FLORIAN STOSSE

LA SURVEILLANCE DE MASSE EN EUROPE ET AUX ÉTATS-UNIS :

UNE MENACE POUR LES LIBERTÉS INDIVIDUELLES ?

TUFTE-LATEX.GOOGLECODE.COM

Ce(tte) œuvre est mise à disposition selon les termes de la Licence Creative Commons Attribution - Partage dans les Mêmes Conditions 4.0 International.

Première impression, Juillet 2015

Sommaire

Sommaire 3

Introduction 5

La surveillance de masse : une histoire de programmes 7

Quis custodiet ipsos custodes ? – Qui gardera les gardes ? 25

Conclusion 29

Table des matières 34

Bibliographie 35

Introduction

QUICONQUE N'A PAS vécu en autarcie complète ces derniers mois a forcément entendu parler des révélations faites par Edward Snowden sur les différents programmes mis en place par les agences de renseignement américaines pour surveiller une grande partie de la population mondiale, y compris leur propres concitoyens.

CES RÉVÉLATIONS N'ONT pas surpris beaucoup de monde dans le milieu de la sécurité informatique, de l'hacktivisme, et de la défense des droits des citoyens en général. En effet, depuis les premières révélations sur le programme ECHELON en 1988 par Duncan Campbell [1], il est de notoriété publique que les États-Unis et leurs alliés des Five Eyes [2], dans le cadre du traité UKUSA, ont mis en place une infrastructure à grande échelle d'écoute du spectre électromagnétique (signaux satellites, GSM, fibre optique, micro-ondes, etc).

1. Duncan Campbell. Somebody's listening. *NEW STATESMAN*, 1988

2. Le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande

CE QUI N'ÉTAIT PAS connu jusqu'alors, c'était l'ampleur de la collecte de renseignements, et surtout qui était concerné par ladite collecte. La réponse courte qu'on peut aujourd'hui donner est : *tout le monde* ! Via des accords bilatéraux, les agences de renseignement occidentales ont accès aux méta-données [3] de toute personne connectée, même leurs propres citoyens (alors qu'un service d'espionnage extérieur ne peut normalement pas collecter des données sur ses propres citoyens, mais nous y reviendrons à la page 25)

3. A la différence des données, les méta-données ne sont que les « enveloppes » des communications : qui parle avec qui, quand, où, etc.

CETTE COLLECTE AVEUGLE n'est pas sans poser quelques soucis à nos principes démocratiques fondamentaux, comme par exemple le droit à la correspondance privée [4], et c'est ce que nous allons voir dans ce rapport.

4. Convention européenne des droits de l'homme. article 8

La surveillance de masse : une histoire de programmes

« THEY WHO CAN GIVE UP ESSENTIAL LIBERTY TO OBTAIN A LITTLE TEMPORARY SAFETY, DESERVE NEITHER LIBERTY NOR SAFETY. »

– BENJAMIN FRANKLIN

COMME IL FUT mentionné dans l'introduction, la surveillance généralisée est permise à un niveau industriel à travers l'existence de programmes, aux bases légales diverses, ayant chacun un but précis. Ces programmes fonctionnent (au moins pour le cas des États-Unis) comme des centaines de rouages permettant de faire tourner la grande machine du renseignement.

SERONT PRÉSENTÉS ICI les programmes de surveillance qui ont fait parler d'eux récemment (et moins récemment) via les révélations de Snowden, c'est à dire les programmes américains et les différents programmes européens.

Le programme global des États-Unis

LE PREMIER PROGRAMME connu pour avoir été massif dans ses interceptions est ECHELON. Comme nous l'avons vu en introduction ce dernier fut révélé en 1988 par un journaliste d'investigation spécialisé dans les services de renseignements, mais son origine remonte jusqu'au traité UKUSA signé en 1946. Les autres membres de Five Eyes ne rejoignirent ces deux pays qu'au cours des années 1980, assurant ainsi une couverture globale des interceptions.

FIGURE 1: Cartes de pays membres des Fives eyes.

CE N'EST QU'À la fin des années 1960 [5] qu'ECHELON fut vraiment développé, lors des lancements des premiers satellites Intelsat. La NSA [6] et le GCHQ [7] avaient besoin d'accéder aux communications passées sur ces satellites, et décidèrent donc de développer un réseau de stations d'écoutes terrestres, leur permettant ainsi d'intercepter toutes les communications. Ainsi naquit ECHELON tel qu'on le connaît encore aujourd'hui.

5. Duncan Campbell. Echelon: World under watch, an introduction. *ZDNet*, 2000
6. National Security Agency, l'agence chargée de la collecte des informations électromagnétiques aux États-Unis
7. Government Communications Headquarters, le pendant britannique de la NSA

LE PROGRAMME S'EST renforcé au fur et à mesure des années, avec de nouvelles stations, une orientation vers des interceptions sur fibre optique, etc. Actuellement, il y aurait une quinzaine de stations d'écoutes réparties dans le monde, selon un document de Snowden datant de 2012 [8].

8. Floor Boon, Steven Derix, and Huib Modderkolk. Nsa infected 50,000 computer networks with malicious software. *NRC Handelsblad*, 2013

COMME LE MONTRE la figure 2, les écoutes concernent aussi maintenant les câbles sous-marins (contenant des fibres optiques) par lesquels transitent 99% des communications mondiales.

LA NSA OPÈRE également toute une myriade de programmes de renseignement, afin de donner du sens aux données recueillies par les stations. Du temps d'ECHELON, cela consistait en de gigantesques dictionnaires contenant des mots-clés, que les supercalculateurs en charge de l'analyse pouvaient isoler.

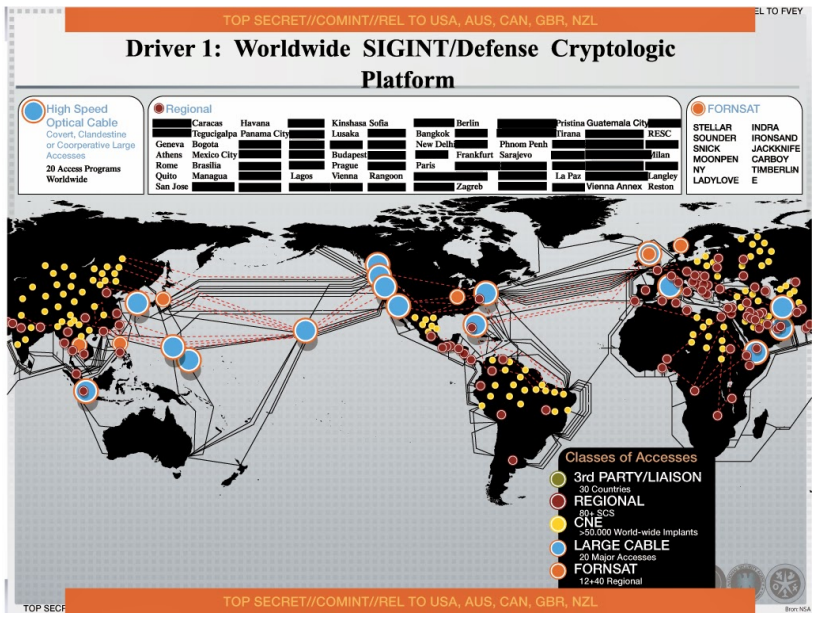


FIGURE 2: Les points oranges représentent les stations d'interceptions satellites.

LES DOCUMENTS DE Snowden ont permis de mettre à jour les détails techniques des nouveaux programmes, dont les plus connus sont :

PRISM

LE PROGRAMME QUI a reçu le plus d'attention médiatique lorsque les premiers documents de Snowden ont commencé à être révélés au public, et certainement à juste titre, puisque le trafic généré par ce programme représente 91% du trafic de la NSA [9]. Les données proviennent exclusivement des grandes entreprises du Web américaines (Google, Facebook, Apple, etc) via l'utilisation de sélecteurs (des mots-clés, ou des requêtes initiées par des analystes) qui vont aller chercher les informations quasiment automatiquement.

9. Barton Gellman and Laura Poitras. U.s., british intelligence mining data from nine u.s. internet companies in broad secret program. *Washington Post*, 2013

CES RÉVÉLATIONS SUR les accès quasi-directs que possède la NSA sur les serveurs des géants du Web furent très mal accueillies par ces derniers, qui ont riposté en activant le chiffrement des communications sur leurs flux internes [10], mettant à mal tout le dispositif clandestin. Il n'en reste pas moins possible de passer par la voie légale pour obtenir les mêmes données.

10. Craig Timberg. Google encrypts data amid backlash against nsa spying. *Washington Post*, 2014

EN EFFET, il est bon de rappeler brièvement que ces programmes ont tous une base légale, à travers le FISA [11]. Ce texte, voté par le Congrès, décrit les modalités de surveillance des citoyens *étrangers*, impliquant que ces écoutes, ces collectes et ces analyses en masse sont légalement permises. Elles n'ont pas été remises en cause depuis l'instauration du Patriot Act en réaction aux attentats du 11 Septembre 2001. Ce n'est que récemment (et suite aux révélations de Snowden) que ces programmes et les pouvoirs qui leurs sont accordés furent remis en

11. Foreign Intelligence Surveillance Act

question.

XKeyScore

L'UN DES PROGRAMME les plus mal connu, malgré les documents publiés, mais également un des plus effrayants, de par l'ampleur de son rayon d'action.

IL PERMETTRAIT, selon Glenn Greenwald, le journaliste qui a interviewé Snowden et récupéré ses documents de « ... lire n'importe quel courriel désiré, écouter n'importe quel appel téléphonique, historique de navigation Web, documents Word. Et tout cela est fait sans demander à une cour, sans demander l'approbation d'un superviseur pour cette part d'analyse. »[12]

12. Snowden-interview: Transcript. *Norddeutscher Rundfunk*, 2014

CE N'EST PAS sans poser problème, puisqu'effectivement, ce dernier ne semble pas avoir besoin de l'approbation de la FISC[13] pour les requêtes qui lui sont fournies[14], contrairement au programme qui le précédait.

13. Foreign Intelligence Surveillance Court

14. Anthony L. Kimery. Nsa x-keyscore does far more than just siphon the net, but is it working ? *Homeland Security Today*, 2013

Bullrun

C'EST ACTUELLEMENT LE programme le plus cher de la NSA, avec un coût total depuis son lancement, il y a dix ans, estimé à 800 millions d'euros[15] (par comparaison, PRISM ne coûte « que » 20 millions d'euros par an...). Sa fonctionnalité première semble être le décryptage de fichiers et de flux chiffrés que l'Agence met de côté lorsqu'elle les intercepte.

15. Ryan W. Neal. Edward snowden reveals secret decryption programs: 10 things you need to know about bullrun and edgehill. *Inernationla Business Times*, 2013

IL SEMBLERAIT AUSSI qu'une autre facette de ce programme soit non plus de l'ordre de la technique, mais dans la manipulation des standards de chiffrement. En effet, il semble que la NSA ait poussé, au sein des instances internationales en charge de la standardisation des méthodes de chiffrement, des protocoles et des algorithmes qu'elle savait pouvoir casser[16] ou dans lesquels elle avait délibérement inséré des portes dérobées.

16. NICOLE PERLROTH, JEFF LARSON, and SCOTT SHANE. N.s.a. able to foil basic safeguards of privacy on web. *The New York Times*, Year

Dishfire

CE PROGRAMME EST actuellement opéré en partenariat avec le GCHQ anglais. Il est spécialisé dans la collecte de messages textes (SMS) et dans la géo-localisation de ces messages, la collecte de cartes de données électroniques, des transactions de cartes de crédit circulant sans chiffrement sur le réseau, les alertes d'appels manqués, les répondeurs, etc.

DES AVEUX MÊME des analystes de la NSA et du GCHQ lors de la présentation interne de ce programme, ce dernier collecte « à peu près tout ce qu'il peut, donc vous pourriez voir des SMS de personnes qui ne sont pas visées par vos requêtes. »[17].

17. James Ball. Nsa collects millions of text messages daily in 'untargeted' global sweep. *The Guardian*, 2014

LE GROS AVANTAGE de ce système est qu'il est possible de venir y fouiller à posteriori. Lorsqu'une nouvelle cible est rentrée dans la base de données, il est ainsi possible de retrouver ses anciens SMS et positions géo-localisées afin d'affiner le profil.

Upstream

LÀ OÙ PRISM pouvait être décrit comme « collecter tout ce qu'il peut être collecté sur les réseaux sociaux », Upstream peut être décrit comme « collecter tout ce qu'on peut sur tout le reste ». Contrairement à PRISM qui est un programme autonome, Upstream se compose de multiples sous-programmes (dont certains se composent eux-même de sous-programmes, il faut arriver à suivre...) :

— FAIRVIEW : le programme chapeautant les trois autres.

— BLARNEY : se concentre sur la collecte de meta-données sur le réseau d'AT&T[18]

18. Grand opérateur de téléphonie américaine.

— STORMBREW : se concentre sur les interceptions au niveau de l'opérateur Verizon.

— OAKSTAR : regroupement de 8 sous programmes, chacun spécialisé dans l'interception de méta-données dans une partie du monde.

SELON LES OFFICIELS, cette collecte génère un flux très important de données, et plusieurs filtres sont appliqués aux données collectées : les opérateurs (AT&T, Verizon, etc) font un premier filtre, en essayant de supprimer au maximum les communications comprenant des citoyens américains. Les communications restantes sont ensuite passées dans des sélecteurs (adresses IP, numéros de téléphone, adresses mail, etc) afin d'en faire ressortir des résultats. Le reste des données Internet peut ensuite être copié et utilisé à travers XKeyScore pour des recherches futures.

TOUT CES PROGRAMMES ne sont que les plus gros exemples qui ont pu être tirés des documents de Snowden. Il en existe encore beaucoup d'autres (BoundLess Informant, RAGTIME, MAINWAY, MonsterMind, MYSTIC, TrailBlazer puis Turbulence, MARINA, Dropmire pour les ambassades, Stateroom, etc), opérés par la NSA seule ou bien en partenariat avec d'autres agences comme le GCHQ ou le BND.

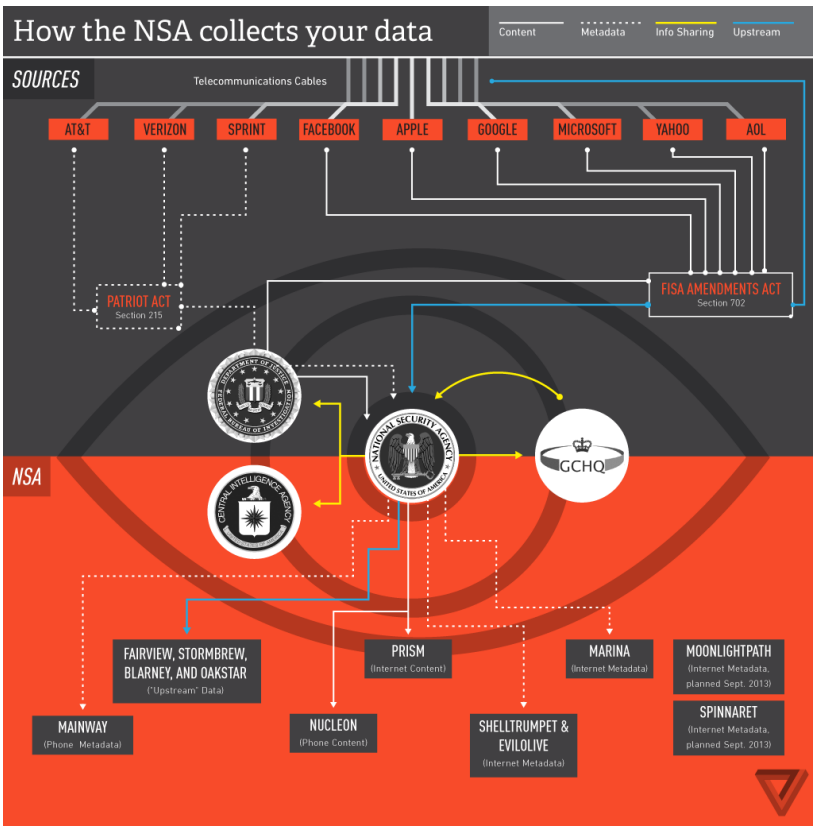


FIGURE 3: Résumé des différents programmes de collecte de données de la NSA.

Les programmes en Europe : introduction

NOUS L'AVONS VU, les agences américaines sont assez prolifiques en matière de programmes de surveillance (avec un budget estimé à 10.3 milliards de dollars pour la NSA[19], en même temps...), mais nous allons voir que les pays européens ne sont pas en reste, avec notamment trois grands compétiteurs sur ce créneau, le Royaume-Uni, l'Allemagne, et la France.

19. Scott Shane. New leaked document outlines u.s. spending on intelligence agencies. *The New-York Times*, 2013

Le Royaume-Uni et le GCHQ

C'EST LE CHAMPION européen de la surveillance électronique de masse. Le Royaume-Uni a une longue tradition dans le domaine du chiffre, il n'est donc pas surprenant de voir les Britanniques très en avance dans ce domaine. Leur partenariat historique avec les États-Unis en font les acteurs désignés pour mener des projets communs avec la NSA, comme nous allons le voir.

LES PLUS GROS programmes britanniques sont les suivant :

Tempora

MIS EN PLACE en 2008, ce programme d'interceptions des communications transitant par fibres optiques est le plus gros programme britannique en matière d'écoute et de renseignement électromagnétique.

ENCORE MAINTENANT, et malgré la publication de divers documents récupérés par Snowden, des doutes subsistent quant aux détails de fonctionnement de ce programme. Par exemple, on ne sait pas si les différents opérateurs propriétaires des fibres optiques mises sur écoutes sont parties prenantes de ce dispositif (il existe de forts soupçons à l'encontre de BT[20], qui collabore déjà avec le GCHQ dans d'autres programmes) ou s'ils sont des victimes forcées des pratiques de services de renseignement.

20. British Telecom

EGALEMENT, NOUS ne savons actuellement pas quelles sont les quantités de données et méta-données collectées, ni si le programme fait la différence entre les données issues des cibles des services et celles des citoyens ordinaires. Le Guardian croit savoir[21] que le programme ne fait pas de différence, ce qui pose de sérieuses questions quant à la légalité de ce programme, puisqu'il n'y a techniquement aucun moyen de différencier de façon fiable les communications de ressortissants britanniques et celles des étrangers, et que l'écoute des premiers n'est pas encadrée par les mêmes lois que l'écoute des seconds.

21. Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. Gchq taps fibre-optic cables for secret access to world's communications. *The Guardian*, 2013

DANS TOUS LES cas, les données recueillies par ce programme sont échangées avec la NSA dans le cadre des accords bilatéraux qui ont cours entre les deux agences de renseignement, ce qui permet à chacune de s'affranchir des limitations juridiques que leur imposent les lois les encadrant. Le GCHQ peut récupérer des informations et des méta-données sur les citoyens américains, chose que ne peut pas faire la NSA légalement, et les transmettre à cette dernière, et inversement[22]. Cela permet aux deux agences d'espionner leurs ressortissants tout en s'affranchissant du contrôle des instances judiciaires de leurs pays respectifs, ce qui est plus que discutable sur le plan de l'éthique.

22. Barton Gellman and Ashkan Soltani. Nsa infiltrates links to yahoo, google data centers worldwide, snowden documents say. *The Washington Post*, 2013

MUSCULAR

MUSCULAR EST LE nom du programme mis sur pied par le GCHQ afin de pénétrer les réseaux internes de deux entreprises américaines, Google et Yahoo !. D'un strict point de vue technique, le programme tirait parti du manque de sécurisation des-dits réseaux[23] [24] (où les responsables de la sécurité ont très mal pris la nouvelle, sachant qu'ils étaient déjà obligés de collaborer dans le cadre de PRISM avec les autorités. . .)

23. Barton Gellman and Ashkan Soltani. Nsa infiltrates links to yahoo, google data centers worldwide, snowden documents say. *The Washington Post*, 2013

24. Russell Brandom. Yahoo plans to encrypt all internal data by early 2014 to keep the nsa out. *The Verge*, 2013

CE PROGRAMME COLLECTE apparemment beaucoup plus de méta-données que ne le fait PRISM (environ deux fois plus[25]), ce qui été un défi technique pour la NSA (XKeyScore se « nourrissant » de ces données en plus de celles de PRISM, il a fallu re-dimensionner une

25. Barton Gellman and Ashkan Soltani. Nsa infiltrates links to yahoo, google data centers worldwide, snowden documents say. *The Washington Post*, 2013

partie de l'architecture).

Squeaky Dolphin

C'EST LE PREMIER programme qui ne sert pas à récolter des données sur des individus. En effet, celui-ci est dédié à l'analyse des tendances sur les réseaux sociaux, notamment via le suivi des données issues des boutons « J'aime » de Facebook (données qui sont depuis cette révélation chiffrées [26]) ainsi que des données statistiques des vidéos vues sur Youtube, des visites faites sur les blogs de la plate-forme Blogspot (propriété de Google), ainsi que des données disponibles sur Twitter.

26. Snowden docs reveal british spies snooped on youtube and facebook. *NBC News*, 2014

Optic Nerve

PROGRAMME UN PEU singulier par son aspect très ouvert, Optic Nerve s'intéresse très spécifiquement aux conversations par webcam des utilisateurs de la messagerie Yahoo ![27], sans chercher précisément des cibles pré-enregistrées.

LE PROGRAMME EST supposé avoir capturé des millions d'images, à raison de cinq images par seconde[28], dont de nombreuses images à caractère sexuel ou pornographique. Cela a permis au GCHQ de tester et de peaufiner des algorithmes de reconnaissance faciale.

A TRAVERS CES quelques exemples, nous voyons bien que la Grande-Bretagne n'est pas en reste en matière de surveillance de masse. Le liens de coopération privilégiée tissés avec la NSA lui assure un accès quasiment illimité à XKeyScore et une grande marge de manoeuvre dans la mise en place de ses propres projets.

27. Spencer Ackerman and James Ball. Optic nerve: millions of yahoo webcam images intercepted by gchq. *The Guardian*, 2014

28. Le service webcam de yahoo, l'oeil de londres pour espionner les internautes ? *La Tribune*, 2014

FIGURE 4: Les bureaux du GCHQ en photographie aérienne.

L'Allemagne et le BND

LE BND[29] EST le service de renseignement extérieur allemand, et le pendant technique de la NSA en Allemagne. Les détails exacts de leur coopération ne sont pas tous connus, mais on peut au moins citer quelques événements récents qui mettent en lumière des liens de coopération étroits (bien que moins solides qu'avec le GCHQ).

29. Bundesnachrichtendienst

Opération EIKONAL

IL EXISTE ACTUELLEMENT très peu de détails techniques sur cette opération, bien que de nombreux documents et témoignages soient venus récemment (mai 2015) apporter un éclairage nouveau sur ce programme qui s'est déroulé entre 2004 et 2008.

CES NOUVEAUX ÉLÉMENTS ont été apportés par les journaux allemands Süddeutsche Zeitung[30], NDR et WDR[31], et montrent que la BND, en partenariat avec Deutsche Telekom, a placé des équipements réseau (des sondes, en l'occurrence) fournis par la NSA au sein du noeud d'échange (noeud PoP) maintenu par l'opérateur allemand, à Francfort.

30. Georg Mascolo, Hans Leyendecker, and John Goetz. Codewort eikonal - der albtraum der bundesregierung. *Sudeutsche Zeitung*, 2014
31. Georg Mascolo, John Goetz, and Demian von Osten. Codename eikonal. *tagesschau.de*, 2014

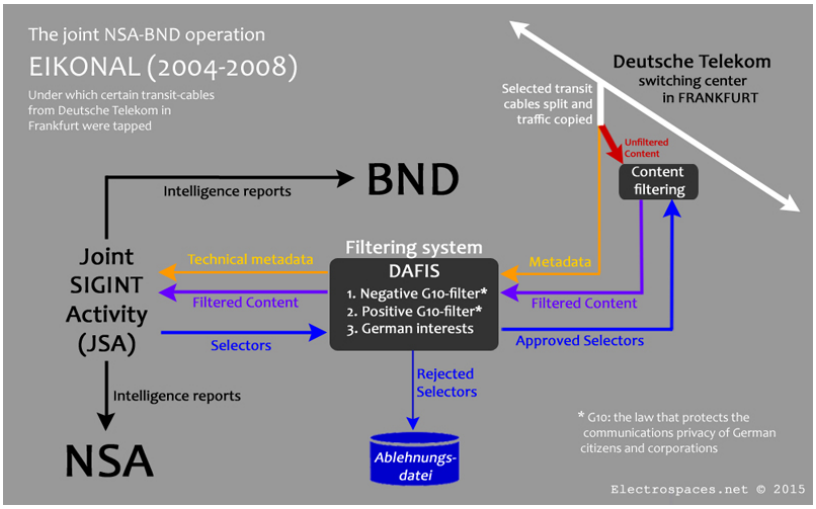


FIGURE 5: Architecture technique de l'opération

CE SCHÉMA MONTRE l'organisation technique de l'opération : les métadonnées ainsi qu'une partie spécifique du trafic sont récupérées et passent à travers un filtre nommé DAFIS, qui sert à différencier les communications provenant de citoyens allemands (que la BND n'a pas, légalement, le droit d'espionner, de part son statut de service de renseignement *extérieur*. Dans ce cas de figure, elle doit passer par un « ordre G10 » pour accéder aux communications). En fonction des résultats après passage dans le filtre, les données sont soit renvoyés à la

BND, soit directement à la NSA. Le schéma décisionnel est reproduit ci-dessous :

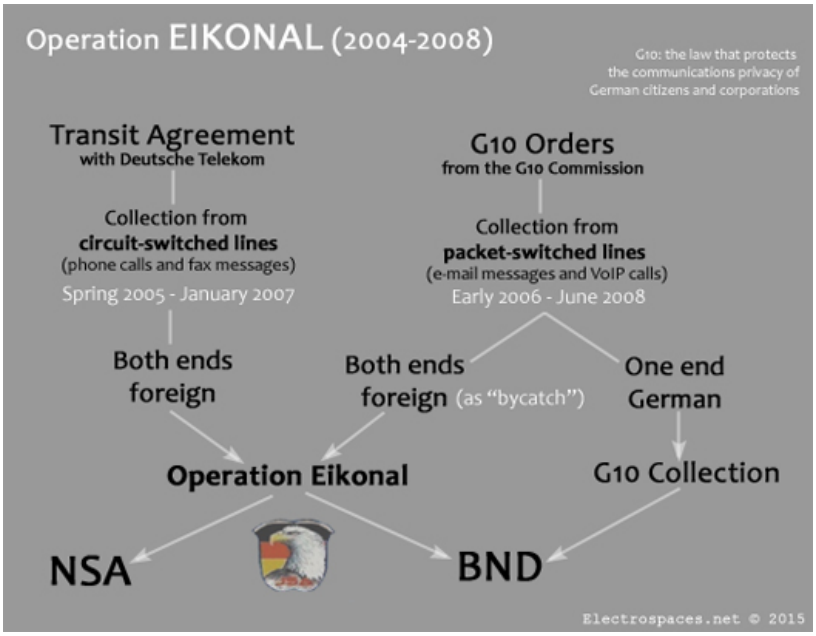
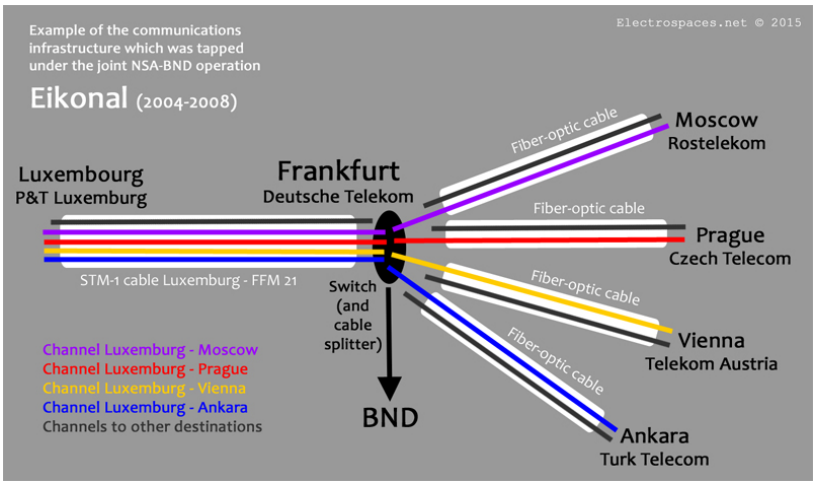


FIGURE 6: Schéma décisionnel

LA MISE SUR ÉCOUTE concernait plus spécifiquement le câble FFM 21 reliant le Luxembourg et Francfort, contenant des canaux de fibres optiques reliant le Luxembourg à Moscou, Prague, Vienne (où se trouvent des instances de l'ONU) et Ankara [32]. Cela permettait à la NSA d'accéder à une partie du monde auquel elle est très mal reliée directement.



32. Andre Meister. Interne e-mail: Bnd und deutsche telekom haben auch osterreich, tschechien und luxemburg abgehort. *Netzpolitik*, 2015

FIGURE 7: Schéma des canaux mis sur écoute

EIKONAL A FAIT parti d'un programme plus large de la NSA de coopération avec des pays dits « tiers », qui sont des pays ne faisant pas partie de Five Eyes, mais qui coopèrent avec la NSA, de façon ponctuelle (comme ici) ou de façon plus constante. Ce programme est nommé RAMPART-A, et concerne un nombre inconnu de pays. L'Allemagne est connue pour en faire partie, alors que de forts soupçons pèsent sur le Danemark[33] et qu'il est rapporté, via des slides publiées par Snowden, qu'au moins cinq pays possèdent des moyens similaires déployés sur leurs réseaux nationaux.

33. Anton Geist, Sebastian Gjerding, and Henrik Moltke. German disclosure raises questions about danish nsa-partnership. *information.dk*, 2015

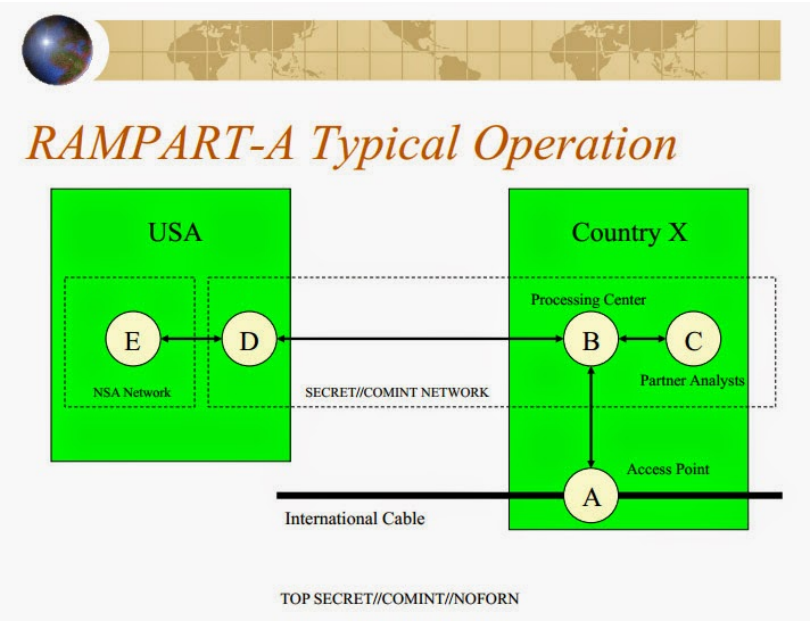


FIGURE 8: Schéma de l'opération RAMPART-A

La station de Bad Aibling : nom de code GARLICK

FIGURE 9: Station d'interception de Bad Aibling, opérée par la BND à partir de 2004.

CETTE STATION EST une ancienne station d'écoute du réseau ECHELON, et appartenait anciennement à la NSA, qui l'a depuis rendue à l'Etat Fédéral en 2004 (tout en gardant une équipe opérationnelle sur le site).[34]

34. Spying together: Germany's deep cooperation with the nsa. *Spiegel*, 2014

IL FUT RÉVÉLÉ que la NSA pouvait accéder directement aux données des interceptions, et fournissait même quatre des cinq listes de sélecteurs utilisées pour savoir quoi chercher dans le flux de données (adresses IP, numéros de téléphone, etc).

INITIALEMENT TRÈS PETITES, c'est listes ce sont graduellement remplies, au point que des contrôles manuels ne furent plus possibles. Elles furent donc envoyées automatiquement plusieurs fois par semaine au siège de la BND, où elles passaient à travers le DAFIS (voir page 16) afin d'exclure les communications impliquant des ressortissants ou citoyens allemands, puis souvent renvoyées tel quel à la NSA.

CES SÉLECTEURS FURENT à l'origine d'un scandale à portée européenne lorsqu'il fut révélé par certains médias allemands que ces listes contenaient des entrées visant des employés du groupe Airbus[35].

35. Bnd-affare: Verdacht der industriespionage gegen airbus erhartet sich. *Spiegel*, 2015

AU TOTAL, la collecte de méta-données, transmises directement à la NSA après être passées par DAFIS, était de l'ordre de 200-220 millions par jour, soit environ 6.6 milliards de méta-données collectées par mois...[36]

36. KAI BIERMANN. Bnd liefert nsa 1,3 milliarden metadaten âĂŞ jeden monat. *Die Zeit*, Year

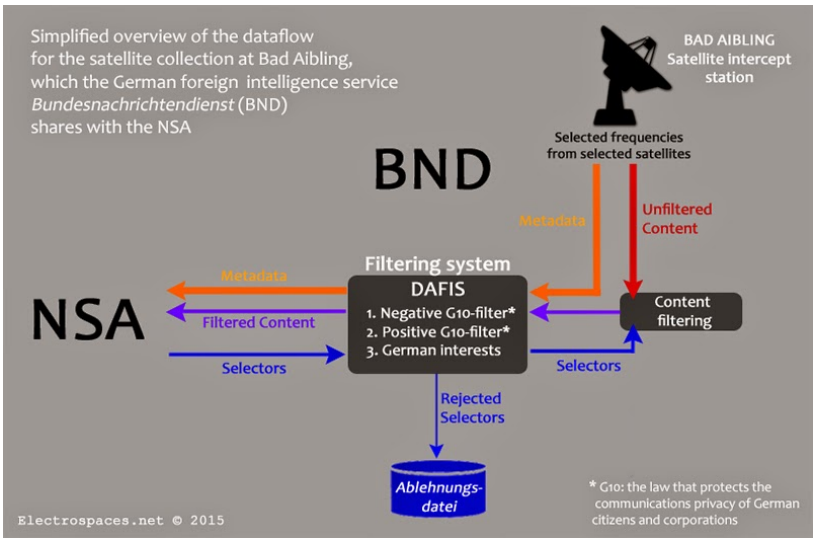


FIGURE 10: Schéma des interceptions à Bad Aibling

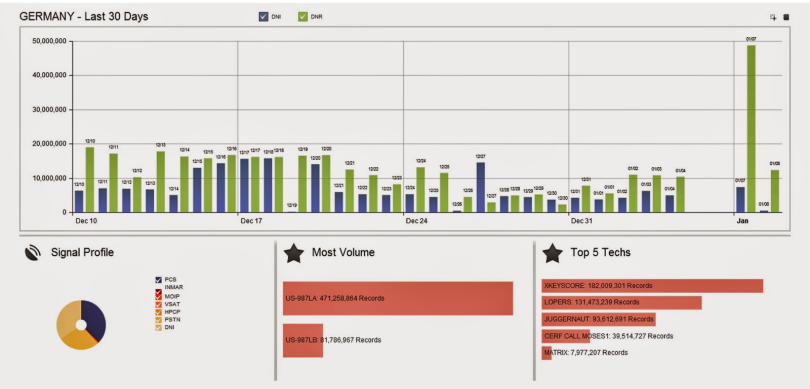


FIGURE 11: 552 millions de meta-données entre décembre 2013 et janvier 2013...

La France et la DGSE

LA FRANCE A elle aussi une longue tradition dans le chiffre, et ses services de renseignement extérieur font partie des meilleurs du monde. Contrairement au Royaume-Uni et à l'Allemagne, elle dispose de gros moyens propres, et n'a donc pas une tradition de coopération avec la NSA aussi forte que ses voisins.

EN EFFET, de part la présence d'un opérateur de catégorie mondiale sur son territoire (Orange) ainsi que de différents points d'arrivées de câbles sous-marins (Marseille pour le Proche-Orient notamment), la France est à un carrefour stratégique des autoroutes numériques. La DGSE l'a bien compris, et opère dans ses locaux parisiens le second plus gros programme de surveillance européen, après celui des anglais. . . [37]

PAS FRANCHEMENT LÉGAL, ce programme est soupçonné d'avoir été complété par des installations [38] d'équipements fournis par une société *française* spécialisée dans la technique dite de DPI [39], Amesys (filiale du géant français Bull. . .). Cette dernière a fait l'objet d'une très longue saga d'articles publiés chez les journalistes d'investigation de Reflets.info, et il n'est pas inutile d'aller lire la centaine de documents publiés pour se rendre compte de la complexité de la chose.

IL SERAIT TROP long de faire un descriptif exhaustif des faits, mais on peut retenir plusieurs choses :

— Amesys a vendu un de ses produit d'interception de masse (au niveau d'un pays), EAGLE, au régime totalitaire de Kadhafi [40]

— Amesys est actuellement en train d'installer le même équipement au Maroc [41], ce qui inquiète fortement les opposants au régime marocain, déjà fortement réprimés.

— Qosmos, un autre leader du DPI et lui aussi français, a vendu des sondes d'inspection au régime de Bachar al-Assad en Syrie [42]

— Une plainte a été déposée par la FIDH pour « complicité de crimes de torture » contre Qosmos et Amesys devant le Parquet de Paris. [43]

CES FAITS SONT d'autant plus troublants que la société Elexo, soeur d'Amesys, vient de candidater [44] pour le marché public ouvert pour la nouvelle Loi sur le Renseignement, votée il y a peu, et instaurant la mise en place de « boîtes noires » sur les coeurs de réseau de l'Internet français [45] (du DPI légal, en somme).

37. Laurent Borredon and Jacques Follorou. En france, la dgse au coeur d'un programme de surveillance d'internet. *Le Monde*, 2013

38. Et si... on etait tous libyens ? *Reflets.info*, 2011

39. Deep Packet Inspection : l'analyse des flux de données en profondeur

40. PAUL SONNE and MARGARET COKER. Firms aided libyan spies. *Wall Street Journal*, 2011

41. Maroc : Le meilleur ami de la france se met au dpi grace a amesys, la filiale de bull. *Reflets.info*, 2011

42. Reflets Mediapart. Surveillance: enquete sur qosmos, le fournisseur de sondes a la syrie dâĂŹal-assad. *Reflets.info*, 20014

43. FIDH. Questions/reponses sur l'affaire qosmos. 2012

44. Etat francais et amesys : business as usual (bis repetita). *Reflets.info*, 2015

45. Claude Malhuret and Francois Pellegrini. La loi renseignement, un projet liberticide en l'etat. *LibÃľration*, 2015

Frenchelon

CONTRACTION DES TERMES « French » et « ECHELON », ce nom désigne les stations d'écoutes opérées sur le territoire national par la DGSE [46] et la DRM [47]. Il en existerait une quinzaine, dont la plus importante se situe à Domme :

46. Direction Générale de la Sécurité Extérieure, les services secrets français
47. Direction du Renseignement Militaire, la branche en charge des renseignements au sein de l'Armée.

FIGURE 12: Station d'écoute de la DGSE à Domme

TOUT COMME ECHELON, le programme français permet d'intercepter de grandes quantités de données sur tout le spectre électromagnétique, afin d'être analysées plus tard. Ces données peuvent être ensuite utilisées par tous les acteurs du renseignement en France, et sont stockées dans les locaux parisiens de la DGSE. [48]

48. Jacques Follorou and Franck Johannes. Revelations sur le big brother franÃğais. *Le Monde*, 2013

LES TECHNOLOGIES UTILISÉES par ce programme sont en partie issues d'appels d'offres de la DGA et de développements assurés par EADS (aujourd'hui Airbus Defence And Space), notamment le système HERISSON [49] [50] en charge de l'extraction de renseignements en sources ouvertes (réseaux sociaux, Internet, etc).

49. Habile extraction du renseignement d'intérêt stratégique à partir de sources ouvertes numérisées
50. Herisson et osint. *Zone d'Interet*, 2009

L'accord LUSTRE

DERRIÈRE CE NOM se cache l'accord d'échange de données interceptées signé entre la DGSE pour la partie française et la NSA pour la partie américaine. C'est l'équivalent de l'accord UKUSA, mais contrairement à ce dernier, très peu d'informations sont disponibles sur les modalités de l'accord.

L'ACCORD FUT SIGNÉ fin 2011[51], et permet à la France d'accéder aux données de la NSA sur des parties du monde où ses capacités de renseignement sont limitées, tandis qu'elle fournit à la NSA des données sur lesquelles la France dispose de bonnes connexions (voir figure 13), notamment le Proche-Orient et l'Afrique (il y a environ trente fois plus de trafic Afrique -> Europe qu'Afrique -> États-Unis).

51. Jacques Follorou. Surveillance : la dgse a transmis des donnees a la nsa americaine. *Le Monde*, 2013

1. Penmarch, France
2. Lisbonne, Portugal
3. Tenerife, Espagne
4. Nouakchott, Mauritanie
5. Dakar, Sénégal
6. Banjul, Gambie
7. Conakry, Guinée
8. Freetown, Sierra Leone
9. Monrovia, Libéria
10. Abidjan, Côte d'Ivoire
11. Accra, Ghana
12. Cotonou, Bénin
13. Lagos, Nigéria
14. Kribi, Cameroun
15. Bata, Guinée Equatoriale
16. Libreville, Gabon
17. Santana, Sao Tomé-et-Principe
18. Muanda, République Démocratique du Congo
19. Luanda, Angola
20. Swakopmund, Namibie
21. Le Cap, Afrique du Sud

FIGURE 13: Câble sous-marin reliant l'Afrique à l'Europe

CES INFORMATIONS EXPLIQUENT en partie le relatif silence des autorités françaises à propos des révélations d'Edward Snowden, puisqu'elle se permet de faire exactement la même chose de son côté. Il est d'ailleurs intéressant de noter que l'accord LUSTRE fut révélé au public par le Général Keith Alexander[52] lors d'une audition devant la commission de renseignement américaine, après que les pays européens, dont la France, ont commencé à protester contre les révélations faites sur PRISM. Faites ce que je dis...

52. La directeur de la NSA de l'époque

Quis custodiet ipsos custodes ? – Qui gardera les gardes ?

« LA SEULE CHOSE QUI PERMET AU MAL DE TRIOMPHER EST L'INACTION DES HOMMES DE BIEN. »

– EDMUND BURKE

LES SERVICES DE RENSEIGNEMENT sont une émanation du pouvoir politique, et sont sensés être sous son contrôle, et donc sous le contrôle indirect du peuple. Cet état de fait rend donc assez difficilement compréhensible la boulimie d'informations dont font preuve les services à l'encontre même de leurs concitoyens.

OUTRE L'INEFFICACITÉ flagrante de ces programmes [53] (la débauche de programmes différents aux États-Unis n'a par exemple pas permises de déjouer les attentats de Boston, pas plus que les écoutes en France n'ont permis de déjouer les attentats de janvier contre Charlie Hebdo), c'est leur aspect légal qui est aujourd'hui remis en question.

53. Bruce Schneier. Why mass surveillance can't, won't, and never has stopped a terrorist. *Digg.com*, 2015

EN EFFET, bien qu'adossés au Patriot Act et FISA, les programmes de surveillance américains sont contestés légalement, d'une part par les pays qui en sont « victimes » ou qui voient leurs communications écoutées, d'autre part par certains élus locaux, qui estiment que l'automatisme caractérisé desdits programmes empêche de facto tout contrôle humain, et donc rend la surveillance incontrôlable.

IL FAUT BIEN comprendre que l'aspect massif de ces programmes nécessite forcément de faire appel à d'autres algorithmes de surveillance, qui n'ont pas une efficacité de 100% (et ne s'en rapprochent même pas d'ailleurs). Le contrôle humain est ainsi très limité, et ne peut de toutes façons que concerner une infime portion de ce qui est réellement récolté. Quelle instance de contrôle pourrait vérifier des dizaines de milliards de données par mois ? Qui peut certifier que dans ce tas de données ne figurent pas des choses qui ne sont pas légalement sensées être là ? A tout hasard, des communications de nos propres citoyens...

LA FRANCE A même réussi à faire encore plus fort que ça, en légalisant *a posteriori* des dispositifs mis en place depuis des années, présents sur le territoire français, alors que ces derniers n'étaient encadrés par aucun texte jusqu'au récent vote de la Loi sur le Renseignement.[54] En effet, malgré l'existence d'une commission chargé du contrôle des interceptions de sécurité (la CNCIS), une grande partie des écoutes opérées sur le territoire nationale se retrouvent hors de sa portée, et donc hors de tout contrôle externe à la hiérarchie des services.

54. LOUISE FESSARD and MATHILDE MATHIEU. Antiterrorisme et grandes oreilles : le contrÃť le des Ãľcoutes est un casse-tÃłte. *Mediapart*, 2015

L'avis du Conseil de l'Europe

APRÈS LES PREMIÈRES révélations d'Edward Snowden et les légitimes questions qu'elles soulèvent, le Conseil de l'Europe a commandé un rapport étudiant la légalité de ces dispositifs au regard du droit européen.

UN AN PLUS TARD, soit début janvier 2015, ce rapport est publié[55] et dénonce de façon très vive et très critique les pratiques de la NSA, et donc de facto celles des autres services, y compris européen. Même les plus conservateurs des membres de ce Conseil ont ratifié le texte en l'état, sans amendement.

55. Pieter Omtzigt. Les opÃľrations massives de surveillance. *Conseil de l'Europe*, 2015

CET ARTICLE est très clair quant à la nature complètement illégale de ces programmes : « Ces opérations mettent en danger les droits de l'homme fondamentaux, notamment le droit au respect de la vie privée [...], le droit à la liberté d'information et d'expression [...], le droit à un procès équitable et à la liberté de religion. » Ce type d'espionnage serait, toujours selon ce rapport, une violation de la Convention européenne des droits de l'homme et de la convention du Conseil de l'Europe sur la protection des données personnelles...

A NOTER QUE pour la rédaction de ce rapport, ni les services américains, ni, et c'est plus surprenant, les services européens ont accepté de collaborer et/ou d'être entendus par les rapporteurs. Si la chose est parfaitement compréhensible pour les services américains, qui ne sont pas tenus de rendre des comptes à une puissance étrangère, l'attitude des services européens est quant à elle bien plus étrange, et prouve qu'un véritable malaise juridique règne quant à la légalité de ces programmes.

LE RAPPORT S'EN prends même indirectement à la classe politique : « L'emballement de cette machine de surveillance est dû au fait que les dirigeants politiques ont perdu le contrôle des activités des services de renseignement. », ce qui est parfaitement en phase avec les révélation faites par Mediapart, décrites plus haut, sur la perte de contrôle de la CNCIS en France.

IL FAUT BIEN comprendre qu'un citoyen peut se retrouver dans plusieurs cas de figure, vis à vis de ces programmes :

— Un citoyen normal ne saura jamais si ses données ont pu être interceptées et exploitées, ni sur quelle base cela fut demandé, alors que c'est pourtant son droit le plus strict. Après tout, « Notre liberté repose sur ce que les autres ignorent de notre existence. »[56]

— Un citoyen curieux n'a actuellement aucun recours, aucune instance juridique vers laquelle se tourner si il soupçonne que ses données aient pu être interceptée sans raison légale.

— Un citoyen soucieux de son droit à la vie privée n'a aujourd'hui que très peu d'options techniques pour échapper à cette surveillance aveugle, la dissymétrie de moyens mis en place par les services (financiers et techniques) étant trop importante.

56. Citation tirée du rapport.

Freedom Act

AUX ÉTATS-UNIS, suite à de nombreuses pressions juridiques (à travers des organismes comme l'ACLU[57] et l'EFF[58]) et populaires, les lignes commencent à bouger. Le récent vote du Freedom Act, sensé rétablir des contrôles et empêcher toute collecte aveugle, a été obtenu de haute lutte[59].

MÊME SI CERTAINS pensent que ce texte ne va pas assez loin et aurait du exiger une abrogation complète de ces programmes et une réforme des services de renseignement, ce texte fut accueilli plutôt positivement par les opposants à la surveillance de masse.

57. American Civil Liberties Union
58. Electronic Frontier Foundation

59. NEEMA SINGH GULIANI. WhatâĂŹs next for surveillance reform after the usa freedom act. *ACLU Blog*, 2015

Conclusion

IL N'EST PAS évident de conclure sur un tel sujet, ne serait-ce que parce des changements peuvent se produire à une vitesse insoupçonnée (comme ce fut le cas avec le Freedom Act), et que des conclusions vraies aujourd'hui s'avéreront sans doute fausses demain.

QUOI QU'IL EN SOIT, certains choses sont aujourd'hui claire concernant ces programmes de surveillance : quand ils ne sont pas purement illégaux, ces derniers bafouent allégrement les libertés individuelles de tout un chacun, au nom d'une sécurité somme toute relative, puisque l'efficacité de ces programmes est remise en cause par tous les rapports (cela n'empêche pas la France de voter une Loi sur le Renseignement qui sera inapplicable techniquement...)

SANS LE SAVOIR, et sans le mériter, des millions de personnes ont perdu ces dernières années une partie de leur liberté, afin de satisfaire aux délires des sécuritaires de nos élites, qui ne pouvaient pas ne pas être au courant des agissements des services (quand ils ne s'occupent pas directement de la chose... En effet, Ziad Takieddine, proche de Nicolas Sarkozy, à négocié directement la vente de l'Eagle d'Amesys avec Kadhafi...)

CES PROGRAMMES, aux dérives caractéristiques des régimes totalitaires, ne peuvent en aucun cas être acceptés sous couvert de la sécurité, ou de tout autre prétexte, ne serait-ce que parce qu'elles sont contraires aux valeurs des Nations qu'ils prétendent protéger. Dans leur forme actuelle, ils sont dangereux pour les libertés individuelles et pour la survie de nos régimes démocratiques.

Table des figures

1 Cartes de pays membres des Five Eyes 8
2 Carte des stations d'interceptions 9
3 Infographie résumant les différents programmes de surveillance américains 12
4 Les bureaux du GCHQ en photographie aérienne 15
5 Architecture de l'opération EIKONAL 16
6 Schéma décisionnel de l'opération EIKONAL 17
7 Schéma des canaux mis sur écoute 17
8 Schéma de l'opération RAMPART-A 18
9 Station d'interception de Bad Aibling 19
10 Schéma des interceptions à Bad Aibling 20
11 Capture écran de BOUNDLESSINFORMANT pour l'Allemagne 20
12 Station d'écoute de Domme 22
13 Câble sous-marin reliant l'Afrique à l'Europe 23

Table des matières

Sommaire 3

Introduction 5

La surveillance de masse : une histoire de programmes 7

Le programme global des États-Unis 8

PRISM 9

XKeyScore 10

Bullrun 10

Dishfire 10

Upstream 11

Les programmes en Europe : introduction 12

Le Royaume-Uni et le GCHQ 12

Tempora 12

MUSCULAR 13

Squeaky Dolphin 14

Optic Nerve 15

L'Allemagne et le BND 16

Opération EIKONAL 16

La station de Bad Aibling : nom de code GARLICK 19

La France et la DGSE 21

Frenchelon 22

L'accord LUSTRE 23

Quis custodiet ipsos custodes ? – Qui gardera les gardes ? 25

L'avis du Conseil de l'Europe 26

Freedom Act 27

Conclusion 29

Table des matières 34

Bibliographie 35

Bibliographie

[1] Convention européenne des droits de l'homme. article 8.

[2] Herisson et osint. *Zone d'Interet*, 2009.

[3] Et si... on etait tous libyens ? *Reflets.info*, 2011.

[4] Maroc : Le meilleur ami de la france se met au dpi grace a amesys, la filiale de bull. *Reflets.info*, 2011.

[5] Le service webcam de yahoo, l'oeil de londres pour espionner les internautes ? *La Tribune*, 2014.

[6] Snowden docs reveal british spies snooped on youtube and facebook. *NBC News*, 2014.

[7] Snowden-interview : Transcript. *Norddeutscher Rundfunk*, 2014.

[8] Spying together : Germany's deep cooperation with the nsa. *Spiegel*, 2014.

[9] Bnd-affare : Verdacht der industriespionage gegen airbus erhartet sich. *Spiegel*, 2015.

[10] Etat francais et amesys : business as usual (bis repetita). *Reflets.info*, 2015.

[11] Spencer Ackerman and James Ball. Optic nerve : millions of yahoo webcam images intercepted by gchq. *The Guardian*, 2014.

[12] James Ball. Nsa collects millions of text messages daily in 'untargeted' global sweep. *The Guardian*, 2014.

[13] KAI BIERMANN. Bnd liefert nsa 1,3 milliarden metadaten – jeden monat. *Die Zeit*, Year.

[14] Floor Boon, Steven Derix, and Huib Modderkolk. Nsa infected 50,000 computer networks with malicious software. *NRC Handelsblad*, 2013.

[15] Laurent Borredon and Jacques Follorou. En france, la dgse au coeur d'un programme de surveillance d'internet. *Le Monde*, 2013.

[16] Russell Brandom. Yahoo plans to encrypt all internal data by early 2014 to keep the nsa out. *The Verge*, 2013.

[17] Duncan Campbell. Somebody's listening. *NEW STATESMAN*, 1988.

[18] Duncan Campbell. Echelon : World under watch, an introduction. *ZDNet*, 2000.

[19] LOUISE FESSARD and MATHILDE MATHIEU. Antiterrorisme et grandes oreilles : le contrôle des écoutes est un casse-tête. *Mediapart*, 2015.

[20] FIDH. Questions/reponses sur l'affaire qosmos. 2012.

[21] Jacques Follorou. Surveillance : la dgse a transmis des donnees a la nsa americaine. *Le Monde*, 2013.

[22] Jacques Follorou and Franck Johannes. Revelations sur le big brother français. *Le Monde*, 2013.

[23] Anton Geist, Sebastian Gjerding, and Henrik Moltke. German disclosure raises questions about danish nsa-partnership. *information.dk*, 2015.

[24] Barton Gellman and Laura Poitras. U.s., british intelligence mining data from nine u.s. internet companies in broad secret program. *Washington Post*, 2013.

[25] Barton Gellman and Ashkan Soltani. Nsa infiltrates links to yahoo, google data centers worldwide, snowden documents say. *The Washington Post*, 2013.

[26] NEEMA SINGH GULIANI. What's next for surveillance reform after the usa freedom act. *ACLU Blog*, 2015.

[27] Anthony L. Kimery. Nsa x-keyscore does far more than just siphon the net, but is it working ? *Homeland Security Today*, 2013.

[28] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. Gchq taps fibre-optic cables for secret access to world's communications. *The Guardian*, 2013.

[29] Claude Malhuret and Francois Pellegrini. La loi renseignement, un projet liberticide en l'etat. *Libération*, 2015.

[30] Georg Mascolo, John Goetz, and Demian von Osten. Codename eikonal. *tagesschau.de*, 2014.

[31] Georg Mascolo, Hans Leyendecker, and John Goetz. Codewort eikonal - der albtraum der bundesregierung. *Suddeutsche Zeitung*, 2014.

[32] Reflets Mediapart. Surveillance : enquete sur qosmos, le fournisseur de sondes a la syrie d'al-assad. *Reflets.info*, 20014.

[33] Andre Meister. Interne e-mail : Bnd und deutsche telekom haben auch osterreich, tschechien und luxemburg abgehort. *Netzpolitik*, 2015.

[34] Ryan W. Neal. Edward snowden reveals secret decryption programs : 10 things you need to know about bullrun and edgehill. *Inernationla Business Times*, 2013.

[35] Pieter Omtzigt. Les opérations massives de surveillance. *Conseil de l'Europe*, 2015.

[36] NICOLE PERLROTH, JEFF LARSON, and SCOTT SHANE. N.s.a. able to foil basic safeguards of privacy on web. *The New York Times*, Year.

[37] Bruce Schneier. Why mass surveillance can't, won't, and never has stopped a terrorist. *Digg.com*, 2015.

[38] Scott Shane. New leaked document outlines u.s. spending on intelligence agencies. *The New-York Times*, 2013.

[39] PAUL SONNE and MARGARET COKER. Firms aided libyan spies. *Wall Street Journal*, 2011.

[40] Craig Timberg. Google encrypts data amid backlash against nsa spying. *Washington Post*, 2014.