NSA

Globale Überwaching und Demokratie?

Leon Bentrup

8. Dezember 2015

Inhaltsverzeichnis

1 Vorwort

Dass Geheimdienste Telefongespräche und Internetverkehr überwachen, hatte ich eigentlich nie bezweifelt. Was das wirklich bedeutet, das wurde mir aber erst vor zwei Jahren bewusst.

Als im Juni 2013 auf einmal eine ganze Ladung an Informationen über geheime Projekte des amerikanischen Geheimdienstes NSA in den Medien auftauchten, als man langsam begriff, dass es sich dabei um etwas richtig Großes handelt, da spürte ich das ungute Gefühl, dass auch bei meinen Recherchen zu dieser GFS immer wieder auftauchte.

Es fühlt sich an, als könnte man den Schlag in die Magengrube der Freiheit spüren, den die totale Überwachung jedes Menschen der Welt darstellt.

Was im Nachhinein auch völlig logisch ist, mich aber trotzdem beunruhigt, ist die Normalität, die innerhalb der Geheimdienste herrscht. Man muss sich klar machen: Analyst, die Berufsbezeichnung für die „modernen Spione“, die die abgefangenen Daten auswerten, ist ein ganz normaler Job. Analysten wechseln Arbeitgeber und haben LinkedIn-Profile mit Lebensläufen.

Manche Dokumente zeigen Geheimdienste eher als Unternehmen, statt als geheime Organisation: Es gibt Newsletter mit „Wusstest du schon?”-Artikeln, die die Mitarbeiter über die Geschichte des ECHELON-Programms aufklären, für das Anwenden neuer Spionage-Techniken bekommen Mitarbeiter „Skillz-Points“. In anderen Worten: Die Digitalisierung der Welt hat „Spion” zu einem Bürojob gemacht.

2 Edward Snowden

Edward Snowden ist die zentrale Persönlichkeit der Enthüllungen. Nach langjähriger Arbeit in verschiedenen Einrichtungen der amerikanischen Regierung sammelte er eigenständig Millionen von Beweisen für geheime Programme der NSA und anderer Geheimdienste, die er dann durch die Medien an die Öffentlichkeit brachte.

2.1 Lebenslauf

Edward Snowden wurde am 21. Juni 1983 geboren. Da seine beiden Eltern für die Regierung arbeiteten, war es für ihn „normal“, das gleiche zu tun.[28] Nach seiner Schulzeit trat er 2004 der U.S.-Army bei, mit dem Ziel, in Irak zu kämpfen. Als er

Abbildung 1: Edward Snowden bei seinem Interview mit Greenwald [10]

nach 3 Monaten bei der Armee einen Trainingsunfall hatte, verließ er sie wieder.[28] Er arbeitete danach für einige nicht-geheime Einrichtungen der Regierung, bis er 2006, beim Besuch einer Jobmesse, von der CIA rekrutiert wurde, wo er unter anderem bei einem internationalen Treffen 2008 in Genf eingesetzt wurde. [28]

2009 wechselte er zu DELL, er kümmerte sich um die Computersysteme von Regierungskunden, darunter auch Systeme der NSA und CIA. Sein Einkommen in dieser Position betrug etwa 200 000$ im Jahr. Schon dort bekam er Einsicht in einige streng geheime Operationen der NSA und sammelte schon einige Dokumente als Beweis.[28]

Seinen endgültigen Beschluss, die Handlungen der NSA und anderer Geheimdienste an die Öffentlichkeit zu bringen, fasste er 2013. In einem Interview sagte Snowden, dass der 12. März 2013 ausschlaggebend für seine Entscheidung gewesen sei. Dort wurde der Director of National Intelligence (nationaler Geheimdienstdirektor) der USA zur Überwachung von Amerikanern befragt, und log die Mitglieder des Kongresses an, obwohl er unter Eid stand.[28][9]

Daraufhin gibt Snowden seinen Job bei DELL auf und wechselte zur Dienstleistungsfirma Booz Allen Hamilton, die Personal für die NSA zur Verfügung stellte. Er war im Geheimdienst offiziell als Systemadministrator tätig, und hatte somit uneingeschränkten Zugriff auf alle Akten des Geheimdienstes. Snowden sagte, dass zu seinen Aufgaben aber auch das Überprüfen und Angreifen feindlicher Computersysteme zählte. Seine Position nannte er „Systems Analyst" [9]

2.2 Enthüllungen

Australien	15 000 Dokumente
Vereinigtes Köngreich	58 000 Dokumente
Department of Defense	960 000 Dokumente
National Security Agency	1 700 000 Dokumente
	ca. 2 700 000 Dokumente

Abbildung 2: Zahl der von Snowden gesammelten Dokumente [28]

Auch wenn Snowden wollte, dass die geheimen Operationen der NSA an die Öffentlichkeit geraten, war er nicht generell gegen Überwachung. Nur solle Überwachung gezielt und auf Verdacht stattfinden, und nicht so massenhaft, wie die NSA es betreibt.[28][9]

Da er also wichtige Operationen der Geheimdienste, zum Beispiel die Überwachung von bekannten Terrororganisationen, nicht gefährden wollte, musste er beim Veröffentlichen der gesammelten Dokumente vorsichtig sein. Er sichtete zunächst selbst alles und sortierte Teile aus, die nichts mit der von ihm kritisierten Massenüberwachung zu tun hatten.[28][9]

Außerdem veröffentlichte er die Dokumente nicht selbst, sondern übergab sie der Filmemacherin Laura Poitras und dem Journalisten Glenn Greenwald. Sie sollten die Dokumente dann über die Medien an die Öffentlichkeit bringen.[28][9]

Abbildung 3: Laura Poitras [15]

Abbildung 4: Glenn Greenwald [2]

2.2.1 Laura Poitras

Laura Poitras, geboren am 2. Februar 1964 in Boston, ist Produzentin und Filmemacherin. Sie arbeitet seit 2005 an einer Filmreihe über die Welt nach dem 11. September 2001. Nachdem sie den ersten Film der Trilogie veröffentlicht hat, wird sie regelmäßig an der amerikanischen Grenze kontrolliert und befragt. Aus diesem Grund zieht sie nach Berlin um, als sie mit ihrem Film „Citizenfour“ beginnt. Sie befürchtet, dass ihr Filmmaterial beschlagnahmt wird.[5][9]

2.2.2 Glenn Greenwald

Der amerikanische Journalist Glenn Greenwald, der am 6. März 1967 in New York geboren wurde, ist die zweite Person, die Snowden kontaktierte. Er studierte Philosophie und Rechtswissenschaften.[29] Von 1996 bis 2005 arbeitete er in einer eigenen Anwaltskanzlei, die sich auf Verfassungs- und Bürgerrechte (von US-Bürgern) spezialisierte.[26]

In seinen Blog „Unclaimed Territory“ schrieb Greenwald bis 2007 unter anderem über frühere Affären der NSA, bis er später zum Online-Magazin „salon.com“ und schließlich im Juni 2012 zur britischen Tageszeitung „The Guardian“ wechselte. Im Guardian veröffentlichte Greenwald auch den ersten Artikel über das Snowden-Material.[29]

2014 gründete er zusammen mit Laura Poitras die Nachrichtenseite „The Intercept“.[8]

3 Überwachung

Aus den von Edward Snowden gesammelten Dokumenten gehen einige Informationen über Programme hervor, die eine massenhafte, globale Überwachung der digitalen Kommunikation ermöglichen.

Heute werden sämtliche Formen der Kommunikation über das Internet abgewickelt. Früher war das Internet noch ein Dienst, der über das Telefonnetz funktionierte, heute ist Telefonie ein Dienst, der über das Internet funktioniert. Der normale Internetverkehr läuft neben Festnetz und Mobilgesprächen, SMS, Fax, Fernsehen, den Bildern von Überwachungskameras und vielem weiteren über ein weltweites Netz von Glasfaserkabeln, die man Internet-Backbone („Rückenmark des Internets“) nennt.

Dies Bedeutet natürlich auch, dass ein Geheimdienst, der Zugriff auf das Internet erhält auch Zugriff auf sämtliche anderen Formen der Kommunikation erhält. Viele Programme der NSA beschäftigen sich aus diesem Grund auch genau damit.

3.1 XKeyscore

Die NSA sammelt auf unterschiedlichste Arten Daten: Partnerschaften mit Internetanbietern und Softwarefirmen wie Microsoft oder RSA, das Infiltrieren von Netzwerkhardware, aktivem Hacken von Systemen, Abhören von Funk- und Satellitenkommunikation und so weiter. Eine riesige Datenmenge, die natürlich nicht von Hand analysiert werden kann.

Das XKeyscore-System beschäftigt sich nicht mit dem Sammeln von Daten, sondern mit dem Auswerten von bereits gesammelten Daten. XKeyscore ist auch nicht nur ein einziges System, sondern es gibt mehrere Instanzen, die Nahe am Ort der Datenerfassung lokalisiert sind.[22] Es gibt aber die Möglichkeit eine Suchanfrage an alle XKeyscore-Systeme der Welt zu schicken.[21]

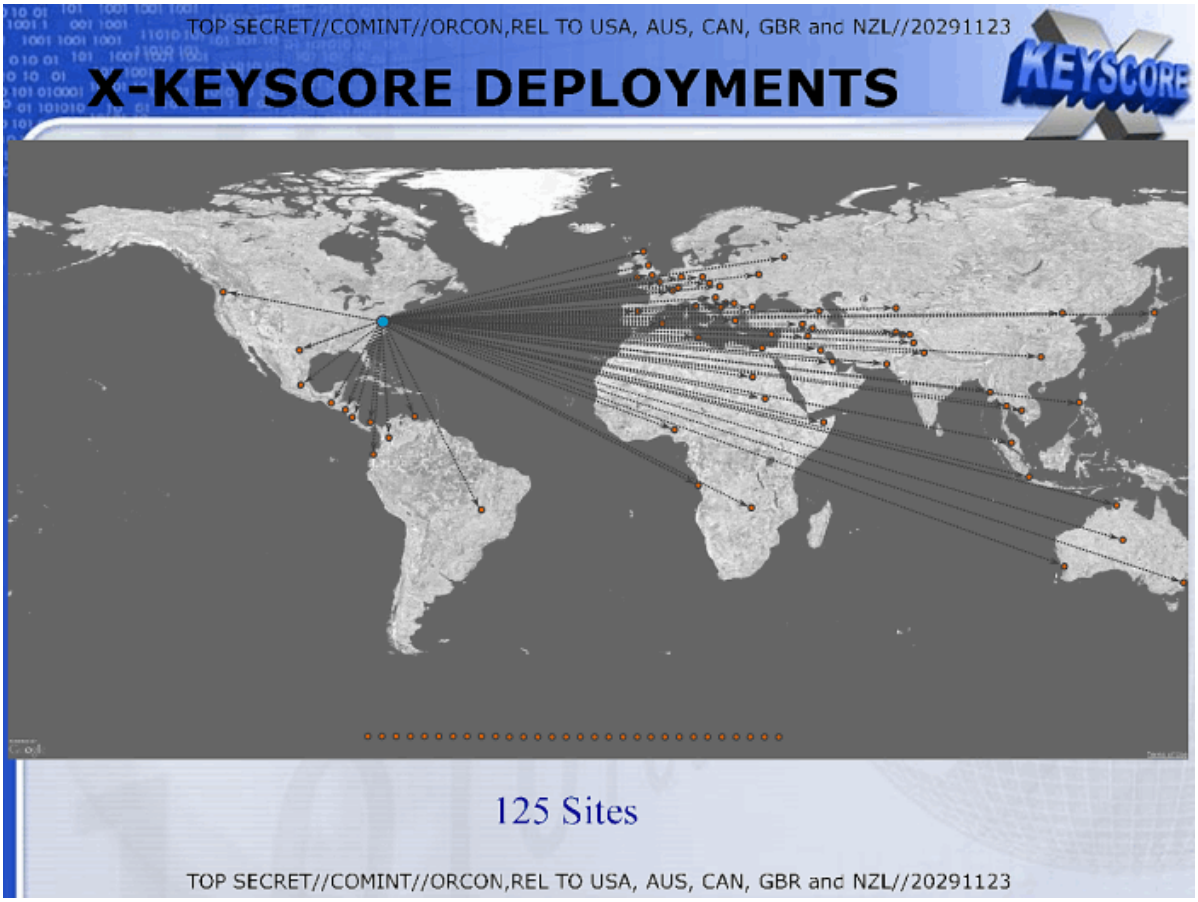

Abbildung 5: XKeyscore-Standorte. NSA-Präsentation [23]

Datenquellen Zunächst werden die Rohdaten von verschiedenen anderen NSA-Projekten und von Geheimdienstpartnern gesammelt. Von folgenden NSA-Operationen ist bekannt, dass sie als Quelle für XKeyscore dienen:

- **SCS** (Special Collection Service), Gezieltes Abhören, z.B. in Botschaften durch das Anbringen „klassischer“ Spionagewerkzeuge (Wanzen, Kameras, Telefonleitung anzapfen, etc.)[17] Zu diesem Projekt gehörte auch das Abhören des Handys von Angela Merkel.[13]

- **SSO** (Special Sources Operations), Kooperationen mit Internetanbietern, um direkten Zugriff auf deren Netzwerk zu erhalten. Dies geschieht entweder im Einverständnis des Anbieters, der dafür auch bezahlt wird, oder durch richterlichen Beschluss.[18]

- **ECHELON** (auch FORNSAT genannt), das Abhören von Satelliten und Funksignalen durch eine Vielzahl an Bodenstationen.[4] Auch die Bad Aibling Station in Bayern mit ihren vielen Antennen und Radomen zählte bis zu ihrer Übernahme durch den BND zu ECHELON.[4]

- **TAO** (Tailored Access Operations), Infiltrieren von Kommunikationssystemen. Die NSA hat eigene Software in Netzwerkequipment (z.B. Router) eingeschleust, mit denen sie Daten abhören, oder sogar eigene Daten in ein Netzwerk einschleusen und damit angeschlossene Geräte „hacken“ können.[14]

- **Overhead**, mehrere Spionagedrohnen, Satelliten und Flugzeuge hören Funkverbindungen ab, die ebenfalls in XKeyscore eingespeist werden.[32]

[24]

Indexieren der Daten Die antreffenden Rohdaten werden dann von einem Verbund aus mehreren leistungsfähigen Linux-Servern verarbeitet. Dabei wird zuerst unwichtiges herausgefiltert, z.B. Internetverkehr von Videoportalen.[19] Die restlichen Daten werden je nach Art von verschiedenen Plug-ins „indexiert“. So gibt es Plug-ins für E-Mails, Webseitenaufrufe oder Telefongespräche, die die Metadaten der Verbindungen (in XKeyscore „Sessions“ genannt) extrahieren und speichern.[20][22]

Speicherung Wie lange die gesammelten Daten gespeichert werden ist nicht bei jeder XKeyscore-Instanz gleich. Je nach untersuchter Datenmenge und Kapazität der Instanz wird der gesamte Internetverkehr mit Inhalt der Verbindungen für kurze Zeit (2-4 Tage) gespeichert, die Metadaten der Verbindungen sind etwa 30 bis 90 Tage lang abrufbar.[22]

Durchsuchen der Daten Über eine Weboberfläche steht berechtigten NSA-Mitarbeitern (Analysten) ein Suchformular zur Verfügung, über das sie auf die riesigen gesammelten Datenmengen zugreifen können.

In einer internen Präsentation der NSA finden sich folgende Beispiele für Suchanfragen, die mittels XKeyscore möglich sind:

- „Zeige mir Personen, die eine für die Region unübliche Sprache verwenden.“
- „Zeige mir alle verschlüsselten Word-Dokumente im Iran.“
- „Zeige mir alle mit PGP verschlüsselten E-Mails im Iran.“
- „Zeige den Ursprung eines Dokuments.“
- „Zeige mir alle von der NSA hackbaren Computer im Land X.“

(Übersetzt nach [22])

3.2 Five Eyes

Die NSA ging mit einigen anderen Geheimdiensten Partnerschaften ein. Darunter zählte auch der Deutsche Bundesnachrichtendienst.[3] Die „wichtigsten“ Partner waren allerdings:

- **GCHQ**, Government Communications Headquarters, *Vereinigtes Königreich*
- **DSD**, Defense Signals Directorate, *Australien*
- **CSEC**, Communications Security Establishment Canada, *Kanada*
- **GCSB**, Government Communications Security Bureau, *Neuseeland*

[31]

Zusammen mit der NSA selbst, nennen sich diese Geheimdienste die „Five Eyes”.[31] Das Abkommen zwischen den Five Eyes beinhaltete eine „No-Spy-Vereinbarung”, die Partner haben sich also gegenseitig nicht abgehört, es gab allerdings auch Außnahmen von dieser Regel. Außerdem teilten die Bündnispartner sämtliche gesammelten Daten und entwickelte Technologien.[31] So hatten alle Geheimdienste der Five Eyes Zugriff auf NSA-Programme wie XKeyscore oder PRISM.[31]

3.2.1 Umgehung von Beschränkungen durch die Verfassung

Das Five Eyes-Bündnis wurde auch genutzt um verfassungsrechtliche Beschränkungen zu umgehen. So darf das GCHQ zum Beispiel nach der Verfassung des Vereinigten Königreichs keinen britischen Staatsbürger abhören. Der amerikanische Geheimdienst NSA, der dies natürlich darf, hört dann für das GCHQ deren Ziel ab und gibt die gesammelten Daten an es weiter.[27]

3.3 TEMPORA

Zu den Technologien, die die Five Eyes untereinander weitergeben, gehört auch das Projekt des britischen GCHQ, „Tempora“. Hinter Tempora verbirgt sich eine Instanz des amerikanischen XKeyscore-Systems.[19]

Tempora ist das mit Abstand größte XKeyscore-System. Mehr als 1000 Server an mehr als 3 Standorten ermöglichen das Mitschneiden der Kommunikation über Glasfaserkabel.[19]

Großbritanniens geografische Lage ist für dieses Unternehmen sehr vorteilhaft. In Europa liegt es am nächsten zur amerikanischen Ostküste. Deshalb verlaufen fast alle Untersee-Glasfaserkabel zwischen Europa und Amerika durch Großbritannien. Über diese Glasfaserkabel werden alle Internet- und Telefonverbindungen zwischen den Kontinenten übertragen.[19]

Der GCHQ verschafft sich durch Abkommen mit den Betreibern der Internetknoten Zugang zu diesen Kabeln, und ist somit in der Lage 460 GBit/s[19] (Das 46 Millionenfache der durchschnittlichen Internetgeschwindigkeit in Deutschland[25]) an Daten in Echtzeit zu sammeln, zu sortieren und zu speichern. Die gesamte Kommunikation, mit Inhalt der Verbindungen werden für 3 Werktage gespeichert. Deshalb nennt der GCHQ das System auch einen „Internet Buffer”, einen Zwischenspeicher für das Internet, der die globale Kommunikation „verlangsamt” und im Nachhinein durchsuchbar macht.[19] Die Metadaten, also Sender, Empfänger, deren Aufenthaltsort und Informationen über deren Endgeräte, Betreff und Zeitpunkt der Nachrichten werden für 30 Tage gespeichert.[19]

4 Verhältnis zu Deutschland

Die NSA nannte Deutschland einen „Partner dritter Klasse“[3]. Das bedeutet, dass Deutschland, obwohl es ein Abkommen mit der NSA geschlossen hat, abgehört wird.[3]

Die NSA sammelt ungefähr so viele Datensätze über Deutschland, wie sie auch über China und Russland sammelt. (Siehe Abbildung 6)

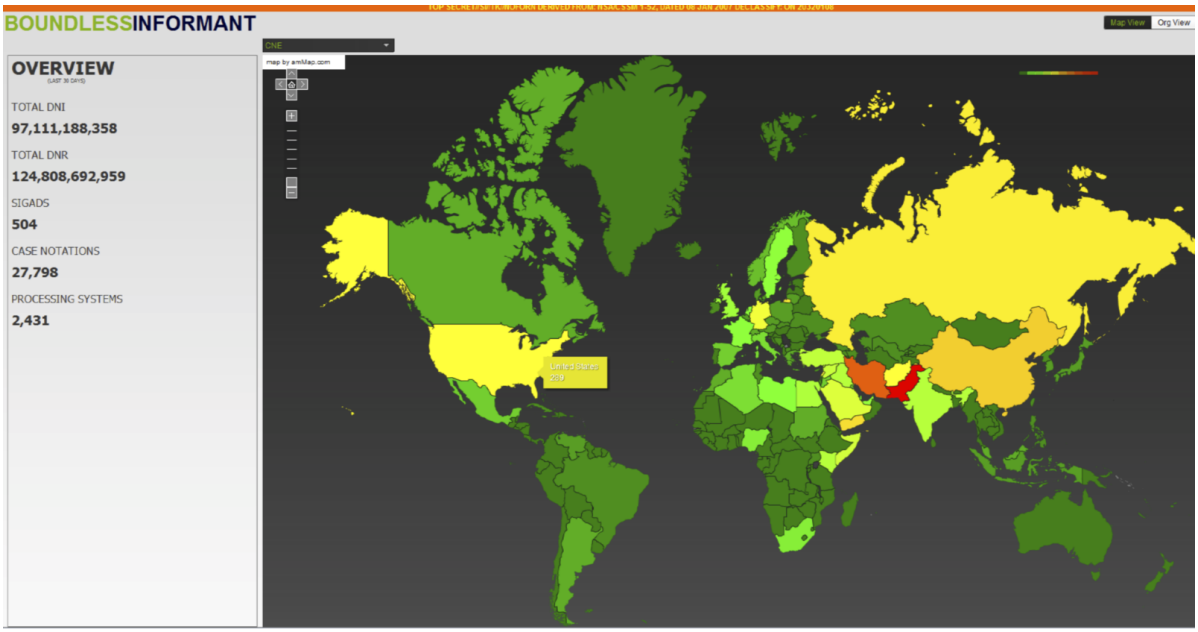

Abbildung 6: Übersicht über von der NSA gesammelten Daten nach Land (Boundless Informant)[16]

4.1 Partnerschaft mit der NSA

Die Rahmenbedingungen, die die Partnerschaft zwischen Bundesnachrichtendienst, Verfassungsschutz und der NSA kennzeichnen, sind in einem Dokument namens „Terms of Reference“ festgehalten.[33]

Die NSA übergibt dem BND das XKeyscore-System, welches dieser dann auf eigenen Servern einsetzen kann. Außerdem darf der BND das System an das Bundesamt für Verfassungsschutz weitergeben. Im Gegenzug gibt Deutschland so viele Daten wie möglich an die NSA weiter, falls diese für deren Ermittlungen relevant sein könnten.[33]

4.2 Operation Eikonal

Die wohl umstrittenste Operation des BND, die bei den Untersuchungen des NSA-Ausschusses im Bundestag bekannt wurde, ist die „Operation Eikonal“. [7]

Neben Großbritannien ist auch Deutschland ein wichtiger Standort des Internet-Glasfasernetzes in Europa. In Frankfurt am Main befindet sich der DE-CIX, der am Datendurchsatz gemessen, der größte Internetknoten der Welt ist.[1]

Zu einigen der vielen Glasfaserleitungen im DE-CIX verschaffte sich der BND Zugang. Er installierte so genannte „Taps“, die den Datenverkehr duplizieren, die Daten werden also zum einen an den Empfänger weitergeleitet, zusätzlich dazu, wird aber eine Kopie der Daten ausgeleitet.[30] Über eine Standleitung der Telekom wird dann ein Teil der so abgefangenen Daten in den BND-Standort in Pullach weitergeleitet, dort kann er analysiert werden.[7]

Auf diese Weise können natürlich nicht alle Daten übertragen werden, die am DE-CIX übertragen werden. Die Daten werden deshalb „selektiert”, das heißt, sie werden mit einer Liste von E-Mailaddressen, Telefonnummern, IP-Adressen, Namen und Benutzernamen abgeglichen, und nur relevante Daten werden dann weitergeleitet. Solch eine Liste erhielt der BND auch von der NSA, sie soll etwa 14 Mio. Selektoren enthalten haben.[11]

Darunter waren allerdings auch Selektoren, die deutsche Ziele beinhalteten. Deshalb wurde diese Liste nach BND-Angaben durch ein eigenes Filterungssystem, „Dafis” genannt aussortiert. Dabei wurden z.B. +49-Telefonnummern und E-Mailaddressen die in .de enden aussortiert. Wie die Selektoren wurden auch die Daten, die an die NSA weitergeleitet werden sollten durch dieses System gefiltert.[6]

Ob dieses Verfahren rechtmäßig ist, wurde schon von Anfang an bezweifelt, auch von Mitarbeitern des BND selbst. Denn das Dafis-Filtersystem soll nicht einwandfrei funktioniert haben. Man geht von einer Trefferquote von 95% aus was im Umkehrschluss bedeutet, dass 5% der Daten von Deutschen nicht vom System erkannt und somit zur NSA weitergeleitet wurden. Dies entspricht etwa 2 Terrabyte „grundrechtswiedriger“ Daten, die die NSA pro Stunden von den Deutschen erhält.[30] Deshalb wurde die Operation Eikonal angeblich 2008 eingestellt. Vor dem NSA-Untersuchungsausschuss sagte ein BND-Mitarbeiter:

> Eikonal beinhaltete selektive Erfassung von Ausland-Ausland-Transitverkehr. Zeit nicht vergessen: Afghanistan, Terror-Aufklärung. Da wurden selektiert Daten erfasst und automatisiert weitergeleitet. Genaueres nur nicht-öffentlich. Wir machen die Methodik ja immer noch.[30]

Es ist also fraglich, ob Eikonal 2008 wirklich eingestellt wurde.

5 Geheimdienste in Deutschland

> **Artikel 10, GG**
>
> (1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.
>
> (2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

Nach dem Grundgesetz ist die private Kommunikation prinzipiell geschützt. Wie in Absatz 2 beschrieben findet aber eine Einschränkung durch das „Gesetz zur Beschränkung des Brief-, Post-, und Fernmeldegeheimnisses“, kurz G-10-Gesetz statt. Dieses Gesetz ermöglicht Polizei und Geheimdiensten bei ihren Ermittlungen Verdächtige abzuhören.

Deutschland verfügt über drei Geheimdienste, jeder mit ganz bestimmten Aufgaben. Die Aufgaben und Befugnisse der Geheimdienste sind jeweils in einem Gesetz geregelt.

5.1 MAD

Der Militärische Abschirmdienst ist, wie der Name schon sagt, der Geheimdienst des Militärs. Seine Hauptaufgabe ist es, die Soldaten der Bundeswehr zu überprüfen (beispielsweise ob sie zu einer rechtsextremen Organisation gehören). Deshalb wird der MAD auch „Verfassungsschutz des Militärs“ genannt.[12]

Außerdem sichert der MAD Bundeswehreinsätze im Ausland und versorgt die Truppen dort mit Informationen.[12]

5.2 BfV

Das Bundesamt für Verfassungsschutz ist der Geheimdienst für das Innere. Der Verfassungsschutz hat zwei Aufgaben: Zum einen soll er extremistische oder verfassungsfeindliche Organisationen überwachen und kontrollieren, zum anderen soll er Deutschland vor Spionage durch das Ausland schützen.[12]

Der Verfassungsschutz verfügt über etwa 2800 Mitarbeiter. Er untersteht dem Bundesinnenministerium.[12]

5.3 BND

Der Bundesnachrichtendienst ist für das Ausland zuständig. Er soll Informationen über das Ausland und *im* Ausland sammeln. Damit soll er für politische Entscheidungen relevante Informationen beschaffen und Bedrohungen, beispielsweise durch internationale Terroristen abwehren.[12]

Mit etwa 6500 Mitarbeitern ist der BND der größte deutsche Geheimdienst. Er wird durch das Kanzleramt kontrolliert.[12]

6 Fazit

Edward Snowden hat mit seinen Veröffentlichungen gezeigt, zu was Geheimdienste in der Lage sind. In den USA waren natürlich die Anschläge vom 11. September 2001 ausschlaggebend für die dramatische Stärkung der Geheimdienste. Einige Jahre freier Entwicklung der Geheimdienste ohne strikte staatliche Kontrollen und wir sind im heutigen Stadium angelangt. Ein weltweites, nahezu lückenloses Netz, das so gut wie jeden Menschen erfasst.

Nach den Enthüllungen 2013 ist das Thema in den Fokus der Öffentlichkeit gerückt. Einige Posten sind geräumt worden, so musste General Keith Alexander, Director der NSA, den Geheimdienst verlassen. Es ist aber nicht davon auszugehen, dass sich am eigentlichen Problem, an der Methodik der Geheimdienste, nach der sie so viel wie möglich sammeln, statt gezielt vorzugehen, etwas ändern wird.

Die großen Geheimdienstprogramme werden weiterentwickelt. Und es werden neue dazukommen. Wenn ich mich entscheiden müsste, was wohl als nächstes in den Fokus der Überwacher rücken wird, würde ich sagen: Verschlüsselung. Bereits jetzt hat die NSA einige Fähigkeiten, wenn es darum geht Verschlüsselungssysteme zu umgehen. Sei es die enorme Rechenleistung, die im NSA-Rechenzentrum in Utah vermutet wird oder absichtlich geschwächte Kryptografiestandards. Im US-Kongress wird derzeit diskutiert, ob man Verschlüsselung gesetzlich beschränken sollte, so dass staatliche Ermittlungsbehörden eine „Hintertür“ zur Verfügung haben.

Verschlüsselung ist, wenn sie richtig angewandt wird das einzige Mittel, um sich vor Spionage durch Staaten zu schützen. Das gilt sowohl für jeden einzelnen Bürger, der mit

akzeptablem Zeitaufwand einen adäquaten Schutz vor Überwachung erhält, als auch für Staaten an sich. Das ist die zweite Aufgabe, die Geheimdienste haben: Eigene Kommunikation schützen. Diese Aufgabe wird von der NSA überhaupt nicht beachtet. Wenn die NSA Schwachstellen in Kryptosysteme integriert, dann ist dies mehr Überwachung auf Kosten der Sicherheit der eigenen Kommunikation.

Was der NSA-Skandal noch gezeigt hat, ist, wie die Geheimdienste parlamentarische Kontrolle untergraben. Operationen von NSA und BND, die eindeutig gegen das Grundrecht verstoßen werden trotzdem durchgeführt. Der Geheimdienstdirektor der USA und auch deutsche Amtsträger lügen vor dem Parlament.

Die Geheimdienste müssen umdenken. Die verdachtlose Überwachung muss aufhören, stattdessen sollte es eine gezielte Überwachung von Personen geben, die auch wirklich verdächtig sind. Jeder Eingriff in die Privatsphäre eines Menschen, egal ob im Inland oder Ausland muss von einem ordentlichen Gericht genehmigt werden. Das Briefgeheimnis ist ein Menschenrecht. Ich glaube, dass solch eine gezielte Überwachung, die von Menschen und nicht von Computersystemen ausgeführt wird deutlich effektiver ist, und zugleich weniger Eingriffe in die persönliche Freiheit jedes Einzelnen mit sich zieht.

Literatur

[1] DE-CIX. *Quick Facts*. URL: https://www.de-cix.net/about/quick-facts (besucht am 03. 12. 2015).

[2] David dos Dantos. *Glenn Greenwald*. 2014. URL: https://commons.wikimedia.org/wiki/File:Glenn_Greenwald_2014-01-20_001.jpg (besucht am 02. 12. 2015).

[3] dpa. *Partner dritter Klasse: Wie die USA Deutschland und die EU bespitzeln*. Die Zeit. 2013. URL: http://www.zeit.de/news/2013-06/30/geheimdienste-partner-dritter-klasse-wie-die-usa-deutschland-und-die-eu-bespitzeln-30164602 (besucht am 30. 11. 2015).

[4] Temporary Committee on the ECHELON Interception System. *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)*. Europäisches Parlament. 2001. URL: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN (besucht am 07. 12. 2015).

[5] Praxis Films. *About Laura Poitras*. URL: http://www.praxisfilms.org/about/laura-poitras (besucht am 02. 12. 2015).

[6] Kurt Gaulich. *Nachrichtendienstliche Fernmeldeaufklärung mit Selektoren in einer transnationalen Kooperation*. Deutscher Bundestag. 2015. URL: https://www.bundestag.de/blob/393598/b5d50731152a09ae36b42be50f283898/mat_a_sv-11-2-data.pdf (besucht am 07. 12. 2015).

[7] John Goetz Georg Mascolo Hans Leydecker. *Codewort Eikonal - der Albtraum der Bundesregierung*. Süddeutsche Zeitung. 2014. URL: http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432 (besucht am 04. 12. 2015).

[8] The Intercept. *Editorial Mission & Staff*. URL: https://theintercept.com/staff (besucht am 28. 11. 2015).

[9] Laura Poitras. *CITIZENFOUR (Film)*. Praxisfilms. 2014. URL: https://citizenfourfilm.com/ (besucht am 07. 12. 2015).

[10] Laura Poitras. *Edward Snowden*. Praxis Film. 2013. URL: https://commons.wikimedia.org/wiki/File:Edward_Snowden-2.jpg (besucht am 02. 12. 2015).

[11] Christoph Prössl. *Sonderermittler wirft USA Vertragsbruch vor*. ARD. 2015. URL: https://www.tagesschau.de/inland/graulich-nsa-bericht-101.html (besucht am 04. 12. 2015).

[12] Reuters. *Die drei im Dienste der Sicherheit*. ARD. 2012. URL: https://www.tagesschau.de/inland/geheimdienstehintergrund100.html (besucht am 07. 12. 2015).

[13] Achim Sawall. *NSA-Abhörtstation in Berliner US-Botschaft*. golem.de. 2013. URL: http://www.golem.de/news/special-collection-services-nsa-abhoerstation-in-berliner-us-botschaft-1310-102374.html (besucht am 03. 12. 2015).

[14] Bruce Schneier. *More about the NSA's Tailored Access Operations Unit*. Schneier on Security. 2013. URL: https://www.schneier.com/blog/archives/2013/12/more_about_the.html (besucht am 07. 12. 2015).

[15] Katy Scoggin. *Laura Poitras*. 2014. URL: https://commons.wikimedia.org/wiki/File:Laura_Poitras_2014.jpg (besucht am 02. 12. 2015).

[16] Edward Snowden. *Boundless Informant heat maps*. NSA. 2013. URL: https://search.edwardsnowden.com/docs/BoundlessInformantheatmaps20130611 (besucht am 07. 12. 2015).

[17] Edward Snowden. *Special Collection Service*. NSA. 2011. URL: https://search.edwardsnowden.com/docs/SpecialCollectionService20140618 (besucht am 07. 12. 2015).

[18] Edward Snowden. *Special Source Operations*. NSA. 2013. URL: https://search.edwardsnowden.com/docs/SpecialSourceOperationsoverview20131104 (besucht am 07. 12. 2015).

[19] Edward Snowden. *TEMPORA - GCWiki*. GCHQ. 2013. URL: http://www.spiegel.de/media/media-34103.pdf (besucht am 03. 12. 2015).

[20] Edward Snowden. *The Unofficial XKEYSCORE User Guide*. NSA. 2013. URL: https://search.edwardsnowden.com/docs/TheUnofficialXKEYSCOREUserGuide20150701 (besucht am 07. 12. 2015).

[21] Edward Snowden. *VoIP in XKEYSCORE*. NSA. 2009. URL: https://theintercept.com/document/2015/07/01/voip-xks/ (besucht am 07. 12. 2015).

[22] Edward Snowden. *XKEYSCORE*. NSA. 2009. URL: https://commons.wikimedia.org/wiki/File:XKeyscore_presentation_from_2008.pdf (besucht am 02. 12. 2015).

[23] Edward Snowden. *X-KEYSCORE as a SIGDEV tool*. NSA. 2009. URL: https://theintercept.com/document/2015/07/01/xks-sigdev-tool/ (besucht am 02. 12. 2015).

[24] Edward Snowden. *XKeyscore data sources*. NSA. 2013. URL: https://search.edwardsnowden.com/docs/XKeyScoredatasources20131211 (besucht am 07. 12. 2015).

[25] Statista. *Deutsches Web weiter zu langsam für Weltspitze*. URL: http://de.statista.com/infografik/1064/top-10-laender-mit-dem-schnellsten-internetzugang (besucht am 02. 12. 2015).

[26] Glenn Greenwald - Unclaimed Territory. *Response to right-wing personal attacks*. URL: http://glenngreenwald.blogpsot.de/2006/07/response-to-right-wing-personal.html (besucht am 28. 11. 2015).

[27] Nicholas Watt. *NSA 'offers intelligence to British counterparts to skirt UK law'*. The Guardian. 2013. URL: http://www.theguardian.com/politics/2013/jun/10/nsa-offers-intelligence-british-counterparts-blunkett (besucht am 30. 11. 2015).

[28] Wikipedia. *Edward Snowden*. URL: https://en.wikipedia.org/wiki/Edward_Snowden (besucht am 30. 11. 2015).

[29] Wikipedia. *Glenn Greenwald*. URL: https://de.wikipedia.org/wiki/Glenn_Greenwald (besucht am 28. 11. 2015).

[30] Wikipedia. *NSA-Untersuchungsausschuss, Operation Eikonal*. URL: https://de.wikipedia.org/wiki/NSA-Untersuchungsausschuss#Operation_Eikonal (besucht am 04. 12. 2015).

[31] Wikipedia. *UKUSA-Agreement*. URL: https://en.wikipedia.org/wiki/UKUSA_Agreement (besucht am 03. 12. 2015).

[32] Wikipedia. *XKeyscore*. URL: https://en.wikipedia.org/wiki/XKeyscore (besucht am 30. 11. 2015).

[33] Die Zeit. *XKeyscore-Vertrag - Das Dokument*. 2015. URL: http://www.zeit.de/digital/datenschutz/2015-08/xks-xkeyscore-vertrag (besucht am 29. 11. 2015).

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst und keine anderen Hilfsmittel als angegeben verwendet habe. Insbesondere versichere ich, dass ich alle wörtlichen und sinngemäßen Übernahmen aus anderen Werken als solche kenntlich gemacht habe.
