LES RÉVÉLATIONS DE SNOWDEN, INTERCEPTION MASSIVE DE DONNÉES ET ESPIONNAGE POLITIQUE

Étude des sources ouvertes[1]

INTRODUCTION

(1) Le présent rapport présente un aperçu, au moyen de sources ouvertes, des types de données susceptibles de porter sur des (ou d'émaner de) personnes, organisations, entreprises ou instances établies en Belgique (ou qui ont un lien avec la Belgique) et qui sont interceptées et enregistrées à grande échelle par la NSA (National Security Agency) américaine, le GCHQ britannique (Government Communications Headquarters), ou des sociétés privées opérant pour le compte de ces services, et ce en vue d'une (éventuelle) exploitation (ultérieure) par leurs services de renseignement. Parallèlement, ce rapport présente des cas dont il ressort que ces services (parmi d'autres) ont mis sur pied, ces dernières décennies, des opérations d'espionnage politique à l'égard de « pays alliés ». Les sources ouvertes consultées aux fins du présent rapport sont de qualité variable. Nous avons autant que possible utilisé des sources primaires (*slides*, documents officiels) qui ont été publiées ces derniers mois par des journalistes d'investigation. L'interprétation critique de ces éléments (incomplets) d'information s'est appuyée sur la consultation d'autres experts. Nous n'avons pas retenu les analyses de presse trop spéculatives, où nous n'avons trouvé aucune information complémentaire venant étayer une piste de réflexion. Une liste explicative des abréviations figure en annexe.

(2) Toutefois, pour mieux comprendre les mécanismes spécifiques de recueil qui ont été dévoilés depuis juin 2013, il convient au préalable de décrire brièvement le contexte légal dans lequel opèrent la NSA et le GCHQ, car il éclaire également le mandat et les mesures de précaution qui s'appliquent ou non à l'exercice de ce mandat. Nous avons aussi tenté de faire dans tous les cas la lumière sur l'ampleur du recueil de données et sur la période d'activité de ces mécanismes de recueil.

(3) L'expérience relative aux documents de Snowden nous apprend à ce stade que les documents confidentiels qui n'ont pas encore été publiés, et qui le seront probablement à l'avenir, auront un impact sur l'interprétation de documents et d'informations déjà publiés à

---

1 Le Comité permanent R a confié la présente étude des sources ouvertes aux bons soins du Dr Mathias Vermeulen, chercheur à l'Institut universitaire européen de Florence et au sein du groupe de recherche LSTS (Law, Science, Technology and Society) de la VUB. De 2008 à 2011, le Dr Mathias Vermeulen a travaillé en tant que chercheur aux côtés du Rapporteur spécial des Nations unies sur la promotion et la protection des droits de l'homme et la lutte contre le terrorisme. Il s'est également penché, pour le compte du Parlement européen, sur le contrôle parlementaire des services de sécurité et de renseignement au sein de l'Union européenne ('Parliamentary oversight of security and intelligence agencies in the European Union').
http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf

propos des révélations. La présente note n'est donc qu'un instantané de la situation au 23 octobre 2013.

I. LA NATIONAL SECURITY AGENCY (NSA) AMÉRICAINE

(4) La NSA est un service de renseignement militaire dirigé par le Général Keith B. Alexander. Alexander rend compte à l'Under Secretary of Defense for Intelligence, Michael G. Vickers, le principal conseiller en renseignement du ministre américain de la Défense, Chuck Hagel. La NSA fait également partie de l'*Intelligence Community* américaine, dirigée par James Clapper. En vertu de l'EO 12333, le directeur de la NSA (DIRNSA) a notamment pour mission de recueillir, de traiter, d'analyser, de produire et de diffuser des *signals intelligence* (SIGINT[2]) (y compris par des moyens clandestins) à des fins de *foreign intelligence* et de *counterintelligence*[3] ainsi qu'en appui d'opérations militaires.[4] Le recueil de SIGINT par la NSA est régi par deux documents majeurs : l'Executive Order 12333 (EO 12333)[5] et le Foreign Intelligence Surveillance Act (FISA).

I.1. Le cadre légal du recueil d'informations sur des cibles étrangères

I.1.1. Executive Order 12333

(5) L'EO 12333 définit le concept de *foreign intelligence* comme désignant toutes les informations relatives aux capacités, aux intentions ou aux activités de puissances, d'organisations ou de personnes étrangères.[6] Le recueil de SIGINT peut se fonder purement et simplement sur cet *executive order*, sans qu'il faille pour autant suivre les procédures FISA plus élaborées.[7] Par exemple, l'EO 12333 constitue la base légale pour l'acquisition de quantités colossales de métadonnées en dehors du territoire américain[8], ainsi que pour le

---

2 Les SIGINT sont des renseignements (*intelligence*) créés par des signaux et systèmes électromagnétiques, tels que des systèmes de communication, des radars, des satellites ou des systèmes d'armement. Voir à cet égard, par exemple, http://www.nsa.gov/sigint/

3 Executive Order 12333 – United States intelligence activities, 4 décembre 1981, section 1.7(c)(1). L'EO 12333 a été amendé par les Executive Orders 13284 (2003), 13355 (2004) et 13470 (2008). La version consolidée de l'EO 12333 est disponible à l'adresse https://www.fas.org/irp/offdocs/eo/eo-12333-2008.pdf. Il convient de noter que l'EO 12333 régit les activités de tous les membres de l'US Intelligence Community, et donc pas seulement de la NSA.

4 *Idem*, section 1.7(c)(3) et (5).

5 Avant l'EO 12333, il y avait déjà l'EO 12139 (Exercise of Certain Authority Respecting Electronic Surveillance), qui fut amendé par l'EO 12333, l'EO 13383 et l'EO 13475.

6 *Idem*, section 3.5(e). L'EO 12333 stipule clairement que la *foreign intelligence* peut être acquise par d'autres moyens que SIGINT, à savoir en ayant recours à d'autres éléments de l'*intelligence community* par le biais de la surveillance physique (voir p.ex. section 2.4(d) "*Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means*").

7 N.S.A., The National Security Agency: Missions, Authorities, Oversight and partnerships, 9 août 2013 (http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf, 2).

8 Foreign Intelligence Surveillance Court, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13 - 109, 29 août 2013, 10, n° 10. ("*The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders*"). Voir également paragraphe 15.

recueil des listes de contacts ou des carnets d'adresses de logiciels de messagerie électronique et de conversation instantanée.[9] En effet, ce type d'information ne relève pas de la définition d'*electronic surveillance* telle qu'utilisée par le FISA.[10] L'EO 12333 semble également offrir une base légale aux activités les plus controversées de la NSA, et ce particulièrement celles de ses subdivisions, telles que l'Office of Tailored Access Operations (TAO) et le Special Collection Service (SCS), comme le contournement des systèmes de cryptage commerciaux[11], le piratage d'ordinateurs étrangers[12] ou l'espionnage de dirigeants étrangers à partir d'ambassades américaines.[13] L'US Senate Intelligence Committee exerce un contrôle limité sur ces activités.[14]

I.1.2. Foreign Intelligence Surveillance Act

(6) Une grande partie de la « surveillance électronique » est régie par le Foreign Intelligence Surveillance Act (FISA) datant de 1978. Le FISA a été codifié au titre 50 de l'U.S.C. § 1801 *et seq.*, puis s'est vu compléter de manière plus significative par de nouvelles dispositions du Patriot Act[15], qui régissent entre autres l'installation et l'utilisation des *pen registers* [16] et des *trap and trace devices* [17], ainsi que la production d''éléments tangibles'.[18] Le FISA a été amendé pour la dernière fois en 2008 par le biais du FISA Amendments Act (FAA).[19] En décembre 2012, le Sénat américain a prolongé les effets du FISA Amendments Act jusqu'au

---

9 Voir paragraphes 25-27.

10 US Code Title 50 - War and National Defence, 50 USC 1801(f).

11 Voir paragraphes 45-48.

12 Voir par exemple paragraphes 29, 47 et 48.

13 Voir par exemple paragraphe 19.

14 Un membre du Committee a indiqué ce qui suit : "*In general, the committee is far less aware of operations conducted under 12333 (…). I believe the NSA would answer questions if we asked them, and if we knew to ask them, but it would not routinely report these things, and, in general, they would not fall within the focus of the committee".* http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story_1.html

15 Voir 50 U.S.C. §1841 *et seq*

16 Le titre 18 de l'U.S.C. § 3127(3) définit un *pen register* comme "*a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business"*.

17 Le titre 18 de l'U.S.C. § 3127(4) définit un *trap and trace device* comme "*a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication"*.

18 Voir 50 U.S.C. § 1861. Il s'agit, par exemple, de la base légale pour la banque de données MAINWAY. Voir paragraphe 37.

19 Voir H.R. 6404, FISA Amendments Act of 2008' sur http://www.gpo.gov/fdsys/pkg/BILLS-110hr6304enr/pdf/BILLS-110hr6304enr.pdf. La section 702 "Procedures for targeting certain persons outside the United States other than United States persons", souvent citée, a été consolidée dans l'U.S Code sous le titre 50 USC §1881a, disponible à l'adresse http://www.law.cornell.edu/uscode/text/50/chapter-36. Auparavant, le FISA avait déjà fait l'objet de modifications majeures par le biais du Patriot Act en 2001.

31 décembre 2017 inclus. Selon la NSA, la principale application du FAA réside dans le recueil des communications de ressortissants étrangers qui utilisent des fournisseurs américains de services de communication.[20] Plusieurs propositions législatives visant à restreindre la collecte par les États-Unis d'informations relatives à des « nationaux »[21] sont actuellement sur la table, mais jusqu'à présent aucune initiative semblable ne cherche à limiter le recueil d'informations relatives à des « étrangers ».[22] Le présent rapport se penchera uniquement sur le récent FISA-Amendments Act, qui vient en complément du titre 50 de l'U.S.C. § 1802. En vertu du titre 50 de l'U.S.C. § 1802, le procureur général américain (*Attorney-General*) peut mandater une surveillance électronique pour une période d'un an si cette surveillance est exclusivement destinée à (1) acquérir le contenu des communications transmises par des moyens de communication uniquement utilisés par ou entre des « puissances étrangères »[23] ou (2) acquérir la *technical intelligence* de lieux qui se trouvent sous le contrôle ouvert et exclusif d'une « puissance étrangère ».

(7) Le FISA Amendments Act confère à l'AG et au DNI la compétence de mandater, pour une période d'un an, la surveillance électronique de personnes dont il peut être raisonnablement admis qu'elles se trouvent en dehors des États-Unis, et ce dans le but spécifique de recueillir des « renseignements étrangers ».[24] Ces « renseignements étrangers » font l'objet d'une définition très large :

> *« (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—*
>
> *(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;*
>
> *(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or*

---

20 N.S.A., "The National Security Agency: Missions, Authorities, Oversight and partnerships", 9 août 2013. http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf, 4.

21 Pour un aperçu des principales initiatives, voir J. GRANICK, "A tale of two surveillance reform bills. Centre for Internet and Society", 29 octobre 2013. https://cyberlaw.stanford.edu/blog/2013/10/tale-two-surveillance-reform-bills

22 Voir par exemple D. POKEMPNER, "Dispatchers: Taming the NSA - Reform bills fall short. Human Rights Watch", 30 octobre 2013. http://www.hrw.org/news/2013/10/30/dispatches-taming-nsa-reform-bills-fall-short

23 Voir définition au paragraphe 8.

24 Il convient de noter que le verbe '*acquire*' n'a pas la même signification que le verbe '*collect*'. Voir par exemple Department of Defense, DoD 5240 1-R, Procedures governing the activities of DoD intelligence components that affect United States persons. December 1982, 15. "*Data acquired by electronic means is "collected" only when it has been processed into intelligible form*". La section 1881a s'intitule : "Procedures for targeting certain persons outside the United States other than United States persons ". Le '*targeting*' n'est toutefois pas défini au titre 50 de l'USC § 1881. Le titre 50 de l'U.S.C. § 1801 définit l''*electronic surveillance*' comme "*the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes* ". Une interprétation pourrait donc être que le '*targeting*' vise uniquement les données recueillies *intentionnellement*. Les informations recueillies accidentellement ne sont pas considérées comme du '*targeting*'.

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States. »[25]

(8) C'est cette dernière catégorie qui permet le recueil en principe illimité d'informations, d'autant plus que la définition de « puissance étrangère » est elle aussi étendue. Ce terme ne désigne pas seulement des gouvernements ou parlementaires étrangers ou des organisations internationales, mais aussi « *une organisation politique à l'étranger, qui n'est pas essentiellement composée de citoyens américains »* [26] et « *une entité dirigée et contrôlée par un ou des gouvernements étrangers* ».[27] En théorie, ces deux catégories pourraient par exemple aussi inclure respectivement des ONG qui organisent des manifestations anti-américaines ou des entreprises publiques.

(9) La Foreign Intelligence Surveillance Court (FISC) vérifie si le mandat de l'AG et du DNI (voir paragraphe 7) satisfait à un certain nombre de conditions procédurales. L'AG et le DNI joignent un certificat écrit au mandat qui atteste du respect de ces conditions procédurales. Ces conditions visent principalement à limiter autant que possible le recueil intentionnel de données concernant des citoyens américains.[28] Aucune loi ou réglementation américaine ne prévoit de telles « procédures de minimisation » censées éviter le recueil et l'enregistrement de données étrangères « innocentes ». Ce certificat doit également mentionner les installations, lieux ou propriétés spécifiques qui sont précisément la cible de la collecte SIGINT.[29] Les autorités américaines ont déclassifié un document datant du 31 octobre 2011, qui décrivait les « procédures de minimisation » appliquées par la NSA pour recueillir des informations de type *foreign intelligence*. Il s'est avéré que les communications émanant de ou relatives à des citoyens américains qui n'ont pas été recueillies intentionnellement pouvaient être conservées jusqu'à cinq ans[30] et pouvaient être partagées avec des autorités étrangères.[31]

(10) Si la FISC marque son accord, l'AG et le DNI peuvent transmettre, sur la base d'un certificat d'une telle portée, des *identifiers* (par exemple, des adresses e-mail ou des numéros de téléphone)[32] à une entreprise américaine, qui est alors obligée de fournir

---

25 50 USC § 1801(e)

26 50 USC § 1801(a)(5)

27 50 USC § 1801(a)(6)

28 50 USC § 1801(g)

29 50 USC § 1801(g)(2)(4)

30 Exhibit B, Minimization Procedures used by the National Security Agency in connection with acquisitions of foreign intelligence information pursuant to section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf), s.3(b)(1)

31 *Idem*, (s.8(a)).

32 N.S.A., "The National Security Agency: Missions, Authorities, Oversight and partnerships", 9 août 2013, (http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf), 4.

immédiatement toutes les « informations, facilités ou autre assistance » nécessaires à la réussite de ce recueil SIGINT.[33] En échange, ces entreprises bénéficient d'une compensation financière et ne peuvent être tenues pour responsables de la fourniture de telles informations « *devant aucun tribunal* ».[34] Une entreprise peut introduire un recours contre une telle demande (par exemple, parce que la demande est trop vaste)[35], à la suite de quoi la FISC peut rejeter la demande ou prononcer une ordonnance définitive de collaboration.[36]

I.1.3. Safe Harbour

(11) Les entreprises américaines peuvent dès lors être obligées de transmettre des données à la NSA, y compris des données émanant et concernant des clients belges. Cette exigence en vertu du droit américain peut se heurter aux principes de l'accord « Sphère de sécurité » (ou *Safe Harbour*) que les États-Unis et l'Union européenne ont conclu en 2000 et qui permet aux entreprises américaines de se conformer volontairement aux principes de cet accord. Par exemple, les entreprises sont censées informer leurs clients que leurs données personnelles ont été transmises à une tierce partie.[37] La Federal Trade Commission (FTC) veille au respect de cet accord. Il peut être dérogé à ces principes au nom de la sécurité nationale ou parce que le maintien de l'ordre public le requiert. Cependant, en raison de la grande ampleur avec laquelle des données personnelles d'utilisateurs européens d'entreprises américaines ont été envoyées à la NSA dans le cadre du programme PRISM (voir paragraphes 32-38), la Commission européenne examine actuellement une éventuelle révision de l'accord *Safe Harbour*.[38]

(12) Le 22 octobre 2013, le Parlement européen a voté en faveur de l'ajout d'une clause dite « anti-FISA », qui ne permettrait pas aux entreprises de transmettre, sans l'autorisation d'une *supervisory authority,* des données personnelles de résidents européens à un pays tiers à la demande d'un tribunal ou d'une autre autorité de ce pays. Cette *supervisory authority* doit d'abord vérifier si ce transfert est nécessaire et conforme à la nouvelle législation européenne en matière de protection des données. Reste à savoir si cet article survivra aux négociations avec le Conseil.[39]

---

33 50 USC § 1802, (a)(4) ; 50 USC § 1881a(1) et (2).

34 50 USC § 1881a (h)(3)

35 En 2007, Yahoo a reçu un tel « ordre » de fournir des données et l'a contesté auprès de la Foreign Intelligence Surveillance Court of Review. Le tribunal a toutefois rejeté les objections de Yahoo. Cette décision n'a été divulguée que récemment. https://www.fas.org/irp/agency/doj/fisa/fiscr082208.pdf

36 50 USC § 1881a (h)(4)

37 2000/520/CE : Décision de la Commission du 26 juillet 2000 conformément à la Directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique (notifiée sous le numéro de document C(2000) 2441) (Texte présentant de l'intérêt pour l'EEE). Voir également http://export.gov/safeharbor/eu/eg_main_018493.asp.

38 Commissaire Reding : "*The Safe Harbor agreement may not be so safe after all (..) It could be a loophole for data transfers because it allows data transfers from EU to U.S. companies-although U.S. data protection standards are lower than our European ones. (…) I have informed ministers that the commission is working on a solid assessment of the Safe Harbor Agreement, which we will present before the end of the year*", European Commission, Memo/13/710, 19/07/2013, http://europa.eu/rapid/press-release_MEMO-13-710_en.htm

39 Voir article 43a de la "unofficial consolidated version of the European Data Protection Regulation after the LIBE Committee vote provided by the rapporteur, 22 October 2013".

I.2. Nature et ampleur du recueil SIGINT par la NSA

(13) Il est difficile de dresser l'inventaire de la totalité du recueil SIGINT de la NSA. Quelques chiffres donnent toutefois déjà une idée de son ampleur. *The Guardian* cite un rapport de 2007 de la NSA qui estimait qu'à l'époque, les différentes bases de données de la NSA contenaient environ 850 milliards de *call events* non définis et environ 150 milliards d'*internet records* non définis. D'après le document, un à deux milliards de *records* viennent s'ajouter chaque jour. [40] Un article du journal *The Washington Post* mentionnait en 2010 que la NSA conservait, par jour, le contenu et les métadonnées de 1,7 milliards d'e-mails, de conversations téléphoniques et d'autres formes de communications, et qu'une fraction était stockée dans quelque 70 bases de données distinctes.[41]

(14) Depuis lors, cette capacité a connu une croissance exponentielle. Des *slides* du programme interne Boundless Informant[42] de la NSA, qui ont été publiés par *The Guardian*, montrent qu'en un mois (mars 2013), la division Global Access Operations (GAO)[43] de la NSA a recueilli 97 milliards de métadonnées de communications internet (e-mails, conversations instantanées...) et près de 125 milliards de métadonnées de conversations téléphoniques provenant de plus de 504 SIGINT Activity Designator (SIGADS).[44] Il ressort du *slide* que la Belgique faisait partie des pays pour lesquels le recueil de métadonnées était le moins important en chiffres absolus.[45] Le *slide* ne révèle rien de la quantité de métadonnées concernée, mais le code couleur de la Belgique indique que la quantité de métadonnées recueillies en Belgique est moindre que celles recueillies aux Pays-Bas, par exemple.

(15) En août 2013, *Der Spiegel* publiait des *slides* supplémentaires du programme qui indiquaient clairement qu'en décembre 2012, environ 1,8 million de métadonnées issues de conversations téléphoniques émanant des Pays-Bas ont été recueillies.[46] Durant cette même période, 70 millions de métadonnées ont été recueillies à partir de communications téléphoniques depuis la France[47], 60 millions depuis l'Espagne et 47 millions depuis l'Italie.[48]

---

http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf. Voir également Caspar Bowden, The US surveillance programmes and their impact on EU citizens' fundamental rights. European Parliament, Directorate General for Internal Policies, 2013, 28.

40 http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu .

41 D. PRIEST, W. M. ARKIN, *The Washington Post* ("Secret America: A Hidden World, Growing Beyond Control"). http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/3/

42 Pour en savoir plus, voir : NSA, Boundless Informant - Frequently Asked Questions, 09-06-2012. http://www.theguardian.com/world/interactive/2013/jun/08/boundless-informant-nsa-full-text

43 La collecte de métadonnées d'autres divisions de la NSA, telles que TAO ou SSO, n'est donc pas concernée.

44 Signals activity/address designators – peuvent faire référence à une plateforme de collecte physique spécifique (comme une base de l'armée américaine à l'étranger, une ambassade, un navire...), une plateforme virtuelle de traitement de données (par exemple, PRISM est connu sous le SIGAD US-984XN) ou un satellite spatial.

45 http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining#

46 http://www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-6.html

47 http://www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-6.html En octobre, *Le Monde* a publié davantage de détails dont il ressort que 62,5 millions de métadonnées issues de communications mobiles ont été recueillies sous le nom de code DRTBOX et 7,8

(16) Durant la même période, plus de 500 millions de métadonnées ont été recueillies depuis l'Allemagne. Ce nombre est bien plus important puisqu'il s'agit de métadonnées Internet. Il ressort d'un document que plus de 471 millions de métadonnées proviennent de SIGAD US-987LA.[49] Selon *Der Spiegel,* le Bundesnachrichtendienst (BND) pense qu'il est ainsi fait référence au site Bad Aibling, qui était exploité par la NSA jusqu'en 2004, puis a été repris par le BND. Depuis ce site, le BND collecte des SIGINT étrangers, principalement en provenance d'Afghanistan et du Moyen-Orient. Ces données sont alors transmises à la NSA.[50]

(17) Selon la NSA, Internet transporte chaque jour 1,826 pétaoctet de données. Sur l'ensemble de ces données, la NSA ne « touche » qu'à 1,6 %, soit environ 29 millions de gigaoctets par jour.[51] Sur ce 1,6 %, 0,025 % est sélectionné en vue d'une évaluation. Selon la NSA, « elle examine donc à peine 0,00004 % de tout le trafic Internet par jour ».[52] Un simple calcul suggérerait que ce chiffre est dix fois plus élevé, et la NSA examinerait dès lors 0,0004 % du trafic Internet, mais selon la NSA, le chiffre initial est correct.[53]Ce qui semble peu, mais représente toutefois une quantité colossale lorsqu'on sait que par exemple, seulement 2,9 % de tout le trafic Internet aux États-Unis sont des communications.[54]

---

millions de métadonnées de conversations du réseau téléphonique public (PSTN – Public switched telephone network) sous le nom de code WHITEBOX. Parmi les cibles figuraient tant des personnes qui ont été associées à des activités terroristes que des personnes issues du monde des affaires, de la politique française ou du monde des affaires français. http://www.lemonde.fr/technologies/article/2013/10/21/france-in-the-nsa-s-crosshair-phone-networks-under-surveillance_3499741_651865.html. Plusieurs médias ont annoncé que 70 millions de communications téléphoniques françaises ont été écoutées. Il s'agit là certainement d'une interprétation erronée des documents de Snowden. Voir également "DNI Statement on Inaccurate and Misleading Information in Recent Le Monde Article", 22 octobre 2013, (http://icontherecord.tumblr.com). : "*The allegation that the National Security Agency collected more than 70 million "recordings of French citizens' telephone data" is false. (…) While we are not going to discuss the details of our activities, we have repeatedly made it clear that the United States gathers intelligence of the type gathered by all nations*."

48 http://www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-5.html

49 http://www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-4.html

50 Selon *Der Spiegel*, pas moins de 62.000 e-mails sont interceptés chaque jour rien qu'à partir du site Bad Aibling. http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html

51 Le terme '*touch*' n'est pas défini par la loi, mais implique que la NSA consulte effectivement ces informations (et ne se contente pas de les recueillir). *The Wall Street Journal* : "*One U.S. official says the agency doesn't itself "access" all the traffic within the surveillance system. The agency defines access as "things we actually touch," this person says, pointing out that the telecom companies do the first stage of filtering*". http://online.wsj.com/article_email/SB10001424127887324108204579022874091732470-lMyQjAxMTAzMDIwMDEyNDAyWj.html

52 N.S.A., "The National Security Agency: Missions, Authorities, Oversight and partnerships". 9 août 2013, 6.

53 V. VINES, porte-parole de la NSA : "*Our figure is valid; the classified information that goes into the number is more complicated than what's in your calculation*". http://www.thewire.com/politics/2013/08/nsa-better-data-collection-math/68490/

54 Par exemple, aux États-Unis, le divertissement en temps réel ('*real time entertainment*') (sites de diffusion en continu tels que Netflix) représente 62 % du trafic Internet et le partage de fichiers *peer-to-*

(18) The Guardian a décrit un document datant du 26 décembre 2012, dans lequel la division « Special Source Operations » (SSO) annonçait l'acquisition d'une nouvelle capacité (nom de code EVILOLIVE) afin de recueillir encore davantage de métadonnées de communications dont une partie n'est pas américaine (One-End Foreign (1EF) solution). La NSA pourrait à présent stocker dans ses propres bases de données plus de la moitié de toutes les métadonnées recueillies via ses SIGADS.[55] Un autre document non publié évoque une autre capacité d'acquisition de métadonnées baptisée SHELLTRUMPET, à propos de laquelle un responsable de la SSO a déclaré le 31 décembre 2012 que ce programme venait de traiter sa trillionième métadonnée. La moitié de ces traitements ont eu lieu en 2012. Deux autres programmes de métadonnées (MOONLIGHTPAD et SPINNERET) devaient devenir opérationnels en septembre 2013.[56]

(19) Un jugement prononcé par la FISC en 2011 et récemment publié suggère que 91 % des données Internet collectées par la NSA sont issues du programme PRISM. [57] Les 9 % restants proviennent du traitement de données en amont (*upstream*) et de missions clandestines dans le cadre du programme SRP (Specialized Reconnaissance Program) qui peuvent être menées en collaboration avec la CIA. *The Washington Post* a divulgué le budget de la US intelligence community en 2013 et il s'est avéré que 2 % du budget total est réservé à deux programmes conjoints CIA-NSA. Le premier, baptisé CLANSIG (*clandestine signals collection*), couvre une multitude de *black bag jobs* ou d'opérations *off-net*. Il s'agit d'opérations clandestines très risquées au travers desquelles l'on cherche à accéder, par exemple, à des radiofréquences et une infrastructure télécom critique d'un pays, mais aussi à obtenir un accès spécifique aux e-mails et ordinateurs de cibles *high interest*, telles que des gouvernements étrangers, des systèmes de communication militaire et d'éminentes multinationales. Cette dernière décennie, plus de cent *black bag jobs* de ce type ont été menés. Par exemple, durant ces opérations, des *spyware* sont installés sur des ordinateurs, ou la CIA fait en sorte que des lignes téléphoniques, routeurs, câbles en fibre optique, centres de commutation de données et autres systèmes protégés puissent être mis sur écoute pour permettre à la NSA d'accéder à ces données. De telles opérations ont surtout lieu au Moyen-Orient et en Asie, principalement en Chine.[58] La deuxième initiative conjointe

---

peer (via des sites tels que Bittorrent, par exemple) 10,5 %. J. JARVIS, *Buzzmachine*, 10 août 2013, ("NSA by the numbers"), http://buzzmachine.com/2013/08/10/nsa-by-the-numbers/

55 http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection "*This new system, SSO stated in December, enables vastly increased collection by the NSA of internet traffic. (…) The 1EF solution is allowing more than 75% of the traffic to pass through the filter," the SSO December document reads. "This milestone not only opened the aperture of the access but allowed the possibility for more traffic to be identified, selected and forwarded to NSA repositories*".

56 http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection

57 Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates), 3 octobre 2011, 71. http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa - partie 8.

58 Exemple : "*In another more recent case, CIA case officers broke into a home in Western Europe and surreptitiously loaded Agency-developed spyware into the personal computer of a man suspected of being a major recruiter for individuals wishing to fight with the militant group al-Nusra Front in Syria, allowing CIA operatives to read all of his email traffic and monitor his Skype calls on his computer*". http://www.foreignpolicy.com/articles/2013/07/16/the_cias_new_black_bag_is_digital_nsa_cooperation

de la NSA et la CIA est le « Special Collection Service » (SCS). Il utilise des bâtiments américains officiels, tels que des ambassades et des consulats, comme point de départ pour l'interception de communications secrètes, entre autres du trafic diplomatique (chiffré) dans le pays où est établi le consulat ou l'ambassade.[59] Le personnel du SCS jouit du statut diplomatique.[60] Leurs opérations se déroulent souvent depuis une Secure Compartmented Intelligence Facility (SCIF), situé au dernier étage d'une ambassade. La plupart des diplomates d'une ambassade semblent ignorer ce qui se passe dans ces *staterooms*.[61] Selon *Der Spiegel*, le SCS est actif dans 80 pays, dont 19 en Europe.[62] Les documents et *slides* divulgués jusqu'à présent semblent suggérer que le SCS n'est pas actif en Belgique.[63] C'est le SCS qui est soupçonné d'avoir mis le téléphone portable d'Angela Merkel sur écoute.[64]

I.3. Recueil en amont (*upstream*) aux États-Unis

(20) Plus de 80 % du trafic Internet et téléphonique mondial passe par des câbles en fibre optique, par des points centraux aux États-Unis qui sont exploités par les trois principaux opérateurs télécoms américains (AT&T, Verizon et Sprint). Ce trafic inclut par définition le trafic de données en provenance et à destination de la Belgique. La division « Special Source Operations » de la NSA contrôle l'équipement placé sur ces points de sorte que toutes les données passant par ces points peuvent être copiées et filtrées sur la base des paramètres définis par la NSA.[65] Le principal filtre est le filtre « légal » : en théorie, seules les

---

59 US Intelligence 2013 budget http://apps.washingtonpost.com/g/page/national/inside-the-2013-us-intelligence-black-budget/420/#document/p13/a117314 Foreign Policy: "*For example, virtually every U.S. embassy in the Middle East now hosts a SCS SIGINT station that monitors, twenty-four hours a day, the complete spectrum of electronic communications traffic within a one hundred mile radius of the embassy site*". http://www.foreignpolicy.com/articles/2013/07/16/the_cias_new_black_bag_is_digital_nsa_cooperation?page=0,1)

60 Voir également note 99.

61 http://www.spiegel.de/fotostrecke/photo-gallery-spies-in-the-embassy-fotostrecke-103079-6.html

62 http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html

63 http://cpunks.files.wordpress.com/2013/10/20131027-191221.jpg?w=545. L'auteur a vérifié l'origine du *slide.*

64 http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205-2.html

65 "*There are two common methods used, according to people familiar with the system. In one, a fiber-optic line is split at a junction, and traffic is copied to a processing system that interacts with the NSA's systems, sifting through information based on NSA parameters. In another, companies program their routers to do initial filtering based on metadata from Internet "packets" and send copied data along. This data flow goes to a processing system that uses NSA parameters to narrow down the data further*". http://online.wsj.com/article/SB10001424127887324108204579025222244858490.html.
En ensuite : " *According to a U.S. official, lawyers at telecom companies serve as checks on what the NSA receives. "The providers are independently deciding what would be responsive," the official says. Lawyers for at least one major provider have taken the view that they will provide access only to "clearly foreign" streams of data - for example, ones involving connections to ISPs in, say, Mexico, according to the person familiar with the legal process. The complexities of Internet routing mean it isn't always easy to isolate foreign traffic, but the goal is "to prevent traffic from Kansas City to San Francisco from ending up" with the NSA, the person says.*", S. GORMAN et J. VALENTINO-DEVRIES, *The Wall Street Journal*, 20 août 2013 ("New Details Show Broader NSA Surveillance Reach"). L'existence de ce type d'activités a déjà été en partie révélée en 2006 par Mark Klein, lanceur d'alerte de AT&T (Declaration of Mark Klein

communications dont au moins un participant n'est pas américain ou ne se trouve pas aux États-Unis peuvent être transmises à la NSA. D'autres filtres doivent veiller à ce que seules les données ayant une valeur en matière de *foreign intelligence* soient transférées à la NSA. Grâce à des programmes tels que XKEYSCORE, les analystes de la NSA sont en mesure d'explorer ces données en amont (*upstream data)* sur la base de *strong selectors* (par exemple : un numéro de téléphone, une adresse e-mail ou un groupe d'adresses IP qui appartiennent à une organisation à laquelle s'intéresse la NSA), de *soft selectors* (comme des mots clés), ou des *selectors* qui détectent un type de trafic crypté (par exemple au moyen de Tor[66] ou d'un réseau VPN (Virtual Private Network)[67]).[68] Pour prendre cette décision, la NSA peut dès lors examiner le contenu *et* les métadonnées d'une communication.[69] XKEYSCORE est détaillé aux paragraphes 28-31.

(21) Un document divulgué et publié par *The Washington Post* mentionne que FAIRVIEW (US-990), STORMBREW (US-983), ORANGEBLOSSOM (US-3251) et SILVERZEPHYR (US-3273) sont tous des *special source operations* qui acquièrent des données issues du trafic passant par les États-Unis, mais dont ni le destinataire ni l'émetteur ne sont américains.[70] Un autre *slide* cite FAIRVIEW, STORMBREW, BLARNEY et OAKSTAR en tant que *upstream* SIGADS.[71] Selon *The Wall Street Journal*, LITHIUM fait également partie de ce *cluster*.[72]

(22) BLARNEY (US-984) est le SIGAD qui faisait initialement référence aux *upstream data* que la NSA obtenait par l'intermédiaire d'AT&T[73], mais il semble avoir été étendu par la suite à plusieurs entreprises.[74] Selon *The Washington Post*, des données provenant de BLARNEY sont toujours traitées.[75] Un *slide* d'une présentation de la NSA, vu l'émission télévisée brésilienne Fantastico, suggérait que BLARNEY assure la *'collection against DNR and DNI FISA Court Order authorized communications'*. DNR est l'acronyme de 'Dial Number Recognition', tandis que DNI signifie « Digital Network Intelligence' . Il est également

---

in support of plaintiffs' motion for preliminary injunction. United States District Court, Northern District of California, 8 June 2006).

66 Tor est un réseau de serveurs qui permettent aux utilisateurs de surfer anonymement. Voir à ce propos https://www.torproject.org/

67 Souvent utilisé par des entreprises pour permettre à leurs collaborateurs d'accéder à leur réseau depuis leur domicile via un 'tunnel' crypté.

68 http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 2.

69 Pour une analyse technique de XKeyscore, voir http://arstechnica.com/information-technology/2013/08/building-a-panopticon-the-evolution-of-the-nsas-xkeyscore/

70 http://apps.washingtonpost.com/g/page/national/nsa-report-on-privacy-violations-in-the-first-quarter-of-2012/395/#document/p2/a114809

71 http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html?wprss=rss_national
The Washington Post avait précédemment censuré les noms STORMBREW et OAKSTAR .

72 http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html

73 S. GORMAN et J. VALENTINO -DEVRIES, *The Wall Street Journal*, 20 août 2013 ("New Details Show Broader NSA Surveillance Reach").

74 "*BLARNEY's top-secret program summary describes it as "an ongoing collection program that leverages IC [intelligence community] and commercial partnerships to gain access and exploit foreign intelligence obtained from global networks*". http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_print.html

75 *Idem.*

mentionné dans le *slide* que BLARNEY cible principalement les éléments suivants : *« diplomatic establishment, counterterrorism, counter proliferation, foreign government, economic, military en political/intention of nations »*.[76] Selon un autre *slide*, BLARNEY a commencé à accéder aux communications de *« foreign establishments, agents of foreign powers and terrorists »* dès 1978.[77] *Der Spiegel* a précédemment mentionné que les techniciens de la NSA qui travaillaient pour le programme BLARNEY étaient parvenus à exploiter le système de vidéoconférence (VTC) interne de l'ONU.[78] Selon ce même *slide*, les informations recueillies dans le cadre de BLARNEY ont été envoyées à des « clients externes », dont : US Department of State, CIA, US UN Mission, Joint Chiefs of Staff, Department of Homeland Security, DNI, 2nd parties to Five eyes, National Counterterorrism Center, White House, Defense Intelligence Agency, NATO, Office of Secretary of Defense, ainsi que des commandements militaires (Army, EUCOM).[79] Le programme ressemble beaucoup au programme de la NSA décrit dans l'affaire opposant Jewel à la NSA.[80]

I.4. Recueil en amont (*upstream*) en dehors des États-Unis

(23) Les informations qui circulent sur les câbles en fibre optique et passent par le territoire d'un des partenaires secondaires des États-Unis (Royaume-Uni, Canada, Australie et Nouvelle-Zélande) sont également partagées avec les États-Unis.[81] Selon Duncan Campbell, l'agence SIGINT suédoise *'Försvarets radioanstalt' (*FRA) partage aussi les données en amont (*upstream data*) qu'elle acquiert via la fibre optique avec « Five Eyes ». Les données ainsi obtenues seraient connues sous le nom de code SARDINE.[82] Campbell affirme que le '*Forsvarets Efterretningstjeneste'* (Danish Defence Intelligence Service) partage aussi des informations avec la NSA. Les données ainsi obtenues seraient connues sous le nom de code DYNAMO.[83] La NSA a également conclu des accords de coopération avec des sociétés de télécoms étrangères *« principalement en Europe et au Moyen-Orient »*, selon une source

---

76 http://leaksource.files.wordpress.com/2013/09/blarney.jpg. *Der Spiegel* a précédemment écrit que "*NSA technicians working for the Blarney program have managed to decrypt the UN's internal video teleconferencing (VTC) system*".

77 Capture d'écran d'un segment montré sur le site http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html; https://pbs.twimg.com/media/BTxAU7ZIYAA3OW_.png:large

78 http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html

79 Capture d'écran du segment montré sur le site http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html; https://pbs.twimg.com/media/BTxAU7ZIYAA3OW_.png:large

80 https://www.eff.org/files/filenode/jewel/jewel.complaint.pdf. Selon Thomas Drake, ancien collaborateur de la NSA, BLARNEY est "*a key access program facilitated by these commercial arrangements that exploits the Internet data at these junctions. (…) BLARNEY is to the international Internet space as PRISM is to the domestic*". http://www.dailydot.com/news/fairview-prism-blarney-nsa-internet-spying-projects/

81 http://apps.washingtonpost.com/g/page/world/how-the-nsa-tried-to-collect-less/518/

82 Témoignage de Duncan Campbell : http://www.youtube.com/watch?v=ZX1tmizZLpc. Ce qui n'a rien de surprenant à la lumière de la « loi FRA » adoptée par la Suède en 2008. http://news.bbc.co.uk/2/hi/europe/7463333.stm.

83 Duncan Campbell testimony to the Council of Europe, 1er octobre 2013. http://www.duncancampbell.org/PDF/CoECultureCommittee1Oct2013.pdf, 19.

anonyme dans *The Wall Street Journal*.[84] D'après Glenn Greenwald, la NSA ne conclut pas d'accords de coopération directement avec des entreprises étrangères, mais utilise l'accès d'une grande société de télécommunications américaine – jusqu'à présent inconnue – qui collabore avec de telles entreprises étrangères. La société américaine en question a un accès direct à l'infrastructure de télécommunications de son partenaire, qui – à son insu – octroie également un accès à la NSA. Selon Greenwald, ces informations aboutissent dans le programme FAIRVIEW.[85] D'autres câbles en fibre optique sont des cibles légitimes pour les États-Unis dans le cadre de l'interception clandestine du trafic Internet et téléphonique en vertu de l'EO 12333.

(24) Le programme *upstream* a également permis l'interception automatique d'e-mails de sociétés de télécommunications françaises tels qu'Alcatel-Lucent. On ne sait pas exactement si le contenu de tous les e-mails de ces adresses a été conservé automatiquement ou si seuls les e-mails contenant certains mots clés et/ou les métadonnées de ce trafic d'e-mails étaient concernés.[86] D'après les fonctions et les opérations effectuées par ces deux sociétés, il ne serait pas impossible que des e-mails similaires d'employés de BICS, Belgacom ou Tecteo aient été interceptés de la même manière.[87]

(25) Parmi les données collectées par la division SSO de la NSA via ce recueil en amont, figurent des millions de listes de contacts ou de carnets d'adresses de programmes de messagerie électronique et de conversation instantanée, ainsi que des captures d'écran de toute une boîte de réception électronique. Les listes de contacts de programmes de conversation instantanée peuvent parfois inclure le contenu d'un message, et la boîte de réception d'une personne affiche souvent la première ligne du message.[88] Une présentation PowerPoint de la NSA mentionne que le 10 janvier 2012, 444 743 carnets d'adresses de Yahoo ont été recueillis en une seule journée, 105.068 de Hotmail, 82 857 de Facebook, 33 697 de Gmail et 22 881 d'autres fournisseurs. Les sociétés américaines en question n'ont – selon leurs dires – absolument pas connaissance de la collecte de ces informations.[89] Ce qui signifie que, sur une année, ce sont plus de 250 millions de carnets d'adresses qui sont collectés.

---

84 S. GORMAN et J. VALENTINO-DEVRIES, *The Wall Street Journal*, 20 août 2013 ("New Details Show Broader NSA Surveillance Reach"). http://online.wsj.com/article_email/SB10001424127887324108204579022874091732470-lMyQjAxMTAzMDIwMDEyNDAyWj.html

85 http://www.theguardian.com/commentisfree/2013/jul/07/nsa-brazilians-globo-spying. Par le passé, l'ancien collaborateur de la NSA, Thomas DRAKE, a décrit FAIRVIEW comme un programme-cadre (*umbrella programma*) dont dépendent beaucoup d'autres programmes. http://www.dailydot.com/news/fairview-prism-blarney-nsa-internet-spying-projects/.

86 http://www.lemonde.fr/technologies/article/2013/10/21/les-services-secrets-americains-tres-interesses-par-wanadoo-et-alcatel-lucent_3499762_651865.html)

87 Alcatel Lucent fournit entre autres une infrastructure essentielle pour les câbles en fibre optique sous-marins. Voir par exemple http://www.alcatel-lucent.com/solutions/submarine-networks)

88 http://apps.washingtonpost.com/g/page/world/the-nsas-overcollection-problem/517/

89 Le nombre élevé de carnets d'adresses Yahoo peut s'expliquer par le fait que Yahoo ne crypte pas automatiquement ses données via SSL - contrairement aux autres fournisseurs. En partie en réponse à ces révélations, Yahoo a annoncé qu'il proposerait également le protocole de sécurité SSL par défaut (*by default*) dès janvier 2014. http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story_2.html

(26) La NSA admet que nombre de ces carnets d'adresses ne présentent aucune *foreign intelligence value*, d'autant plus que dans 22 % des cas, le propriétaire de la liste d'adresses est inconnu.[90] Or une analyse de ces données permet à la NSA de voir les « connexions secrètes » et les relations d'un groupe beaucoup plus restreint de cibles du type *foreign intelligence*. Ces listes sont stockées dans plusieurs bases de données de la NSA, telles que MARINA, MAINWAY, PINWALE et CLOUDs. Selon une source *intelligence* de *The Washington Post*, un analyste NSA n'est pas autorisé à explorer ces bases de données ni à diffuser les informations qu'elles contiennent, sauf s'il peut démontrer qu'une cible *foreign intelligence* valide se trouve dans ces données.[91]

(27) Depuis novembre 2010, les métadonnées collectées en vertu de l'Executive Order 12333 peuvent être utilisées pour établir un *contact chaining* afin d'identifier les relations entre les *foreign intelligence targets* et les habitants des « Five Eyes ».[92] En outre, les données peuvent être complétées par des *enrichment data,* c'est-à-dire des données émanant essentiellement de sources publiques et commerciales, telles que des listes de passagers, des profils Facebook, des codes bancaires, des registres d'électeurs, des données GPS de TomTom et des données fiscales américaines.[93] Étant donné que selon la NSA, il s'agit ici purement de métadonnées et de sources ouvertes, aucun contrôle de la FISC n'est nécessaire pour créer de tels profils.[94]

I.5. Classement et analyse des données (en amont) avec XKEYSCORE

(28) Une présentation divulguée et datant de février 2008 décrit XKEYSCORE (également connu sous le nom de CrossKeyScore ou XKS) comme étant un *DNI exploitation system/analytic Framework »*.[95] Durant trois à cinq jours[96], XKEYSCORE consigne les données Internet non filtrées *full take*), et durant 30 jours, les métadonnées qui sont recueillies

---

90 http://apps.washingtonpost.com/g/page/world/an-excerpt-from-intellipedia/519/

91 http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story_1.html

92 http://www.nytimes.com/interactive/2013/09/29/us/documents-on-nsa-efforts-to-diagram-social-networks-of-us-citizens.html.

93 "*A top-secret document titled "Better Person Centric Analysis" describes how the agency looks for 94 "entity types", including phone numbers, e-mail addresses and IP addresses. In addition, the N.S.A. correlates 164 "relationship types" to build social networks and what the agency calls "community of interest" profiles, using queries like "travelsWith, hasFather, sentForumMessage, employs". (. . .) A 2009 PowerPoint presentation provided more examples of data sources available in the "enrichment" process, including location-based services like GPS and TomTom, online social networks, billing records and bank codes for transactions in the United States and overseas*". http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?pagewanted=all

94 *Idem*.

95 http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 2.

96 Il arrive que ce type de données ne soit conservé qu'une seule journée. "*One document explains: "At some sites, the amount of data we receive per day (20+ terabytes) can only be stored for as little as 24 hours*". http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu

auprès de 150 SIGADS aux quatre coins du monde.[97] Il ne s'agit pas seulement de recueillir des informations en amont (*upstream*), par exemple par le biais de câbles sous-marins, mais aussi des informations émanant de satellites (Fornsat[98]) et de missions diplomatiques et consulaires des États-Unis partout dans le monde (sites F6).[99] En 2012, XKEYSCORE contenait, sur une période de 30 jours, en moyenne 41 milliards d'enregistrements.[100] D'après le *slide*, un tel *full-take* permet à un analyste de trouver dans les métadonnées des cibles qui n'étaient pas encore connues.[101] Un analyste doit d'abord prouver qu'il est sûr à 51 % que sa recherche porte sur une cible étrangère. Les analystes peuvent ensuite explorer XKEYSCORE en temps réel[102] et envoyer des données vers d'autres bases de données, telles que PINWALE, MARINA ou TRAFFICTHIEF,[103] où ces informations brutes sont stockées pendant une plus longue période.

(29) Les exemples cités dans les *slides* démontrent qu'un analyste peut analyser un très grand volume de données via XKEYSCORE. XKEYSCORE peut lire le contenu de toute activité http, c'est-à-dire tous les e-mails et toutes les pièces jointes, toutes les conversations instantanées[104], toutes les métadonnées d'une communication internet, tout l'historique de navigation et toutes les recherches qu'une personne effectue en ligne.[105] En outre, il peut

---

97 http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 6. L'expert de la NSA, Marc AMBINDER, qui a écrit pour les documents de Snowden, décrit Xkeyscore comme suit : " *(it's) not a thing that DOES collecting; it's a series of user interfaces, backend databases, servers and software that selects certain types of metadata that the NSA has ALREADY collected using other methods*". http://theweek.com/article/index/247684/whats-xkeyscore

98 Selon Duncan CAMPBELL, qui a dévoilé l'existence du GCHQ en 1976, il s'agit du successeur d'Echelon. Ce programme existe toujours, mais a perdu de son intérêt, car les données téléphoniques se déplacent aujourd'hui en grande partie via les câbles en fibre optique. Témoignage de Duncan CAMPBELL au Parlement européen, à visionner sur http://www.youtube.com/watch?v=ZX1tmizZLpc

99 Présentation de Xkeyscore, divulguée sur http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 5. Selon AMBINDER, d'un point de vue technique, « F6 » renvoie au quartier général du Special Collection Service (SCS) à Beltsville, Maryland , qui recueille des informations à partir d'au moins 75 sites F6, principalement implantés dans des pays où il est impossible d'envoyer des informations à la NSA par le biais des câbles téléphoniques ou en fibre optique ordinaires, puisque les États-Unis ne sont pas techniquement censés y être présents. La NSA ne reconnaît pas l'existence du SCS parce que la plupart des membres du personnel travaillent comme responsables du State Department. http://theweek.com/article/index/247684/whats-xkeyscore et http://theweek.com/article/index/247761/5-nsa-terms-you-must-know

101 Présentation de Xkeyscore, divulguée sur http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 2

102 *Idem*. Pour de plus amples informations sur ce processus (ainsi que d'autres *slides* originaux), voir http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu

103 *Idem*.

104 Xkeyscore permet également d'effectuer des recherches en demandant, par exemple, *« affiche-moi toutes les feuilles de calcul Excel provenant d'Irak et contenant des Media Access Control Addresses »* (23) ou *« affiche-moi tous les documents Word qui mentionnent l'AIEA ou Oussama Ben Laden »* (26), http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation,

105 Xkeyscore enregistre toutes les recherches ainsi que l'utilisation de Google Maps, par exemple. http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 20.

détecter l'utilisation d'une technologie de cryptage ou VPN donnée[106] ou vérifier la langue utilisée par une personne en ligne.[107] XKEYSCORE peut également contrôler les adresses IP de toutes les personnes qui consultent un site web défini par l'analyste.[108] En outre, XKEYSCORE permet de vérifier qui est l'auteur d'un document envoyé en ligne.[109] Au moyen des « profils de vulnérabilité » fournis par les Tailored Access Operations (TAO) de la NSA, XKEYSCORE peut également être utilisé pour trouver des « machines exploitables » dans un pays donné.[110] Un analyste peut également recourir au programme DNI PRESENTER pour lire dans XKEYSCORE le contenu des e-mails et des conversations ou messages privés Facebook stockés.[111]

(30) Les *slides*, qui datent de 2008, indiquent qu'à l'époque, XKEYSCORE ne pouvait pas encore intercepter le protocole VoIP (Voice over Internet Protocol)[112], mais que l'on s'attendait à ce qu'il intercepte à l'avenir davantage de métadonnées telles que les *exif tags*.[113]

(31) La NSA a reconnu l'existence de XKEYSCORE comme composante de son *lawful foreign signals intelligence collection system*, mais a souligné que l'accès à XKEYSCORE est restreint et que toutes les recherches sont *fully auditable* par un analyste. La NSA insiste sur le fait que plus de 300 terroristes ont été arrêtés sur la base des renseignements issus de XKEYSCORE.[114]

I.6. PRISM : recueil en aval de SIGINT

(32) En partie parce qu'un nombre sans cesse croissant d'étrangers ont commencé à faire appel aux services d'entreprises américaines, et en partie parce que ces entreprises ont

---

106 Par exemple, XKeyscore permet d'afficher *« tous les documents Word cryptés provenant d'Iran ou toutes les utilisations de PGP en Iran »*. http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 16). Un analyste peut également demander à Xkeyscore de détecter l'utilisation de certaines technologies, par exemple en demandant : *« affiche-moi tous les démarrages VPN dans le pays X et donne-moi les données pour que je puisse identifier les utilisateurs de ce service »*. http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation (17)

107 Xkeyscore permet également un suivi des langues (*language tracking*) au moyen du plugin « http activity », qui suit les balises HTML de langue (*HTML language tags*). http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation (p.19)

108 *Idem*. Par exemple : tous les Belges qui consultent un site web extrémiste X.

109 http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 21.

110 Pour une analyse technique, voir http://arstechnica.com/tech-policy/2013/08/nsas-internet-taps-can-find-systems-to-hack-track-vpns-and-word-docs/

111 http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu

112 Fait référence à des services tels que Skype et Facetime d'Apple.

113 Présentation de Xkeyscore, divulguée sur http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 32. L'*« exchangeable image file format »* (exif) est une norme technique qui enregistre les métadonnées d'appareils photo numériques, comme la date et l'heure auxquelles une photo numérique a été prise.

114 http://www.nsa.gov/public_info/press_room/2013/30_July_2013.shtml

commencé à crypter leurs communications à l'aide du protocole SSL[115], la NSA a décidé de conclure un accord de coopération avec les plus éminentes de ces entreprises afin qu'elles lui transmettent les données d'utilisateurs d'une manière efficace et rationalisée.[116] Ces négociations ont donné naissance au programme PRISM, qui a permis à la NSA – contrairement à la collecte en amont (*upstream*) – de réceptionner d'une manière structurée des données en aval de neuf grandes sociétés technologiques : Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL et Apple.[117]

(33) Tous les fournisseurs PRISM se sont vu octroyer un code. P1 : Microsoft[118], P2 : Yahoo, P3 : Google[119], P4 : Facebook, P5 : PalTalk, P6 : YouTube, P7 : Skype[120], P8 : AOL, PA : Apple.[121]

(34) Neuf grands types de données sont recueillis par l'intermédiaire de PRISM et se sont eux aussi vu attribuer un code. A = communications enregistrées (p. ex. les messages privés sur les sites de réseaux sociaux, l'historique des conversations, les e-mails…), B = Instant Messaging (messagerie instantanée), C = RTN-EDC (notification en temps réel du nom d'utilisateur d'un compte et d'un message envoyé), D = RTN-IM (notification en temps réel de la connexion ou déconnexion à une conversation), E = e-mail, F = VoIP (services tels que

---

115 Protocole de cryptage utilisé pour sécuriser les communications sur Internet.

116 C. C. MILLER, *The New York Times*, 7 juin 2013 (*"Tech companies concede to surveillance programme"*).

117 Les *slides* les plus complets de PRISM ont été publiés en octobre par le journal *Le Monde*. http://www.lemonde.fr/technologies/article/2013/10/21/espionnage-de-la-nsa-tous-les-documents-publies-par-le-monde_3499986_651865.html

118 *The Guardian* a en outre décrit des documents de la SSO, qui démontraient que Microsoft et le FBI ont permis que la NSA puisse contourner aisément le cryptage de conversations instantanées d'outlook.com. Un autre document démontre que la NSA a accès aux e-mails de Hotmail, de Windows Live et d'Outlook.com avant qu'ils soient cryptés. http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

119 La NSA a ainsi accès à Gmail, aux appels audio et vidéo de Google, aux fichiers Google Drive, au service photo Picasa Web de Google et à la surveillance (en temps réel) des termes de recherche qu'une personne introduit dans Google. http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_3.html

120 *"According to a separate "User's Guide for PRISM Skype Collection", that service can be monitored for audio when one end of the call is a conventional telephone and for any combination of "audio, video, chat, and file transfers" when Skype users connect by computer alone."* http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_3.html. Un autre document mentionnait que "*Prism monitoring of Skype video production has roughly tripled since a new capability was added on 14 July 2012. (…) The audio portions of these sessions have been processed correctly all along, but without the accompanying video. Now, analysts will have the complete 'picture', it says*". http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

121 Les fournisseurs ont commencé à participer au programme PRISM à des moments différents. Microsoft : 11/09/2007, Yahoo : 12/3/2008, Google : 14/01/2009, Facebook : 3/6/2009, PalTalk : 7/12/2009, Youtube : 24/9/2010, Skype : 6/2/2011, AOL : 31/3/2011, Apple : octobre 2012. PRISM a donc seulement démarré après l'adoption du Protect America Act en 2007. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1# En avril 2013, ce journal titrait que l'ajout de Dropbox était imminent. http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_2.html

Skype, y compris la vidéoconférence), G = Full (forum web), H = OSN ('Online Social Networking' – photos, publications sur le mur, activités sur les sites de médias sociaux…) I = informations OSN fournies lors de l'inscription à un service OSN. J = vidéos.[122]

(35) Le système semble fonctionner comme suit : un analyste de la NSA peut saisir des *selectors* (adresse e-mail, numéro de téléphone, nom, mais aussi termes de recherche) dans un *Unified Targeting Tool* .[123] Ces *selectors* sont examinés par un supérieur, qui vérifie s'il y a 51 % de chance qu'il s'agisse d'une cible étrangère.[124] Si la NSA souhaite consulter les données enregistrées (par exemple les e-mails dans une boîte de réception), le FBI doit vérifier qu'aucun Américain n'est espionné. Si la NSA souhaite procéder à une surveillance en temps réel, cette vérification supplémentaire du FBI n'est pas nécessaire. Dans les deux cas, l'unité DITU (Data Intercept Technology Unit) du FBI utilise du matériel (*government equipment*) d'une des entreprises participant au programme PRISM pour obtenir des informations sur ces cibles. Le FBI transmet ensuite ce matériel à la CIA ou à la NSA.[125]

(36) Le recueil d'informations à propos d'une cible peut également impliquer le recueil des informations relatives à toutes les personnes avec lesquelles la cible a communiqué jusqu'au second degré. Un simple exemple hypothétique démontre que le recueil d'informations à propos d'une cible signifie dans la pratique que les données d'un très grand nombre de personnes peuvent être potentiellement collectées. Lorsqu'une cible a communiqué avec 700 personnes via Facebook ou par e-mail et que ces personnes ont à leur tour communiqué chacune avec 700 personnes, la NSA peut recueillir des données concernant 490 000 personnes.[126]

---

122 http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1#

123 " *In another classified report obtained by The Post, the arrangement is described as allowing "collection managers [to send] content tasking instructions directly to equipment installed at company-controlled locations", rather than directly to company servers.*" http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_1.html

124 Notons que chaque année, la FISC examine uniquement les certificats (voir paragraphe 9), et pas les termes de recherche individuels.

125 "*The information the NSA collects from Prism is routinely shared with both the FBI and CIA. A 3 August 2012 newsletter describes how the NSA has recently expanded sharing with the other two agencies. The NSA, the entry reveals, has even automated the sharing of aspects of Prism, using software that "enables our partners to see which selectors [search terms] the National Security Agency has tasked to Prism". The document continues: "The FBI and CIA then can request a copy of Prism collection of any selector…"* http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

126 http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1# *The Washington Post* fait également remarquer ceci : "*it is true that the PRISM program is not a dragnet, exactly. From inside a company's data stream the NSA is capable of pulling out anything it likes, but under current rules the agency does not try to collect it all*". http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_2.html Et d'ajouter plus loin : "*To collect on a suspected spy or foreign terrorist means, at minimum, that everyone in the suspect's inbox or outbox is swept in. Intelligence analysts are typically taught to chain through contacts two "hops" out from their target, which increases "incidental collection" exponentially.*" http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_3.html

(37) La NSA trie à son tour les données obtenues en fonction de leur type, puis les soumet à un filtre pour vérifier qu'aucune donnée américaine n'est examinée. Le contenu DNI[127] et les vidéos sont envoyés vers la base de données PINWALE.[128] Les métadonnées des *internet records* sont envoyées vers MARINA[129] et les métadonnées des conversations téléphoniques, vers MAINWAY.[130] Un bulletin interne de la NSA indiquait qu'en 2011, MAINWAY avait réceptionné quotidiennement les métadonnées issues de 700 millions de communications téléphoniques. À partir d'août 2011, 1,1 milliard de métadonnées de conversations téléphoniques est venu s'ajouter chaque jour.[131]

(38) Le 5 avril 2013, la *counterterrorism database* de Prism contenait 117 675 cibles de surveillance active.[132] Selon les *slides* divulgués, PRISM est le SIGAD dont sont issues la plupart des informations brutes utilisées pour tous les rapports de la NSA.[133] En 2012, des données PRISM sont apparues dans 1 477 éléments du Daily Intelligence Brief du Président américain.[134] Le directeur Clapper de la DNI a confirmé l'existence de PRISM (sans citer nommément le programme) et en a parlé comme étant l'*« une des principales sources »* de la NSA.[135]

I.7. Données financières

---

127 Par exemple : des publications sur des forums, des conversations, des e-mails… Bref, du contenu Internet (*internet content*).

128 Pinwale conserve le contenu des communications pendant cinq ans. Le flux de ces informations semble se fonder sur des *dictionary tasked terms* prédéfinis et émaner entre autres des programmes Xkeyscore et PRISM. http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu

129 Un *slide* Xkeyscore décrivait Marina comme contenant les "*user activity meta-data with front end full take feeds and back-end selected feeds"*.
http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu
The Guardian cite un document qui décrit l'application Marina : "*The Marina metadata application tracks a user's browser experience, gathers contact information/content and develops summaries of target," the analysts' guide explains. "This tool offers the ability to export the data in a variety of formats, as well as create various charts to assist in pattern-of-life development." (…) "Of the more distinguishing features, Marina has the ability to look back on the last 365 days' worth of DNI metadata seen by the Sigint collection system, regardless whether or not it was tasked for collection".*
http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents

130 http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1#

131 http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?pagewanted=all

132 En comparaison : en décembre 2011, la liste *Terrorist Identities Datamart Environment* (TIDE) du gouvernement américain comptait 740.000 enregistrements (*records*), où une même personne peut apparaître plusieurs fois si son nom est mal orthographié. http://www.dni.gov/files/Tide_Fact_Sheet.pdf

133 Ce qu'a également confirmé la FISC, voir paragraphe 19. "*According to the slides and other supporting materials obtained by The Post, "NSA reporting increasingly relies on PRISM" as its leading source of raw material, accounting for nearly 1 in 7 intelligence reports"*.
http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_1.html

134 http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_1.html

135 http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa

(39) Selon des documents que *Der Spiegel* a pu consulter, la NSA dispose d'une branche *'Follow the money'*, qui surveille les flux monétaires internationaux, surtout en Afrique et au Moyen-Orient. Ces informations atterrissent dans une base de données, baptisée TRACFIN. En 2011, cette base contenait déjà 180 millions d'ensembles de données (*datasets*) concernant des transferts bancaires, des transactions de cartes de crédit et des transferts de fonds. Selon *Der Spiegel*, la NSA conserve ce type de données durant cinq ans.[136]

(40) Toujours selon *Der Spiegel*, la NSA connaît en détail les processus internes de sociétés telles que Visa et MasterCard (par exemple, les *payment authorisation processes* et les communications internes chiffrées[137]) et surveille également des modes de paiement alternatifs tels que Bitcoin. Selon *Der Spiegel*, la NSA recueille, via le programme DISHFIRE, des informations relatives à des transactions exécutées à l'aide des cartes de crédit de plus de 70 banques dans le monde – surtout dans les 'territoires en crise' et y compris dans des pays tels que l'Italie, l'Espagne et la Grèce. DISHFIRE est actif depuis le printemps 2009. Les transactions de clients Visa en Europe, au Moyen-Orient et en Afrique ont également été analysées dans le but de mettre au jour des associations financières.[138] Grâce à ces connaissances, plusieurs banques arabes ont été mises sur la *blacklist* du Trésor américain.[139]

(41) D'autres documents démontrent que la division Tailored Access Operations (TAO) de la NSA a acquis, depuis 2006, un accès clandestin au trafic de données interne de SWIFT (Society for Worldwide Interbank Financial Telecommunication).[140] Ce qui est remarquable, étant donné que les États-Unis ont un accord avec l'UE visant à partager les données SWIFT, mais cet accord n'autorise pas l'envoi de données en vrac (*bulk data*).[141] Après ces révélations, le Parlement européen a voté la suspension du 'Terrorist Finance Tracking Program' (TFTP Agreement) le 23 octobre 2013.[142] Dans une déclaration, le Commissaire Malmström a fait savoir que l'accord TFTP ne serait pas suspendu.[143]

---

136 http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html

137 "*According to the presentation, the NSA was previously only able to decrypt payment transactions by bank customers, but now they have access to the internal encrypted communication of the company's branch offices. This "provides a new stream of financial data and potentially encrypted internal communications" from the financial service provider, the analysts concluded with satisfaction. This bank data comes from countries that are of "high interest." It's interesting to note that the targeted company is also one of the many SWIFT service partners*". http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430-2.html

138 "*Furthermore, the author concluded, thanks to network analyses and the use of the XKeyscore spying program, NSA analysts had stumbled across the encrypted traffic of a large financial network operator in the Middle East*". http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430-2.html

139 "*In one case, the NSA provided proof that a bank was involved in illegal arms trading -- in another case, a financial institution was providing support to an authoritarian African regime*". http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html

140 http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html "Since then, it has been possible to read the 'SWIFT printer traffic from numerous banks'".

141 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:195:0005:0014:EN:PDF

142 European Parliament resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance (2013/2831(RSP))

I.8. Métadonnées de conversations téléphoniques américaines

(42) Aux États-Unis, le débat relatif à la NSA porte surtout sur le recueil de données téléphoniques américaines par la NSA, entre autres sur la base de la section 215 *business records* introduite par le Patriot Act dans le FISA.[144] En vertu de cette section, les États-Unis ont pu contraindre les principaux opérateurs télécoms américains à mettre à la disposition de la NSA toutes les métadonnées des conversations téléphoniques au départ ou à destination des États-Unis. Selon la NSA, ces données peuvent uniquement être consultées aux fins de la lutte contre le terrorisme. La consultation peut uniquement commencer par un numéro de téléphone ayant été précédemment associé à une organisation terroriste étrangère (*a seed*).[145]

I.9. Données de smartphones

(43) Selon *Der Spiegel*, la NSA dispose de la capacité requise pour obtenir un large éventail de données de smartphones émanant de *high interest targets*.[146] La NSA avait accès aux listes de contacts, journaux d'appels, trafic SMS, brouillons de SMS et données de localisation de plateformes mobiles d'Apple (IOS), de Google (Android) et de BlackBerry.[147] Par exemple, la NSA a accès à 38 applications iPhone, telles que l'utilisation de la fonction de cartographie intégrée, la messagerie vocale et les photos, Google Earth, Yahoo et Facebook Messenger.[148]

I.10. Données PNR

(44) Par le biais de l'accord Passenger Name Records (PNR) de 2012, le ministère américain de la Sécurité intérieure (US Department of Homeland Security (DHS)) obtient les données PNR des passagers qui prennent l'avion sur le territoire de l'UE à destination des États-Unis. Ces données se composent des informations qu'un passager a fournies à la compagnie aérienne, par exemple : le nom du passager et des personnes qui l'accompagnent éventuellement, leurs adresses et numéros de téléphone, les dates de voyage, la destination finale, les détails du billet, le mode de paiement, le numéro de carte de crédit, les détails des bagages… La liste exhaustive figure en annexe à l'accord.[149] Le DHS

---

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0449+0+DOC+XML+V0//EN

143 European Commission, Memo, 23 octobre. http://europa.eu/rapid/press-release_MEMO-13-928_en.htm

144 Voir paragraphe 6.

145 N.S.A., The National Security Agency: Missions, Authorities, Oversight and partnerships. 9 août 2013.

146 Voir aussi paragraphe 19.

147 *"The presentation notes that the acquisition of encrypted BES (Blackberry Services) communications requires a "sustained" operation by the NSA's Tailored Access Operation department in order to "fully prosecute your target. (…) The alleged telecommunications surveillance has been a targeted activity that was performed without the smartphone makers' knowledge".* M. ROSENBACH, L. POITRAS et H. STRAK, *Der Spiegel,* 9 septembre 2013, ("iSpy: How the NSA Accesses Smartphone Data*").*

148 *Idem*.

149 http://register.consilium.europa.eu/pdf/en/11/st17/st17434.en11.pdf,36.

peut partager ces données avec des services nationaux[150] et des pays tiers.[151] Ces données sont utilisées à des fins de prévention, de recherche et de jugement de crimes terroristes et autres crimes transfrontaliers graves.[152] Après six mois, toutes les données personnelles sont masquées et après cinq ans, les données sont stockées dans une base de données 'passive'. Les données peuvent être utilisées pendant dix ans à des fins de prévention de crimes transfrontaliers et pendant quinze ans dans le cadre de la lutte contre le terrorisme.[153]

I.11. Efforts de la NSA contre le cryptage

(45) *The New York Times* a publié une *briefing sheet* que la NSA a portée à l'attention du GCHQ en 2010 à propos d'un programme intitulé BULLRUN. Dans ce briefing, la NSA suggère qu'elle peut décrypter ou contourner les protocoles de cryptage les plus utilisés pour la sécurisation du commerce mondial, des systèmes bancaires, des données médicales et de l'utilisation d'Internet (comme l'envoi d'e-mails, les recherches en ligne, les conversations instantanées et les conversations téléphoniques en ligne). Sont concernés les protocoles suivants : TLS/SSL[154], HTTPS[155], SSH[156], VPN[157], ainsi que les conversations instantanées[158] et les communications VOIP[159] cryptées. Jusqu'à présent, les détails techniques de ce qui a été précisément piraté n'ont pas été divulgués.[160] [161] L'existence de ces moyens de décryptage ainsi que l'utilisation de toutes les données exploitées (tant sous la forme de *plaintext* que de métadonnées) qui en sont issues ont été classifiées comme 'Exceptionally Controlled Information' (ECI), un niveau (*level*) supérieur à 'Top Secret'.[162]

---

150 *Idem*, article 16.

151 *Idem*, article 17.

152 *Idem*, article 4.

153 *Idem*, article 8.

154 Transport Layer Security/Secure Sockets Layer. Protocole le plus utilisé pour l'envoi d'informations sur Internet et sur des serveurs internes. La sécurisation du protocole HTTPS consiste à appliquer le cryptage TLS/SSL à un site web.

155 Hypertext Transfer Protocol Secure. Méthode permettant d'envoyer en toute sécurité des informations financières et des mots de passe d'un ordinateur à un réseau. Des sites tels que Facebook, Twitter et Gmail utilisent souvent le HTTPS par défaut. Cette sécurisation est reconnaissable au verrou qui s'affiche avant « https » dans la barre d'adresse du navigateur web.

156 Secure Shell. Permet aux utilisateurs Linux et Mac d'accéder à un ordinateur à distance.

157 Virtual Private Network. Souvent utilisé par des entreprises pour permettre à leurs collaborateurs d'accéder à leur réseau depuis leur domicile via un 'tunnel' crypté.

158 Par exemple, le programme Adium permet un cryptage de bout en bout (*end to end*) et les données ne peuvent être décryptées à aucun stade du transfert.

159 Fait référence à des services tels que Skype et Facetime d'Apple.

160 http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us Des experts ont remarqué que les documents ne montrent pas quels systèmes la NSA a décryptés au moyen de simples formules mathématiques et lesquels l'ont été au moyen d'un piratage ou d'une collaboration avec des développeurs. Un système tel que PGP (Pretty Good Privacy) fonctionnerait toujours. Pour de plus amples informations, voir (les liens) : http://www.washingtonmonthly.com/political-animal-a/2013_09/the_nsa_is_mostly_not_breaking046760.php ou http://www.newyorker.com/online/blogs/elements/2013/09/the-nsa-versus-encryption.html

161 http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us

162 http://www.theguardian.com/world/interactive/2013/sep/05/nsa-classification-guide-cryptanalysis.

(46) Une demande de budget datant de 2012 a également révélé l'existence du projet Sigint Enabling Project, qui vise à influencer en secret des sociétés Internet américaines et étrangères à adapter la conception de leurs produits de manière à permettre leur exploitation. Le programme englobe toute une série d'activités : (1) Collaborer avec des entreprises en vue d'installer des 'portes dérobées' dans des systèmes de décryptage commerciaux, des systèmes informatiques, des réseaux et des terminaux de communication (*endpoint communication devices)* qui sont utilisés par des 'cibles'.[163] Cette collaboration peut être volontaire[164] ou imposée en vertu du FISA.[165] (2) Influencer des normes et spécifications techniques en matière de technologies commerciales à clé publique (*commercial public key technologies)*, y compris la norme de 2006 du National Institute of Standards and Technology.[166] (3) Poursuivre la collaboration avec d'éminents opérateurs de télécommunications (*telecommunications carriers)*.[167] La méthode la plus controversée consiste toutefois à dérober subrepticement des clés de cryptage. Des documents de la NSA démontrent que la NSA possède une base de données interne (Key Provisioning Service), qui contient les clés de cryptage de produits commerciaux spécifiques. Lorsqu'une clé donnée ne figure pas dans la base, une demande est adressée au Key Recovery Service, dont on affirme qu'il acquiert des clés en piratant les serveurs des entreprises qui ont créé lesdites clés. Pour que cette méthode reste secrète, la NSA ne partagerait que des messages décryptés avec d'autres services lorsque les clés ont été obtenues par des moyens légaux.[168]

(47) Le 4 octobre 2013, *The Guardian* et *The Washington Post* ont révélé comment la NSA a tenté, depuis 2006, d'identifier et d'espionner des utilisateurs du réseau Tor.[169] Il s'agit d'un réseau de serveurs qui permet aux utilisateurs de surfer anonymement.[170] Les utilisateurs peuvent utiliser ce réseau à l'aide d'un logiciel spécial et complexe. Une autre méthode plus simple consiste à télécharger le Tor Browser Bundle (TBB), une version de Firefox qui transfère automatiquement des données sur le réseau Tor. Il ressort des documents qu'en 2007, la NSA a pu distinguer des utilisateurs TBB de simples utilisateurs Firefox,[171] mais que,

---

163 http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&_r=1&hp&&pagewanted=all

164 *"In one case, after the government learned that a foreign intelligence target had ordered new computer hardware, the American manufacturer agreed to insert a back door into the product before it was shipped, someone familiar with the request told The Times"*. http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&_r=1&hp&&pagewanted=all

165 http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&_r=1&hp&&pagewanted=all

166 *Idem.*

167 http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us

168 http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&_r=1&hp&&pagewanted=all

169 *The Washington Post* a mis en ligne un document de 49 pages datant de 2006, qui décrit les méthodes qui permettraient la désanonymisation potentielle à grande échelle d'utilisateurs Tor. http://apps.washingtonpost.com/g/page/world/nsa-research-report-on-the-tor-encryption-program/501/. Déclaration de J. CLAPPER à propos des révélations : http://icontherecord.tumblr.com/post/63103784923/dni-statement-why-the-intelligence-community

170 http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/04/everything-you-need-to-know-about-the-nsa-and-tor-in-one-faq/

171 http://apps.washingtonpost.com/g/page/world/nsa-slideshow-on-the-tor-problem/499/#document/p5/a124608

cette même année, elle n'était pas encore parvenue à pirater le réseau Tor. Une présentation de la NSA datant de juin 2012 mentionne que la NSA ne sera jamais en mesure de désanonymiser simultanément tous les utilisateurs Tor et qu'elle ne possède pas de technique permettant de désanonymiser un utilisateur donné sur demande. Une analyse manuelle permet toutefois de désanonymiser un 'très petit nombre' d'utilisateurs Tor.[172] Les *slides* de la division Tailored Access Operations (TAO) de la NSA décrivent comment la NSA a exploité les vulnérabilités de JavaScript dans Firefox à l'aide des programmes EGOTISTICALGOAT et EGOTISTICALGIRAFFE.[173] Ces vulnérabilités auraient disparu avec la dernière mise à jour de Firefox en janvier 2013[174], mais on ne sait pas très bien si la NSA est parvenue à contourner ce problème entre-temps.[175]

(48) Sous le nom de code Quantum, la NSA a placé des serveurs Quantum secrets à des emplacements importants de l'infrastructure Internet afin de pouvoir mener une attaque de type 'homme du milieu' (*man in the middle*) sur des utilisateurs Tor.[176] Ce qui signifie que ces serveurs peuvent réagir plus rapidement que d'autres sites Internet et peuvent envoyer l'utilisateur vers une imitation infectée du site Internet demandé qui se trouve sur un serveur FoxAcid. Les serveurs de ce système FoxAcid sont exploités par la TAO et peuvent contaminer des ordinateurs de différentes façons et pour de longues périodes.[177] La consultation de la page d'accueil d'un serveur FoxAcid n'engendrerait pas directement la contamination, car il faut pour cela une URL spécifique créée par la TAO. Cette URL permettrait au serveur FoxAcid de savoir exactement quelle cible visite le serveur FoxAcid.[178] FoxAcid est un système CNE général utilisé pour plusieurs formes de cyberattaques. Il ne sert donc pas seulement à identifier des utilisateurs Tor, loin de là. Des documents émanant de *Der Spiegel* suggèrent, par exemple, que des serveurs Quantum seraient (en partie) à l'origine de l'attaque de Belgacom.[179]

---

172 http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document?utm_source=hootsuite&utm_campaign=hootsuite

173 http://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document

174 http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption

175 "*In anticipation of a new release of Firefox, one agency official wrote in January that a new exploit was under development: 'I'm confident we can have it ready when they release something new, or very soon after'".* http://www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade-a1f23cda135e_story_2.html

176 B. SCHNEIER : "*More specifically, they are examples of "man-on-the-side" attacks".* http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

177 *"After identifying an individual Tor user on the internet, the NSA uses its network of secret internet servers to redirect those users to another set of secret internet servers, with the codename FoxAcid, to infect the user's computer. FoxAcid is an NSA system designed to act as a matchmaker between potential targets and attacks developed by the NSA, giving the agency opportunity to launch prepared attacks against their systems. Once the computer is successfully attacked, it secretly calls back to a FoxAcid server, which then performs additional attacks on the target computer to ensure that it remains compromised long-term, and continues to provide eavesdropping information back to the NSA".* http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

178 *Idem.*

179 http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

II. LE GOVERNMENT COMMUNICATIONS HEADQUARTERS (GQHQ) BRITANNIQUE

II.1. Le cadre légal britannique du recueil d'informations sur des cibles étrangères

(49) En 1994, l'Intelligence Services Act a défini pour la première fois les fonctions du Government Communications Headquarters (GCHQ). L'agence SIGINT britannique a notamment pour mandat de surveiller ou de perturber « *les émissions électromagnétiques, acoustiques et autres, ainsi que tout dispositif produisant de telles émissions* ».[180] L'agence doit transmettre des informations sur ces émissions à l'armée britannique, au gouvernement et à d'autres services[181] lorsque le requièrent la sécurité nationale du Royaume-Uni (avec une référence spécifique à la politique de défense et étrangère du Royaume-Uni) et le bien-être économique du Royaume-Uni (eu égard aux actes et intentions de personnes en dehors des Iles britanniques), ainsi qu'à des fins de prévention et de recherches de crimes graves.[182]

(50) Le Royaume-Uni ne dispose d'aucune législation spécifique régissant exclusivement l'utilisation de *foreign intelligence*, mais le Regulation of Investigatory Powers Act (RIPA) opère une distinction entre la surveillance 'interne' et 'externe', où cette dernière catégorie renvoie à la surveillance de communications dont au moins une extrémité se trouve au Royaume-Uni.[183] Dans ces cas-là, le GCHQ ne doit demander aucune réquisition visant une personne ou un endroit spécifique,[184] mais peut demander une réquisition pour, par exemple, intercepter des données d'une liaison externe de télécommunications (comme un câble en fibre optique spécifique qui court entre le Royaume-Uni et le continent européen).[185] À titre d'exemple, tous les câbles en fibre optique qui arrivent en Belgique sont reliés à un point d'atterrissement au Royaume-Uni. Le câble Tangerine relie Broadstairs à Ostende ; Concerto relie Zeebruges à Sizewell et Thorpeness, et le Pan-European Crossing relie Bredene à Dumpton Gap. Le grand câble SeaMeWe-3, qui est en partie détenu par Belgacom, relie Ostende à Goonhilly Downs au Royaume-Uni, mais compte de nombreux autres points d'atterrissement en Arabie saoudite, en Malaisie et en Chine.

(51) Une réquisition à si large portée est délivrée par le Secretary of State, qui décrit dans un 'certificat' quel élément requiert précisément un examen[186] dans l'intérêt de la sécurité

---

180 Intelligence Services Act 1994, Chapter 13, s3, (1)(a)

181 Intelligence Services Act 1994, Chapter 13, s3, (1)(b)

182 Intelligence Services Act 1994, Chapter 13, s3, (2).

183 RIPA, s20.

184 RIPA, s.8.4. L'interception est définie de la manière suivante à la section s.2.2 : "*A person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he- (a) so modifies or interferes with the system, or its operation, (b) so monitors transmissions made by means of the system, or (c) monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system, as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication*. "

185 "*Lawyers at GCHQ speak of having 10 basic certificates, including a "global" one that covers the agency's support station at Bude in Cornwall, Menwith Hill in North Yorkshire, and Cyprus. Other certificates have been used for "special source accesses" – a reference, perhaps, to the cables carrying web traffic. All certificates have to be renewed by the foreign secretary every six months*". http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world

186 RIPA, s8.4(b).

nationale du Royaume-Uni, pour prévenir ou rechercher des crimes graves ou pour préserver le bien-être économique du Royaume-Uni.[187] Le contenu des certificats est secret, mais selon des documents consultés par *The Guardian*, la formulation utilisée est très large et permet d'intercepter des éléments sur des thèmes vastes, tels que les intentions politiques de gouvernements étrangers, la situation militaire d'autres pays, le terrorisme, le trafic de drogues international et la fraude. Selon *The Guardian*, il existe au moins dix certificats de ce type.[188] Selon le RIPA, un tel mandat est initialement valable trois mois[189], mais peut être renouvelé tous les six mois.[190] Des sociétés de télécommunications peuvent être obligées de collaborer à l'interception de ces communications.[191]

(52) Il convient de souligner que le contenu de la réquisition et du certificat n'est pas clairement précisé. La loi n'est pas non plus très claire à ce sujet. L'Intelligence Security Committee (ISC), qui contrôle le GCHQ, a annoncé que *« des directives et procédures plus détaillées seront élaborées afin que le GCHQ respecte le Human Rights Act de 1998 »*. L'ISC va désormais examiner l'interaction complexe entre l'ISA, le Human Rights Act et le RIPA, et les procédures qui les régissent.[192]

(53) La loi permet également au GCHQ de pirater à distance des systèmes informatiques dans le but d'obtenir des données.[193] En vertu de la section 7 de l'ISA, toute action du GCHQ en dehors du Royaume-Uni est exemptée de toute responsabilité civile ou pénale si elle s'appuie sur une autorisation du Secretary of State.

II.2. Nature et ampleur du recueil de données britannique

(54) Selon *The Guardian*, le GCHQ a entamé les préparatifs du projet Mastering the Internet (MTI) à la base de Bude début 2007.[194] L'objectif était de recueillir des données étrangères en amont (*upstream*), en plaçant du matériel *deep packet inspection* sur les câbles sous-

---

187 RIPA, s.5(3)a-c. *The Guardian* cite un document du GCHQ comme suit : "*The certificate is issued with the warrant and signed by the secretary of state and sets out [the] class of work we can do under it … cannot list numbers or individuals as this would be an infinite list which we couldn't manage"*. http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world

188 http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world. *The Guardian* cite un mémo interne au GCHQ datant d'octobre 2011 : "*[Our] targets boil down to diplomatic/military/commercial targets/terrorists/organised criminals and e-crime/cyber actors "*. http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet

189 RIPA, s9.6.c.

190 RIPA, s9.6.b. Pour de plus amples informations sur les *s(8)4 warrants*, voir UK Home Office, Interception of Communications Code of Practice. TSO, London, p.22-27, disponible à l'adresse https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97956/interception-comms-code-practice.pdf

191 RIPA, s.12

192 Intelligence and Security Committee of Parliament, Statement on GCHQ's alleged interception of communications under the US PRISM Programme. 17 juillet 2013, disponible à l'adresse http://isc.independent.gov.uk/news-archive/17july2013

193 Voir Computer Misuse Act 1990, s.10 ; RIPA, s32 et ISA, s.5

194 Outre le projet MTI, il convient également de citer un autre programme, baptisé *Global Telecoms Exploitation*, dont l'objectif n'est pas clair. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

marins à leur arrivée sur les côtes britanniques. [195] En mai 2009, *The Register* et *The Sunday Times* ont annoncé que le financement du MTI avait été approuvé en octobre 2007. Plus d'un milliard de livres sterling seraient affectées à cette collecte en amont (*upstream*) pour les trois années suivantes.[196] Le GCHQ a reconnu l'existence du projet MTI, mais a souligné qu'il n'était pas en train d'élaborer une technologie capable de surveiller toutes les utilisations d'Internet et du téléphone *au Royaume-Uni*.[197]

(55) À un moment indéterminé entre 2010 et 2011, le GCHQ a atteint son objectif et a commencé à contraindre par mandat les exploitants de câbles commerciaux en fibre optique de collaborer en tant qu'*intercept partners*. Ce processus de collaboration forcée porte le nom de *special source exploitation,* et les *intercept partners* sont indemnisés pour les coûts générés.[198] Plu
s tard, le *Suddeütsche Zeitung* divulguait le nom des entreprises participantes. Elles étaient toutes les sept connues sous un autre nom de code : BT (Remedy), Verizon Business (Dacron), Vodafone Cable (Gerontic), Global Crossing (Pinnage), Level 3 (Little), Viatel (Vitreous) et Interoute (Streetcar).[199] Les câbles en fibre optique qui arrivent en Belgique (voir paragraphe 50) sont tous exploités par une de ces entreprises.

(56) Ces informations en amont (*upstream*) sont d'abord filtrées via le programme TEMPORA afin d'exclure le trafic Internet qui occupe un volume important (comme les téléchargements de films ou de musique) et d'ainsi réduire le volume d'environ 30 %.[200] Le reste des informations en amont (*upstream*) est filtré sur la base de *hard selectors* (comme des numéros de téléphone et des adresses e-mail) et de *soft selectors* (comme des critères de recherche). Selon *The Guardian*, 40 000 de ces sélecteurs ont été choisis par le GCHQ et 31 000 par la NSA.[201] Les certificats élaborés déterminent le choix de ces *selectors*. Les données non filtrées sont jetées, les métadonnées restantes sont conservées durant trente jours et le contenu, durant trois jours.[202] Une source du journal *The Guardian* semble suggérer que toutes les données 'filtrées' sont conservées et peuvent être consultées par l'Interception Commissioner britannique, sans savoir précisément s'il s'agit de toutes les informations stockées après filtrage des *selectors* ou uniquement des données effectivement utilisées.[203] Ces données peuvent ensuite être – entre autres – examinées rétroactivement

---

195 http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet. Un premier projet expérimental connu sous le nom de *Cheltenham Processing Centre* (CPC) poursuivait le même objectif. À partir de mars 2010, il est fait référence à ce projet en tant qu'initiative conjointe GCHQ/NSA baptisée TINT.

196 Selon ces articles, Lockheed Martin et Detica collaboreraient au projet MTI. Depuis 2008, ces sociétés ont effectivement publié des offres d'emploi relatives au contrat MTI. http://www.theregister.co.uk/2009/05/03/gchq_mti/ ; http://www.timesonline.co.uk/tol/news/politics/article6211101.ece

197 (impression de l'auteur) http://www.telegraph.co.uk/technology/news/5271796/Government-not-planning-to-monitor-all-web-use.html

198 http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

199 http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq

200 http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

201 *Idem*.

202 http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work Il est intéressant de noter que dans certains cas, le GCHQ considère même des mots de passe comme des métadonnées.

203 http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

dans le cadre de la recherche de suspects encore inconnus des services de renseignement britanniques ou américains.[204]

(57) Pour le reste, le recueil porte également sur toutes les informations en amont (*upstream*) qui sont également recueillies par la NSA dans le cadre de sa collecte en amont (voir paragraphe 29) : contenu des e-mails, historique de navigation, messages Facebook, documents ajoutés en pièces jointes... Il convient de remarquer ici que des analystes peuvent également décider de recueillir toutes les métadonnées et tout le contenu des contacts d'une cible s'ils l'estiment proportionnel.[205] Au moins 300 analystes du GCHQ et 250 de la NSA ont un accès direct aux données de TEMPORA. [206] Nombre de métadonnées sont stockées par la NSA.[207] En février 2011, la NSA indiquait dans un document que le GCHQ « *traitait plus de données* » que la NSA.[208] En 2012, le GCHQ est parvenu à traiter 600 millions d' 'événements téléphoniques' par jour, écouter 200 câbles en fibre optique et traiter des données de 46 de ces câbles simultanément. *The Guardian* a estimé que le GCHQ a ainsi accès en théorie à 21,6 pétaoctets par jour, soit 192 fois le contenu de tous les livres de la British Library ou du Congress.[209]

II.3. Logiciel malveillant chez Belgacom

(58) Le 21 juin 2013, Belgacom trouve un logiciel malveillant (*malware)* dans son système informatique interne. Après l'aide infructueuse de sous-traitants tels que Microsoft et HP, Belgacom demande à la société néerlandaise Fox-IT d'examiner ce logiciel malveillant.[210] Après un examen approfondi par Fox-IT, Belgacom dépose, le 19 juillet 2013, une plainte contre X auprès du parquet fédéral pour accès frauduleux à ses systèmes informatiques internes. L'enquête est dirigée par la police judiciaire de Bruxelles (Regional Computer Crime Unit) avec le soutien (technique) de la Federal Computer Crime Unit (FCCU) et du Service général du renseignement et de la sécurité (SGRS).[211] En septembre, le président de la Commission de la protection de la vie privée décide d'ouvrir une enquête distincte, en collaboration avec Belgacom et l'Institut belge des services postaux et des

---

204 http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work

205 "*If analysts believe it is proportional, they can look at all the traffic – content and metadata – relating to all of the target's contact*". http://www.theguardian.com/uk/2013/jun/23/mi5-feared-gchq-went-too-far

206 http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet

207 http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection

208 http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet

209 http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa?CMP=twt_fd Et *The Guardian* d'ajouter : "*The system seems to operate by allowing GCHQ to survey internet traffic flowing through different cables at regular intervals, and then automatically detecting which are most interesting, and harvesting the information from those. The documents suggest GCHQ was able to survey about 1,500 of the 1,600 or so high-capacity cables in and out of the UK at any one time, and aspired to harvest information from 400 or so at once – a quarter of all traffic. As of last year, the agency had gone halfway, attaching probes to 200 fibre-optic cables, each with a capacity of 10 gigabits per second. In theory, that gave GCHQ access to a flow of 21.6 petabytes in a day, equivalent to 192 times the British Library's entire book collection*". http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work

210 Belgacom GCHQ Affair - EP/LIBE hearing on surveillance 3 October 2013. Voir http://www.youtube.com/watch?v=ayR6CAuNE4w

211 M. EECKHAUT, P. DE LOBEL, *De Standaard*, 17 septembre 2013 ("Natuurlijk zat de NSA hier achter").

télécommunications (IBPT), afin de déterminer les circonstances exactes de cet incident. Dans un communiqué de presse du 16 septembre 2013, Belgacom annonce avoir supprimé « *un virus inconnu* » durant le week-end des 14 et 15 septembre. Selon Belgacom, « *au stade actuel, il n'y a aucune indication d'impact pour les clients ou leurs données* ».[212] Le coût de l'opération de nettoyage est alors estimé à cinq millions d'euros.[213]

(59) D'après un communiqué de presse du parquet, vu l'engagement de moyens financiers et logistiques considérables par les intrus et sa complexité technique, l'attaque pointe dans la direction d'une opération d'espionnage étatique visant le recueil d'informations stratégiques.[214] Par la suite, Belgacom confirme que 124 des 26 600 appareils[215] connectés au système Windows interne de Belgacom ont été compromis[216] par ce que les experts appellent une *advanced persistent threat* (menace persistante avancée).[217] La description des symptômes de ce *malware* relève du secret de l'instruction, mais la FCCU a autorisé la divulgation du *malware*, dans la mesure du possible, afin que d'autres institutions (belges et européennes) puissent vérifier si elles ont été infectées. Les informations sont entre autres partagées avec la Computer Emergency Response Team (CERT-EU) de l'Union européenne.

(60) *De Standaard* mentionne, en s'appuyant sur des sources proches du dossier et évoluant dans les milieux des services de sécurité, que la NSA se cache derrière cette attaque et que la NSA visait particulièrement les activités de BICS (Belgacom International Carrier Services), une filiale de Belgacom.[218] Belgacom détient 57,6 % de BICS, Swisscom 22,4 % et l'opérateur sud-africain MTN 20 %. BICS fournit des services à différents opérateurs de télécommunications dans différents pays et exploite entre autres – avec un groupe d'autres entreprises – les câbles sous-marins en fibre optique TAT-14, SEA-ME-WE3 et SEA-ME-WE4 (voir également paragraphe 50). Ce qui permettrait, par exemple, d'intercepter le trafic Internet et téléphonique en provenance de la Syrie, du Yémen et de l'Afghanistan. C'était une des raisons de l'attaque que *De Standaard* a citées dans son premier article.[219] Dans un communiqué, BICS affirme le 16 septembre 2013 que « *nous n'avons aucune indication permettant de dire que notre réseau télécoms, par lequel le trafic de communication est acheminé, a été touché par ces opérations d'espionnage. C'est notre système informatique interne, qui est intégré avec celui de Belgacom, qui est concerné par le hacking* ».[220]

---

212 Belgacom, Belgacom prend action dans le cadre de sa sécurisation IT. 16 septembre 2013. http://www.belgacom.com/be-fr/newsdetail/ND_20130916_Belgacom.page

213 P. DE LOBEL, N. VANHECKE, *De Standaard*, 21 septembre 2013, ("Op het randje van de catastrofe").

214 M. EECKHAUT, P. DE LOBEL, *De Standaard*, 17 septembre 2013 ("Natuurlijk zat de NSA hier achter").

215 Belgacom GCHQ Affair - EP/LIBE hearing on surveillance 3 October 2013. http://www.youtube.com/watch?v=ayR6CAuNE4w

216 X., *De Standaard*, 16 septembre 2013 ("Bellens : 'Geen aanwijzing dat Belgacomklanten zijn getroffen'"). http://www.standaard.be/cnt/dmf20130916_00743534

217 DOD, *De Standaard*, 17 septembre 2013 ("Zeg nooit 'virus' tegen advanced persistent attack"). http://www.standaard.be/cnt/dmf20130916_00745157. Pour de plus amples informations, voir par exemple https://www.damballa.com/knowledge/advanced-persistent-threats.php

218 M. EECKHAUT, P. DE LOBEL, N. VANHECKE, *De Standaard*, 16 septembre 2013 ("NSA verdacht van hacken Belgacom"). Voir http://www.standaard.be/cnt/dmf20130915_00743233

219 M. EECKHAUT, P. DE LOBEL, *De Standaard*, 17 septembre 2013 ("Natuurlijk zat de NSA hierachter").

220 G. QUOISTIAUX, *Trends*, 16 septembre 2013 ("Découvrez BICS, la filiale de Belgacom qui serait visée par la NSA"). http://trends.levif.be/economie/actualite/decouvrez-bics-la-filiale-de-belgacom-qui-serait-visee-par-la-nsa/article-4000400052938.htm

(61) Le 20 septembre 2013, *Der Spiegel* a publié des *slides* non datés issus des documents de Snowden, dans lesquels le 'Network Analyses Centre' du GCHQ évoque les réussites obtenues dans le cadre de l''Operation Socialist'. Dans cette opération, Belgacom était connue sous le nom de Merion Zeta. Il semble que des employés qui occupent des fonctions-clés au sein de BICS ont été dirigés, via des serveurs Quantum contrôlés par la NSA, vers un autre serveur contrôlé par la NSA (serveur Fox Acid), lequel a utilisé à son tour une vulnérabilité du navigateur de la cible pour installer un logiciel malveillant sur l'ordinateur de la victime (voir aussi paragraphe 48). D'après les *slides* de *Der Spiegel*, le but ultime de l''Operation Socialist' était d'exploiter le principal routeur GRX de Belgacom afin de pouvoir mener à partir de là des attaques *man in the middle* sur des cibles qui utilisent les services itinérants (*roaming*) depuis leur smartphone à l'étranger.[221] Selon les *slides*, le GCHQ était très proche du but.[222] BICS est connu dans le monde entier en tant que fournisseur de services 3GRX. Ces services doivent entre autres permettre à un opérateur téléphonique local d'assurer le roaming des appels de ses clients dans plus de 190 pays.[223] Les connexions VPN de BICS et MyBICS, application en ligne utilisée pour le contact avec les clients, ont également été considérées comme des cibles intéressantes.

(62) Après les révélations parues dans *Der Spiegel*, *De Standaard* a cité des sources proches de l'instruction judiciaire qui restent convaincues que l'attaque provient des États-Unis étant donné la signature du logiciel malveillant et surtout l'endroit vers lequel mènent les pistes. Selon les enquêteurs, les États-Unis sont la principale destination, et les pistes ne conduisent que « *dans une mesure très restreinte* » au Royaume-Uni.[224] À la demande du Premier ministre Di Rupo, la Sûreté de l'État belge a officiellement demandé des explications à son homologue britannique.[225]

(63) En s'appuyant sur 'diverses sources', la chaîne néerlandaise NOS indique le 3 octobre que fin 2011, une équipe du GCHQ a attaqué le cœur de Belgacom par le biais de canaux nommés (*named pipes)*, méthode sophistiquée utilisée pour envoyer une communication presque invisible sur un réseau. Selon la chaîne NOS, des données de conservation (*loggegevens*) confirment qu'il s'agit de l'Angleterre : les activités d'espionnage sont clairement moins nombreuses pendant les jours fériés et le temps de midi anglais.[226] NOS affirme qu'une fois le réseau piraté, les Britanniques ont eu un accès presque illimité au réseau Belgacom.[227] Avant cela, une autre source a révélé au journal *De Standaard* que celui qui faisait cela pouvait faire tout ce que le gestionnaire réseau le plus haut placé de Belgacom peut faire et possédait toutes les clés, tous les mots de passe et tout le contrôle.[228] NOS affirme également qu'une autre équipe a ensuite cherché des informations

---

221 http://www.spiegel.de/fotostrecke/photo-gallery-operation-socialist-fotostrecke-101663.html. Pour de plus amples détails techniques, voir https://www.troopers.de/wp-content/uploads/2011/10/TR12_TelcoSecDay_Langlois_Attacking_GRX.pdf

222 http://www.spiegel.de/fotostrecke/photo-gallery-operation-socialist-fotostrecke-101663-3.html

223 http://www.bics.com/sites/default/files/mosaic/3GRX_web.pdf

224 N. VANHECKE, *De Standaard*, 21 septembre 2013 ("Operatie socialist: succes!").

225 K. VAN DE PERRE, *De Morgen*, 4 octobre 2013 ("België vraag uitleg aan Britten over Belgacom-hacking").

226 http://nos.nl/artikel/558286-hoe-belgacom-werd-gekraakt.html

227 NOS Journaal, 3 octobre 2013, 20h CET. http://nos.nl/uitzendingen/12720-nos-journaal-3-oktober-2013-2000u.html

228 P. DE LOBEL, N. VANHECKE, *De Standaard*, 21 septembre 2013 ("Op het randje van de catastrofe").

spécifiques. Informations qui ont par la suite été partagées avec la NSA.[229] Selon des « *sources proches de l'enquête* », les responsables ont regardé un peu partout et ont pris ce qu'ils pouvaient.[230] Selon *De Standaard*, BICS fournit des services que de nombreux clients importants peuvent utiliser : Swift, Electrabel, bpost, Belgocontrol, l'OTAN à Evere, la Commission européenne et le Parlement européen à Bruxelles et Strasbourg, le SHAPE (Supreme Headquarters Allied Powers Europe) à Mons, mais aussi le quartier général du Commandement aérien allié de l'OTAN à Ramstein.[231] Lors d'une audition au Parlement européen, deux hauts responsables de Belgacom ont nié que le service secret britannique aurait eu accès aux réseaux téléphoniques d'institutions européennes. Selon Belgacom, il n'y a eu aucun débordement via leur système vers des systèmes de clients. Et donc pas non plus vers des systèmes d'instances européennes.[232]

(64) À l'heure actuelle, il est cependant impossible de dire avec certitude quelles données ont été précisément interceptées. Tant Belgacom[233], la FCCU[234], que Frank Robben[235], co-rapporteur du rapport Belgacom de la Commission de la protection de la vie privée, ont déclaré que le virus proprement dit utilisait des techniques de cryptage pour masquer les données compromises. Selon la chaîne NOS, il n'est plus possible de déterminer qui a été précisément concerné par les écoutes et quelles informations ont été exactement obtenues. Pour le savoir, il fallait plus de temps. Or ce n'était pas possible, parce que Belgacom voulait que son réseau soit de nouveau opérationnel le plus vite possible.[236] On ne sait pas non plus exactement pendant combien de temps le virus est resté sur le réseau. Lors d'une conférence de presse le 16 septembre 2013, le responsable de Belgacom a affirmé n'avoir aucune idée du moment où le virus s'est retrouvé sur le réseau de Belgacom. Selon *Der Spiegel,* il ressort d'un document (jusqu'à présent non publié) que l'accès était possible depuis 2010.[237] Selon *De Standaard* et la chaîne NOS*,* le virus était déjà présent depuis 2011.[238]

(65) Le 18 octobre 2013, Belgacom signale que des contrôles poussés ont mis au jour de nouvelles irrégularités sur un routeur de BICS. *« Les premières analyses indiquent que des modifications ont été réalisées dans le logiciel du router, ce qui a pu avoir lieu pendant la récente intrusion digitale. »*[239] Belgacom n'exclut plus le piratage des données de ses clients. *« L'enquête en cours devra évaluer s'il y a un impact sur les données des clients »*, a déclaré

---

229 NOS Journaal, 3 octobre 2013, 20h CET. http://nos.nl/uitzendingen/12720-nos-journaal-3-oktober-2013-2000u.html

230 P. DE LOBEL, N. VANHECKE, *De Standaard*, 21 septembre 2013 ("Op het randje van de catastrofe").

231 *Idem.*

232 http://nos.nl/artikel/558285-spionage-belgacom-omvangrijker.html

233 Belgacom GCHQ Affair - EP/LIBE hearing on surveillance 3 October 2013. http://www.youtube.com/watch?v=ayR6CAuNE4w

234 N. VANHECKE, *De Standaard*, 20 septembre 2013 ("Info over malware Belgacom verspreid").

235 Belgacom GCHQ Affair - EP/LIBE hearing on surveillance 3 October 2013. http://www.youtube.com/watch?v=ayR6CAuNE4w

236 http://nos.nl/artikel/558286-hoe-belgacom-werd-gekraakt.html

237 http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

238 M. EECKHAUT, P. DE LOBEL, N. VANHECKE, *De Standaard*, 16 septembre 2013 ("NSA verdacht van hacken Belgacom"). http://www.standaard.be/cnt/dmf20130915_00743233

239 http://www.belgacom.com/be-fr/newsdetail/ND_20131017_Belgacom.page

Belgacom dans *Le Soir*.[240] Le 23 octobre, Belga annonce que Tecteo a également été victime d'une cyberattaque similaire à celle perpétrée contre les opérateurs de télécommunications Belgacom, France-Telecom et Wanadoo. C'est ce qu'affirme la société. À l'heure actuelle, il est encore trop tôt pour dire si des informations ont été piratées au sein du groupe ou des filiales VOO ou RESA.[241]

II.4. Efforts britanniques contre le cryptage

(66) L'équivalent britannique du programme BULLRUN (voir paragraphe 45) a été baptisé EDGEHILL. Des documents que *The Guardian* a pu consulter suggèrent que le Royaume-Uni n'est pas aussi loin que les États-Unis et n'a pu décrypter des informations qu'au cas par cas. L'objectif initial d'EDGEHILL était de déchiffrer le trafic Internet crypté de trois grandes sociétés Internet et de 30 types de VPN. D'ici 2015, le GCHQ espérait avoir décrypté le trafic Internet chiffré de 15 grandes sociétés Internet et 300 types de VPN.[242] Un autre programme, appelé CHEESY NAME, a été mis sur pied pour pirater certaines clés de cryptage (connues sous le nom de *certificates*) à l'aide de superordinateurs du GCHQ.[243] Le GCHQ a également créé une *Humint Operations Team* (HOT) chargée d'identifier, de recruter et de gérer des informateurs (*covert agents*) dans le secteur mondial des télécommunications, entre autres pour obtenir l'accès à certaines clés.[244]

(67) Des documents qui ont été montrés lors d'une émission de Fantastico suggèrent que la *network exploitation unit* du GCHQ a utilisé des programmes (FLYING PIG et HUSH PUPPY) capables de surveiller des réseaux TLS/SSL. Les programmes semblent avoir vu le jour parce qu'un nombre croissant de fournisseurs de messagerie électronique, tels que Yahoo, Google ou Hotmail, utilisaient le cryptage SSL et que ces messages étaient dès lors devenus illisibles dans le cadre de la collecte directe en amont (*upstream*). Un document au moins montre que tant la NSA que le GCHQ ont eu recours à des attaques de type *man in the middle* pour

---

240 X., *Belga*, 19 octobre 2013 ("Belgacom n'exclut plus le piratage des données de ses clients").

241 X., *Belga*, 23 octobre 2013 ("Tecteo a également été victime de la vague d'espionnage informatique").

242 "*GCHQ's phrasing of beating "30" then "300" VPNs suggest it's done on a case-by-case basis, rather than a blanket capability. It's also worth noting that just because the NSA can, say, beat SSL in some (or many, or most) cases, it doesn't mean they can do it all the time, especially as they often seem to circumvent rather than directly beat security".* http://www.theguardian.com/commentisfree/2013/sep/06/nsa-surveillance-revelations-encryption-expert-chat. *The Guardian* mentionne également : "*Analysts on the Edgehill project were working on ways into the networks of major webmail providers as part of the decryption project. A quarterly update from 2012 notes the project's team "continue to work on understanding" the big four communication providers, named in the document as Hotmail, Google, Yahoo and Facebook, adding "work has predominantly been focused this quarter on Google due to new access opportunities being developed".* http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

243 *Idem.*

244 *Idem.*

contourner le cryptage.[245] FLYING PIG semble également pouvoir montrer des informations sur l'utilisation de Tor (Tor Events).[246]

(68) Un document datant du 10 octobre 2012 décrit comment, lors de l'opération MULLENIZE, le GCHQ est parvenu à identifier des utilisateurs individuels sur une adresse IP utilisée simultanément par plusieurs personnes, et ce via la technique du *user agent staining*. C'est par exemple le cas dans un cybercafé, mais aussi dans certaines régions où des milliers d'utilisateurs se servent d'une même adresse IP. Cette technique permet également de reconnaître des utilisateurs Tor individuels. En deux mois, le GCHQ a réussi à infecter ainsi quelque 200 ordinateurs avec des *stains* uniques.[247]

III. ÉNUMÉRATION DES CAS D'ACTIVITÉS D'ESPIONNAGE RELATIFS À DES ACTIVITÉS POLITIQUES DE 'PAYS AMIS' CITÉS DANS DES SOURCES OUVERTES

III.1. Activités d'espionnage (supposées) hors affaire Snowden

(69) La présente liste se concentre sur l'espionnage de pays amis par les États-Unis ou le Royaume-Uni. L'espionnage de pays européens qui faisaient partie du Pacte de Varsovie durant la Guerre froide n'entre pas en ligne de compte. Les exemples historiques sont donnés à titre d'illustration.

(70) L'historien britannique Richard Aldrich a décrit comment, depuis 1940, le prédécesseur du GCHQ écoutait les communications diplomatiques de ses partenaires, dont la France libre sous la direction de De Gaulle, la Turquie, l'Espagne et une vingtaine d'autres pays.[248] Des informations diplomatiques émanant d'Italie, de France, d'Espagne, du Portugal, du Japon et de l'Allemagne de l'Ouest étaient partagées avec les États-Unis sur une base *ad hoc*.[249]

(71) Le 21 février 1967, le journal britannique *Daily Express* a révélé comment des entreprises telles que Western Union et Cable & Wireless ont transmis aux autorités britanniques tous les télégrammes et télex internationaux (y compris du matériel issu d'ambassades étrangères), qui ont ensuite été copiés. D'après Aldrich, cette tradition remontait à la Première Guerre mondiale : le Royaume-Uni a donc eu accès à tout le trafic diplomatique de toutes les ambassades sur son territoire pendant une période de plus de cinquante ans.[250]

---

245 *"The document illustrates with a diagram how one of the agencies appears to have hacked into a target's Internet router and covertly redirected targeted Google traffic using a fake security certificate so it could intercept the information in unencrypted format".* http://www.slate.com/blogs/future_tense/2013/09/09/shifting_shadow_stormbrew_flying_pig_new_snowden_documents_show_nsa_deemed.html

246 *Idem.*

247 http://apps.washingtonpost.com/g/page/world/gchq-report-on-mullenize-program-to-stain-anonymous-electronic-traffic/502/

248 R. ALDRICH, *GCHQ. The uncenseored story of Britain's most secret intelligence agancy*, Harper Press, London, 2010, 28; 52-53.

249 R. ALDRICH, *o.c.*, 44.

250 R. ALDRICH, *o.c.*, 238-240.

(72) Selon Aldrich, le service néerlandais a intercepté des communications diplomatiques de la Belgique et de l'Allemagne dans les années 1980.[251]

(73) En 2006, le rapport annuel *top secret* de 1985-1986 du Government Communications Security Bureau (GCSB), l'agence SIGINT de la Nouvelle-Zélande, était révélé. Ce rapport mentionnait les pays et agences que la Nouvelle-Zélande avait espionnés cette année-là, ainsi que les communications diplomatiques de l'ONU, de l'Égypte, du Japon, des Philippines, de plusieurs îles de l'océan Pacifique, de la France, du Vietnam, de l'Union soviétique, de la Corée du Nord, de l'Allemagne de l'Est, du Laos et de l'Afrique du Sud.[252] En 1985, le service secret français a fait couler le 'Rainbow Warrior' de Greenpeace, et le GCSB a sollicité l'aide de la NSA et du GCHQ pour espionner des sources en France.[253]

(74) Alastair Campbell, Director of Communications and Strategy du gouvernement de Tony Blair entre 1997 et 2003, a décrit dans ses mémoires comment des agents de sécurité britanniques ont découvert deux *bugs* dans la chambre d'hôtel qui était destinée à Tony Blair lors de sa visite à New Delhi en octobre 2001. Ces *bugs* ont été attribués au service secret indien.[254]

(75) En 1999, la presse américaine a publié plusieurs rapports qui affirmaient que tant la NSA que le GCHQ avaient infiltré la mission de l'UNSCOM avec des inspecteurs en désarmement de l'ONU afin d'entreprendre des opérations SIGINT sensibles en Irak. Toutes les informations qui ont été trouvées par ce biais n'ont pas été partagées avec l'UNSCOM.[255] Selon l'inspecteur principal des Nations unies, Hans Blix, ces informations étaient particulièrement pertinentes pour une éventuelle invasion ultérieure. [256]

(76) En 2003, *The Observer* a publié l'intégralité d'un mémo de la NSA au GCHQ, dans lequel elle demandait l'aide de ce dernier pour écouter les membres non permanents du Conseil de sécurité des Nations unies de l'époque (Angola, Cameroun, Chili, Bulgarie et Guinée), et ce afin de connaître la position de ces pays à l'égard d'une éventuelle résolution du Conseil de sécurité approuvant une intervention militaire contre l'Irak.[257]

(77) À peu près à la même époque, en février 2003, un dispositif d'écoute était trouvé dans les parties du bâtiment Juste Lipse du Conseil européen qui étaient occupées par les délégations britanniques, françaises, allemandes et espagnoles. L'enquête a suggéré que ce dispositif se trouvait dans le bâtiment depuis sa construction en 1993. Bien que cela n'ait

---

251 R. ALDRICH, *o.c.*, 604.

252 H. BAIN, *Sunday Star*, 15 janvier 2006 ("Lange's secret papers reveal USA's bully tactics").

253 R. ALDRICH, *o.c.*, 446.

254 A. CAMPBELL, *The Blair Years: The Alastair Campbell diaries*, Knopf Doubleday Publishing Group, 2011, 577.

255 C. LYNCH, Boston Globe, 6 janvier 1999 ("US used UN to spy on Iraq, aides say"); B. GELLMAN, *The Washington Post,* 6 janvier 1999 ("Annan suspicious of UNSCOM probe").

256 H. BLIX, *Disarming Iraq : The search for weapons of mass destruction*, Bloomsbury, 2005, 36-37.

257 Le mémo mentionnait également : "*We have a lot of special UN-related diplomatic coverage (various UN delegations) from countries not sitting on the UNSC right now that could contribute related perspectives/insights/whatever.*" X., *The Observer*, 2 mars 2003 ("US plan to bug Security Council: the text"). Voir aussi : http://www.theguardian.com/world/2003/mar/02/iraq.unitednations1

jamais été prouvé de manière irréfutable, plusieurs indicateurs ont pointé dans la direction d'Israël en tant que responsable de cet espionnage.[258]

(78) En 2004, l'ancienne ministre britannique Clare Short a déclaré lors de l'émission Today sur BBC Radio 4 qu'elle avait régulièrement eu connaissance de SIGINT, où l'on pouvait entendre des conversations du Secrétaire général des Nations unies, Kofi Annan, dans son bureau privé du quartier général de l'ONU à New York, juste avant le début de la guerre en Irak en 2003.[259]

(79) En 2004, des dispositifs d'écoute ont été trouvés dans le 'Salon français' du Palais des Nations de l'ONU à Genève. Ce salon faisait partie des pièces utilisées, en septembre 2003, pour des négociations privées sur la question de l'Irak. Aucun responsable n'a jamais été identifié.[260]

(80) En décembre 2004, l'on a suggéré que la NSA avait écouté des dizaines de conversations téléphoniques entre Mohamed ElBaradei, responsable de l'Agence internationale de l'énergie atomique (AIEA), et des diplomates iraniens. Le journal *The Washington Post* a avancé que l'on cherchait des éléments susceptibles d'évincer ElBaradei de la direction de l'AIEA.[261]

III.2. Révélations émanant des documents de Snowden

(81) Selon *Der Spiegel*, le Special Collection Service a intercepté des SIGINT clandestins à partir de 80 ambassades et consulats américains.[262] Cette équipe est aussi responsable d'opérations de surveillance top secrètes dans d'autres ambassades et consulats, opérations connues sous le nom de code STATEROOM au sein de la NSA.[263]

(82) *Der Spiegel* a également décrit le type d'informations qui intéressait la NSA à propos de l'Union européenne. Les informations relatives à la stabilité économique et à la politique commerciale figuraient au niveau 3 d'une échelle de priorités allant de 1 (plus haut intérêt) à 5 (plus faible intérêt). Les informations concernant la sécurité énergétique, les denrées alimentaires et l'innovation technologique arboraient une priorité 5.[264] *Der Spiegel* a publié des détails sur la manière dont la NSA espionnait l' 'ambassador's room' au 31e étage de la délégation de l'UE auprès des Nations unies à New York, également connue au sein de la

---

258 Voir entre autres COMITÉ PERMANENT R, *Rapport d'activités 2010*, Intersentia, Anvers, 2010, 6-13.

259 C. SHORT, *An honourable deception? New Labour, Iraq and the misuse of power*, Free Press, 2005, 242-243.

260 B. WHITAKER, *The Guardian*, 18 décembre 2004 ("Bugging device found at UN offices").

261 D. LINZER, *The Washington Post*, 12 décembre 2004 ("IAEA Leader's phone tapped"). El Baradei avait sérieusement mis en doute les renseignements américains relatifs à l'Irak et avait également adopté à l'époque une position très prudente à l'égard de l'Iran.

262 Voir paragraphe 19.

263 http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html

264 "*Of particular note, the data systems of the EU embassies in America are maintained by technicians in Brussels; Washington and New York are connected to the larger EU network. Whether the NSA has been able to penetrate as far as Brussels remains unclear. What is certain, though, is that they had a great deal of inside knowledge from Brussels*". http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html

NSA sous le nom de code 'Apalachee'. La NSA avait accès aux plans du bâtiment et a infiltré le réseau VPN interne entre la représentation de l'Union européenne auprès de l'ONU à New York et celle à Washington, connue sous le nom de code MAGOTHY. Les missions de l'UE à Washington et à New York ont toutes deux été mises sur écoute. Dans la représentation de l'UE à New York, des disques durs ont également été copiés, tandis qu'à Washington, le réseau informatique interne a été infiltré.[265]

(83) Aux Nations unies, la NSA s'est surtout intéressée à tout ce qui a trait au contrôle des armes à l'AIEA (priorité 1), à la politique étrangère (priorité 2) et aux droits de l'homme, aux crimes de guerre, à l'environnement et aux matières premières (tous de priorité 3). Aux Nations unies, la NSA dispose d'une équipe qui travaille sous couverture diplomatique et qui est renforcée par une équipe à Washington pour toutes les séances de l'Assemblée générale. La NSA a également écouté les vidéoconférences de diplomates de l'ONU.[266]

(84) *Der Spiegel* a également divulgué l'existence du programme RAMPART-T dans le cadre duquel la NSA intercepte, depuis 1991, les communications de chefs d'État et de leur entourage direct de plus de vingt pays, et ce dans le but de pouvoir mieux informer le Président et ses conseillers en matière de sécurité nationale. *Der Spiegel* a indiqué que ces interceptions ne visaient pas seulement des cibles en Chine et en Russie, mais aussi dans des pays de l'Europe de l'Est.[267]

(85) *The Guardian* a mentionné que les 38 ambassades et délégations étaient considérées comme des cibles dans un document de la NSA datant de septembre 2010. Aucun bâtiment d'Europe occidentale n'y figure, mais bien les représentations de l'UE susmentionnées, ainsi que les ambassades de France, d'Italie et de Grèce, et les ambassades du Japon, du Mexique, de la Corée du Sud, d'Inde[268] et de Turquie. Les missions grecque et française auprès de l'ONU ont également été espionnées. [269] Le 18 octobre, *Le Monde* a publié un document qui indiquait qu'une collecte de type 'close access' sur le territoire américain contre des cibles diplomatiques étrangères était connue sous le nom de SIGAD US-3136. Un suffixe de deux lettres désigne l'emplacement et la mission concernés. Le document du 10 septembre 2010 décrit une quinzaine de manières qui pouvaient être utilisées pour obtenir des informations.[270] La collecte de type 'close access' de sources diplomatiques en dehors des

---

265 http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html

266 http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html

267 http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html

268 Pour de plus amples informations, voir S. SAXENA, *The Hindu*, 25 septembre 2013 ("NSA planted bugs at Indian missions in D.C., U.N ").

269 *"The US intelligence service codename for the bugging operation targeting the EU mission at the United Nations is "Perdido". The operation against the French mission to the UN had the covername "Blackfoot" and the one against its embassy in Washington was "Wabash". The Italian embassy in Washington was known to the NSA as both "Bruneau" and "Hemlock". The eavesdropping of the Greek UN mission was known as "Powell" and the operation against its embassy was referred to as "Klondyke"."* http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies

270 HIGLANDS: collection from implants, VAGRANT: collection of computer Screens, MAGNETIC: sensor collection of magnetic emanations, MINERALIZE: collection from LAN implant, OCEAN: optical collection system for raster-based computer screens, LIFESAVER: imaging of the hard drive, GENIE: multi-stage

États-Unis est connue sous le nom de SIGAD US-3137 avec un suffixe de deux lettres.

(86) *Der Spiegel* a également décrit la manière dont la NSA exploite les informations émanant de la diplomatie française. Un document interne à la NSA et datant de juin 2010 décrivait comment la NSA était parvenue à accéder au réseau VPN du ministère français des Affaires étrangères (réseau qui relie toutes les ambassades et tous les consulats français avec Paris), ainsi qu'aux sous-domaines (internes) de l'URL 'diplomatie.gouv.fr'. Des agents de la NSA ont installé des *bugs* au sein de l'ambassade française à Washington et de la mission française à New York. Toujours selon *Der Spiegel*, la NSA s'intéresse surtout à la politique étrangère (plus particulièrement le commerce des armes) et économique de la France.[271]

(87) Un document datant du 17 mai 2006 et publié sur le site Internet du Globo indiquait que la mission International Security Issues (ISI) au sein de la NSA est responsable de treize États individuels sur trois continents. Ces treize pays ont un point commun : ils sont importants pour l'économie, le commerce et la politique étrangère des États-Unis. La division 'Western Europe and Strategic Partnerships' au sein de cette mission se concentre principalement « *sur la politique étrangère et les activités commerciales de la Belgique, la France, l'Allemagne, l'Italie, l'Espagne, ainsi que le Brésil, le Japon et le Mexique* ». Cette division transmet également la *key intelligence* concernant 'des activités militaires et de renseignement dans plusieurs de ces pays'. La 'Aegean and Ukraine division' s'occupe de tous les aspects liés à la Turquie ('governmental/leadership, military and intelligence'). L'ISI collabore avec F6 et des partenaires étrangers *second and third party* qui contiennent à la fois des 'données analytiques et capacités techniques précieuses'.[272] Selon *Le Monde*, les numéros qui commencent par US-98 (comme US — 985D (France), US-987 (Allemagne)) font référence à des SIGADS sur le territoire de partenaires *third party* de la NSA. Selon *Der Spiegel,* il s'agit entre autres de la France, l'Allemagne, l'Autriche, la Pologne et la Belgique.[273] Ce même document faisait référence au fait que l'ISI collabore activement avec les *« Combating Proliferation (CP, S2G) and Counterterrorism (CT, S2I) product lines to incorporate financial intelligence analysis into their mission build-out plans »*.[274]

---

operatoins; jumping the airgap...; BLACKHEART: collection from an FBI implant, PBX: Public Branch Exchange Switch, CRYPTO ENABLED: collection derived from AO's efforts to enable crypto, DROPMIRE (1) passive collection of emanations using an antenna (2) laser printer collection, purely proximal access, DEWSWEEPER: USB hardware host tap that provides covert link over USB link into a target network. Operates w/RF delay sybsytem to provide wireless bridge into target network. RADON: bi-directional host tap that can inject Ethernet packets onto the same target. Allows bi-direction exploitation of denied networks using standard on-net tools. Par exemple, les techniques HIGHLAND, VAGRANT et PBX ont été utilisées contre les missions françaises. https://www.documentcloud.org/documents/807030-ambassade.html#document/p1

271 X., *Der Spiegel*, 1er septembre 2013 (" 'Success Story': NSA targeted French Foreign Ministry").

272 http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html

273 http://www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-3.html

274 "*The idea is to integrate financial analysis with traditional target efforts as opposed to working the target from two separate perspectives, as is done in NSA Washington. ISI's long-term goal is to introduce financial analysis a part of the Intelligence Analysis curriculum so any target can be enriched with the use of financial intelligence*." http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html Dans ce sens, il est peut-être intéressant de souligner que, selon certaines sources du journal *De Standaard*, des problèmes auraient été constatés

(88) Un document datant d'août 2010 confirme que la NSA a intercepté les communications de huit membres du Conseil de sécurité de l'ONU. Seuls la France, le Japon, le Mexique et le Brésil ont été explicitement cités. L'objectif était de fournir à la mission américaine auprès de l'ONU (et à d'autres services américains) les informations les plus actuelles sur leurs intentions de vote et les positions de négociation à propos d'une résolution de l'ONU traitant de sanctions contre l'Iran.[275]

(89) Dans une de ses éditions, le *Globo* a confirmé la manière dont la NSA espionnait des pays d'Amérique du Sud tels que le Mexique, le Venezuela, l'Argentine, la Colombie, l'Équateur, le Panama, le Costa Rica, le Nicaragua, le Honduras, le Chili, le Salvador et le Pérou. La NSA s'intéressait à la politique du Venezuela en matière de pétrole, la politique du Mexique en matière d'énergie et de drogues, et la position de la Colombie à l'égard des FARC. L'utilisation de XKEYSCORE a permis de dépister un 'étranger' grâce à la langue qu'il utilisait pour communiquer.[276]

(90) Un document *top secret* datant de novembre 2010, publié par *Der Spiegel*, montre que la division TAO de la NSA était parvenue, lors de l'opération FLATLIQUID, à accéder au compte de messagerie public du Président mexicain de l'époque, Felipe Calderon, pour « *se faire une idée du système politique et de la stabilité interne du Mexique* ». Ce compte était aussi utilisé par des membres du cabinet de Calderon.[277] Durant deux semaines, au début de l'été 2012, la NSA a également lancé une campagne de 'surveillance structurelle' intensive contre l'actuel Président, Enrique Pena Nieto. Ses schémas de communication ont permis de connaître neuf de ses conseillers les plus proches. Les données de ces personnes ont été stockées dans la base de données DISHIRE, à la suite de quoi leurs communications ont également été interceptées. Par exemple, 85 489 SMS ont ainsi été interceptés. Cette opération avait pour objectif de déterminer si le Mexique adoptait une nouvelle stratégie à l'égard des cartels de la drogue.[278] La NSA s'intéresse surtout au trafic de drogue (niveau 1), aux dirigeants du Mexique, à la stabilité économique, aux capacités militaires, aux droits de l'homme et aux relations commerciales internationales du Mexique (niveau 3) ainsi qu'au contre-espionnage (niveau 4). Pour atteindre ces objectifs, la TAO a mené, en août 2009, l''Operation Whitetamale', par laquelle elle a pu accéder aux e-mails de plusieurs hauts fonctionnaires du 'Public Security Secretariat' mexicain, qui s'occupe notamment du trafic de drogue et de la traite des êtres humains. Grâce à l'opération EVENINGEASEL, la division SCS de la NSA a écouté des conversations téléphoniques depuis l'ambassade de Mexico et a lu les SMS envoyés par le biais du réseau téléphonique mobile mexicain.[279]

---

au sein du SPF Finances et que l'on a cherché à savoir s'il s'agissait du même logiciel malveillant que chez Belgacom. Hans D'Hondt, qui est à la tête du SPF Finances, a toutefois formellement démenti toute contamination ou tout piratage de ses services. N. VANHECKE, P. DE LOBEL, *De Standaard*, 4 octobre 2013 ("Vrees voor massale besmetting").

275 http://epoca.globo.com/tempo/noticia/2013/07/spies-bdigital-ageb.html

276 http://oglobo.globo.com/mundo/espionagem-dos-eua-se-espalhou-pela-america-latina-8966619

277 http://www.spiegel.de/fotostrecke/photo-gallery-nsa-hacked-into-mexican-president-s-email-account-fotostrecke-102797-2.html

278 http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html

279 http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html

(91) L'émission d'information Fantastico de la chaîne brésilienne *Globo* a montré des *slides* qui illustraient les schémas de communication entre la Présidente brésilienne Dilma Roussef, ses principaux conseillers et des tiers.[280] Selon Glenn Greenwald, le programme de la NSA en question avait obtenu l'accès à l'ensemble du réseau de communication de la Présidente brésilienne et de son équipe, y compris aux conversations téléphoniques, aux e-mails et aux échanges sur les sites de réseaux sociaux.[281]

(92) Le directeur de la DNI, James Clapper, a réagi en déclarant que « ce n'est pas un secret que l'Intelligence Community recueille des informations sur des questions économiques et financières et sur le financement du terrorisme ». D'après Clapper, les États-Unis collectent ce type d'informations notamment pour alerter (*early warnings*) les États-Unis et ses partenaires de l'imminence de crises financières internationales susceptibles d'avoir un impact négatif sur l'économie mondiale.[282]

(93) Le lendemain, Fantastico faisait savoir que la NSA considérait également le réseau informatique interne de la compagnie pétrolière brésilienne Petrobras comme une cible d'espionnage. Une présentation datant de mai 2012 qui avait pour but de former de nouveaux agents de la NSA aux méthodes employées pour obtenir l'accès à des réseaux informatiques privés mentionnait la société en tant que cible. On ne sait pas exactement quelles informations étaient recherchées ou quelles informations avaient été obtenues, mais *Globo* suggère qu'il pouvait s'agir, par exemple, de détails sur les gisements pétrolifères inexploités les plus intéressants que Petrobras proposerait à brève échéance aux enchères ou d'informations sur une technologie de pointe en matière d'exploration des fonds marins (*ocean-floor exploration*). La présentation n'a pas (encore) été mise en ligne.[283] Cette même présentation mentionnait également que Google, des diplomates français ayant accès au réseau privé du ministère français des Affaires étrangères[284] et SWIFT étaient considérés comme des cibles.

(94) Des *slides* du GCHQ montrent comment le GCHQ a recueilli des données des smartphones, y compris des Blackberries, de plusieurs délégations diplomatiques à la réunion du G20 à Londres en 2009.[285] Ces données ont pu être transmises presque en temps

---

280 http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html

281 Y.MARULL, AFP, 2 septembre 2013 ("Brazil, Mexico summon US envoys over spy claims). Un représentant du State Department a déclaré : "*while we are not going to comment publicly on every specific alleged intelligence activity, as a matter of policy we have made clear that the United States gathers foreign intelligence of the type gathered by all nations* ".

282 Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage, 8 septembre 2013. http://icontherecord.tumblr.com/post/60712026846/statement-by-director-of-national-intelligence. "*What we do not do, as we have said many times, is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of - or give intelligence we collect to - US companies to enhance their international competitiveness or increase their bottom line*".

283 http://www.reuters.com/article/2013/09/09/us-usa-security-snowden-petrobras-idUSBRE98817N20130909

284 http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies

285 "*The document refers to a tactic which was "used a lot in recent UK conference, eg G20 (…) the tactic is defined in an internal glossary as "active collection against an email account that acquires mail messages without removing them from the remote server". A PowerPoint slide explains that this means*

réel à des analystes, qui ont pu rédiger des briefings pour des ministres britanniques, dont Gordon Brown.[286] Ces informations ont permis d'identifier vingt nouveaux 'e-mail selectors'.[287] Le GCHQ est allé très loin pour obtenir ces informations diplomatiques. Par exemple, il a mis sur pied un faux cybercafé où des *key-loggers* ont pu voir ce qu'un délégué tapait à l'ordinateur. Un autre document démontrait que le GCHQ était parvenu à pirater le réseau du ministre sud-africain des Affaires étrangères et à intercepter ainsi des briefings destinés à des délégués aux réunions du G20 et du G8. Il est également fait mention de tentatives du GCHQ d'intercepter des conversations téléphoniques cryptées entre Medvedev et d'autres représentants russes lorsque ces derniers se trouvaient à Londres. Le GCHQ a aussi espionné le ministre turc des Finances à la réunion, ainsi que quinze autres membres de sa délégation. En outre, le GCHQ a testé, à la réunion, une nouvelle technique visant à inventorier le trafic téléphonique de tous les participants.[288]

(95) Le Royaume-Uni prévoyait une opération visant à espionner plusieurs délégations à la réunion des chefs de gouvernement du Commonwealth à Trinidad en 2009, et ce afin d'obtenir des informations diplomatiques supplémentaires. Par exemple, un document décrit comment des SIGINT devaient être recueillis concernant l'opinion de l'Afrique du Sud sur le Zimbabwe avant une réunion entre le Premier ministre Brown et Zuma. Il n'est pas clairement indiqué si ces SIGINT ont été effectivement recueillis.[289]

"reading people's email before/as they do". Voir http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits

286 Gordon Brown présidait le G20 et souhaitait enregistrer des progrès sur deux fronts : la coordination de la relance économique mondiale pour éviter une nouvelle récession et un accord visant à renforcer la gouvernance économique mondiale et à réformer les institutions financières internationales.

287 http://www.theguardian.com/uk/interactive/2013/jun/16/gchq-surveillance-the-documents

288 http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits

289 http://www.theguardian.com/world/2013/jun/16/uk-intelligence-agencies-spy-commonwealth-delegates

ANNEXE : ABRÉVIATIONS ET CONCEPTS

1 EF solution	One-End Foreign solution
AG	Attorney General
BICS	Belgacom International Carrier Services
BND	Bundesnachrichtendienst (DE)
CERT-EU	Computer Emergency Response Team
CLANSIG	clandestine signals collection
CIA	Central Intelligence Agency
CNE	Computer Network Exploitation
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DITU	Data Intercept Technology Unit du FBI
DNI	(1) Director of National Intelligence aux États-Unis (James Clapper), (2) Digital Network Intelligence
DNR	Dialed Number Recognition
ECI	Exceptionally Controlled Information
EO 12333	Executive Order 12333
EXIF	EXchangeable Image File format
FAA	FISA Amendments Act
FBI	Federal Bureau of Investigation
FCCU	Federal Computer Crime Unit
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
Five eyes	Les agences SIGINT des États-Unis, du Royaume-Uni, de l'Australie, du Canada et de la Nouvelle-Zélande
Fornsat	Informations provenant de satellites
FTC	Federal Trade Commission
FRA	Försvarets radioanstalt (agence SIGINT suédoise)
GAO	Division Global Access Operations (NSA)
GCHQ	Government Communications Headquarters (UK)
HOT	Humint Operations Team
IBPT	Institut belge des services postaux et des télécommunications
IM	Instant Messaging
ISA	Intelligence Services Act (UK)
ISC	Intelligence Security Committee
Métadonnées	Les métadonnées – ou 'metadata', parfois également appelées 'communications data' ou 'traffic data' – désignent les informations créées lors de l'envoi des données. Le contenu exact dépend du type de données envoyé et parfois de la législation locale.

- Pour les lignes téléphoniques fixes : les numéros qui ont été appelés via cet appareil, ainsi que la date et l'heure de l'appel. Parfois aussi le nom et l'adresse de la personne qui a conclu le contrat de la ligne fixe.
- Téléphones portables : (1) les numéros qui ont été appelés ou auxquels on a envoyé un SMS via cet appareil, (2) la date et l'heure de l'appel ou de l'envoi ou la réception du SMS, (3) l'endroit d'où l'appel a été passé ou le SMS envoyé et où cette communication a été reçue. (4) Parfois aussi le nom et l'adresse de la personne qui a conclu le contrat de la ligne fixe. (5) Parfois aussi le numéro d'abonné IMSI (International Mobile Subscriber Identity) et (6) le numéro d'équipement IIEM (identité internationale d'équipement mobile). (6) Parfois aussi le numéro de la carte téléphonique utilisée.

- Protocole VoIP (Voice over Internet), e-mail, messagerie instantanée, messages Facebook : (1) le nom d'utilisateur en ligne, le nom de connexion (*login*) ou le nom du compte utilisé pour passer ou recevoir un appel, envoyer des e-mails, des messages instantanés, (2) l'adresse IP des ordinateurs utilisés, (3) l'heure et la date de la communication. Certains pays semblent également considérer la ligne d'objet des e-mails comme une métadonnée.
- Comportement sur Internet : (1) l'adresse IP de l'appareil utilisé pour surfer, (2) l'heure et la date de la connexion et de la déconnexion, ainsi qu'une liste des domaines consultés sur Internet.

NCtC	National Counterterorrism Center
MTI	Mastering the Internet
NSA	National Security Agency
OSN	Online Social Networking
PNR	Passenger Name Records
PSTN	Public switched telephone network
RIPA	Regulation of Investigatory Powers Act (UK)
SCIF	Secure Compartmented Intelligence Facility
SCS	Special Collection Service
SGRS	Service général du renseignement et de la sécurité
SHAPE	Supreme Headquarters Allied Powers Europe
SIGAD	« Signals activity/address designators » – peuvent faire référence à une plateforme de collecte physique spécifique (comme une base de l'armée américaine à l'étranger, une ambassade, un navire...), une plateforme virtuelle de traitement de données (par exemple, PRISM est connu sous le SIGAD US-984XN) ou un satellite spatial.
SIGINT	Signals Intelligence
Sites F6	Missions diplomatiques et consulaires des États-Unis
SRP	Specialized Reconnaissance Program
SSL	Secure Sockets Layer
SSO	Special Source Operations
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAO	Tailored Access Operations
TBB	Tor Browser Bundle
TFTP	Terrorist Finance Tracking Program
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTC	Video Teleconferencing Systeem
XKS	Xkeyscore