# Geheimdienste unter sich

## NSA, BND und die deutsche Großmacht

*von Rainer Rehak*

In diesem Text soll es um die planetare Totalüberwachung durch die Intelligence Community – also die Geheimdienste – gehen, sowie um die Rolle und Zukunft Deutschlands dabei.

Um den Stand der globalen Überwachung zu beschreiben, sind ein paar Grundlagen zum Verständnis der „digitalen Gesellschaft“ vonnöten; zuerst wird jedoch kurz der Haupthinweisgeber Edward Snowden beleuchtet. Es folgen eine Beschreibung und Einordnung der vergangenen deutschen Aktivitäten, die aktuelle Reaktion des BND auf die Enthüllungen und abschließend ein kurzes Fazit.

### Die Quelle: Edward Snowden

Für die aktuellen politisch-gesellschaftlichen Überwachungsdiskussionen ist im Wesentlichen Edward Snowden verantwortlich, denn er gab einen Schatz an brisanten Informationen über geheimdienstliche Tätigkeiten der US-Dienste an Journalisten wie Glenn Greenwald oder Laura Poitras weiter. Dabei ist darauf hinzuweisen, dass Snowden selbst keine Dokumente veröffentlicht hat, sondern dies und die nötige Schwärzungs- sowie Selektionsarbeit den Journalisten überlassen hat.[1]

Wie zu erwarten war, folgte eine Strategie der persönlichen und fachlichen Diskreditierung Edward Snowdens, die aber wenig erfolgreich war und nicht darüber hinwegtäuschen konnte, dass der Inhalt der Dokumente zu keiner Zeit bestritten worden ist, weder vom Präsidenten der USA noch von US-Behörden oder anderen involvierten Personen. Es wurden nur Begründungen formuliert, warum solche Vorgehensweisen für die „nationale Sicherheit“ – wenig später dann „nationalen Interessen“ – der USA alternativlos nötig sind.

Interessant ist außerdem, dass Snowden laut US-Gesetzen kein Whistleblower ist, denn er wird wegen Spionagetätigkeit (Espionage Act) gesucht, einem Gesetz von 1917, das sich ursprünglich gegen ausländische Spione richtete und keine Ausnahmen kennt. Chelsea Manning ist das jüngste Beispiel für diese Art von „Verfahren“.[2] Laut gewordene Forderungen, Snowden solle sich in den USA einem fairen, offenen Verfahren stellen, zielen also tatsächlich auf härteste Bestrafung ab.

Um auch die letzten beiden vom Inhalt der Dokumente ablenkenden Angriffe anzusprechen: Es gibt zwar eine Vielzahl von Versuchen, Edward Snowden eine Zusammenarbeit mit Russland oder China anzudichten oder echte Gefährdungen für Geheimdienstpersonen aufgrund der Veröffentlichungen zu konstruieren, aber für beides gibt es bislang keinerlei Belege.[3]

### Allgemeine Grundlagen der vernetzten, digitalisierten Gesellschaft

Unsere Gesellschaft befindet sich gerade in einem langsamen, aber tiefgreifenden Wandel was den Einsatz vernetzter Computer angeht. Dabei sind die Verweise auf die Privatssphärenproblematik zwar richtig, aber gänzlich unzureichend.[4] Das wird deutlicher, wenn man betrachtet, welche Daten wo anfallen. Unsere sozialen Daten liegen beim Email-/Telefonanbieter, die Postadressdaten bei Versandhändlern und den Meldeämtern, die Bonitätsinformationen bei den Banken, die Lohn- und Steuerdaten beim Finanzamt, die Krankendaten bei den Krankenkassen und möglicherweise dank elektronischer Gesundheitskarte (eGK) bald auf staatlichen Servern, Rentendaten sind bei den Rentenkassen, Bewegungsdaten liegen beim Mautbetreiber oder Mobilfunkanbieter und Betreibern von Videoüberwachungssystemen, Daten über den Medienkonsum entstehen in meinem Browser, Fernseher und eBook-Reader und (Ess-)Gewohnheiten liegen auf den Servern der Payback- und Kreditkartenanbieter. All diese Daten werden elektronisch gespeichert, verarbeitet und über Netze ausgetauscht. Von Dropbox, Facebook, Apple, Google oder Microsoft – also dort, wo Kalender, Emails bis hin zu Dokumenten liegen – ist hier noch nicht einmal die Rede, denn die obige Aufzählung macht klar: Das Datenaufkommen erzeugt komplexe Profile von Personen auch dann, wenn man selbst das Internet gar nicht verwendet.

Man denke nur daran, dass beispielsweise die Positionsdaten von Mobiltelefonen mit den Daten öffentlich angemeldeter Demonstrationen verknüpft werden könnten, und schon hätte man Listen der Personen, die an den jeweiligen Demonstrationen teilgenommen haben. Daran erkennt man auch, dass die Informationen nicht nur einzelne Personen betreffen, sondern das gesellschaftliche Gefüge insgesamt.

Ein weiteres Beispiel: Die individuelle Entscheidung für einen bestimmten E-Mailanbieter betrifft natürlich jeden Kommunikationspartner gleichermaßen, obwohl diese nicht in eine wie auch immer geartete Datenhandhabung eingewilligt haben. Gleiches gilt für Fotos und mittlerweile auch für moderne Fernseher, deren Sprachbefehlssoftware auch alle Umgebungsgespräche zur Analyse an die Server der Hersteller schickt.

Somit wird klar, dass es mitnichten (nur) um die Privatssphäre geht, sondern insgesamt um die Handlungs- und Entscheidungsfreiheit aller Menschen im digitalen Zeitalter, denn mit Informationen hat man auch Macht über den Menschen und – wie oben angedeutet – über ganze Gesellschaften.[5]

### Die NSA am Werk

Um eines voranzustellen: Das Ziel der NSA ist es, den Datenverkehr des gesamten Planeten für 100 Jahre zu speichern, dazu ist kürzlich das „Utah Data Center“ (Bluffdale, USA) in Betrieb genommen worden. Der ehemalige Direktor der NSA, Keith B. Alexander, meinte dazu: „Um die Nadel im Heuhaufen zu finden, brauchen wir zunächst den gesamten Heuhaufen.“[6]

Wie kommt die NSA aber an all diese Daten? Dafür hat sie sich mit ihrem Budget von mindestens 10 Mrd. USD pro Jahr viele Methoden geschaffen. Das wohl nach wie vor bekannteste Programm dafür ist PRISM, also der Direktzugriff auf die Serverfarmen von Unternehmen. Darunter fallen mindestens Microsoft,

NSA-Hauptquartier in Fort Meade Foto: Trevor Paglen 2013 über Wikipedia

Yahoo!, Google, Facebook, YouTube, AOL, Skype und Apple.[7] Auch Metadaten (wer wann wo mit wem kommuniziert) und Inhaltsdaten werden direkt von Telekommunikationsanbietern wie Verizon oder Orange abgezogen.

Darüber hinaus werden auch direkt Internetkabel und andere Verbindungswege angezapft, um durchfließende Daten auszuleiten. Weiterhin wurde auch direkt die Internetinfrastruktur (Provider, Netzknoten etc.) angegriffen, infiltriert und so für die eigenen Zwecke nutzbar gemacht. Auf diese Weise kam und kommt die NSA z. B. an die Daten von Institutionen der EU, der UN, der IAEA, des französischen Außenministeriums, der G7/8-Gipfel, der G20-Gipfel, der COP15 (UN Climate Change Conference in Kopenhagen), der deutschen Bundeskanzlerin sowie ihres Kabinetts, der türkischen und brasilianischen Regierung, von südamerikanischen Ölfirmen, den Betreibern von Visa und Mastercard, der Society for Worldwide Interbank Financial Telecommunication (SWIFT), der Chinesischen Führung, von US-Anwälten und Journalisten.

Dies ist bei weitem keine vollständige Liste, aber die Aufzählung soll andeuten, was das NSA-Motto „Wir wollen alles sammeln, alles wissen und alles nutzen“ wirklich meint und welche Macht in diesen Daten und dem daraus ableitbaren Wissen steckt. Was das ganze mit „Terrorabwehr“ zu tun hat, bleibt an dieser Stelle offensichtlich geheim, denn sogar die Untersuchungskommissionen des Weißen Hauses bescheinigten den Überwachungsprogrammen gänzlich fehlende Effektivität bei der Terrorabwehr.[8]

Doch nicht nur auf der rein technischen Ebene ist die NSA aktiv, technische Standardisierungsgremien wie das NIST (das DIN-Pendant in den USA) wurden unterwandert, damit bestimmte, global genutzte Verschlüsselungsstandards unsicher definiert werden.[9] So kann ausgesuchte verschlüsselte Kommunikation zumindest teilweise geknackt werden, leider nicht nur von der NSA. Aber auch das Abfangen von Postpaketen, um die verschickten Waren zu verwanzen, wird von der NSA schon praktiziert.[10]

Alle so erlangten Daten werden sauber sortiert, gefiltert, verknüpft und kategorisiert, sodass sie durch ein Werkzeug namens XKeyscore von Analysten durchsucht werden können.

Natürlich gibt es bei der NSA auch Programme, wie man die gehorteten Daten nutzen kann, um missliebige Personen psychisch zu zerstören oder zumindest geschäftlich und privat zu diskreditieren.[11] Passend ist hierfür zweifelsohne der alte DDR-Stasibegriff „Zersetzung“, doch um diesen Aspekt soll es hier nicht weiter gehen.

## Die Rolle Deutschlands und des BND

In den Enthüllungen von Edward Snowden ist zu finden, dass Deutschland innerhalb der EU das am meisten überwachte Land ist. Doch bevor die Deutschen sich als Opfer verstehen und entrüstet über den Atlantik – zumindest aber in Richtung Großbritannien – zeigen, muss der ganze Zusammenhang analysiert werden. Sucht man nämlich in den Enthüllungen nach Informationen darüber und zieht man die mageren, aber dennoch erhellenden Ergebnisse des NSA-Untersuchungsausschusses des Bundestages hinzu und vervollständigt das Bild mit den Aussagen von Geheimdienstexperten, so ergibt sich ein ganz anderes Bild:

Die Ausspähungen wurden und werden mit komplettem Wissen der jeweiligen Regierungen und des Bundeskanzleramtes aktiv vom BND unterstützt, wobei es regelmäßige Koordinationsbesuche des BND bei der NSA gibt. Bemerkenswert ist auch der Umstand, dass der BND und der Verfassungsschutz Zugriff auf das oben angesprochene Suchwerkzeug XKeyscore haben.[12] Snowden selbst formuliert es so, dass der BND mit der NSA „zusammen im Bett“ sei. Deutschland ist also mitnichten passives Opfer der Überwachung.

Beispielhaft für die Zusammenarbeit der Dienste kann konkret die Operation Eikonal herangezogen werden, die der BND von sich aus an die NSA herantrug. Im Rahmen dieser Operation

wurden zwischen 2004 und 2008 alle Telefon- und Internetdaten, die über den weltgrößten Glasfaser-Netzknoten DE-CIX in Frankfurt liefen, ausgeleitet und der NSA zugeführt.[13] Die Daten von Deutschen sollten zwar ausgefiltert werden, aber der Filter funktionierte nachweislich von Anfang an nicht korrekt. Im Jahre 2008 wurde die Operation dann von der NSA aufgekündigt, vermutlich weil sie anders und einfacher an die gleichen Daten kamen. Zudem kann der BND seit 2009 mit Hilfe eines großen deutschen Internet-Providers den kompletten Datenstrom ausleiten. Dass der BND seit rund zehn Jahren die Mobilfunkdaten von Terrorverdächtigen an internationale Partnerdienste, auch an den US-Geheimdienst NSA weitergibt, der damit extralegale Drohnenmorde durchführt, soll hier nur am Rande erwähnt werden; denn die Bundesregierung zeigt auch nach den Enthüllungen weiterhin großes Interesse an einem engen Austausch mit den US-Diensten.

Ohne näher auf die Details eingehen zu wollen, sollte man trotzdem auf das einhellige Ergebnis der sachverständigen Rechtswissenschaftler im NSA-Untersuchungsausschuss und später auf der FIfF-Konferenz 2014 bezüglich der BND-Aktivitäten hinweisen: „die gesamte Auslandsaufklärung ist rechtswidrig“, und im Inland darf der BND nicht aktiv werden.[14] Auch der moralische Vorsprung („Ausspähen unter Freunden - das geht gar nicht“) der „Merkelabhöraffäre“ hat sich nun in Luft aufgelöst, da der BND selbst u.a. Hillary Clinton und John Kerry während seiner Zeit als US-Außenminister abgehört hatte.

## Reaktion der deutschen Dienste

Was ist nun aber die Reaktion auf die Enthüllungen, die langjährigen Verquickungen von BND und NSA und das Mitwissen der deutschen Regierung(en) in diesen Belangen? Personell gibt es keine Konsequenzen, aber der BND – und somit Deutschland – will nun auch ganz groß mitmischen, vermutlich gerade jetzt, wo man um die technischen Möglichkeiten weiß. Beantragt sind also 300 Mio. € für die SIT (Strategische Initiative Technik) mit insgesamt 26 Projekten, um „im Cyberbereich auf Augenhöhe mit den Partnern“[15] zu kommen. Dabei geht es unter anderem um:

- SWOP (Operative Unterstützung von Switch-Operationen): Die Netze „fremder“ Internetanbieter infiltrieren
- EASD (Echtzeitanalyse von Streamingdaten): Allgemein zugängliche Informationen von Social Media abgreifen, zusammenführen und strategisch analysieren
- ZEUS (Zentrales Enwicklungs- und Unterstützungsprojekt SSCD [sigint suport to cyber defense]): Daten angezapfter Glasfaserkabel analysieren
- SSL-verschlüsselte Verbindungen knacken (4,5 Mio.): Auf „graue[m] Markt Informationen über Software-Schwachstellen ein[zu]kaufen“, um sie später nutzen zu können

Dass diese Mittel auch in den USA offensichtlich keinen Terror verhindern konnten, wurde schon angesprochen. Und auch hier werden wieder die gesellschaftlichen Folgen verkannt: Mit jeder neuen Nachfrage wächst z.B. der globale Markt für Sicherheitslücken, obwohl man diese Lücken eigentlich vom Hersteller schließen lassen müsste. In der Folge wird/bleibt Software unsicher.

Leider soll die gnadenlos unterbesetzte und ineffektive parlamentarische Kontrolle im Rahmen der SIT nicht entsprechend aufgestockt (oder überhaupt komplett reformiert) werden. Die Prioritäten sind somit leider klar und eindeutig.

## Fazit

Abschließend kann man also ein positives und ein negatives Fazit ziehen: Es ist schön, dass die deutschen Geheimdienste nicht außer Kontrolle geraten sind und somit nur genau das tun, was Regierung und Bundeskanzleramt anweisen oder gestatten.[16] Das negative Fazit über den Zustand der Welt und Deutschlands Rolle dabei soll dem Leser in Anbetracht der obigen Ausführungen selbst überlassen bleiben. Doch es regt sich großflächig Widerstand, sowohl in Deutschland als auch in den USA, denn faktisch ist mit Snowden der Super-GAU für Geheimdienste und Regierungen eingetreten:

Sie müssen ihre geheimen Praktiken rechtfertigen... und das können sie nicht.

## Weiterführende Links

- FIfF-Konferenz 2014 zur Rolle deutscher Geheimdienste https://www.fiffkon.de
- Investigatives Nachrichtenportal „The Intercept“ u. a. von Glenn Greenwald https://firstlook.org/theintercept
- Eine Einstiegsdiskussion: Beckmann: „Informiert oder manipuliert – wie die digitale Welt unser Leben verändert“, ARD http://www.daserste.de/unterhaltung/talk/beckmann/sendung/17042014-informiert-oder-manipuliert-100.html
- Informationen zum digitalen Computergrundschutz http://berlin.fiff.de/workshop2204.html
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V. http://www.fiff.de

## Anmerkungen

1 Poitras, Laura: Citizenfour, 2014
2 Greenwald, Glenn: „CNN’s The Lead“, 2.1.2014
3 Sledge, Matt: One Year After Edward Snowden’s Leaks, Government Claims Of Damage Leave Public In Dark, Huffington Post, 2014
4 Rost, Martin: Zur Soziologie des Datenschutzes, in: Datenschutz und Datensicherheit – DuD, Volume 37, Issue 2, S. 85-91, 21.2.2013
5 Knaut, Andrea und Pohle, Jörg (Hrsg.): Fundationes I: Geschichte und Theorie des Datenschutzes, 2014
6 Alexander, Keith: Aspen Security Forum, 18.7.2013
7 Greenwald, Glenn und MacAskill, Ewen: NSA Prism program taps in to user data of Apple, Google and others, The Guardian, 7.6.2013
8 Privacy and Civil Liberties Oversight Board: Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, 2.7.2014
9 Siehe die Programme „Bullrun“ und „Edgehill“
10 Holland, Martin: NSA manipuliert per Post versandte US-Netzwerktechnik, Heise.de, 13.5.2014
11 Greenwald, Glenn: How Covert Agents Infiltrate the Internet to Manipulate, Deceive and Destroy Reputations, The Intercept, 25.2.2014
12 dpa: BND nutzt NSA-Spähsoftware für Auslandsaufklärung, via Zeit Online, 9.8.2013
13 Mascolo, Georg und Goetz, John sowie Von Osten, Demian: Codename „Eikonal“, Tagesschau, 3.10.2014
14 Bäcker, Matthias: Strategische Telekommunikationsüberwachung auf dem Prüfstand, FIfF-Konferenz 2014, 7.11.2014
15 Biermann, Kai: Die geheime Überwachungswunschliste des BND, Zeit Online, 13.11.2014
16 Schmidt-Eenboom, Erich: Gleiche Brüder, gleiche Kappen? – Die angelsächsischen Geheimdienste und der BND im Vergleich, FIfF-Konferenz 2014, 8.11.2014