# DE SNOWDEN-REVELATIES, MASSALE DATA-CAPTATIE EN POLITIEKE SPIONAGE

**Open bronnenonderzoek**[1]

## INLEIDING

(1) Dit verslag biedt een overzicht – aan de hand van open bronnen – van de soorten gegevens die mogelijks betrekking hebben op (of afkomstig zijn van) in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België) en die door het Amerikaanse National Security Agency (NSA) het Britse Government Communications Headquarters (GCHQ), of private firma's in opdracht van deze diensten, op grote schaal worden gecapteerd en opgeslagen en dit met het oog op een (eventuele latere) exploitatie door hun inlichtingendiensten. Tevens werd een overzicht geboden van gevallen waaruit blijkt dat onder meer deze diensten de afgelopen decennia operaties hebben opgezet die gericht waren op politiek spionage ten aanzien van zogenaamde 'bevriende landen'. De open bronnen die voor dit verslag geconsulteerd werden zijn van wisselende kwaliteit. Waar mogelijk werd zoveel mogelijk gebruikt gemaakt van primaire bronnen (*slideshows*, officiële documenten) die in de laatste maanden gepubliceerd werden door onderzoeksjournalisten. De kritische interpretatie van deze (onvolledige) stukken informatie werd geholpen door de consultatie van andere experten. Te speculatieve persanalyses waarbij geen extra informatie gevonden werd ter ondersteuning van een denkpiste werden niet weerhouden. Als bijlage bij dit verslag werd een verklarende afkortingenlijst opgenomen.

(2) Om de specifieke collectiemechanismen die onthuld werden sinds juni 2013 beter te begrijpen, is het vooreerst evenwel nodig om summier de wettelijke context te beschrijven waarin respectievelijk de NSA en GCHQ actief zijn, om vervolgens inzicht te krijgen in het mandaat en de voorzorgsmaatregelen die al dan niet van toepassing zijn in de uitvoering van dat mandaat. Ook werd getracht om telkens een inzicht te krijgen in de grootteorde van de gegevensverzameling en de tijdsspanne waarin deze collectiemechanismen actief zijn.

(3) De ervaring met de Snowden-documenten tot nu toe leert dat vooralsnog ongepubliceerde, vertrouwelijke documenten die mogelijks in de toekomst gepubliceerd zullen worden, een impact zullen hebben op de interpretatie van eerdere gepubliceerde documenten en berichtgeving over de revelaties. Deze nota is dus onvermijdelijk een tijdsopname, die een stand van zaken weergeeft tot en met 23 oktober 2013.

---

[1] Dit open bronnenonderzoek werd in opdracht van het Vast Comité I uitgevoerd door drs. Mathias Vermeulen, Research Fellow aan het European University Institute in Firenze en het Centre for Law, Science and Technology Studies aan de VU Brussel. Werkte van 2008 tot 2011 als onderzoeker voor de toenmalige United Nations Special Rapporteur on the promotion and protection of human rights while countering terrorism, en deed onderzoek voor het Europese Parlement over 'Parliamentary oversight of security and intelligence agencies in the European Union'.
Zie:http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf).

# I. HET AMERIKAANSE NATIONAL SECURITY AGENCY (NSA)

(4) De NSA is een militaire inlichtingendienst die geleid wordt door Generaal Keith B. Alexander. Alexander rapporteert aan de Under Secretary of Defense for Intelligence, Michael G. Vickers, de voornaamste intelligence-adviseur van de Amerikaanse Minister van Defensie, Chuck Hagel. De NSA is ook een onderdeel van de US 'Intelligence Community', die geleid wordt door James Clapper. Volgens EO 12333 heeft de directeur van de NSA (DIRNSA) onder meer de taak om *signals intelligence* (SIGINT[2]) te verzamelen (inclusief via clandestiene middelen), verwerken, analyseren, produceren en te verspreiden voor *foreign intelligence* en *counterintelligence* doelen[3] en om militaire operaties te ondersteunen.[4] De NSA's SIGINT-verzameling is geregeld door twee belangrijke documenten: Executive Order 12333 (EO 12333)[5] en de Foreign Intelligence Surveillance Act (FISA).

## I.1. Het wettelijke kader voor het inzamelen van informatie over buitenlandse doelwitten

### *I.1.1. Executive Order 12333*

(5) *Foreign intelligence*' wordt in EO 12333 gedefinieerd als alle informatie die gerelateerd is aan de capaciteiten, intenties of activiteiten van buitenlandse machten, organisaties of personen.[6] Het verzamelen van SIGINT kan gebaseerd worden louter en alleen op basis van deze *executive order*, zonder dat daarbij de uitgebreidere FISA-procedures moeten gevolgd worden.[7] EO 12333 vormt bijvoorbeeld de wettelijke basis voor het verwerven van enorme hoeveelheden metadata buiten Amerikaans grondgebied[8], alsook voor het verzamelen van contactlijsten of adresboeken van e-mail- en chatprogramma's.[9] Dat soort informatie valt

---

2 SIGINT is *intelligence* die gecreëerd wordt door elektronische signalen en systemen, zoals communicatiesystemen, radars, satellieten of wapensystemen. Zie hierover bijvoorbeeld http://www.nsa.gov/sigint/

3 Executive Order 12333 – United States intelligence activities, 4 December 1981, sectie 1.7(c)(1). EO 12333 werd geamendeerd door de Executive Orders 13284 (2003), 13355 (2004) en 13470 (2008). De geconsolideerde versie van EO 12333 is consulteerbaar op https://www.fas.org/irp/offdocs/eo/eo-12333-2008.pdf. Er moet opgemerkt worden dat EO 12333 de activiteiten van alle leden van de US Intelligence Community regelt, en dus niet alleen van de NSA.

4 *Idem*, sectie 1.7(c)(3) en (5).

5 Voor EO 12333 was er al EO 12139 (Exercise of Certain Authority Respecting Electronic Surveillance), die werd geamendeerd door EO 12333, EO 13383 en EO 13475.

6 *Idem*, sectie 3.5(e). EO 12333 maakt ook duidelijk dat *foreign intelligence* niet alleen via SIGINT kan verzameld worden, maar ook door andere elementen van de *intelligence community* kan gebeuren via fysieke surveillance (zie bijv. sectie 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 Augustus 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 August 2013 op pag. 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*".) Zie ook paragraaf 15.

9 Zie paragrafen 25-27.

immers niet onder de definitie van *electronic surveillance* zoals FISA die gebruikt.[10] EO 12333 lijkt ook de wettelijke basis te vormen voor de meest controversiële activiteiten van de NSA, en dan vooral van subdivisies zoals het Office of Tailored Access Operations (TAO) en de Special Collection Service (SCS), zoals het omzeilen van commerciële encryptiebeveiligingen[11], het hacken van buitenlandse computers[12] of het bespioneren van buitenlandse leiders vanuit Amerikaanse ambassades.[13] Er is weinig tot geen toezicht over deze activiteiten door het US Senate Intelligence Committee.[14]

### *I.1.2. Foreign Intelligence Surveillance Act*

(6) Een groot deel van de 'elektronische surveillance' wordt geregeld door de Foreign Intelligence Surveillance Act (FISA) uit 1978. FISA werd gecodificeerd in 50 U.S.C. § 1801 *et seq.*, en werd daarna onder meer significant aangevuld met nieuwe provisies uit de Patriot Act[15], die onder meer de installatie en het gebruik van 'pen registers'[16] en '*trap and trace devices*'[17] en het produceren van 'tastbare dingen' regelen[18]. FISA werd het meest recent geamendeerd in 2008 door de FISA Amendments Act (FAA).[19] In december 2012 verlengde de Amerikaanse Senaat de werking van de FISA Amendments Act tot en met 31 december 2017. Volgens de NSA is de belangrijkste toepassing van FAA het verzamelen van de communicaties van buitenlandse personen die Amerikaanse aanbieders van communicatiediensten gebruiken. [20] Momenteel liggen er verschillende wetgevende

---

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

11 Zie paragrafen 45-48.

12 Zie bijvoorbeeld paragrafen 29, 47 en 48.

13 Zie bijvoorbeeld paragraaf 19.

14 Een staflid van het Committee hierover: "*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 Zie 50 U.S.C. §1841 *et seq*.

16 Een '*pen register*' wordt gedefinieerd in 18 U.S.C. § 3127(3) als "*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 Een '*trap and trace device*' wordt gedefinieerd in 18 U.S.C. § 3127(4) als "*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 Zie 50 U.S.C. § 1861. Dit is bijvoorbeeld de wettelijke basis voor de MAINWAY database, zie para. 37.

19 Zie H.R. 6404, FISA Amendments Act of 2008' (zie http://www.gpo.gov/fdsys/pkg/BILLS-110hr6304enr/pdf/BILLS-110hr6304enr.pdf. De vaak aangehaalde 'Section 702. Procedures for targeting certain persons outside the United States other than United States persons' werd geconsolideerd in de U.S Code als 50 USC §1881a, (http://www.law.cornell.edu/uscode/text/50/chapter-36). Eerder werd FISA ingrijpend geamendeerd door de Patriot Act in 2001.

20 N.S.A., "The National Security Agency: Missions, Authorities, Oversight and partnerships", 9 Augustus 2013.

voorstellen op tafel die de binnenlandse collectie van informatie door de VS zou moeten beperken[21], maar tot nu toe zijn er geen gelijkaardige initiatieven om de collectie van informatie van 'buitenlanders' in te perken.[22] In dit verslag zal alleen verder ingegaan worden op de recentste FISA-Amendments Act, die op zich een aanvulling vormen op 50 USC § 1802. Onder 50 U.S.C. § 1802 kan de Amerikaanse Procureur-Generaal (*Attorney-General*) elektronische surveillance machtigen voor een periode van één jaar als die surveillance exclusief gericht is op (1) het verwerven van de inhoud van de communicaties die uitgezonden worden communicatiemiddelen die alleen door of tussen 'buitenlandse machten'[23] gebruikt worden of (2) het verwerven van *technical intelligence* van plaatsen die onder de openlijke en exclusieve controle van een 'buitenlandse macht' staan.

(7) De FISA Amendments Act geeft de AG en de DNI de bevoegdheid om voor een periode van één jaar elektronische surveillance te machtigen van personen waarvan redelijkerwijs kan aangenomen kan worden dat die zich buiten de Verenigde Staten bevinden, met als specifiek doel om 'buitenlandse inlichtingen' te verzamelen.[24] 'Buitenlandse inlichtingen' worden zeer breed gedefinieerd als:

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

---

21 zie http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf, 4. Voor een overzicht van de twee belangrijkste initiatieven, zie J. GRANICK, "A tale of two surveillance reform bills. Centre for Internet and Society", 29 October 2013, zie https://cyberlaw.stanford.edu/blog/2013/10/tale-two-surveillance-reform-bills

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

23 Zie definitie in para. 8.

24 Het moet opgemerkt worden dat *acquire* niet hetzelfde betekent als *collect*. Zie bijvoorbeeld 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"*. De titel van sectie 1881a heet voluit: *"Procedures for targeting certain persons outside the United States other than United States persons.*" De betekenis van *targeting* wordt echter niet gedefinieerd in 50 USC § 1881. 50 USC § 1801 definieert *electronic surveillance* als *"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*". Een interpretatie zou dus kunnen zijn de gegevens van informatie pas gezien wordt als *targeting*, als het de *bedoeling* was om bepaalde informatie te verzamelen. Incidenteel verzamelde informatie wordt dan niet gezien als *targeting*.

*(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) Vooral die laatste categorie staat een in principe ongelimiteerde inzameling van informatie toe. Dat is nog meer het geval aangezien de definitie van een 'buitenlandse macht' ook uitgebreid gedefinieerd wordt. De term houdt niet alleen buitenlandse regeringen, parlementsleden of internationale organisaties in, maar ook bijvoorbeeld "*een politieke organisatie in het buitenland, die niet substantieel bestaat uit Amerikaanse burgers*" [26] en "*een entiteit die gestuurd en gecontroleerd wordt door een buitenlandse overheid*".[27] Beide categorieën zouden in theorie bijvoorbeeld respectievelijk NGO's die anti-Amerikaanse betogingen organiseren of staatsbedrijven kunnen inhouden.

(9) De Foreign Intelligence Surveillance Court (FISC) gaat na of de machtiging van de AG en DNI (zie para. 7) aan een aantal procedurele voorwaarden voldoet. De AG en DNI voegen een geschreven certificaat toe aan de machtiging die aantoont hoe men aan die procedurele voorwaarden voldoet. Die voorwaarden hebben voornamelijk als doel dat zo weinig mogelijk gegevens van Amerikaanse burgers intentioneel wordt verzameld.[28] Er zijn nergens in de Amerikaanse wetgeving gelijkaardige 'minimizatie procedures' voorzien die moeten voorkomen dat 'onschuldige' buitenlandse gegevens verzameld en bewaard kunnen worden. Het certificaat moet ook nergens vermelden welke specifieke faciliteiten, plaatsen of eigendommen precies het doelwit zijn van de SIGINT-verzameling.[29] De Amerikaanse overheid declassificeerde een document van 31 oktober 2011 dat de 'minimizatie procedures' beschreef die de NSA hanteerde om '*foreign intelligence* informatie' te verzamelen. Daaruit bleek dat communicaties van of over Amerikaanse burgers die niet met opzet werden verzameld tot vijf jaar bewaard mochten worden[30] en gedeeld mochten worden met buitenlandse overheden.[31]

(10) Als de FISC zijn goedkeuring geeft, dan kunnen de AG en DNI op basis van een dergelijk breed certificaat, '*identifiers*' (bijvoorbeeld e-mailadressen of telefoonnummers) [32] doorgeven aan een Amerikaans bedrijf dat dan verplicht is om onmiddellijk alle "*informatie, faciliteiten of andere assistentie*" te geven om die SIGINT-verzameling te doen slagen.[33] Die bedrijven worden daarvoor financieel gecompenseerd, en kunnen in "*geen enkele*

---

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 Augustus 2013, 4.

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

*rechtbank*" aansprakelijk worden gesteld voor het leveren van dergelijke informatie.[34] Een bedrijf kan in beroep gaan tegen een dergelijke vraag (bijvoorbeeld omdat de vraag te breed is)[35], waarna de FISC de vraag kan verwerpen of een finaal bevel tot medewerking kan uitspreken.[36]

### *I.1.3. Safe Harbour*

(11) Amerikaanse bedrijven kunnen dus verplicht worden om gegevens over te dragen aan de NSA, inclusief gegevens van en over Belgische klanten. Die eis naar Amerikaans recht kan botsen met de principes van het EU-US Safe Harbour akkoord uit 2000, waarbij Amerikaanse bedrijven vrijwillig de principes in dat akkoord kunnen onderschrijven. Bedrijven worden daar bijvoorbeeld geacht om aan hun klanten te kennen geven dat hun persoonlijke data aan een derde partij werd doorgegeven.[37] De Federal Trade Commission (FTC) ziet toe op de handhaving van het akkoord. Van deze principes mag afgeweken worden in naam van nationale veiligheid of omdat rechtshandhaving het vereist. De grote schaal waarop persoonlijke gegevens van Europese gebruikers van Amerikaanse bedrijven naar de NSA werden verstuurd binnen het PRISM-programma (zie para's 32-38), leidde er echter toe dat de Europese Commissie momenteel onderzoekt of het Safe Harbour akkoord niet herzien moet worden.[38]

(12) Op 22 oktober 2013 stemde het Europese Parlement voor het toevoegen van een zogenaamde 'anti-FISA clausule', die bedrijven niet zou toestaan om zonder toelating van een *supervisory authority* persoonlijke data van Europese inwoners door te sturen naar een derde land op vraag van een rechtbank of een andere autoriteit in dat land. Die *supervisory authority* moet eerst nagaan of de transfer noodzakelijk is en in conformiteit met de nieuwe Europese databeschermingswetgeving. Het valt af te wachten of dit artikel de onderhandelingen met de Raad zal overleven.[39]

---

34 50 USC § 1881a (h)(3).

35 In 2007 kreeg Yahoo een dergelijke *order* om data te geven. Yahoo vocht deze aan bij het Foreign Intelligence Surveillance Court of Review. De rechtbank verwierp echter Yahoo's tegenwerpingen. Die beslissing werd recent pas vrijgegeven. Zie https://www.fas.org/irp/agency/doj/fisa/fiscr082208.pdf

36 50 USC § 1881a (h)(4).

37 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.)
Zie ook http://export.gov/safeharbor/eu/eg_main_018493.asp.

38 Commisaris 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 Zie artikel 43a van de "Unofficial consolidated version of the European Data Protection Regulation after the LIBE Committee vote provided by the rapporteur", 22 October 2013, beschikbaar op http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf Zie ook C., "The US surveillance programmes and their impact on EU citizens' fundamental rights", European Parliament, Directorate General for Internal Policies, 2013, 28.

## I.2. Aard en schaal van SIGINT-verzameling door de NSA

(13) Het is moeilijk om de totaliteit van de SIGINT-verzameling van de NSA in kaart te brengen. Enkele cijfers geven alvast een idee over de grootteorde. *The Guardian* citeert een NSA-rapport uit 2007 dat schat dat er op dat moment ongeveer 850 miljard ongedefinieerde *call events* in verschillende NSA-databases te vinden zijn, en ongeveer 150 miljard ongedefinieerde *internet records*. Volgens het document worden er elke dag één tot twee miljard *records* toegevoegd. [40] Een artikel uit *The Washington Post* stelde in 2010 dat de NSA per dag de inhoud en metadata van 1,7 miljard e-mails, telefoongesprekken en andere vormen van communicatie bewaarde, en dat een fractie daarvan in ongeveer 70 aparte databases werd bewaard.[41]

(14) Die capaciteit is sindsdien exponentieel toegenomen. Slides van de NSA's interne Boundless Informant programma[42] die gepubliceerd werden door *The Guardian* tonen dat in de periode van een maand (maart 2013) de NSA's Global Access Operations divisie (GAO)[43] 97 miljard metadata van internet communicaties (e-mails, chats...) verzamelde en bijna 125 miljard metadata van telefoongesprekken die afkomstig waren uit meer dan 504 SIGINT Activity Designator (SIGADS).[44] Uit de slide blijkt dat België één van de landen was van waaruit in absolute getallen het minst metadata werden verzameld.[45] De slide verraadt niet over hoeveel metadata het gaat, maar aan de hand van de kleurcode die België daar heeft, lijkt het dat er alvast op dat er minder metadata vanuit België wordt verzameld in vergelijking met bijvoorbeeld Nederland.

*(15) Der Spiegel* publiceerde extra slides uit het programma in augustus 2013 die duidelijk maakten dat in december 2012 vanuit Nederland er ongeveer 1,8 miljoen metadata van telefoongesprekken verzameld werden.[46] In diezelfde periode werd er vanuit Frankrijk 70 miljoen metadata van telefoongesprekken verzameld[47], uit Spanje 60 miljoen en uit Italië 47 miljoen.[48]

---

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 Meer informatie zie: NSA, Boundless Informant – Frequently Asked Questions (09-06-2012), zie http://www.theguardian.com/world/interactive/2013/jun/08/boundless-informant-nsa-full-text

43 Dit houdt dus niet de metadata collectie in van andere NSA-divisies zoals TAO of SSO.

44 *Signals activity/address designators* – kunnen verwijzen naar een specifiek fysiek collectieplatform (zoals bijvoorbeeld een Amerikaanse legerbasis in het buitenland, een ambassade, een schip…), een virtueel dataverwerkingsplatform (PRISM staat bijvoorbeeld bekend als SIGAD US-984XN) of een ruimtesatelliet.

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 *Le Monde* publiceerde in oktober 2013 meer details waaruit het lijkt dat onder de codenaam DRTBOX 62,5 miljoen metadata werd verzameld van mobiele telefoongespreken en onder de codenaam WHITEBOX de metadata van 7,8 miljoen gesprekken van het openbare telefoonnet (*Public switched telephone network (PSTN)*). Doelwitten waren zowel mensen die geassocieerd werden met terroristische activiteiten alsook mensen uit de zakenwereld, de Franse politiek of de Franse zakenwereld. http://www.lemonde.fr/technologies/article/2013/10/21/france-in-the-nsa-s-crosshair-phone-networks-under-surveillance_3499741_651865.html Verschillende media berichtten dat er 70

(16) Vanuit Duitsland werd er in dezelfde periode meer dan 500 miljoen metadata verzameld. Dat aantal is veel groter omdat het ook over internet-metadata gaat. Uit een document blijkt dat meer dan 471 miljoen metadata uit SIGAD US-987LA komen.[49] Volgens *Der Spiegel* gelooft de Bundesnachrichtendienst (BND) dat hiermee verwezen wordt naar de Bad Aibling site, een site die tot 2004 gerund werd door de NSA, maar daarna werd overgenomen door de BND. Vanuit die site verzamelt de BND buitenlandse SIGINT, vooral uit Afghanistan en het Midden Oosten. Die data wordt dan doorgespeeld naar de NSA.[50]

(17) Volgens de NSA vervoert het internet iedere dag 1,826 petabytes aan informatie. Daarvan 'raakt' de NSA 1,6% 'aan', ongeveer 29 miljoen gigabyte per dag.[51] Van die 1,6% wordt 0,025% geselecteerd om geëvalueerd te worden. Volgens de NSA "bekijkt het dus amper 0,00004% van alle internetverkeer per dag".[52] Een gewone berekening zou suggereren dat dat aantal 10 keer zo hoog ligt, waardoor de NSA dus 0,0004% van alle internetverkeer berekent, maar volgens de NSA is het originele cijfer correct.[53]Dat lijkt weinig, maar dat is nog een enorme hoeveelheid wetende dat bijvoorbeeld slechts 2,9% van alle webtraffiek in de VS bestaat uit communicaties.[54]

*(18) The Guardian* beschreef een document van 26 december 2012 waarin de 'Special Source Operations' (SSO) divisie aankondigde dat het een nieuwe capaciteit (codenaam EVILOLIVE) zou verwerven om nog meer metadata te verzamelen van communicaties waarvan een partij niet-Amerikaans is (One-End Foreign (1EF) solution). De NSA zou nu meer dan de helft van

---

miljoen Franse telefoongesprekken afgeluisterd werden. Dat is zeker een foute interpretatie van de Snowden-documenten. Zie hierover ook "DNI Statement on Inaccurate and Misleading Information in Recent Le Monde Article", 22 oktober 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 Volgens *Der Spiegel* worden er vanuit Bad Aibling alleen al 62.000 e-mails per dag onderschept. http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html

51 '*Touch*' is geen term die wettelijk gedefinieerd is, maar impliceert informatie waar de NSA effectief naar kijkt (in tegenstelling tot de loutere verzameling van informatie). *The Wall Street Journal* hierover: "*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 Augustus 2013, 6.

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

54 In de VS bijvoorbeeld is '*real time entertainment*' (*streaming* sites zoals Netflix bijvoorbeeld) verantwoordelijk voor 62% van alle webtraffiek en *peer-to-peer file-sharing* (via sites zoals Bittorrent bijvoorbeeld) voor 10,5%. Zie J. JARVIS, *Buzzmachine*, 10 Augustus 2013 ("NSA by the numbers"), http://buzzmachine.com/2013/08/10/nsa-by-the-numbers/.

alle metadata informatie die het verzamelt via haar SIGADS in haar eigen databases kunnen opslaan.[55] Een ander, niet vrijgegeven document spreekt over een ander metadata-verwervings-capaciteit genaamd SHELLTRUMPET, waarvan op 31 december 2012 een SSO-official zei dat dit programma net haar triljoenste metadata-record had verwerkt. De helft van die verwerkingen vond in 2012 plaats. Nog twee andere metadata-programma's (MOONLIGHTPAD en SPINNERET) werden verwacht operationeel te worden tegen september 2013.[56]

(19) Een recent vrijgegeven uitspraak van de FISC uit 2011 suggereert dat 91% van de internetdata die de NSA verzamelt uit het PRISM programma komt.[57] De rest komt van zogenaamde '*upstream*' dataverwerking, en clandestiene missies uit het zogenaamde 'Specialized Reconnaissance Program' (SRP) die uitgevoerd kunnen worden samen met de CIA. *The Washington Post* gaf het budget van de 'US intelligence community' in 2013 vrij, en daaruit blijkt dat 2% van het totale budget gereserveerd werd voor twee gezamenlijke CIA-NSA programma's. Het eerste programma heet CLANSIG ('*clandestine signals collection*'), dat een variëteit aan *black bag jobs* of *off-net* operaties dekt. Dat zijn zeer risicovolle clandestiene operaties waarbij toegang gezocht wordt tot bijvoorbeeld radiofrequenties en cruciale telecominfrastructuur van een land, maar ook de specifieke toegang tot de e-mails en computers van *high interest* doelwitten zoals buitenlandse overheden, militaire communicatiesystemen en grote multinationals. Het laatste decennium zijn er meer dan honderd van dergelijke *black bag jobs* uitgevoerd. In deze operaties wordt bijvoorbeeld *spyware* geïnstalleerd op computers of worden beveiligde telefoonlijnen, routers, glasvezelkabels, data switch centra en andere systemen 'afluisterbaar' gemaakt de CIA, waardoor de NSA toegang krijgt tot die gegevens. Dergelijke operaties hebben vooral plaatsgevonden in het Midden Oosten en Azië, vooral in China.[58] Het tweede gezamenlijke initiatief van de NSA en de CIA is de Special Collection Service (SCS), die officiële VS-gebouwen zoals ambassades en consulaten als uitvalsbasis gebruikt om in het geheim communicaties te onderscheppen, onder meer van (geëncrypteerd) diplomatiek verkeer in het land waar de ambassade of het consulaat gevestigd is.[59] SCS-personeel bezit

---

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 October 2011, 71. Zie 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 - deel 8.

58 Bijvoorbeeld: "*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

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.*

diplomatieke status.[60] Hun operaties verlopen vaak vanuit een Secure Compartmented Intelligence Facility (SCIF) op de bovenste verdieping van een ambassade. De meeste diplomaten van een ambassade lijken niet te weten wat er in deze *staterooms* gebeurt.[61] Volgens *Der Spiegel* is de SCS actief in 80 landen, waaronder 19 Europese.[62] Tot nu toe vrijgegeven documenten en slides lijken te suggereren dat de SCS niet actief lijkt te zijn in België.[63] Het is de SCS die verdacht wordt van het afluisteren van de mobiele telefoon van Angela Merkel.[64]

### I.3. 'Upstream'-verzameling in de VS

(20) Via glasvezelkabels passeert meer dan 80% van het wereldwijde telefoon- en internetverkeer cruciale punten in de VS die uitgebaat worden door de drie grootste Amerikaanse telecom-operatoren (AT&T, Verizon en Sprint). Daar zit per definitie communicatieverkeer bij met een Belgische oorsprong of bestemming. De NSA's 'Special Source Operations' divisie controleert apparatuur die op deze punten wordt geplaatst, waardoor alle data die langs deze punten passeren, gekopieerd en gefilterd kunnen worden op basis van door de NSA ingestelde parameters .[65] De belangrijkste daarvan is een 'wettelijke' filter: alleen communicaties waarvan op zijn minst een deelnemer geen Amerikaan is, of zich niet in de VS bevindt, mogen in theorie doorgestuurd worden naar de NSA. Andere filters moeten ervoor zorgen dat alleen data met een *foreign intelligence*-waarde worden doorgestuurd naar de NSA. Programma's zoals XKEYSCORE stellen NSA-analisten in staat om deze *upstream data* te doorzoeken op basis van *strong selectors* (bijvoorbeeld een telefoonnummer, of een e-mailadres of een groep IP-adressen die

---

http://www.foreignpolicy.com/articles/2013/07/16/the_cias_new_black_bag_is_digital_nsa_cooperation?page=0,1)

60 Zie noot 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 Oorsprong van de slide is geverifieerd door de auteur.

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

65 *The Wall Street Journal*: "*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 verder: "*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",* in S. GORMAN en J. VALENTINO-DEVRIES, *The Wall Street Journal*, 20 Augustus 2013 ("New Details Show Broader NSA Surveillance Reach"). Een deel van het bestaan van dit soort activiteiten werd al bekend in 2006 door AT&T klokkenluider Mark Klein (Declaration of Mark Klein in support of plaintiffs' motion for preliminary injunction. United States District Court, Northern District of California. 8 June 2006).

toehoren aan een organisatie waarin de NSA geïnteresseerd is), *soft selectors* (zoals trefwoorden), of selectors die een bepaald type van geëncrypteerd trafiek detecteren (zoals Tor[66] of Virtual Private Network (VPN)-gebruik[67]).[68] Om deze beslissing te maken kan de NSA dus zowel naar de inhoud als naar de metadata van een communicatie kijken.[69] Informatie uit XKEYSCORE wordt dan naar tal van andere databases gestuurd. XKEYSCORE wordt in detail in paragrafen 28-31 behandeld.

(21) Een gelekt document gepubliceerd door *The Washington Post* meldt dat FAIRVIEW (US-990), STORMBREW (US-983), ORANGEBLOSSOM (US-3251), en SILVERZEPHYR (US-3273) allemaal *special source operations* zijn die data verwerven van dataverkeer dat passeert door de VS, maar waarvan beide kanten niet-Amerikaans zijn.[70] Een andere gelekte slide spreekt over FAIRVIEW, STORMBREW, BLARNEY en OAKSTAR als *upstream* SIGADS.[71] Volgens *The Wall Street Journal* valt ook LITHIUM onder deze cluster.[72]

(22) BLARNEY (US-984) is de SIGAD die initieel verwees naar *upstream data* die de NSA verkreeg via AT&T[73] maar lijkt later uitgebreid te zijn naar meerdere bedrijven.[74] Volgens *The Washington Post* wordt er nog altijd data uit BLARNEY verwerkt.[75] Een slide van een NSA-presentatie die te zien was in het Braziliaanse TV-programma Fantastico suggereerde dat BLARNEY zorgt voor "*collection against DNR and DNI FISA Court Order authorized communications*". DNR staat voor Dial Number Recognition, terwijl DNI staat voor Digital Network Intelligence. De slide vermeldt verder dat de hoofddoelen van BLARNEY "*diplomatic establishment, counterterrorism, counter proliferation, foreign government, economic, military en political/intention of nations"* zijn.[76] Volgens een andere slide startte BLARNEY al in 1978 om toegang te krijgen tot de communicaties van *"foreign establishments, agents of*

---

66 Tor is een netwerk van servers die gebruikers toelaten om anoniem te surfen. Zie hierover https://www.torproject.org/

67 Vaak gebruikt door bedrijven om werknemers van thuis uit toegang te verschaffen – via een geëncrypteerde 'tunnel' tot het bedrijfsnetwerk.

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

69 Voor een technische analyse van XKeyscore zie 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* had eerder de namen 'STORMBREW' en 'OAKSTAR' gecensureerd.

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

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

74 Zie *The Washington Post*: "*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*.

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

*foreign powers and terrorists*".[77] *Der Spiegel* meldde eerder dat NSA-technici die voor het BLARNEY-programma werkten erin geslaagd waren om de VN's interne video teleconferentie systeem (VTC) te exploiteren.[78] Informatie uit BLARNEY werd volgens dezelfde slide verstuurd naar 'externe klanten' zoals het US Department of State, de CIA, de US UN Mission, the 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 en military commands (Army, EUCOM).[79] Het programma heeft veel weg van het NSA-programma dat beschreven wordt in de rechtszaak Jewel v. NSA.[80]

### I.4. 'Upstream'-verzameling buiten de VS

(23) Informatie uit glasvezelkabels die het grondgebied van een van de secundaire partners van de VS passeren (UK, Canada, Australië en Nieuw-Zeeland) worden ook met de VS gedeeld.[81] Volgens Duncan Campbell, deelt ook het Zweedse SIGINT-agentschap 'Försvarets radioanstalt' *(*FRA) upstream data die het verwerft via glasvezelkabels met Five Eyes. De data die zo verkregen zou worden zou bekend staan onder de codenaam SARDINE.[82] Campbell claimt dat ook de Deense *Forsvarets Efterretningstjeneste* (Danish Defence Intelligence Service) op deze manier informatie deelt met de NSA. De data die zo verkregen zou worden, zou bekend staan onder de codenaam DYNAMO.[83] De NSA heeft ook gelijkaardige samenwerkingsverbanden met buitenlandse telecombedrijven *"vooral in Europa en het Midden Oosten"* volgens een anonieme bron in *The Wall Street Journal*.[84] Volgens Glenn Greenwald sluit de NSA geen rechtstreekse samenwerkingsverbanden af met buitenlandse bedrijven, maar gebruikt het de toegang van een groot – tot nu toe onbekend – Amerikaans telecombedrijf dat samenwerkt met dergelijke buitenlandse bedrijven. Het Amerikaanse bedrijf in kwestie heeft direct toegang tot de telecominfrastructuur van haar partner, dat daarmee – onbewust – ook toegang geeft tot de NSA. Deze info komt dan in het FAIRVIEW

---

77 *Screengrab* van een segment dat werd getoond op 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 *Screengrab* van segment getoond op 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 Zie https://www.eff.org/files/filenode/jewel/jewel.complaint.pdf Volgens ex-NSA werknemer Thomas Drake is BLARNEY "*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 Duncan Campbell testimony : http://www.youtube.com/watch?v=ZX1tmizZLpc. Dit is geen verrassing in het licht van de 'FRA-wet' die Zweden in 2008 aannam, zie http://news.bbc.co.uk/2/hi/europe/7463333.stm.

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

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

programma, aldus Greenwald.[85] Andere glasvezelkabels zijn voor de VS legitieme doelwitten om clandestien internet- en telefoonverkeer te onderscheppen op basis van EO 12333.

(24) Via het *upstream* programma werden e-mails van Franse telecombedrijven als Alcatel - Lucent automatisch onderschept. Het is niet duidelijk of de inhoud van alle e-mails van die adressen automatisch werd bijgehouden, enkel e-mails die bepaalde trefwoorden bevatten, en/of de metadata van dat e-mailverkeer.[86] Op basis van de functies en operaties die beide bedrijven uitvoeren, lijkt het niet onmogelijk dat gelijkaardige e-mails van werknemers van BICS, Belgacom of Tecteo op eenzelfde manier onderschept werden.[87]

(25) Een van de data die de SSO-divisie van de NSA collecteert via dergelijke 'upstream verzameling' zijn miljoenen contactlijsten of adresboeken van e-mail- en chatprogramma's alsook *screenshots* van een volledige e-mail-inbox. Contactlijsten van chatprogramma's kunnen soms de inhoud van een bepaald bericht bijhouden, en in de e-mail inbox van een persoon is ook vaak de eerste lijn van het bericht te zien.[88] Een PowerPoint presentatie van de NSA stelt dat op 10 januari 2012 op één dag 444.743 adresboeken van Yahoo werden verzameld, 105.068 van Hotmail, 82857 van Facebook, 33.697 van Gmail en 22.881 van andere providers. De Amerikaanse bedrijven in kwestie hebben – naar zij zeggen – ook geen weet van de collectie van dergelijke informatie.[89] Op jaarbasis zou dit neerkomen op het verzamelen van meer dan 250 miljoen adreslijsten per jaar.

(26) De NSA geeft toe dat de veel van deze adresboeken geen '*foreign intelligence value*' hebben – zeker omdat men in 22% van de gevallen niet weet wie de eigenaar is van de adreslijst[90]. Maar een analyse van die data stelt de NSA in staat om 'geheime connecties' en relaties te zien van een veel kleinere groep van '*foreign intelligence*' doelwitten. Die lijsten worden dan in verschillende NSA-databases opgeslagen zoals MARINA, MAINWAY, PINWALE en CLOUDs. Volgens een *intelligence* bron van *The Washington Post* mag een NSA-analist deze databases niet doorzoeken, of informatie hieruit niet verspreiden tenzij hij/zij kan aantonen dat er zich in deze gegevens een *valid foreign intelligence* doelwit bevindt.[91]

(27) Metadata die op basis van Executive Order 12333 wordt verzameld, mag sinds november 2010 gebruikt worden om aan '*contact chaining*' te doen om relaties tussen

---

85 http://www.theguardian.com/commentisfree/2013/jul/07/nsa-brazilians-globo-spying. Eerder noemde ex-NSA werknemer Thomas DRAKE FAIRVIEW, een *umbrella programma* waaronder veel andere programma's resorteren. 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 levert bijvoorbeeld cruciale infrastructuur voor onderwater glasvezelkabels. Zie hierover: http://www.alcatel-lucent.com/solutions/submarine-networks)

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

89 Het hoge aantal Yahoo-adresboeken kan verklaard worden doordat Yahoo niet automatisch data encrypteert via *secure socket layer* (SSL) – in dit in tegenstelling tot de andere providers. Deels als antwoord op de onthullingen heeft Yahoo aangekondigd om vanaf januari 2014 ook 'SSL by default' aan te bieden. 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

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

*foreign intelligence targets* en inwoners van de Five Eyes in kaart te brengen.[92] De data mag verder aangevuld worden met *enrichment data,* data uit voornamelijk publieke en commerciële bronnen zoals passagierslijsten, Facebook profielen, bank codes, kiesregistratie lijsten, GPS data van TomTom en Amerikaanse belastingdata.[93] Aangezien het hier volgens de NSA louter om metadata en open bronnen gaat, is er geen toezicht van de FISC nodig om dergelijke profielen te maken.[94]

### I.5. (Upstream) data ordenen en doorzoeken met XKEYSCORE

(28) Een gelekte presentatie uit februari 2008 beschrijft XKEYSCORE (ook gekend als CrossKeyScore of XKS) als een *DNI exploitation system/analytic Framework*.[95] XKEYSCORE houdt gedurende drie tot vijf dagen[96] ongefilterde internet data bij (*'full take'*), en gedurende 30 dagen metadata, bij die verzameld worden van 150 SIGADS overal ter wereld.[97] Dat houdt niet alleen het verzamelen van *upstream* informatie via bijvoorbeeld onderwaterkabels in, maar ook informatie vanuit satellieten (Fornsat[98]) en vanuit diplomatieke en consulaire missies van de VS overal ter wereld (F6 sites).[99] In 2012 bevatte

---

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*." In: 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 Soms kan dit soort data maar één dag bijgehouden worden: "*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.*" In: http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu

97 http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 6. Volgens NSA-expert Marc AMBINDER, die al voor de Snowden documenten over XKeyscore schreef, is Xkeyscore "*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*." In: http://theweek.com/article/index/247684/whats-xkeyscore

98 Volgens Duncan CAMPBELL, de man die het bestaan van GCHQ onthulde in 1976, is dit de opvolger van Echelon. Het programma bestaat nog steeds, maar boette aan belang in aangezien veel telefoondata zich nu ook verplaatsen via glasvezelkabels. Voor Duncan CAMPBELL getuigenis in het Europese Parlement, zie http://www.youtube.com/watch?v=ZX1tmizZLpc

99 Xkeyscore presentatie, gelekt op http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 5. Volgens AMBINDER verwijst 'F6' technisch gezien naar het hoofdkwartier van de Special Collection Service (SCS) in Beltsville, Maryland, die informatie verzamelt uit minstens 75 F6-sites die zich vooral bevinden in landen waar het onmogelijk is om informatie naar de NSA te sturen via gewone telefoonkabels of glasvezelkabels omdat de V.S. technisch gezien niet verondersteld wordt om daar aanwezig te zijn. De NSA erkent het bestaan van de SCS niet omdat de meeste personeelsleden als State Department officials werken.
Zie http://theweek.com/article/index/247684/whats-xkeyscore en http://theweek.com/article/index/247761/5-nsa-terms-you-must-know.

XKEYSCORE gedurende een periode van 30 dagen gemiddeld 41 miljard records[100] Volgens de slide laat een dergelijke *full-take* een analist onder meer toe om via metadata doelwitten te vinden die daarvoor niet gekend waren.[101] Een analist moet eerst aantonen dat hij voor 51% zeker is dat zijn zoekopdracht gaat over een buitenlands doelwit. Analisten kunnen XKEYSCORE dan doorzoeken *in real time*,[102] en data doorsturen naar andere databases zoals PINWALE, MARINA of TRAFFICTHIEF.[103] Daar wordt die ruwe informatie gedurende een langere periode opgeslagen.

(29) De voorbeelden die in de slides aangehaald worden, tonen aan dat een analist via XKEYSCORE zeer veel data kan analyseren. XKEYSCORE kan de inhoud van elke http-activiteit lezen: dus elke e-mail en elke attachment en chatconversatie[104], alle metadata van een internetcommunicatie, alle surfgeschiedenis en alle *online* zoekopdrachten die een persoon uitvoert.[105] Verder kan het ook het gebruik van een bepaalde encryptie- of VPN-technologie detecteren[106] of nagaan welke taal iemand *online* gebruikt.[107] XKEYSCORE kan ook de IP-adressen nagaan van elke persoon die een door de analist gespecificeerde website bezoekt.[108]Met XKEYSCORE kan ook nagegaan worden wie de auteur is van een document dat *online* verstuurd werd.[109] Aan de hand van 'kwetsbaarheidprofielen' die geleverd worden door de NSA's Tailored Access Operations (TAO), kan XKEYSCORE ook gebruikt worden om 'exploiteerbare machines' in een bepaald land te vinden.[110] De inhoud van opgeslagen e-mails en Facebook-chats of privéberichten kan ook binnen XKEYSCORE gelezen worden door een analist die het programma DNI PRESENTER gebruikt.[111]

---

101 Xkeyscore presentatie, gelekt op http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 2.

102 *Idem*. Voor meer details over dit proces (inclusief andere originele slides) zie http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu

103 *Idem.*

104 Xkeyscore kan dingen opzoeken zoals "*toon me elke Excel-spreadsheet uit Irak waarin Media Access Control Addresses te vinden zijn"* (23) of, "*toon me elk word-document dat de IAEA of Osama Bin Laden vermeldt*" (26), http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation,

105 Xkeyscore houdt alle zoekopdrachten bij, of het gebruik van bijv. Google Maps. http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 20.

106 Met XKeyscore is het bijvoorbeeld mogelijk om "*alle geëncrypteerde word-documenten uit Iran, of elk PGP-gebruik in Iran*" te tonen. http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation (16). Een analyst kan ook aan Xkeyscore vragen om het gebruik van bepaalde technologieën te detecteren, bijv. door te vragen: "*toon me alle VPN start-ups in land X, en geef me de data zodat ik de gebruikers van die service kan identificeren*". Zie: http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation (17).

107 Xkeyscore kan ook gebruikt worden om aan *language tracking* te doen, via Xkeyscore's 'http activity plugin' die html language tags bijhoudt. http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation (19).

108 *Idem.* Bijvoorbeeld: elke Belg die extremistische website X bezoekt.

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

110 Voor een technische analyse zie 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

(30) De slides, die uit 2008 dateren, laten zien dat XKEYSCORE op dat moment nog geen Voice over Internet Protocol (VoIP)[112] kon onderscheppen, maar het verwachtte in de toekomst ook meer metadata te onderscheppen zoals *exif tags*.[113]

(31) De NSA erkende het bestaan van XKEYSCORE als een onderdeel van de NSA's *lawful foreign signals intelligence collection system*, maar benadrukte dat toegang tot XKEYSCORE gelimiteerd is en dat elke zoekopdracht door een analist *fully auditable* is. De NSA benadrukt dat meer dan 300 terroristen werden gevat op basis van intelligence die uit XKEYSCORE komt. [114]

### I.6. PRISM: downstream verzameling van SIGINT

(32) Deels omdat steeds meer buitenlanders de diensten van Amerikaanse bedrijven begonnen te gebruiken, en deels omdat die bedrijven hun communicaties begonnen te encrypteren via SSL[115], besloot de NSA om met de belangrijkste van deze bedrijven een samenwerkingsverband te sluiten om gebruikersdata op een efficiënte en gestroomlijnde manier door te sturen naar de NSA.[116] Het resultaat van deze onderhandelingen was het PRISM-programma. Via PRISM kreeg de NSA – in vergelijking met de *upstream* collectie – op een gestructureerde manier *downstream* data van negen grote technologiebedrijven binnen: Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL en Apple.[117]

(33) Alle PRISM-providers hebben een code gekregen. P1: Microsoft[118], P2: Yahoo, P3: Google[119], P4: Facebook, P5: PalTalk, P6: YouTube, P7: Skype[120], P8: AOL, PA: Apple.[121]

---

112 Verwijst naar services zoals Skype en Apple's Facetime.

113 Xkeyscore presentatie, gelekt op http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 32. Een *exchangeable image file format* (exif) is een technische standaard die metadata van digitale camera's bijhoudt, zoals bijvoorbeeld de datum en tijd wanneer een digitale foto werd genomen.

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

115 Een encryptieprotocol om communicatie op het internet te beveiligen.

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

117 De meest volledige slideshow van PRISM werd in oktober gepubliceerd door *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* beschreef verder SSO documenten die aantoonden dat Microsoft en de FBI ervoor zorgden dat de NSA makkelijk de encryptie van outlook.com chats kon omzeilen. Een ander document toont aan dat de NSA toegang heeft tot e-mails van Hotmail, Windows Live en Outlook.com vooraleer die geëncrypteerd worden. http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

119 De NSA heeft hiermee toegang tot Gmail, Google voice and video chat, Google Drive files, Google's fotodienst Picasa Web, en (real time) surveillance van zoektermen die door een persoon worden ingetypt in 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".* Zie: 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

(34) Er zijn negen grote types aan content die via PRISM worden verzameld, die ook weer een codeletter hebben gekregen. A= opgeslagen communicaties (zoals privéberichten op een sociale netwerksites, chat-geschiedenis, e-mails etc.), B: Instant Messaging (chat), C: RTN-EDC (notificatie in *real time* van een login op een account of een verstuurd bericht), D: RTN-IM (notificatie in *real time* voor een chat login of logout), E: E-mail, F: VoIP (services zoals Skype, inclusief videoconferencing), G: Full (Webforum), H: OSN (Online Social Networking information – foto's, *wallposts*, activiteiten op sociale media sites…) I: OSN informatie die geleverd wordt wanneer men zich inschrijft voor een OSN-dienst. J: video's.[122]

(35) Het systeem lijkt als volgt te werken: een NSA-analist kan zelf de *selectors* (e-mailadres, telefoonnummer, naam, maar ook zoektermen) invoeren in een *Unified Targeting Tool*.[123] Die *selectors* worden bekeken door een overste, die nagaat of er 51% kans is dat het om een buitenlands doelwit gaat.[124] Als de NSA opgeslagen data (bijv. e-mails in een inbox) wil consulteren, dan moet de FBI een extra check doen om te zien of er geen Amerikanen bespioneerd worden. Als de NSA in '*real-time*' surveillance wil doen, dan is die extra check niet nodig. In beide gevallen gebruikt de FBI's Data Intercept Technology Unit (DITU) materiaal (*government equipment*) om informatie over die doelwitten te verkrijgen van een van de bedrijven die meedoen aan PRISM. De FBI stuurt dat materiaal dan door naar de CIA of de NSA.[125]

(36) Als er informatie over een doelwit wordt verzameld, dan betekent dat ook dat informatie kan verzameld worden over iedereen waarmee het doelwit tot in de tweede graad mee gecommuniceerd heeft. Een eenvoudig hypothetisch voorbeeld toont aan dat informatie inwinnen over een doelwit in de praktijk betekent dat data van een enorm aantal

---

Een ander document stelde dat "*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 De providers startten hun deelname in PRISM op verschillende tijdstippen. 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: oktober 2012. PRISM startte dus maar na de aanname van de Protect America Act in 2007. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1# In April 2013 heette het dat de toevoeging van Dropbox nakende was. 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

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*." Zie: 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 Merk op dat de FISC alleen de certificaten jaarlijks onderzoekt (zie para. 9), niet de individuele zoektermen.

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…*". Zie: http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

mensen potentieel kan verzameld worden. Als een doelwit gecommuniceerd heeft met 700 mensen via Facebook of e-mail, en die mensen hebben op hun beurt ook elk gecommuniceerd met 700 mensen, dan kan de NSA gegevens verzamelen over 490.000 mensen.[126]

(37) De NSA sorteert op haar beurt de verkregen data op basis van datatype, en haalt de ze nog eens door een filter om na te gaan of geen Amerikaanse gegevens worden bekeken. DNI content[127] en video worden doorgestuurd naar de PINWALE database.[128] Metadata van '*internet records*' worden verstuurd naar MARINA[129] en metadata van telefoongesprekken naar MAINWAY.[130] Een intern NSA bulletin gaf aan dat MAINWAY in 2011 per dag metadata binnen kreeg van 700 miljoen telefoongesprekken. Vanaf augustus 2011 kwamen daar nog eens 1,1 miljard metadata van telefoongesprekken extra bij per dag.[131]

(38) Op 5 april 2013 waren er 117.675 actieve surveillance doelwitten in PRISM's *counterterrorism database*.[132] Volgens de vrijgegeven slides is PRISM de SIGAD waaruit de meeste ruwe informatie komt voor alle NSA-rapporten.[133] In 2012 verscheen PRISM-data in

---

126 http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1#
*The Washington Post* merkt verder op: "*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
Verder: "*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*." Zie: 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

127 Zoals forum posts, chats, e-mails… of simpel gezegd: "internet content".

128 Pinwale houdt de inhoud van communicaties bij voor een periode van vijf jaar. Die informatie lijkt te komen op basis van op voorhand ingestelde *dictionary tasked terms* die het onder andere krijgt uit Xkeyscore en PRISM. http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu

129 Marina wordt in een Xkeyscore slide beschreven als "*user activity meta-data with front end full take feeds and back-end selected feeds*". Hierover:
http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu
*The Guardian* quote uit een document waarin Marina verder wordt beschreven. "*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*." In:
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 Ter vergelijking: de Terrorist Identities Datamart Environment (TIDE) van de Amerikaanse overheid telde in december 2011 740.000 'records', waarbij eenzelfde persoon een aantal keer kan voorkomen wegens een foute spelling van zijn/haar naam. http://www.dni.gov/files/Tide_Fact_Sheet.pdf

133 Dat wordt ook bevestigt door de FISC, zie para.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*." In:

1.477 items van de Amerikaanse President's Daily Intelligence Brief.[134] DNI-director Clapper bevestigde het bestaan van PRISM (zonder het programma bij naam te noemen), en noemde het "*een van de belangrijkste bronnen*" van de NSA.[135]

### I.7. Financiële data

(39) Volgens documenten die *Der Spiegel* kon inzien, heeft de NSA een '*Follow the money*'-tak die internationale geldstromen – vooral in Afrika en het Midden Oosten – in de gaten houdt. Die informatie komt terecht in een database, genaamd TRACFIN, die in 2011 al 180 miljoen datasets had over banktransfers, kredietkaarttransacties en geldtransfers. Volgens *Der Spiegel* houdt de NSA dit soort data gedurende vijf jaar bij.[136]

(40) Nog steeds volgens *Der Spiegel* heeft de NSA een grondige kennis van de interne processen van maatschappijen zoals Visa en Mastercard (zoals '*payment authorisation processes*' en interne geëncrypteerde communicaties[137]), en houdt het ook alternatieve betaalmethodes zoals Bitcoin in het oog. Volgens *Der Spiegel* verzamelt de NSA via het DISHFIRE-programma informatie over transacties die met kredietkaarten worden uitgevoerd van meer dan 70 banken wereldwijd – vooral in 'crisisgebieden', inclusief in landen als Italië, Spanje en Griekenland. DISHFIRE is actief sinds de lente van 2009. De transacties van Visa-klanten in Europa, het Midden Oosten en Afrika werden ook geanalyseerd om financiële associaties bloot te kunnen leggen.[138] Door deze kennis werden verschillende Arabische banken op de *blacklist* van de US Treasury geplaatst.[139]

(41) Andere documenten tonen aan dat de NSA's Tailored Access Operations (TAO) divisie sinds 2006 clandestien toegang heeft verworven tot de interne data trafiek van de Society

---

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

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

for Worldwide Interbank Financial Telecommunication (SWIFT).[140] Dat is opmerkelijk, aangezien de VS een akkoord heeft met de EU om SWIFT-data te delen – maar dat akkoord laat niet het versturen van *bulk data* toe.[141] Na deze onthullingen stemde het Europese Parlement op 23 oktober 2013 in met de opschorting van het Terrorist Finance Tracking Program (TFTP Agreement).[142] In een statement liet Commissaris Malmström weten dat het TFTP-akkoord niet zal opgeschort worden.[143]

### I.8. Metadata van Amerikaanse telefoongesprekken

(42) In Amerika spitst het NSA-debat zich vooral toe op het verzamelen van Amerikaanse telefoondata door de NSA, onder meer op basis van de *business records* sectie 215 die door de Patriot Act geïntroduceerd werd in FISA.[144] Op basis van deze sectie kon de VS de grootste Amerikaanse telecom-operatoren verplichten om alle metadata van telefoongesprekken met een Amerikaans begin- of eindpunt ter beschikking te stellen van de NSA. Volgens de NSA kunnen deze data enkel geconsulteerd worden voor anti-terreurdoeleinden. Een consultatie kan enkele beginnen met een telefoonnummer dat eerder geassocieerd werd met een buitenlandse terroristische organisatie (*a seed*).[145]

### I.9. Smartphone data

(43) Volgens *Der Spiegel* heeft de NSA de capaciteit om een grote waaier aan smartphonedata te verkrijgen van *high interest targets*.[146] De NSA had toegang tot de contactlijsten, call logs, sms-trafiek, drafts van sms'en en locatie-informatie van de mobiele platformen van Apple (IOS), Google (Android) en Blackberry.[147] De NSA heeft bijvoorbeeld toegang tot 38 iPhone applicaties zoals het gebruik van de ingebouwde kaartfunctie, voicemail en foto's, Google Earth, Yahoo en Facebook Messenger.[148]

### I.10. PNR-data

(44) Via het Passenger Name Records (PNR) akkoord uit 2012 verkrijgt het US Department of Homeland Security (DHS) PNR-data van passagiers die van de EU naar de VS vliegen. Die data

---

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)), zie: 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 October, zie: http://europa.eu/rapid/press-release_MEMO-13-928_en.htm

144 Zie para 6.

145 N.S.A., The National Security Agency: Missions, Authorities, Oversight and partnerships, 9 Augustus 2013, 5.

146 Zie ook para. 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*." In: M. ROSENBACH, L. POITRAS en H. STARK, *Der Spiegel*, 9 September 2013 ("iSpy: How the NSA Accesses Smartphone Data").

148 *Idem*.

bestaat uit informatie die een passagier gegeven heeft aan de luchtvaartmaatschappij zoals de naam van de passagier en zijn eventuele medepassagiers, hun adressen en telefoonnummers, reisdata, eindbestemming, ticket informatie, de manier van betalen, credit card nummer, bagage informatie enz. De volledige lijst kan teruggevonden worden in de annex bij het akkoord.[149] DHS mag die data delen met binnenlandse diensten[150] en derde landen.[151] De data worden gebruikt ter preventie, opsporing en berechting van terroristische misdrijven en ernstige grensoverschrijdende misdaden.[152] Na zes maanden worden alle persoonlijke data gemaskeerd, en na vijf jaar worden de data in een 'slapende' database gestoken. De data mogen gedurende tien jaar gebruikt worden ter preventie van grensoverschrijdende misdaad, en vijftien jaar voor terrorisme.[153]

### I.11. NSA-inspanningen tegen encryptie

(45) *The New York Times* publiceerde een *briefing sheet* van de NSA aan het GCHQ uit 2010 over een programma genaamd BULLRUN, waarin de NSA suggereert dat de meest gebruikte encryptie-protocollen die verantwoordelijk zijn voor de beveiliging van de wereldwijde handel, banksystemen, medische data en internet surfgedrag (zoals het zenden van e-mails, online opzoekingen, chats en online telefoongesprekken) door de NSA gekraakt of omzeild konden worden. Het gaat over TLS/SSL[154], https[155], SSH[156], VPNs[157] en geëncrypteerde chats[158] en VOIP communicaties[159]. De specifieke technische details over wat er precies werd gekraakt werden tot nu toe niet vrijgegeven.[160, 161] Het bestaan van deze decryptiemogelijkheden én het gebruik van alle geëxploiteerde data (zowel *plaintext* als

---

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

150 *Idem*, artikel 16.

151 *Idem*, artikel 17.

152 *Idem*, artikel 4.

153 *Idem*, artikel 8.

154 Transport Layer Security/Secure sockets layer. De meest gebruikte manier om informatie te verzenden over het internet en interne servers. HTTPS is beveiligd door TLS/SSL toe te passen op een website.

155 Hypertext transfer protocol secure. Manier om financiële informatie en paswoorden veilig te versturen van een computer naar een netwerk. Sites zoals Facebook, Twitter en Gmail gebruiken vaak https 'by default'. Herkenbaar aan het slotje voor de https in de web-browser.

156 Secure Shell. De manier voor Linux en Max gebruikers om toegang te krijgen tot een computer vanop afstand.

157 Virtual Private Network. Vaak gebruikt door bedrijven om werknemers van thuis uit toegang te verschaffen – via een gencrypteerde 'tunnel' tot het bedrijfsnetwerk.

158 Een voorbeeld is het Adium programma, waarmee 'end to end' encryptie mogelijk is, waarbij de data niet kan gedecrypteerd worden op enig punt gedurende de transfer.

159 Verwijst naar services zoals Skype en Apple's Facetime.

160 http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us
Experts hebben opgemerkt dat de documenten niet tonen welke geëncrypteerde systemen de NSA gekraakt heeft door pure wiskunde, en welke door hacking of samenwerking van ontwikkelaars. Een systeem als Pretty Good Privacy (PGP) zou nog altijd werken. Voor meer info zie (de links) hierin: http://www.washingtonmonthly.com/political-animal-a/2013_09/the_nsa_is_mostly_not_breaking046760.php of 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

metadata) die uit deze mogelijkheden voortkwamen, werden geclassificeerd als Exceptionally Controlled Information (ECI), een *level* hoger dan 'Top Secret'.[162]

(46) Een budgetaanvraag uit 2012 onthulde verder het bestaan van het Sigint Enabling Project dat erop gericht is om in het geheim Amerikaanse en buitenlandse internetbedrijven te beïnvloeden het design van hun producten aan te passen zodat deze kunnen geëxploiteerd worden. Het programma omvat een hele reeks activiteiten: (1) Samenwerking met bedrijven om 'achterpoortjes' te installeren in commerciële encryptie systemen, IT-systemen, netwerken en *endpoint communication devices* die gebruikt worden door 'doelwitten'.[163] Die samenwerking kan vrijwillig zijn[164], of afgedwongen worden door FISA-dwangbevelen.[165] (2) Het beïnvloeden van technische standaarden en specificaties voor commerciële *public key technologies*, inclusief de standaard uit 2006 van het National Institute of Standards and Technology.[166] (3) Het voortzetten van de samenwerking met grote *telecommunications carriers*.[167] De meest controversiële manier is echter het clandestien stelen van encryptie-sleutels. NSA-documenten tonen aan dat de NSA een interne database heeft (de Key Provisioning Service), die de encryptiesleutels bevat van specifieke commerciële producten. Als een bepaalde sleutel niet aanwezig is, dan gaat een aanvraag naar de Key Recovery Service, waarvan beweerd wordt dat die sleutels verkrijgt door in te breken in de servers van de bedrijven die de sleutel gemaakt hebben. Om deze methode geheim te houden, zou de NSA alleen gedecrypteerde boodschappen met andere diensten delen als de sleutels verkregen werden door legale middelen.[168]

(47) Op 4 oktober 2013 onthulden *The Guardian* en *The Washington Post* hoe de NSA sinds 2006 probeerde om gebruikers van het Tor-netwerk te identificeren en te bespioneren.[169] Tor is een netwerk van servers die gebruikers toelaten om anoniem te surfen.[170] Gebruikers kunnen dat netwerk via speciale, complexe software gebruiken, maar een alternatieve, gemakkelijkere manier om Tor te gebruiken is het downloaden van de Tor Browser Bundle (TBB) – een versie van Firefox die automatisch data verzendt over het Tor-netwerk. Uit de

---

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

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*." In: 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* plaatste een document uit 2006 van 49 pagina's online dat beschrijft welke methodes potentieel de grootschalige de-anonymisatie van Tor gebruikers zouden toelaten. In: http://apps.washingtonpost.com/g/page/world/nsa-research-report-on-the-tor-encryption-program/501/. James Clapper statement op de onthullingen : 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/

documenten blijkt dat de NSA in 2007 TBB-gebruikers kon onderscheiden van gewone Firefox gebruikers,[171] maar dat het er in 2007 nog niet in geslaagd was om het Tor-netwerk zelf te hacken. Een NSA-presentatie uit juni 2012 stelt dat de NSA nooit in staat zal zijn om alle Tor-gebruikers tegelijkertijd te de-anonimiseren, en dat de NSA ook geen technieken heeft die toestaan om een specifieke gebruiker op verzoek te de-anonimiseren. Door manuele analyse is het echter mogelijk om een 'zeer kleine fractie' van Tor gebruikers te de-anonimiseren.[172] Slides van de NSA's Tailored Access Operations (TAO) beschrijven hoe de NSA Javascript-kwetsbaarheden in Firefox exploiteerde via de programma's EGOTISTICALGOAT en EGOTISTICALGIRAFFE.[173] Deze kwetsbaarheden zouden verdwenen zijn met de meest recente *update* van Firefox in januari 2013[174], maar het is onduidelijk of de NSA dit intussen al omzeild heeft.[175]

(48) Onder de codenaam Quantum plaatste de NSA geheime Quantum-servers op belangrijke plaatsen van de infrastructuur van het internet, waardoor de NSA een *man in the middle* aanval kon uitvoeren op Tor-gebruikers.[176] Dit betekent dat deze servers sneller kunnen reageren dan andere websites, waardoor ze de gebruiker naar een geïnfecteerde imitatie van de gevraagde website kunnen sturen die op een FoxAcid-server staat. De servers in dit FoxAcid-systeem worden gerund door TAO, en kunnen op verschillende manieren computers voor lange periodes besmetten.[177] Het bezoek van de homepage van een FoxAcid-server zou niet direct tot besmetting leiden; daarvoor is een door TAO gecreëerde specifieke URL voor nodig. Die URL zou de FoxAcid server in staat stellen om precies te weten welk doelwit de FoxAcid server bezoekt.[178] FoxAcid is een algemeen CNE-systeem dat gebruikt wordt voor verschillende digitale aanvalsvormen. Het wordt dus voor veel meer gebruikt dan om Tor-gebruikers te identificeren. Documenten uit *Der Spiegel* suggereren bijvoorbeeld dat de Belgacom-aanval (deels) via Quantumservers zou uitgevoerd zijn.[179]

---

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

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:)."*
In: 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".* In: http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

178 *Idem.*

179 *Idem.*

# II. HET BRITSE GOVERNMENT COMMUNICATIONS HEADQUARTERS (GQHQ)

## II.1. Het Britse wettelijke kader voor het inzamelen van informatie over buitenlandse doelwitten

(49) De Intelligence Services Act uit 1994 zette voor het eerst de functies uit van het Government Communications Headquarters (GCHQ). Het Britse SIGINT-agentschap heeft onder meer als mandaat om "*elektromagnetische, akoestische en andere emissies, alsook ieder toestel dat zulke emissies produceert"* te monitoren of te storen.[180] Het agentschap moet informatie over die emissies doorsturen naar het Britse leger, de regering en andere diensten[181] als dat nodig is voor de nationale veiligheid van de UK (waarbij specifiek verwezen wordt naar de defensie- en buitenlandse politiek van de UK), het economische welzijn van de UK (met betrekking tot de handelingen en intenties van personen buiten de Britse eilanden) en ter ondersteuning van de preventie en het opsporen van ernstige misdaden.[182]

(50) De UK heeft geen specifieke wetgeving die exclusief het gebruik van *foreign intelligence* reguleert, maar de Regulation of Investigatory Powers Act (RIPA) maakt een onderscheid tussen 'interne' en 'externe' surveillance, waarbij die laatste categorie refereert naar surveillance van communicaties waarvan op zijn minst een uiteinde buiten de UK ligt.[183] In deze gevallen moet GCHQ geen bevelschrift aanvragen op naam van een specifieke persoon of een specifieke locatie,[184] maar kan het een bevelschrift vragen om bijvoorbeeld data van een externe communicatielink te onderscheppen, zoals bijvoorbeeld een specifieke glasvezelkabel die tussen de UK en het Europese vasteland loopt.[185] Ter illustratie, alle glasvezelkabels die aan land komen in België zijn verbonden met een landingspunt in de UK. De Tangerine-kabel verbindt Broadstairs met Oostende; Concerto verbindt Zeebrugge met Sizewell en Thorpeness en de Pan-European Crossing verbindt Bredene met Dumpton Gap. De grote SeaMeWe-3 kabel, waarvan Belgacom deels eigenaar is, verbindt Oostende met Goonhilly Downs in de UK, maar heeft ook landingspunten in Saudi Arabië, Maleisië en China.

(51) Een dergelijk breed bevelschrift wordt dan uitgevaardigd door de Secretary of State, die in een 'certificaat' beschrijft welk materiaal precies noodzakelijk is om onderzocht te

---

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. Interceptie wordt als volgt gedefinieerd in 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*." In: http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world

worden[186] in het belang van de UK's nationale veiligheid, om ernstige misdaden te voorkomen of op te sporen of om het economische welzijn van de UK veilig te stellen.[187] De inhoud van de certificaten is geheim, maar volgens documenten die *The Guardian* heeft ingezien, zijn deze heel breed geformuleerd, en laten deze toe om materiaal te onderscheppen over wijde thema's zoals de politieke intenties van buitenlandse overheden, de militaire toestand van andere landen, terrorisme, internationale drugshandel en fraude. Volgens *The Guardian* zijn er minstens tien van die certificaten.[188] Volgens RIPA is zo'n bevelschrift initieel drie maanden geldig[189], maar het bevelschrift kan elke zes maand hernieuwd worden.[190] Telecombedrijven kunnen verplicht worden om mee te werken met de interceptie van deze communicaties.[191]

(52) Het moet opgemerkt worden dat het niet duidelijk is wat er precies in het bevelschrift en het certificaat moet staan. Onder meer hierover is de wet onduidelijk. Het Intelligence Security Committee (ISC), dat toezicht houdt over GCHQ, heeft aangekondigd dat "*meer gedetailleerde beleidslijnen en procedures in het leven zijn geroepen zodat GCHQ de Human Rigts Act van 1998 naleeft*". De ISC gaat nu onderzoek doen naar de 'complexe interactie tussen de ISA, de Human Rights Act en RIPA en de procedures die dit regelen.[192]

(53) De wet staat GCHQ ook toe om vanop afstand in te breken in computersystemen om op die manier data te verkrijgen.[193] Op basis van sectie 7 ISA is iedere actie van GCHQ buiten de UK vrijgesteld van burgerlijke of strafrechtelijke aansprakelijkheid indien deze gebeurt op basis van een machtiging van de Secretary of State.

---

186 RIPA, s8.4(b).

187 RIPA s.5(3)a-c. *The Guardian* quote een GCHQ document als volgt: "*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*." In: http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world

188 *The Guardian* quote een interne GCHQ memo uit oktober 2011: "*[Our] targets boil down to diplomatic/military/commercial targets/terrorists/organised criminals and e-crime/cyber actors*". In: http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet

189 RIPA, s9.6.c

190 RIPA s9.6.b. Voor meer informatie over s(8)4 warrants, zie: UK Home Office, Interception of Communications Code of Practice. TSO, London, 22-27, op 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 juli 2013, zie: http://isc.independent.gov.uk/news-archive/17july2013

193 Zie Computer Misuse Act 1990, s.10; RIPA, s32 en ISA, s.5.

## II.2. Aard en schaal van de Britse gegevensinzameling

(54) Volgens *The Guardian* startte GCHQ begin 2007 met de voorbereidingen voor het Mastering the Internet (MTI) project in de basis in Bude.[194] Het doel was om buitenlandse *upstream* data te verzamelen door *deep packet inspection* materiaal te plaatsen op de onderwaterkabels wanneer die de Britse kust raakte. [195] In mei 2009 berichtten *The Register* en *The Sunday Times* dat de financiering van MTI was goedgekeurd in oktober 2007. Meer dan één miljard pond zou de komende drie jaar uitgetrokken worden om die *upstream* collectie mogelijk te maken.[196] GCHQ erkende het bestaan van MTI, maar benadrukte dat het geen technologie aan ontwikkelen was die het mogelijk zou maken om al het Internet- en telefoongebruik *in de UK* te monitoren.[197]

(55) Op een onbekend moment tussen 2010 en 2011 slaagde GCHQ in haar opzet, en begon het de uitbaters van de commerciële glasvezelkabels via een bevelschrift te verplichten om mee te werken als *intercept partners*. Dit afgedwongen samenwerkingsproces wordt '*special source exploitation*' genoemd, en de '*intercept partners*' worden vergoed voor de kosten die dit meebrengt.[198] De namen van de samenwerkende bedrijven werden later bekend gemaakt door de *Suddeütsche Zeitung*. Ze stonden alle zeven bekend onder een andere codenaam: BT (Remedy), Verizon Business (Dacron), Vodafone Cable (Gerontic), Global Crossing (Pinnage), Level 3 (Little), Viatel (Vitreous) en Interoute (Streetcar).[199] De glasvezelkabel die aankomen in België (zie para. 50) worden allen uitgebaat door een van deze bedrijven.

(56) Die *upstream* informatie wordt via het TEMPORA-programma eerst gefilterd om internet trafiek dat veel volume inneemt (zoals downloads van films of muziek) uit te sluiten, waardoor het volume met ongeveer 30% daalt.[200] De overblijvende *upstream*-informatie wordt gefilterd op basis van 'harde selectors' (zoals telefoonnummers en e-mailadressen) en 'zachte selectors' (zoals zoektermen). Volgens *The Guardian* werden 40.000 van deze selectors gekozen door GCHQ en 31.000 door de NSA.[201] Die baseren zich op de brede certificaten om die *selectors* zelf te kiezen. De ongefilterde data wordt weggesmeten, en de metadata die overblijft wordt bijgehouden gedurende dertig dagen en inhoud gedurende

---

194 Naast MTI is er ook een programma dat Global Telecoms Exploitation heet, maar het is niet duidelijk wat daarmee bedoeld wordt. Zie: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

195 http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet. Een eerste experimenteel project om dat te bereiken stond bekend als het Cheltenham Processing Centre (CPC). Vanaf maart 2010 werd naar dit project als een gezamenlijk GCHQ/NSA-initiatief verwezen genaamd TINT.

196 Volgens die berichten zouden Lockheed Martin en Detica meehelpen om MTI te ontwikkelen. Sinds 2008 werden inderdaad jobadvertenties aangeboden die te maken hadden met het MTI-contract http://www.theregister.co.uk/2009/05/03/gchq_mti/ ; http://www.timesonline.co.uk/tol/news/politics/article6211101.ece

197 (Eigen nadruk) 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*.

drie dagen.[202] Een bron van *The Guardian* lijkt te suggereren dat alle 'gefilterde' data gelogd worden en ingezien kan worden door de UK's Interception Commissioner, maar het is onduidelijk of dit gaat over alle informatie die wordt opgeslagen na de *selector*-filtering, of alleen die data die effectief gebruikt wordt.[203] Deze data kan dan – onder andere – retroactief onderzocht worden op zoek naar verdachten die nog niet bekend waren bij de Britse of Amerikaanse inlichtingendiensten.[204]

(57) Voor het overige kan alle *upstream*-informatie verzameld worden die ook door de NSA verzameld wordt via haar *upstream*collectie (zie para 29): inhoud van e-mails, browsergeschiedenis, Facebook-berichten, documenten die als attachment werden toegevoegd etc. Hier moet opgemerkt worden dat analisten ook kunnen beslissen om alle metadata en inhoud van de contacten van een doelwit te verzamelen als zij dat proportioneel achten.[205] Minstens 300 GCHQ-analisten en 250 NSA-analisten hebben directe toegang tot de data van TEMPORA. [206] Veel metadata wordt ook opgeslagen door de NSA. [207] In februari 2011 meldde de NSA in een document dat GCHQ nu "*meer metadata verwerkte"* dan de NSA.[208] In 2012 kon GCHQ 600 miljoen 'telefoon events' per dag verwerken, tapte het 200 glasvezelkabels af en was het in staat om van 46 van die kabels tegelijkertijd data te verwerken. *The Guardian* schatte dat GCHQ daarmee in theorie toegang heeft tot 21,6 petabytes per dag – 192 keer de inhoud van alle boeken de zich in de British Library of Congress bevinden.[209]

### II.3. De malware bij Belgacom

(58) Op 21 juni 2013 vindt Belgacom *malware* op haar intern computersysteem. Nadat hulp van onder meer toeleveranciers Microsoft en HP geen soelaas brachten, wordt op 25 juni de Nederlandse firma Fox-IT ingehuurd om naar de malware te kijken.[210] Na verder onderzoek van Fox-IT dient Belgacom vervolgens op 19 juli 2013 een klacht in tegen onbekenden bij het federale parket wegens frauduleuze toegang tot zijn interne computersystemen. Dat

---

202 http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work Het is interessant dat GCHQ in bepaalde gevallen zelfs paswoorden als metadata beschouwd.

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

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*." In: 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 *The Guardian* meldt verder: "*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*".
In: 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. Zie: http://www.youtube.com/watch?v=ayR6CAuNE4w

onderzoek wordt geleid door de gerechtelijke politie van Brussel (Regional Computer Crime Unit) met de (technische) steun van de Federal Computer Crime Unit (FCCU) en Algemene Dienst inlichting en veiligheid (ADIV).[211] De voorzitter van de Privacycommissie besluit in september om in samenwerking met Belgacom en het Belgisch Instituut voor Postdiensten en Telecommunicatie (BIPT), een apart onderzoek in te stellen naar wat er precies is gebeurd. Belgacom communiceert in een persbericht op 16 september 2013 dat in het weekend van 14 en 15 september "*een onbekend virus*" verwijderd werd. Volgens Belgacoms is er "*tot dusver geen enkele aanwijzing van impact op de klanten of hun gegevens"*. [212] De kostprijs van de schoonmaakoperatie wordt tot dan op vijf miljoen euro geschat.[213]

(59) Volgens een persbericht van het parket wijst de aanval, gezien "*de inzet van belangrijke financiële en logistieke middelen door de inbreker*" en "*de technische complexiteit ervan"* in de richting van "*state-sponsored cyberspionage gericht op het verzamelen van strategische informatie*".[214] Later bevestigt Belgacom dat 124 van de 26.600 apparaten[215] die aangesloten zijn op het interne Windows-systeem van Belgacom werden gecompromitteerd[216] door wat experts een *advanced persistent threat* noemen. [217] De omschrijving van de symptomen van de *malware*, valt onder het geheim van het gerechtelijk onderzoek, maar de FCCU heeft de *malware* in de mate van het mogelijke vrijgeven zodat andere (Belgische en Europese) instellingen na kunnen gaan of ze zijn besmet. Informatie is onder meer gedeeld met het permanente Computer Emergency Response Team (CERT-EU) van de EU.

(60) *De Standaard* meldt op basis van "*bronnen dicht bij het dossier"* en "*in kringen van de veiligheidsdiensten*" dat de NSA achter de aanval zit, en dat de NSA het in het bijzonder gemunt had op de activiteiten van Belgacom International Carrier Services (BICS), een dochteronderneming van Belgacom. [218] Belgacom heeft 57,6% van BICS in handen, Swisscom 22,4% en het Zuid-Afrikaanse MTN 20%. BICS levert diensten aan verschillende telecomoperatoren in verschillende landen, en baat onder meer – samen met een groep andere bedrijven – de TAT-14, SEA-ME-WE3 en SEA-ME-WE4 onderwater-glasvezelkabels uit (zie ook para. 50). Op die manier zou bijv. telefoon- en internetverkeer vanuit Syrië, Yemen en Afghanistan onderschept kunnen worden. Dat was een van de redenen achter de aanval die door *De Standaard* werd aangehaald in haar eerste berichtgeving.[219] In een mededeling zegt BICS op 16 september 2013 dat er geen enkele aanwijzing is "*dat ons telecomnetwerk, langs waar ons communicatieverkeer loopt, door spionageoperaties werd getroffen. Het is*

---

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

212 Belgacom, Belgacom onderneemt actie in het kader van haar IT-beveiliging. 16 september 2013. Zie http://www.belgacom.com/be-nl/newsdetail/ND_20130916_Belgacom.page

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

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

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

216 X., *De Standaard*, 16 september 2013 ("Bellens: 'Geen aanwijzing dat Belgacomklanten zijn getroffen'").

217 DOD, *De Standaard*, 17 september 2013 ("Zeg nooit 'virus' tegen advanced persistent attack"). http://www.standaard.be/cnt/dmf20130916_00745157. Voor meer informatie, zie bijvoorbeeld https://www.damballa.com/knowledge/advanced-persistent-threats.php

218 M. EECKHAUT, P. DE LOBEL, N. VANHECKE, *De Standaard*, 16 september 2013 ("NSA verdacht van hacken Belgacom").

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

*ons intern informaticasysteem dat geïntegreerd is met dat van Belgacom dat gehackt werd".*[220]

(61) Op 20 september 2013 publiceerde *Der Spiegel* ongedateerde slides uit de Snowden-documenten waarin GCHQ's 'Network Analyses Centre' vertelt over de successen die behaald werden in 'Operation Socialist'. Belgacom stond in de operatie bekend onder de naam Merion Zeta. In deze operatie lijkt het erop dat werknemers die sleutelposities bezetten bij BICS via door de NSA-gecontroleerde Quantum-servers naar een andere NSA-gecontroleerde server werden geleid (Fox Acid server), waarbij die laatste op hun beurt een kwetsbaarheid in de browser van het doelwit gebruikte om *malware* op de computer van het slachtoffer te installeren. (zie ook para 48). Het ultieme doel van 'Operation Socialist' was volgens de slides van *Der Spiegel* om Belgacom's core GRX router te exploiteren om van daar *man in the middle* aanvallen te kunnen uitvoeren op doelwitten die met hun smartphone aan het *roamen* zijn.[221] Volgens de slides was GCHQ erg dicht bij dit doel.[222] BICS heeft wereldfaam in het aanbieden van 3GRX-diensten, die een lokale telefoonoperator onder meer moet toelaten aan haar klanten om te *roamen* in meer dan 190 landen.[223] De VPN-verbindingen van BICS en MyBICS, de online toepassing waarlangs het contact met klanten verloopt, werden ook als interessante doelwitten gezien.

(62) Na de onthullingen in *Der Spiegel* citeerde *De Standaard* bronnen dicht bij het gerechtelijk onderzoek die op basis van "*de handtekening van de malware"* en "*vooral de plaats waar de sporen heen leiden"* nog steeds overtuigd zijn dat de aanval uit de VS komt. Volgens de speurders is Amerika de belangrijkste bestemming, en leiden er slechts "*in zeer beperkte mate"* sporen naar het Verenigd Koninkrijk.[224] Op vraag van Premier Di Rupo heeft de Belgische Veiligheid van de Staat nu officieel haar Britse tegenhanger om uitleg gevraagd.[225]

(63) Op basis van 'verschillende bronnen' meldt de Nederlandse zender NOS op 3 oktober dat eind 2011 "*een team van GCHQ (…) het hart van Belgacom aan heeft gevallen*" via *named pipes*, een geavanceerde manier om vrijwel onzichtbaar communicatie te versturen over een netwerk. Volgens de NOS "*bevestigen loggegevens dat het om Engeland gaat: tijdens Engelse feestdagen en lunchtijd is er duidelijk minder spionageactiviteit"*.[226] De NOS beweert dat "*nadat het netwerk gekraakt werd*", de Britten *"bijna onbeperkte toegang hadden tot het Belgacom netwerk*".[227] Eerder vertelde een andere bron aan *De Standaard* dat degene die dit deed, alles kon "*wat de hoogst geplaatste netwerkbeheerder bij Belgacom kon* (…) *Het had alle sleutels, alle paswoorden en de volledige controle"*.[228] De NOS beweert

---

220 G. QUOISTIAUX, *Trends*, 16 september 2013 ("BICS, succesvolle dochter van Belgacom en doelwit NSA").

221 http://www.spiegel.de/fotostrecke/photo-gallery-operation-socialist-fotostrecke-101663.html. Voor een meer technische achtergrond; zie 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 september 2013 ("Operatie socialist: succes!").

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

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

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

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

ook dat "*een ander team*" vervolgens op zoek ging naar "*specifieke informatie*". De informatie werd vervolgens gedeeld met de NSA.[229] Volgens "*bronnen bij het onderzoek*" hebben de verantwoordelijken "*een beetje overal zitten rondkijken en gepakt wat ze konden*".[230] Volgens *De Standaard* levert BICS diensten waar tal van belangrijke klanten gebruik van maken: Swift, Electrabel, bpost, Belgocontrol, de Navo in Evere, de Europese Commissie en het Europese Parlement in Brussel en Straatsburg, het Supreme Headquarters Allied Powers Europe (SHAPE) in Bergen, maar ook bijvoorbeeld het hoofdkwartier van de Allied Air Command van de Navo in Ramstein.[231] Tijdens een hoorzitting in het Europees Parlement ontkenden twee topmannen van Belgacom dat de Britse geheime dienst toegang zou hebben gehad tot telefoonnetwerken van Europese instellingen. Volgens Belgacom is er via hun systeem "*geen overflow geweest naar systemen van klanten. Dus ook niet naar systemen van de Europese instanties"*.[232]

(64) Het is echter op dit moment onmogelijk om met zekerheid te zeggen welke data er precies onderschept werden. Zowel Belgacom[233], de FCCU[234], als Frank Robben[235], co-rapporteur van het Belgacom-rapport van de Privacycommissie, hebben verklaard dat het virus zelf encryptietechnieken gebruikte om te verhullen welke gegevens er precies gecompromitteerd werden. Volgens de NOS is het "*niet meer te achterhalen wie er precies is afgeluisterd en welke informatie er precies is verkregen. Om daar achter te komen, was meer tijd nodig geweest. Maar dat kon niet, omdat Belgacom het netwerk zo snel mogelijk weer operationeel wilde hebben*". [236] Het is ook onduidelijk hoe lang het virus al aanwezig was. Op een persconferentie van 16 september 2013 zegt het hoofd van Belgacom dat "*hij geen enkel idee heeft"* van wanneer het virus zich op Belgacoms netwerk bevindt. Volgens *Der Spiegel* blijkt uit een (tot nu toe ongepubliceerd) document dat toegang mogelijk was sinds 2010.[237] Volgens *De Standaard* en de *NOS* was het virus al aanwezig sinds 2011. [238]

(65) Op 18 oktober 2013 meldt Belgacom dat doorgedreven controles nieuwe onregelmatigheden aan het licht brachten op een router bij BICS. "*Het eerste onderzoek wijst erop dat er wijzigingen zijn aangebracht in de software van de router, wat gebeurd kan zijn tijdens de recente digitale inbraak*".[239] Belgacom sloot niet meer uit dat gegevens van klanten zijn gehackt. "*Het lopende onderzoek zal moeten uitwijzen of er impact is geweest op de gegevens van klanten"*, aldus Belgacom in *Le Soir*.[240] Op 23 oktober bericht Belga dat ook

---

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

230 P. DE LOBEL en N. VANHECKE, *De Standaard*, 21 September 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. Zie http://www.youtube.com/watch?v=ayR6CAuNE4w

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

235 Belgacom GCHQ Affair - EP/LIBE hearing on surveillance 3 October 2013, verkrijgbaar op 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 september 2013 ("NSA verdacht van hacken Belgacom").

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

240 X., Belga, 19 oktober 2013 ("Belgacom sluit hacking gegevens klanten niet meer uit").

Tecteo het slachtoffer is geworden van een cyberaanval die gelijkaardig lijkt te zijn aan die op telecomoperatoren Belgacom, France-Telecom en Wanadoo. Dat zegt het bedrijf. Het is momenteel nog te vroeg om te zeggen of er informatie is gehackt bij de groep of bij de filialen VOO of RESA.[241]

### II.4. Britse inspanningen tegen encryptie

(66) De Britse tegenhanger van het BULLRUN-programma (zie para 45) werd EDGEHILL genoemd. Documenten die *The Guardian* kon inkijken suggereren dat de UK nog niet zo ver staat als de VS en slechts op een *case-by-case* basis informatie kon decrypteren. Het oorspronkelijke doel van EDGEHILL was om de geëncrypteerde internettrafiek van drie grote internetbedrijven te ontcijferen en 30 VPN-types. Tegen 2015 hoopte GCHQ de geëncrypteerde internettraffiek van 15 grote internetbedrijven ontcijferd te hebben, en 300 VPN-types.[242] Een ander programma, genaamd CHEESY NAME, was erop gericht om bepaalde encryptiesleutels (bekend als *certificates*) te kraken met behulp van GCHQ 'supercomputers'.[243] GCHQ richtte ook een *Humint Operations Team* (HOT) op dat verantwoordelijk is voor het identificeren, rekruteren en runnen van informanten (*covert agents*) in the globale telecom industrie, onder andere om zo toegang te krijgen tot bepaalde sleutels.[244]

(67) Documenten die in een programma van Fantastico werden getoond, suggereren dat GCHQ's *network exploitation unit* programma's gebruikten (FLYING PIG en HUSH PUPPY) die TLS/SSL netwerken konden monitoren. De programma's lijken te zijn opgestart omdat steeds meer e-mailproviders zoals Yahoo, Google of Hotmail, SSL-encryptie gebruikten waardoor die berichten niet meer leesbaar waren via de directe *upstream* collectie. Minstens één document toont dat zowel de NSA als GCHQ hun toevlucht zochten tot *man in the middle attacks* om de encryptie te omzeilen.[245] FLYING PIG lijkt ook informatie te kunnen tonen over het gebruik van Tor (Tor Events).[246]

---

241 X., *Belga*, 23 oktober 2013 ("Ook Tecteo slachtoffer van spionage").

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*." In: http://www.theguardian.com/commentisfree/2013/sep/06/nsa-surveillance-revelations-encryption-expert-chat. *The Guardian* meldt ook het volgende : "*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.*

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*.

(68) Een document van 10 oktober 2012 beschrijft hoe GCHQ in operatie MULLENIZE erin geslaagd is via *user agent staining* individuele gebruikers te herkennen op een IP-adres dat simultaan gebruikt wordt door veel gebruikers. Dat is bijvoorbeeld het geval in een internet café, maar ook in bepaalde regio's gebruiken duizenden gebruikers ook één IP-adres. De techniek staat ook toe om individuele Tor-gebruikers te herkennen. In een periode van twee maanden slaagde GCHQ er in om op deze manier ongeveer 200 computers te besmetten met unieke *stains*.[247]

# III. OPSOMMING VAN DE IN OPEN BRONNEN VERSCHENEN CASUSSEN VAN SPIONAGEACTIVITEITEN TEN AANZIEN VAN POLITIEKE ACTIVITEITEN VAN ZOGENAAMDE 'BEVRIENDE LANDEN'

## III.1. (Vermeende) spionageactiviteiten los van de Snowden-*case*

(69) In deze lijst wordt gefocust op het bespioneren van bevriende landen door de VS of de UK Het bespioneren van Europese landen die deel uitmaakten van het Warschau Pact tijdens de Koude Oorlog worden niet meegeteld. De historische voorbeelden zijn illustratief.

(70) De Britse historicus Richard Aldrich heeft beschreven hoe de voorloper van GCHQ sinds 1940 de diplomatieke communicaties afluisterde van haar geallieerde partners, onder andere de Vrije Fransen onder leiding van De Gaulle, Turkije, Spanje en een twintigtal andere landen.[248] Op *adhoc* basis werd diplomatieke informatie uit Italië, Frankrijk, Spanje, Portugal, Japan en West-Duitsland met de VS gedeeld.[249]

(71) Op 21 februari 1967 onthulde de Britse krant de *Daily Express* hoe bedrijven zoals Western Union en Cable & Wireless alle internationale telegrammen en telexen, inclusief materiaal van buitenlandse ambassades, naar de Britse overheid bracht, waarop deze gekopieerd werden. Volgens Aldrich ging deze traditie terug tot WO I – en had het VK dus voor een periode van meer dan vijftig jaar toegang tot alle diplomatieke verkeer van alle ambassades vanop haar grondgebied.[250]

(72) Volgens Aldrich onderschepte de Nederlandse dienst diplomatieke communicaties van België en Duitsland in de jaren 1980.[251]

(73) In 2006 kwam het 'top secret' jaarrapport van 1985-1986 boven water van het Government Communications Security Bureau (GCSB), Nieuw Zeeland's sigint agentschap. Het rapport vermeldde de landen en agentschappen die Nieuw Zeeland dat jaar bespioneerd had, inclusief diplomatieke communicaties van de VN, Egypte, Japan, de Filippijnen, verschillende eilanden in de Stille Oceaan, Frankrijk, Vietnam, de Sovjet Unie, Noord Korea,

---

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

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

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

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

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

Oost Duitsland, Laos en Zuid Afrika.[252] De Franse geheime dienst had in 1985 de 'Rainbow Warrior' van Greenpeace doen zinken, en de GCSB schakelde dat jaar de hulp in van de NSA en GCHQ om bronnen in Frankrijk te bespioneren.[253]

(74) Alastair Campbell, Director of Communications and Strategy voor Tony Blair tussen 1997 en 2003 beschreef in zijn memoires hoe Britse veiligheidsagenten twee 'bugs' ontdekten in de hotelkamer die bedoeld was voor Tony Blair tijdens zijn bezoek aan New Delhi in oktober 2001.De bugs werden toegeschreven aan de Indische geheime dienst.[254]

(75) In 1999 verschenen er verschillende rapporten in de Amerikaanse pers die stelden dat zowel de NSA als GCHQ de UNSCOM-missie met wapeninspecteurs van de VN hadden geïnfiltreerd om gevoelige sigint-operaties te ondernemen in Irak. Niet alle informatie die op deze manier gevonden werd, werd gedeeld met UNSCOM.[255] Volgens VN-hoofdinspecteur Hans Blix, was dergelijke informatie uiterst valabel voor een potentiële latere inval. [256]

(76) In 2003 publiceerde *The Observer* een volledige memo van de NSA aan GCHQ waarin het die laatste om hulp vroeg om de toenmalige niet-permanente leden van de VN-Veiligheidsraad (Angola, Kameroen, Chili, Bulgarije en Guinea) af te luisteren om inzicht te krijgen in de houding van die landen tegenover een potentiële resolutie van de Veiligheidsraad om een militaire interventie tegen Irak goed te keuren.[257]

(77) Rond hetzelfde tijdstip, in februari 2003, werd er in het Justus Lipsius gebouw van de Europese Raad afluisterapparatuur gevonden in die delen van het gebouw die gebruikt werden door de Britse, Franse, Duitse en Spaanse delegaties. Onderzoek suggereerde dat de apparatuur al in het gebouw was geplaatst sinds haar constructie in 1993. Hoewel nooit onomstotelijk bewezen, wezen een aantal indicatoren in de richting van Israël als de verantwoordelijke voor de spionage.[258]

(78) In 2004 verklaarde voormalig Brits minister Clare Short op BBC Radio 4's Today programma dat ze regelmatig sigint had gehoord waarop conversaties van VN Secretaris Generaal Kofi Annan in zijn privé-kantoor in het VN-hoofdkwartier in New York te horen waren net voor de oorlog in Irak begon in 2003.[259]

(79) In 2004 werd er afluisterapparatuur gevonden in het 'Salon Francais' in het Palais des Nations van de VN in Geneve. Het salon was een van de kamers die in september 2003

---

252 H. BAIN, *Sunday Star*, 15 januari 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 januari 1999 ("US used UN to spy on Iraq, aides say"); B. GELLMAN, *The Washington Post*, 6 January 1999 ("Annan suspicious of UNSCOM probe").

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

257 De memo stelde verder: "*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 maart 2003 ("US plan to bug Security Council: the text"). Zie ook http://www.theguardian.com/world/2003/mar/02/iraq.unitednations1

258 Zie onder meer VAST COMITÉ I, *Activiteitenverslag 2010,* Intersentia, Antwerpen, 2010, 6-14.

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

gebruikt werden om private onderhandelingen te voeren over de kwestie Irak. Er werd nooit een verantwoordelijke gevonden.[260]

(80) In december 2004 werd er gesuggereerd dat de NSA tientallen telefoongesprekken van Mohamed ElBaradei, het hoofd van het Internationale Atoomagentschap (IAEA), met Iraanse diplomaten had afgeluisterd. De *Washington Post* suggereerde dat er naar materiaal werd gezocht om ElBaradei af te zetten als hoofd van het IAEA.[261]

### III.2. Onthullingen uit de Snowden-documenten

(81) Volgens *Der Spiegel* wordt er vanuit 80 Amerikaanse ambassades en consulaten clandestien sigint onderschept door de Special Collection Service.[262] Dit team is ook verantwoordelijk voor top-secret surveillance-operaties in andere ambassades en consulaten die bij de NSA gekend zijn onder de naam STATEROOM.[263]

(82) *Der Spiegel* beschreef in wat voor soort informatie de NSA geïnteresseerd is inzake de EU. EU informatie die gerelateerd is aan de economische stabiliteit en handelspolitiek kreeg een '3' op een prioriteitenschaal van 1 (hoogste interesse) tot 5 (laagste interesse). Informatie die gerelateerd was aan energy security, voedselproducten en technologische innovatie kreeg een 5.[264] Der Spiegel gaf details vrij over hoe de NSA de 'ambassador's room' bespioneerde op de 31ste verdieping van de EU's delegatie aan de VN in New York, die bij de NSA gekend is onder de codenaam 'Apalachee'. De NSA had toegang tot de bouwplannen van het gebouw, en infiltreerde het interne VPN-netwerk tussen de EU-missie aan de VN in New York en Washington. Die laatste stond gekend onder de codenaam MAGOTHY. Zowel de EU-missies in Washington en New York werden afgeluisterd. In de EU-missie in New York werden ook harde schijven gekopieerd, en in Washington werd het interne computernetwerk geïnfiltreerd.[265]

(83) De NSA is bij de VN vooral geïnteresseerd in alles wat te maken heeft met wapencontrole in de IAEA (prioriteit 1), buitenlandse politiek (prioriteit 2) en mensenrechten, oorlogsmisdaden, milieuzaken en ruwe materialen (allen prioriteit 3). De NSA heeft een eigen team in de VN die onder cover van diplomaat werken. Ze worden versterkt door een team uit Washington voor iedere sessie van de Algemene Vergadering.

---

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

261 D. LINZER, *The Washington Post*, 12 december 2004 ("IAEA Leader's phone tapped"). El Baradei had de Amerikaanse intelligence inzake Irak ernstig betwijfeld, en nam in die periode ook een zeer voorzichtige houding aan ten opzichte van Iran.

262 Zie paragraaf 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

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

De NSA luisterde ook mee naar de videoconferenties van VN-diplomaten.[266]

(84) Der Spiegel onthulde ook het ontstaan van het RAMPART-T programma waaronder de NSA sinds 1991 de communicaties van staatshoofden en hun directe omgeving uit meer dan twintig landen onderschept om de President en zijn national security adviseurs beter te kunnen informeren. Der Spiegel meldde dat niet alleen doelwitten in China en Rusland geviseerd werden, maar ook in Oost-Europese staten.[267]

(85) The Guardian meldde dat de 38 ambassades en missies als doelwitten beschouwd werden in een NSA-document van september 2010. Daar zijn geen West-Europese gebouwen bij, maar wel de eerder genoemde EU-missies, en de ambassades van de Frankrijk, Italië en Griekenland, alsook de ambassades van Japan, Mexico, Zuid Korea, India[268] en Turkije. Ook de Franse en Griekse missie bij de VN werden bespioneerd. [269] Le Monde gaf op 18 Oktober een document vrij dat aangaf dat 'close access' collectie op Amerikaans grondgebied tegen buitenlandse diplomatieke doelwitten bekend stond als SIGAD US-3136. Een suffix van twee letters daarnaast duidt op de specifieke locatie en missie. Het document van 10 September 2010 beschrijft een 15-tal manieren waarop informatie kon worden verkregen.[270] 'Close acces' collectie van diplomatie bronnen buiten de VS staat bekend als SIGAD US-3137 met een suffix van twee letters.

(86) *Der Spiegel* beschreef verder hoe de NSA informatie uit de Franse diplomatie exploiteert. Een intern NSA-document uit juni 2010 beschreef hoe de NSA succesvol toegang had verkregen tot het VPN-netwerk van het Franse Ministerie van Buitenlandse Zaken, dat alle Franse ambassades en consulaten verbind met Parijs, en (interne) sub-domeinen van de 'diplomatie.gouv.fr' URL. NSA-agenten installeerden *bugs* in de Franse ambassade in Washington en in de Franse missie in New York. Nog steeds volgens *Der Spiegel*, is de NSA is

---

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 Voor meer info zie S. SAXENA, *The Hindu,* 25 September 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 operatoins; jumping the airgap etc.; 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. Tegen de Franse missies werden bijvoorbeeld de HIGHLAND, VAGRANT en PBX technieken gebruikt.
https://www.documentcloud.org/documents/807030-ambassade.html#document/p1

vooral geïnteresseerd in Frankrijks buitenlandse politiek, vooral wapenhandel, en Frankrijks economische politiek.[271]

(87) Een document van 17 mei 2006 dat gepost werd op de website van Globo meldde dat de International Security Issues (ISI) missie binnen de NSA verantwoordelijk is voor dertien individuele staten in drie continenten. Die dertien landen hebben met elkaar gemeen dat ze belangrijk zijn voor de VS inzake economie, handel en buitenlandse politiek. De 'Western Europe and Strategic Partnerships division' binnen die missie focust zich voornamelijk "*op de buitenlandse politiek en handelsactiviteiten van België, Frankrijk, Duitsland, Italië, Spanje als ook Brazilië, Japan en Mexico*". Deze divisie geeft ook *key intelligence* over 'militaire en intelligence activiteiten in enkele van deze landen'. De 'Aegean and Ukraine division' houdt zich bezig met alle aspecten van Turkije - 'governmental/leadership, military and intelligence'. ISI werkt samen met F6 en *second and third party* buitenlandse partners die zowel 'waardevolle analytische inzichten als technische capaciteiten' bevatten.[272] Volgens *Le Monde* verwijzen nummers die beginnen met US-98 (zoals US- 985D (Frankrijk), US-987 (Duitsland)) naar SIGADS op het territorium van *third party* partners van de NSA. Die bestaan volgens *Der Spiegel* onder meer uit Frankrijk, Duitsland, Oostenrijk, Polen en België.[273] Hetzelfde document maakte melding van het feit dat de 'ISI' actief samenwerkt met de "*Combating Proliferation (CP, S2G) and Counterterrorism (CT, S2I) product lines to incorporate financial intelligence analysis into their mission build-out plans*".[274]

(88) Een document van augustus 2010 bevestigt dat de NSA de communicaties onderschepte van acht leden van de VN Veiligheidsraad. Alleen Frankrijk, Japan, Mexico en Brazilië werden expliciet genoemd. Doel was om de US missie aan de VN (en andere Amerikaanse diensten) van de meest *up-to-date* informatie te voorzien over hun stemintenties en onderhandelingsposities over een VN-resolutie over sancties tegen Iran.[275]

(89) Een bericht in *Globo* bevestigde hoe de NSA Latijns-Amerikaanse landen als Mexico, Venezuela, Argentinië, Colombia, Ecuador, Panama, Costa Rica, Nicaragua, Honduras, Chili, El Salvador en Peru bespioneerde. De NSA was geïnteresseerd in de olie-politiek van Venezuela, de energie- en drugspolitiek van Mexico en de Colombiaanse positie tegenover de FARC. Door het gebruik van XKEYSCORE kon een 'buitenlander' opgespoord worden door de taal die hij gebruikte om te communiceren.[276]

---

271 X., *Der Spiegel*, 1 september 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*." In: http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html In die zin is het misschien interessant om op te merken dat volgens sommige bronnen van *De Standaard* er problemen zouden zijn vastgesteld bij de FOD Financiën, waarbij onderzocht werd of het om dezelfde malware als bij Belgacom gaat. Topman Hans D'Hondt van Financiën sprak echter formeel tegen dat zijn diensten gehackt of besmet zouden zijn. In: N. VANHECKE, P. DE LOBEL, *De Standaard*, 4 oktober 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

(90) Een top-secret document uit November 2010, gepubliceerd door *Der Spiegel*, toont dat de NSA's TAO-divisie geslaagd was in operatie FLATLIQUID om toegang te krijgen tot de publieke e-mail account van de toenmalig Mexicaanse president Felipe Calderon om *"inzicht te krijgen in Mexico's politieke systeem en interne stabiliteit"*. De account werd ook gebruikt door leden van Calderon's kabinet.[277] Gedurende een periode van twee weken in de vroege zomer van 2012 lanceerde de NSA ook een intensieve 'structurele surveillance' campagne tegen huidig president Enrique Pena Nieto. Op basis van zijn communicatiepatronen werd bepaald wie negen van zijn dichtste adviseurs waren. De gegevens van deze personen werden in de DISHIRE database gestoken, waarna ook hun communicaties onderschept werden. Op die manier werden bijvoorbeeld 85.489 sms'en onderschept. Doel van de operatie was om te bepalen of Mexico een nieuwe strategie zou aannemen vis-a-vis de drugskartels.[278] De NSA is vooral geïnteresseerd in de drughandel (niveau 1), de leiders van Mexico, Mexico's economische stabiliteit, militaire capaciteiten, mensenrechten en internationale handelsrelaties (niveau 3) en contraspionage (niveau 4). Om die doelen te bereiken voerde TAO in augustus 2009 'Operatie Whitetamale', waarmee het toegang kreeg tot de e-mails van verschillende hoge ambtenaren in Mexico's 'Public Security Secretariat' dat zich onder andere bezighoudt met drugshandel en mensenhandel. Via operatie EVENINGEASEL tapte de SCS divisie van de NSA vanuit de ambassade in Mexico stad telefoonconversaties af en las het sms'en die verstuurd werden via Mexico's mobiele telefoonnetwerk.[279]

(91) Het Braziliaanse nieuwsprogramma Fantastico op de zender *Globo* toonde een slideshow waarin de communicatiepatronen tussen Braziliaans president Dilma Roussef, haar voornaamste adviseurs en derden werden getoond.[280] Volgens Glenn Greenwald had het desbetreffende NSA programma toegang tot het volledige communicatienetwerk van de Braziliaanse presidente en haar staff in kaart te brengen, inclusief telefoonconversaties, e-mails en uitwisselingen op sociale netwerk sites.[281]

(92) DNI Clapper reageerde door te zeggen dat het 'geen geheim is dat de Intelligence community informatie verzamelt over economische en financiële zaken, en de financiering van terrorisme'. Volgens Clapper verzamelt de VS dit soort informatie onder meer om de VS en haar partners *early warnings* te geven over internationale financiële crisissen die een negatief effect zouden kunnen hebben op de wereldeconomie.[282]

---

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

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

281 Y. MARULL, *AFP*, 2 september 2013 ("Brazil, Mexico summon US envoys over spy claims"). Een vertegenwoordiger van het State Department zei: "*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 september 2013, zie: 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*

(93) Een dag later melde Fantastico dat de NSA ook het interne computernetwerk van de Braziliaanse oliemaatschappij Petrobras als een spionagedoelwit zag. Een presentatie uit mei 2012 die als doel had om nieuwe NSA-agenten op te leiden in manieren om toegang te verkrijgen tot private computernetwerken, vermeldde de maatschappij als doelwit. Het is niet duidelijk welke informatie precies werd gezocht of verkregen, maar *Globo* suggereert dat dit over informatie kon gaan zoals details over de meest waardevolle ongeëxploiteerde olievelden die binnenkort door Petrobras zouden aangeboden worden in een veiling, of over informatie over *state-of-the art ocean-floor exploration* technologie. De presentatie werd (nog) niet online gezet.[283] Dezelfde presentatie melde ook dat Google, Franse diplomaten die toegang hadden tot het privé netwerk van het ministerie van Buitenlandse Zaken van Frankrijk[284] en SWIFT gezien werden als doelwitten.

(94) Een GCHQ-slideshow toont hoe GCHQ data verzamelde van de smartphones, inclusief Blackberries, van verschillende diplomatieke delegaties op de G20 meeting in Londen in 2009.[285] Die data kon bijna in 'real time' doorgestuurd worden naar analisten, die briefings konden maken voor Britse ministers, inclusief Gordon Brown.[286] Op basis van deze informatie werden ook twintig nieuwe 'e-mail selectors' gevonden.[287] GCHQ ging heel ver om dergelijke diplomatieke informatie in te winnen. Zo werd een vals internetcafé opgezet waar *key-loggers* alles konden zien wat een délégué intypte op een computer. Een ander document toonde aan dat GCHQ succesvol het netwerk van het Zuid-Afrikaanse Ministerie van Buitenlandse Zaken had gekraakt, waardoor onder meer briefings onderschept konden worden voor délégués op de G20 en G8 meetings. Ook wordt melding gemaakt van GCHQ-pogingen om geëncrypteerde telefoongesprekken van Medvedev en andere Russische délégués te onderscheppen wanneer deze zich in Londen bevonden. GCHQ bespioneerde ook de Turkse Minister van Financiën op de meeting, alsook vijftien andere leden van zijn delegatie. GCHQ probeerde ook een nieuwe techniek uit op de meeting die het telefoonverkeer van alle deelnemers in kaart bracht.[288]

(95) De UK plande een operatie om verschillende delegaties op de Commonwealth 'Heads of Government' meeting te bespioneren in Trinidad in 2009 om de UK extra diplomatieke informatie te geven. Een document beschrijft bijvoorbeeld hoe sigint moest verzameld

---

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

286 Gordon Brown zat de G20 voor en wou vooruitgang boeken op twee fronten: de coordinatie van de globale economisch heropleving om een nieuwe recessie te voorkomen en een overeenkomst om *global economic governance* te versterken en internationale financiële institutions te hervormen.

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

worden over Zuid Afrika's opinie over Zimbabwe vooraleer Prime Minister Brown een ontmoeting had met Zuma. Het is niet duidelijk of er effectief sigint verzameld werd.[289]

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

**BIJLAGE: AFKORTINGEN EN BEGRIPPEN**

| | |
|---|---|
| 1EF solution | One-End Foreign solution |
| ADIV | Algemene Dienst inlichting en veiligheid |
| AG | Attorney General |
| BICS | Belgacom International Carrier Services |
| BIPT | Belgisch Instituut voor Postdiensten en Telecommunicatie |
| 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 van de FBI |
| DNI | (1) Director of National Intelligence in de V.S. (James Clapper),<br>(2) Digital Network Intelligence |
| DNR | Dialed Number Recognition |
| ECI | Exceptionally Controlled Information |
| EO 12333 | Executive Order 12333 |
| ECI | Exceptionally Controlled Information |
| 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 | De SIGINT-agentschappen van de V.S., de U.K, Australië, Canada en Nieuw Zeeland |
| Fornsat | Informatie afkomstig van satellieten |
| FTC | Federal Trade Commission |
| FRA | Försvarets radioanstalt (Zweeds SIGINT-agentschap) |
| F6-sites | Diplomatieke en consulaire missies van de VS |
| GAO | Global Access Operations-divisie (NSA) |
| GCHQ | Government Communications Headquarters (UK) |
| HOT | Humint Operations Team |
| IM | Instant Messaging |
| ISA | Intelligence Services Act (UK) |
| ISC | Intelligence Security Committee |
| Metadata | Metadata – soms ook ‘communications data’ of ‘traffic data’ genoemd, is de informatie die gecreëerd wordt wanneer data verzonden wordt. De precieze inhoud is afhankelijk van het type data dat verzonden wordt en hangt ook soms af van de lokale wetgeving. |

- Voor vaste telefoonlijnen: nummers die gebeld werden via dat toestel, alsook de datum en de tijd waarop een nummer gebeld en opgebeld werd. Soms ook de naam en het adres van de persoon die het contract van de vaste lijn heeft afgesloten.
- Mobiele telefoons: (1) nummers die gebeld of ge-sms’t werden via dat toestel, (2) de datum en de tijd waarop een nummer gebeld of opgebeld werd of een sms stuurde of ontving, (3) de locatie van waar er gebeld of ge-sms’t werd, en waar die communicatie ontvangen werd. (4) Soms ook de naam en het adres van de persoon die het contract van de vaste lijn heeft afgesloten. (5) Soms ook het International Mobile Subscriber Identity (IMSI) nummer en (6) het International Mobile station

Equipment Identity (IMEI) nummer. (6) Soms ook de nummer van de telefoonkaart die gebruikt werd.

- Voice over Internet Protocol (VoIP), e-mail, chat, Facebookberichten : (1) online gebruikersnaam, login naam of accountnaam waarmee iemand belt, gesprekken ontvangt, e-mails verzendt, chatberichten verstuurd (2) het IP adres van de computers die gebruikt werden, (3) de tijd en datum van de communicatie. Sommige landen lijken ook de onderwerp-lijn van e-mails als metadata te zien.
- Internet surfgedrag: (1) IP adres van het toestel waarmee iemand online gaat (2) de tijd en datum van het in- en uitloggen, en een lijst van webdomeinen die bezocht werden.

| | |
|---|---|
| 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 |
| SHAPE | Supreme Headquarters Allied Powers Europe |
| SIGAD | Signals activity/address designators – kunnen verwijzen naar een specifiek fysiek collectieplatform (zoals bijvoorbeeld een Amerikaanse legerbasis in het buitenland, een ambassade, een schip..), een virtueel dataverwerkingsplatform (PRISM staat bijvoorbeeld bekend als SIGAD US-984XN) of een ruimtesatelliet. |
| SIGINT | Signals Intelligence |
| 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 |
| TIDE | Terrorist Identities Datamart Environment |
| VoIP | Voice over Internet Protocol |
| VPN | Virtual Private Network |
| VTC | Video teleconferencing systeem |
| XKS | Xkeyscore |