dimanche 21 juillet 2013

La DGSE a le « droit » d'espionner ton Wi-Fi, ton GSM et ton GPS aussi

Jean-Marc MANACH

La Direction générale de la sécurité extérieure (DGSE, les services spéciaux français) ne serait pas, en l'état, en mesure de collecter "systématiquement les signaux électromagnétiques émis par les ordinateurs ou les téléphones en France".

Une chose est de stocker "tous les mots de passe" qu'elle a pu intercepter sur les "réseaux grand public", comme je l'avais écrit en 2010 (voir Frenchelon : la DGSE est en « 1ère division »), une autre est de pouvoir espionner "la totalité de nos communications", en France, comme l'écrivait Le Monde, la semaine passée, avec ses "Révélations sur le Big Brother français".

A contrario, et comme l'écrivait *Le Monde* mi-juin, la DGSE est bien "au cœur d'un programme de surveillance d'Internet" lui permettant de surveiller "le flux du trafic Internet entre la France et l'étranger en dehors de tout cadre légal"...

Le monde a bien changé depuis les plombiers de la DST

S'il est certes techniquement possible d'espionner tout type de réseau de communication, le maillage décentralisé du réseau Internet, en France, fait qu'il est par contre improbable que la DGSE ait pu concrètement, financièrement et structurellement, placer l'intégralité de nos télécommunications sous surveillance afin de collecter et stocker nos méta-données (qui communique avec qui, quand, pendant combien de temps, d'où).

Contrairement à des pays comme la Libye, où l'Internet était centralisé – ce qui a permis à l'entreprise française Amesys d'y installer un système de surveillance généralisée des télécommunications (voir Barbouzeries au Pays de « Candy »), l'historique du développement des télécommunications en France a débouché sur une infrastructure décentralisée.

Si la DGSE voulait placer tout l'Internet sous surveillance, elle ne pourrait pas se contenter de demander à Orange, Bouygues Télécom, SFR ou Free de dupliquer le trafic Internet. D'une part parce qu'il existe de nombreux autres FAIs, particulièrement étrangers (les opérateurs européens, américains, voir indiens sont présents en France), d'autre part parce que ça ne suffirait pas : l'Internet n'est pas une série de tuyaux contrôlés par quelques gros "telcos",

c'est un peu plus compliqué.

Espionner les FAI ? Une fausse bonne idée

Comme l'avait très bien rappelé Benjamin Bayart dans sa conférence "Internet libre ou minitel 2.0", "sur Internet on a mis l'intelligence en périphérie du réseau" :

« Dans Minitel on a mis l'intelligence au centre, c'est le contenu, c'est les bases de données avec des terminaux débiles autour. Internet c'est le contraire, on a mis des routeurs idiots au centre et on a mis en périphérie des ordinateurs qui réfléchissent. »

Illustrations : quand un abonné Orange regarde DailyMotion (filiale d'Orange), le trafic peut ne pas sortir du réseau de France Télécom, ou même sortir du réseau d'Orange et y re-rentrer de nouveau au gré des règles de routage. Plus généralement, en matière d'interconnexion entre opérateurs (Peering), certains prestataires français préfèrent passer par des points d'échange situés à l'étranger, afin de payer moins cher... ce qui fait qu'un fichier envoyé par abonné Free à un internaute Orange passera peut-être par Londres ou Francfort, ou encore la Belgique s'ils utilisent Google, sans que jamais ni Free, ni Orange, ni personne à Londres, Francfort ou Bruxelles ne sache exactement ce qu'ils ont échangé.

Le problème se complique avec les services types web 2.0 : quand un internaute se connecte à l'un des services proposés par Google, son FAI ne sait pas lequel, ni ce qu'il cherche à y faire (consulter son gmail, faire une recherche, travailler sur un document stocké dans le "cloud" de Google, etc.), car le trafic est chiffré (ssl), et que la réponse à la requête de l'abonné sera routée par les serveurs de Google, et non par le FAI.

Rajoutez-y le fait que nombreux sont les internautes qui passent par Google pour consulter tel ou tel site, plutôt que de rentrer son URL dans son navigateur, et vous commencez à prendre la mesure de la complexité du routage de l'Internet, et du fait qu'on ne peut pas installer de "Big Brother" au coeur des FAI.

L'an passé, le sénateur Jean-Marie Bockel voulait interdire la vente de routeurs de coeur de réseau chinois en Europe, au motif qu'ils pourraient permettre à la Chine de nous espionner. Comme le rappelait alors *L'Express*, ces routeurs, utilisés par les opérateurs de télécommunications pour gérer les flux de communications, peuvent en effet "intercepter, analyser, exfiltrer, modifier, voire détruire toutes les informations" qu'ils voient transiter.

Une hypothèse récemment battue en brèche par Stéphane Bortzmeyer, dans un article intitulé Un routeur de cœur de réseau peut-il espionner le trafic ?. Techniquement, c'est possible, et il existe effectivement des routeurs espions. Mais ils ne peuvent pas pour autant analyser tout le trafic en temps réel ; et

s'ils faisaient remonter le trafic aux autorités, ça se verrait, les opérateurs s'en apercevraient, des ingénieurs auraient protesté ou démissionné, et l'information aurait fuité bien avant les "révélations" du *Monde*.

Comment les internautes sont mis sur écoute

Pour Kave Salamatian, professeur d'informatique et de réseaux, et spécialiste de la géographie de l'Internet, cette histoire de "PRISM" français relève d'une "tentative de désinformation, de manœuvre de roulement de muscles, ce qui est habituel dans le monde du renseignement : plus c'est gros, plus ça passe" :

« L'architecture du réseau téléphonique et internet en France est très différente de celle des États-Unis. C'est une décision prise dans les années 40-50 : les USA sont allés vers une architecture avec des centraux téléphoniques très gros, qui concentrent le trafic, et des lignes très longues vers l'utilisateur.

En Europe, on a fait un maillage dense de centraux téléphoniques de plus petites tailles, avec des lignes beaucoup plus courtes vers l'utilisateur : on est toujours à moins de 4-5 kilomètres d'un DSLAM, l'architecture est beaucoup plus dense. »

Et c'est précisément sur ces DSLAM, qui récupèrent le trafic transitant sur les lignes téléphoniques afin de router les données vers les gros tuyaux des FAI, au plus près des abonnés, que s'effectuent les écoutes Internet, comme me l'a expliqué, sous couvert d'anonymat, le responsable d'un gros FAI :

« Le réseau français est fait de sorte que pour l'intercepter il faut aller au plus près de l'abonné, source ou destinataire, sachant que les deux canaux de communications sont disjoints : chaque acteur ne maîtrise que ce qui sort du réseau. La voie retour, quand c'est Google qui envoie l'info, c'est Google qui décide par quels chemins le flux doit revenir à l'abonné, et au final c'est le DSLAM qui réassemble les flux depuis et vers l'abonné.

Quand on reçoit un ordre d'un tiers de confiance (Justice ou Invalides -qui gère les interceptions de sécurité pour le compte de Matignon), on duplique le flux, qui est renvoyé via des liaisons dédiées et chiffrées ; et on s'est débrouillé pour que la fonctionnalité de duplication soit limitée à quelques abonnés par équipement, et que seules deux personnes puissent la débloquer. »

Non content d'avoir été conçu pour ne permettre que quelques placements sur écoute en simultané, par DSLAM, le dispositif ne peut pas être activé par le FAI seul, pas plus qu'à la seule initiative du ministère, mais seulement lorsque les deux s'accordent pour activer la mise sur écoute :

« Si le logiciel est hacké ou évolue vers des fonctionnalités non documentées, le hardware, chez nous, va le bloquer. Et tout est tracé. Et si la DGSE vient

nous voir, on leur répond qu'on ne discute qu'avec la PNIJ (la Plateforme nationale d'interception judiciaire de la Justice) ou le GIC (le Groupement interministériel de contrôle, dépendant du Premier Ministre). »

Pour faire du massif, il faudrait pirater les "box"

Si la DGSE avait voulu placer des bornes d'écoute clandestine afin de pouvoir surveiller l'intégralité du trafic, elle aurait donc du installer des portes dérobées dans tous les DSLAM, et plusieurs autres points d'interconnexion, sans que cela se voit.

Or, en France, on dénombre près de 16 000 répartiteurs téléphoniques, et quelques 40 000 DSLAM.

Save Kalamatian estime que, pour faire un point de collecte sur un lien à 10GB/s, avec de la reconnaissance par mot-clef, il faudrait investir de 100 à 150 000 € par porte dérobée. Or, à raison de 20 000 portes dérobées, il faudrait investir de 200 à 300 millions € (en hypothèse basse), voire 750 M€ si on voulait espionner tous les DSLAMs (sans la gestion, ni la maintenance, ni la bande passante pour faire remonter le trafic espionné au siège de la DGSE, boulevard Mortier).

"Pour faire de la surveillance massive, il faudrait aller au niveau de la Box" qui permet aux abonnés de se connecter, explique Stéphane Bortzmeyer, et y installer un logiciel espion.

Mettons d'emblée de côté l'aspect particulièrement improbable d'une telle opération, dans la mesure où les employés des FAI ou des fabricants de ces Box auraient forcément détecté la manip', sans parler des bidouilleurs qui auraient remarqué le trafic sortant de leur Box, et qu'il y aurait donc forcément eu des fuites dans les médias si la DGSE avait voulu tenter ce coup-là.

On dénombre près de 13 millions d'abonnés, en France. A raison de 40€ par logiciel espion (ramené à l'ensemble du parc), estime le responsable du FAI, l'investissement représenterait donc plus de 500M€, à quoi il faudrait rajouter les frais de bande passante.

Or, le budget annuel de la DGSE est de l'ordre de 600M€.

A quoi il faudrait aussi rajouter la surveillance des méta-données issues de la téléphonie fixe et mobile. Là, pour le coup, le système est plus centralisé, puisque les méta-données des statistiques d'appel (ou call data record, CDR) sont générées par les opérateurs, qui les conservent pour la facturation, et la détection d'incident.

Suite à la panne d'Orange, en juillet 2012, une inspection de sécurité avait été

lancée, pour vérifier l'infrastructure des opérateurs de téléphonie mobile. Les ingénieurs de l'ANSSI -en charge de la cyberdéfense- tout comme ceux des opérateurs n'auraient alors pas manqué d'identifier d'éventuelles installations espion de la DGSE, ce qui aurait donc dû être dénoncé à la Justice, et n'aurait pas manqué de sortir dans la presse.

Avec des "si", on mettrait Internet en bouteille

Entre 5 et 10% du trafic Internet français transite par l'association France-IX, le plus important des points d'échange internet français, qui permettent aux différents FAI d'échanger du trafic grâce à des accords de "peering". Raphaël Maunier, son président, est formel :

« On ne m'a jamais demandé d'intercepter du trafic. Sur France-IX, il n'y a pas d'écoute, c'est hors de question, je démissionnerais direct, et j'en parlerais, c'est anticonstitutionnel.

Si on voulait forcer Free, Orange Numéricable, Bouygues ou SFR à intercepter, ça coûterait de l'argent, ça se verrait, et la plupart des opérateurs que je connais refuseraient : intercepter sur le coeur de réseau, ça ne marcherait pas. »

"Intercepter les données sur le Net sans que ça se sache ? C'est délicat, et je ne vois pas comment techniquement ce serait possible", renchérit Pierre-Yves Maunier, son frère, architecte Réseau chez Iguane Solutions, qui héberge physiquement le "cloud" de nombreux services web : "si on voulait tapper les DSLAMs, les opérateurs le sauraient ; écouter tout en temps réel, de tous les opérateurs, c'est faisable, mais demanderait des moyens colossaux, tant pour les opérateurs que pour le gouvernement."

« Je suis intimement convaincu que c'est difficilement faisable ; mais je ne sais pas tout. »

Les professionnels des réseaux que j'ai contacté sont unanimes : techniquement, tout est possible. Mais si la DGSE avait vraiment voulu mettre le Net et la téléphonie sous surveillance constante et généralisée, le réseau est tellement décentralisé, et implique tellement d'opérateurs divers et variés qu'ils s'en seraient forcément aperçus et ce, bien avant les révélations d'Edward Snowden.

Il est impossible, en l'état, d'espionner tout le trafic de tous les abonnés sans que les ingénieurs et techniciens en charge du bon fonctionnement de ces réseaux ne s'en aperçoivent, ou n'en soient tenus informés.

Pourquoi aucun d'entre-eux n'a réagi, ne serait-ce que sur la mailing-liste du FRench Network Operators Group (FRnOG), qui "rassemble des personnes intéressées par les domaines de la sécurité, la recherche et le fonctionnement

d'Internet en France" (et qui discutait récemment de cette possibilité d'espionner un routeur de coeur de réseau) ? Parce qu'ils sont habitués... à entendre "beaucoup de conneries de la part des journalistes" :

« On est tellement habitué à ce que les journalistes disent n'importe quoi qu'on ne réagit même plus. »

La DGSE a le "droit" d'espionner ton Wi-Fi, ton GSM et ton GPS aussi

Pour autant, cela ne veut pas dire que la DGSE n'espionne pas tout ou partie des télécommunications qui transitent par satellite. Comme le rappelle Vincent Jauvert, un des journalistes qui, en avril 2001, fut l'un des premiers à évoquer le système "Frenchelon" d'espionnage des télécommunications de la DGSE (voir Le DGSE écoute le monde (et les Français) depuis plus de trente ans), la loi de 1991 relative au secret des correspondances émises par la voie des communications électroniques, censée encadrer les interceptions de communications électroniques et désormais intégrée au Code de la sécurité intérieure, excluait le spectre hertzien de toute forme de contrôle :

« Cette dérogation a été exigée par les plus hautes autorités de l'Etat, confie un ancien conseiller du ministre de la Défense de l'époque, Pierre Joxe. Pourquoi ? Souvenez-vous, à cette époque, la DGSE lançait un vaste plan de modernisation de ses « grandes oreilles ». Il était hors de question de le compromettre.

Un ancien de l'Elysée dit : « Nous voulions laisser les coudées franches au service secret, ne pas l'enfermer dans son quota d'écoutes autorisées. »

Accessoirement, les ondes hertziennes servent aussi en matière de radio-identification (RFiD), de GPS, de GSM et de Wi-Fi... technologies qui, en 1991, n'étaient pas utilisées par le grand public, contrairement à aujourd'hui.

Reste aussi la question des câbles de fibres optiques sous-marins, qui ne relèvent pas du spectre hertzien, et qui ne sauraient donc être légalement espionnables par la DGSE. Et il serait vraiment très intéressant de savoir ce que la DGSE espionne, et ce qu'elle fait pour ne pas espionner les Français.

Dans son article, Vincent Jauvert écrivait que "nos communications avec l'étranger ou les Dom-Tom peuvent être interceptées, recopiées et diffusées par la DGSE, sans qu'aucune commission de contrôle ait son mot à dire. Aucune ! Une situation unique en Occident." :

« Tous les pays démocratiques qui se sont dotés de services d'écoute « satellitaire » ont mis en place des garde-fous, des lois et des instances de contrôle afin de protéger leurs citoyens contre la curiosité de ces « grandes oreilles ». Tous, l'Allemagne et les Etats-Unis en tête. Pas la France. »

Son article date de 2001. Depuis, rien n'a changé. Et la DGSE a continué à faire monter en puissance son système d'interception des télécommunications.

Big Brother est dans vos têtes, pas sur l'Internet

Le "Bug Facebook" avait révélé, l'an passé, à quel point la perte de contrôle de leur vie privée pouvait effrayer les internautes, mais également à quel point ils pouvaient être "crédules" (il s'agissait d'une rumeur, cf Facebook et le « paradoxe de la vie privée »).

Le fait qu'Eric Filiol, un ancien militaire, chercheur en cryptologie et virologie -qui aurait travaillé à la DGSE- ait été le seul à qualifier de "fantaisiste" le Big Brother de la DGSE tel que décrit par Le Monde est tout aussi instructif, et plutôt effrayant.

La banalisation des technologies de surveillance, la montée en puissance de cette société de surveillance, la primauté faite au renseignement et aux technologies sécuritaires -au détriment de nos libertés- sont telles qu'un barbouze s'est fait passer pour une gorge profonde afin de faire croire aux lecteurs du Monde que la DGSE était aussi puissante que la NSA...

Le budget de la NSA est classifié, mais on estime qu'elle reçoit de 10 à 15 milliards de dollars, par an, soit 25 fois plus que la DGSE. La NSA emploierait 40 000 personnes, dont 32 000 pour le SIGINT (pour SIGnals INTelligence, l'accronyme anglais désignant le renseignement d'origine électromagnétique), alors que la DGSE n'en emploie que 4750, dont 1100 dans sa direction technique (chargée de "rechercher et d'exploiter les renseignements d'origine technique").

Et personne n'a moufté, à l'exception de Matignon, et de Jean-Jacques Urvoas, président de la Commission des lois de l'Assemblée nationale et spécialiste du renseignement, qui ont rappelé que la DGSE n'espionnaient pas "tous" les Français, parce qu'elle était encadrée par la loi de 1991 (sachant, par ailleurs, que la DGSE a aussi le "droit" de violer les lois, à l'étranger).

Il suffisait pourtant de contacter les professionnels des réseaux, ceux qui nous permettent de communiquer sur Internet, pour comprendre qu'a priori, le système décrit par Le Monde ne peut pas exister, en l'état, en France.

La DGSE espionne-t-elle les Français depuis l'étranger ?

A contrario, rien n'interdit la DGSE d'écouter les Français depuis l'étranger. Mi-juin, Le Monde écrivait que la DGSE "examine, chaque jour, le flux du trafic Internet entre la France et l'étranger en dehors de tout cadre légal" :

« La justification de ces interceptions est avant tout liée à la lutte antiterroriste sur le sol français. De facto, au regard de l'absence d'encadrement légal strict de ces pratiques, l'espionnage des échanges Internet peut porter sur tous les sujets.

Interrogée par Le Monde, la DGSE s'est refusée à tout commentaire sur ces éléments couverts par le secret-défense. De plus, les autorités françaises arguent que les centres d'hébergement des sites sont, pour la plupart, basés à l'étranger, ce qui exonère la DGSE de répondre à la loi française. »

Le magazine spécialisé Intelligence Online révélait récemment que le nouveau datacenter de la DGSE, construit dans un ancien bunker allemand de 100 mètres de long sur 10 de large, situé près de sa station d'interception des télécommunications satellitaires des Alluets, dans les Yvelines, (voir Frenchelon : la carte des stations espion du renseignement français), stockait "toutes les communications électroniques passivement interceptées par les stations du service à l'étranger, notamment à Djibouti, proche de plusieurs dorsales télécoms" (ou Internet Backbone), laissant entendre que la DGSE pourrait aussi écouter les câbles sous-marins dans lesquels transitent, par fibres optiques, une partie importante du trafic Internet international.

En février dernier, Fleur Pellerin qualifiait le savoir-faire d'Alcatel Submarine Networks (ASN), qui couvre la production, l'installation et la maintenance des câbles sous-marins, d'"unique", tout en déclarant qu'ASN ne faisait pas que transporter des paquets de données, mais également de la "cybersurveillance" :

« C'est une activité stratégique pour connecter l'Outre-Mer et tout le continent africain en haut débit. Il y a aussi un enjeu lié à la cybersurveillance et la sécurité du territoire. »

Le site Reflets.info évoque depuis des mois une thèse abracadabrantesque, relayée par l'ONG Survie, selon laquelle le renseignement français aurait externalisé une partie de son système de surveillance des télécommunications dans des pays où elle aurait contribué à installer des systèmes Eagle de surveillance massive de l'Internet, comme elle l'avait fait en Libye (voir Barbouzeries au Pays de « Candy »).

S'il n'existe donc pas, a priori, de "Big Brother" en France, il a bien des petits frères, installés à l'étranger de sorte d'"exonérer la DGSE de répondre à la loi française", tout en lui permettant d'espionner le trafic Internet.

En 2010, Bernard Barbier, directeur technique de la DGSE, avait ainsi expliqué que les réseaux grand public était la "cible" principale, et qu'elle stockait "tous les mots de passe" (voir Frenchelon : la DGSE est en « 1ère division »).

L'ancien directeur de la DGSE, le préfet Érard Corbin de Mangoux, en parlait

lui aussi ouvertement, en février 2013, au Parlement :

« À la suite des préconisations du Livre blanc de 2008, nous avons pu développer un important dispositif d'interception des flux Internet. »

Marc Trévidic, juge d'instruction au pôle antiterroriste du TGI de Paris, expliquait au Sénat l'an passé que « les gens qu'on arrête, dans la plupart de nos dossiers, c'est grâce à Internet », des propos réitérés en février dernier à l'Assemblée :

« La totalité des affaires d'associations de malfaiteurs terroristes comporte des preuves acquises sur internet. Au surplus, parmi ces affaires, 80 % d'entre elles sont même exclusivement déferrées devant la Justice grâce à ce type de preuves. De fait, la surveillance d'internet représente pour les services de renseignement un enjeu majeur. »

Le problème, c'est que la DGSE est moins contrôlée que la NSA, et qu'on a plus d'informations sur la NSA que sur l'"infrastructure de mutualisation" (qui centralise les données espionnées) de la DGSE...

NB : et si vous pensez que vous n'avez rien à vous reprocher, donc rien à cacher, et que donc vous ne risquez pas d'être espionné, lisez donc ce pourquoi la NSA espionne aussi votre papa (#oupas) et, pour vous protéger, Comment (ne pas) être (cyber)espionné, ainsi que les nombreux articles de Reflets.info, particulièrement en pointe sur ces questions.

PS : @H_Miser me fait remarquer que je pourrais induire les lecteurs en erreur : un GPS n'émet rien, il ne fait que recevoir des ondes émises par des satellites, et qui sont donc ... "publiques", on ne peut pas vous géolocaliser à distance avec votre GPS de voiture ou de smartphone.

Voir aussi :
Lettre ouverte à ceux qui n'ont rien à cacher
Frenchelon : la DGSE est en « 1ère division »
Du droit à violer la vie privée des internautes au foyer
Frenchelon : la carte des stations espion du renseignement français
Amesys : les documents qui impliquent Ziad Takieddine et Philippe Vannier, le PDG de Bull

jean.marc.manach (sur Facebook & Google+) @manhack (sur Twitter)
Et pour me contacter, de façon anonyme & sécurisée (#oupas /-), c'est par là - See more at : http://bugbrother.blog.lemonde.fr/2013/07/11/la-dgse-a-le-droit-despio...

http://bugbrother.blog.lemonde.fr/2013/07/11/la-dgse-a-le-droit-despio...

http://bugbrother.blog.lemonde.fr/2013/07/11/la-dgse-a-le-droit-despionner-ton-wi-fi-ton-gsm-et-ton-gps-aussi/

http://www.legrandsoir.info/la-dgse-a-le-droit-d-espionner-ton-wi-fi-ton-gsm-et-ton-gps-aussi.html