sur les terminaisons de ces communications : qui émet quoi et reçoit des informations à quel endroit. Ce sont déjà des informations de grande valeur ! En quelques sortes, le graphe social des criminels !

Faut-il s'inquiéter ?

Deux arguments s'opposent : d'un côté celui selon lequel le renseignement est utile pour préserver l'état de la société et de l'autre celui selon lequel toute forme d'espionnage des citoyens est liberticide.

D'un point de vue pratique, votre vie privée n'intéresse pas du tout la NSA ou la DGSE sauf si vous menez des activités potentiellement dangereuses pour la sécurité des pays concernés. Dans le reste des cas, c'est-à-dire, 99,999% des situations, la NSA et la DGSE se tapent de vos faits et gestes comme de l'an 40 ! C'est un argumentaire qui ne justifie rien, mais qui permet de relativiser les menaces. Pour l'instant.

Sans être délinquants, vous êtes par contre concernés et potentiellement vulnérables si vous détenez des secrets industriels ou politiques. Les dispositifs de renseignement sont utilisés pas seulement pour prévenir des menaces terroristes mais aussi pour faire du renseignement politique et économique actif. C'est à ce titre que l'ANSSI fournit des recommandations aux organismes publics et aux entreprises industrielles françaises pour leur permettre de se protéger.

Il y a aussi le "big brother" dont on ne parle jamais : les hypermarchés qui savent ce que vous achetez et les banques qui en savent autant, sans compter les organismes de santé qui en savent aussi beaucoup sur vous. Les données qu'ils collectent sur nous sont rarement bien utilisées et les lois françaises ainsi que la CNIL nous protègent de rapprochements entre les bases correspondantes.

Ce n'est pas faute d'envie, mais plutôt de moyens, d'outils adaptés et de savoir faire. On a beau nous abreuver de concepts "big data" depuis au moins deux ans et de "marketing 1 to 1" depuis encore plus longtemps, la mise en pratique dans les grandes entreprises est bien rare. Le virus de la recommandation de produits n'a pas encore atteint ces acteurs. On se contente d'en bénéficier dans les systèmes de vidéo à la demande ou avec les publicités plus ou moins bien ciblées sur Internet (via AdWords, ou le re-ciblage sauce Critéo).

Autre menace : les services en ligne pour qui la vie privée est une valeur relative malgré toutes les déclarations de bonnes intentions. Les risques sont réels avec Facebook qui change ses règles d'utilisation comme de chemise et où l'on ne sait jamais clairement ce qui est public ou pas dedans tant son interface utilisateur est

devenue compliquée. C'est pareil dans Google+, dans Flickr, et tout un tas de services en ligne. Là encore, la prudence est de mise concernant les traces de votre vie que vous laisser dans ces services ou que d'autres y laissent concernant votre vie.

Dernière menace et non des moindres : l'Etat qui sait tout et voit tout de nos gestes et nous réprimande à la moindre incartade. L'Etat omniprésent qui fait respecter la loi à 100%. Le respect à 100% des lois préparées par nos gouvernement librement choisis et votées légalement par nos représentants tout aussi choisis au suffrage universel peut pourtant être liberticide. Dura lex sed lex, mais trop de lois tue la loi et le peuple ! Difficile de concilier sécurité et liberté. La loi du même nom de début 1981 votée à la fin du septennat de Valéry Giscard d'Estaing contenait plus de mesures sur la sécurité que sur les libertés !

Prenons comme exemple les radars routiers qui enquiquinent pas mal de conducteurs. Leur concept pourrait s'étendre à tout un tas d'activités. Et pourquoi s'embêter avec des radars ? Il suffirait dans un monde ultra-répressif d'installer des boites noires dans les voitures, comme dans les camions. Elles mesureraient les coordonnées GPS de nos déplacements et la vitesse correspondante. En temps réel ou en différé, on pourrait recevoir une amende mensualisée intégrant nos inévitables dépassements de vitesse et autre violations de priorités, stops et feux rouges. Le système réduirait nos points de permis d'autant. Ce genre de surveillance permanente demanderait une punition moins ponctuelle pour les dépassements. Elle serait "moyennée" et reflèterait notre style de conduite dans la durée et pas seulement dans le passage "piège" de la route qui passe subrepticement de 70 km/h à 50 km/h sans forcément prévenir.

Ce concept est d'ailleurs déjà opérationnel en France avec plus de 50 **radars tronçons** qui mesurent votre vitesse moyenne sur un tronçon de route. Ce n'est pas de la science fiction ! Est-ce acceptable ? Pas évident ! Est-ce plus juste que les amendes ponctuelles ? A méditer… ! Mais la question ne se posera plus dans 10 ou 20 ans quand nous utiliserons des voitures à conduite automatique ! Elles seront probablement programmées pour respecter scrupuleusement le code de la route.

Le risque est cependant là : la mesure permanente de nos faits et gestes, en ligne ou hors ligne. Tout ce qui se mesure et se transmet numériquement est potentiellement liberticide. Et les objets connectés couplés au big data et au cloud permettront de surmultiplier ces scénarios. Cela pourrait aboutir à la pénalisation de tous les errements, petits ou grands, ponctuels ou moyennés. Les objets connectés, le quantified self, la communication "machine to machine", la vidéosurveillance à tout va et tout le toutim peuvent générer ce genre de dérives. Au niveau des Etats comme dans les entreprises, aussi potentiellement friandes de métriquisation des activités de leurs salariés.

Toutes ces dérives potentielles ou avérées sont plus inquiétantes que PRISM et la NSA ! Il est donc bon de rester vigilant.

PS : je vais ralentir le rythme de publication pendant ces deux mois d'été… et plus que d'habitude. Besoin d'un

peu de repos !

Cet article a été publié le 7 juillet 2013 et édité en PDF le 15 mars 2024.