fhwedel
UNIVERSITY OF APPLIED SCIENCES

Seminararbeit

in der Fachrichtung

Wirtschaftsingenieurwesen

Edward Snowden: Spionage, Terrorismus, Bürgerrechte, Überwachung im Netz, Internetkriminalität und die Vorratsdatenspeicherung. Wohin könnte, wohin sollte sich unsere westliche Gesellschaft entwickeln?

Erstellt von:	Abdulkerem Akpinar Mat-Nr.: 101740 E-Mail: wing101740@fh-wedel.de
Erarbeitet im:	6. Semester
Abgegeben am:	20.04.2018
Betreuender Dozent:	Prof. Dr. Michael Anders Fachhochschule Wedel Feldstraße 140 22880 Wedel Tel.: 04103/ 804824 E-Mail: an@fh-wedel.de

Inhaltsverzeichnis

1. Einleitung

„Ausspähen unter Freunden - das geht gar nicht"[1] – Diese Aussage von der deutschen Bundeskanzlerin Angela Merkel im Jahr 2013 zu dem Verdacht der Spionage ihres Handys lässt erahnen wie weitreichend die Datensammlung von Geheimdiensten in Deutschland wirklich war bzw. möglicherweise noch ist. Angetrieben von der Überzeugung, dass jeder Mensch selbst über seine eigenen Daten frei entscheiden dürfen sollte, veröffentlichte der Whistleblower Edward Joseph Snowden geheime Dokumente der NSA (National Security Agency), die die Vorratsdatensammlung belegten. Die Aufdeckung führte in Deutschland zur Berufung eines parlamentarischen Untersuchungsausschusses, durch dessen Ermittlungen das tatsächliche Ausmaß der Vorratsdatensammlung in Deutschland festgestellt und die Zusammenarbeit von staatlichen Organisationen aufgedeckt werden konnte. Dabei stellte sich die Frage, ob ein Verstoß gegen die deutschen Gesetze vorlag und inwieweit jeder Bürger in seiner Privatsphäre verletzt wurde.

Das Ziel der Seminararbeit ist es dem Leser einen Überblick auf die Ereignisse nach der Veröffentlichung der geheimen NSA-Dokumente zu verschaffen. Dabei richtet sich der Fokus auf die Bundesrepublik Deutschland. Zudem soll der Leser über die Aktivitäten von Geheimdiensten und staatlichen Behörden, wie bspw. die ZITiS, bezüglich der Vorratsdatensammlung aufgeklärt werden. Des Weiteren sollen nicht nur die Gefahren, sondern auch die möglichen Vorteile der Datensammlung im Zeitalter der Digitalisierung dem Leser nahegebracht werden. Jene Erkenntnisse sollen zu einer fundierten Meinungsbildung des Lesers beitragen und zum bewussten Umgang mit den eigenen Daten animieren.

Im Verlauf der Seminararbeit wird zunächst die globale Überwachungs- und Spionageaffäre seitens der USA aufgezeigt. Um im Speziellen die Spionage in Deutschland und die Reaktionen, die daraufhin ausgelöst wurden, zu verdeutlichen, wird auf die Berufung des NSA-Untersuchungsausschusses und die wichtigsten Thematiken, die bei den Ermittlungen aufkamen, wie bspw. die Spionage des Handys von Angela Merkel oder die „Operation Eikonal“, eingegangen. Anschließend wird die Gesetzeslage in Deutschland in Bezug auf die Datensammlung der Daten des deutschen und in Deutschland lebenden Bürgers aufgezeigt. Um zu verdeutlichen wie weit Geheimdienste bei der Spionage gehen, wird die Spionage des NS-Untersuchungsausschusses selbst behandelt. Die Ergebnisse und Folgen des Ausschusses werden im dritten Kapitel durch diverse Meinungen von wichtigen Personen aus der Wirtschaft,

[1] Vgl. (aar/flo/dpa/Reuters/AFP, 2013)

der Politik und der Justiz ergänzend aufgezeigt. Im Weiteren werden die Berufung und die Aufgaben der deutschen Bundesbehörde, ZITiS, thematisiert. Auch der Anstieg der deutschen Nutzerzahlen des Tor-Browsers gilt als eine Folge der NSA-Affäre, die dadurch im Verlauf der Seminararbeit genauer betrachtet wird. Um dem Leser nicht nur ein negatives Bild über die Datensammlung zu vermitteln, wird auch auf die wirtschaftlichen und technisch-innovativen Möglichkeiten, die die Datensammlung birgt, eingegangen. Zum Schluss gibt der Autor seine persönliche Meinung zur Datensammlung wieder.

2. Globale Überwachungs- und Spionageaffäre

Nach der Veröffentlichung von geheimen Dokumente durch den ehemaligen NSA-Mitarbeiter Edward Snowden im Juni 2013 wurde das Ausmaß der systematischen Massenüberwachung der Telekommunikation und insbesondere des Internets durch die USA erstmals ersichtlich. Als enger Verbündeter der NSA galt dabei die britische GCHQ (Government Communications Headquarters). Die Partnerschaft und die gemeinsame Spionage der beiden Organisation bzw. Staaten besteht schon seit dem Ende des Zweiten Weltkriegs. Durch das Anzapfen unterseeischer Glasfaserkabel, die um den ganzen Globus verlaufen, konnten die NSA und die GCHQ einen immensen Anteil des globalen Datenaustausches und der Kommunikation verfolgen und mitlesen. Nicht nur durch das Anzapfen von Leitungen, sondern auch durch den Einsatz von geheimen Gerichten wurden Telefongesellschaften gezwungen, Daten auszuhändigen. Zudem wurde diese Macht der Überwachung durch den direkten Zugriff zu Servern diverser Technikriesen, wie z.B. Google, Microsoft und Facebook, gestärkt. Bis zur Aufdeckung dieser globalen Affäre durch Edward Snowden wurden die Spionageaktivitäten verdeckt gehalten, sodass die weltweite Bevölkerung ahnungslos blieb und ein Großteil der Menschen Medien nutzten, ohne den Verdacht der Spionage an der eigenen Person zu haben.

Bei der Veröffentlichung der Dokumente wurde festgestellt, dass die USA nicht nur terroristische Gruppierungen, wie bspw. die Al-Qaida, ausspionierte, sondern auch Verbündete, wie z.B. Deutschland oder Frankreich. Die Spionage ging sogar soweit, dass die Kommunikationsdaten der eigenen Bevölkerung überwacht und aufgezeichnet wurden.[2] Dabei wurde nicht zwischen Kriminellen, Terroristen oder unschuldigen Bürgern unterschieden. Um die amerikanische Bevölkerung zu besänftigen, sprach der Präsident Barack Obama[3] davon,

[2] Vgl. (Harding, 2014)
[3] Ehemaliger Präsident der USA vom 20. Januar 2009 bis zum 20. Januar 2017

dass der Geheimdienst nur die Länge der Telefonate und die dazugehörigen Telefonnummern archivierte. Zudem seien hauptsächlich Ausländer abgehört worden. Neben der in den USA gesammelten Daten, stammte ein Großteil aus Deutschland. Das liegt darin begründet, da Deutschland bei der Vorratsdatensammlung mithalf bzw. dem immer noch nachgeht.[4]

Abbildung 1: Von Boundless Informant erzeugte Karte[5]

Wie man Anhand der Karte, die durch das Computersystem der NSA „Boundless Informant“[6] erzeugt wurde, erkennen kann, gehört Deutschland in Europa zu den Ländern, aus denen die meisten gespeicherten Daten stammen. Dabei steigt die Relevanz der überwachten Länder von dunkel- und hellgrün über gelb und orange zu rot.

3. Spionage in Deutschland und die Reaktionen

Nachdem bekannt wurde, dass nicht nur gewöhnliche Bürger in Deutschland abgehöhrt und ausspioniert wurden, sondern auch führende Politiker, wie u.a. Bundeskanzlerin Angela Merkel, reagierte die Bundesregierung und galt neben Brasilien als Vorreiter der öffentlichen

[4] Vgl. (Hamm, 2013)
[5] Nach (Greenwald & MacAskill, 2013)
[6] Boundless Informant ist ein Computersystem der NSA und wird zum Herausfiltern von Zusammenhängen aus einer Menge von Daten mit Hilfe der Technik des Data Minings verwendet, z.B. um die Kommunikation einer einzelnen Person aus einer Menge von E-Mails zu filtern.

Empörung über die Spionageaktivitäten und Vorratsdatenspreicherung der NSA.[7] Daraufhin führte die Bundeskanzlerin mit dem amerikanischen Präsidenten ein Telefonat und forderte eine Aufklärung über den Umfang der Spionage in Deutschland. Um zukünftige Spionageaktivitäten der USA einzuschränken bzw. ganz zu verhindern, versuchte die deutsche Regierung ein No-Spy-Abkommen[8] mit den USA in die Wege zu leiten, was jedoch erfolglos blieb. Der damalige Außenminister Frank-Walter Steinmeier gab nach seinem Besuch in Washington im Januar 2014 als Grund dafür an, dass Deutschland und die USA unterschiedliche Ansichten von Sicherheit, Freiheit und Privatsphäre hätten.[9] Jedoch deckte der NDR, WDR und die Süddeutsche Zeitung im Mai 2015 auf, dass es nie eine erfolgversprechende Aussicht auf solch ein Abkommen gegeben habe und dass das Bundeskanzleramt schon seit Januar 2014 davon Kenntnis hatte. Dennoch wurde seitens des Bundeskanzleramtes vor dem Bundestag und den Medien bis zur Aufdeckung das Gegenteil behauptet.[10] „Bundeskanzlerin Merkel hat wohl ausgereicht, dass sie aus dem Spionageprogramm rausgenommen wird.“[11]

Damit die Tat der NSA auch strafrechtliche Folgen nach sich ziehen kann, hat Generalbundesanwalt Harald Range „Ermittlungen wegen des Verdachts der Ausforschung des Handys der Bundeskanzlerin“ im Juni 2014 eingeleitet. Da die Beweise, die dem Generalbundesanwalt vorlagen, für nicht „gerichtsfest“ erachtet wurden, mussten die Ermittlungen eingestellt werden. Das Dokument, welches als Beweis für das Abhören des Telefons der Bundeskanzlerin in der Öffentlichkeit als Beweisstück vorlag, war nur eine Abschrift eines NSA-Dokumentes und konnte nicht als Original beschaffen werden.[12]

3.1 Der NSA-Untersuchungsausschuss – NSAUA

Als Reaktion auf die Enthüllung der geheimen Dokumente der NSA durch Edward Snowden berief der Bundestag am 20. März 2014 im Auftrag aller Fraktionen den NSA-Untersuchungssauschuss ins Leben, um „[…] Ausmaß und Hintergründe der Ausspähungen durch ausländische Geheimdienste in Deutschland auf[zu]klären“[13] und zu untersuchen, ob

[7] Vgl. (Greenwald, Die globale Überwachung - Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen, 2014)
[8] Ein No-Spy-Abkommen ist ein Vertrag zwischen zweier Parteien, der ein Verbot gegenseitiger politischer und wirtschaftlicher Spionage und des Austausches von Daten impliziert
[9] Vgl. (Reuters, 2014)
[10] Vgl. (Goetz, Kempmann, & Baars, 2015)
[11] Zitat von der damalige FDP-Justizministerin Leutheusser-Schnarrenberger (Medick, 2015)
[12] Vgl. (dpa, AFP, sdo, 2015)
[13] (Bundestag, 2014)

deutsche Stellen von solchen Spionageprogrammen wussten und eventuell dabei halfen oder sogar Daten weitergaben.[14] Außerdem soll der parlamentarische Ausschuss nach Methoden suchen, wie die Telekommunikation in Deutschland technisch besser geschützt werden kann. Die Anzahl der Mitglieder des Ausschusses wurde dabei auf acht und dem entsprechend vielen Stellvertretern festgelegt.[15] Dabei sind vier Mitglieder von der CDU/CSU, zwei von der SPD und jeweils einer von der Partei die Linke bzw. die Grüne. Nachdem der CDU-Abgeordnete Clemens Binninger nach der ersten Sitzung des Ausschusses als Vorsitzender zurücktrat, übernahm der ebenfalls von der CDU stammende Abgeordnete Patrick Sensburg das Amt. Der Grund für den Rücktritt sei einerseits das Beantragen der Vorladung des Whistleblower Snowdens von der Opposition, welches ihm zeigte, dass eine vertrauensvolle Zusammenarbeit nicht möglich sei. Da sich die Opposition Minderheitenrechte sicherte, könne sie Vorladungen erzwingen. Andererseits sei sein Amt als Vorsitzender des PKGR (Parlamentarischen Kontrollgremiums) hinderlich, weil Abgeordnete des PKGR deutsche Geheimdienste kontrollieren sollen. Dabei müssen sie vertrauliche Informationen, die sie von den Diensten bekommen, für sich behalten. Durch die geplanten Befragungen des NSA-Ausschusses derselben Personen zu denselben Themen wie die des PKGR sorgte sich Binninger um seine Vertrauenswürdigkeit im PKGR.[16]

Damit eine gewisse Sicherheit für die Untersuchungen des NSAUA und die Dokumente gewährleistet werden konnte, wurden geheime Schutzstellen, an denen die Dokumente analysiert werden durften, vorgesehen und zur Kommunikation verschlüsselte Krypto-Telefone benutzt. Beim geheimen Teil der Sitzungen wurden sogar Handys und Tablets eingesammelt und klassische Musik aufgelegt, um in gewisser Weise ein Abhörschutz zu kreieren.[17]

Zur Prüfung der NSA-Affäre lagen dem Ausschuss 1988 Ordner vor. Jedoch wurden einige Dokumente und Akten an diversen Stellen geschwärzt und dem Ausschuss durch den BND (Bundesnachrichtendienst) und das Bundeskanzleramt gar nicht erst vorgelegt. „[…] in den Dokumenten seien ausländische Interessen berührt, daher müssten die entsprechenden Länder zuerst einmal gefragt werden, ob die Aufklärer des Parlaments in die Akten schauen dürften.“[18] Einige Mitglieder des Ausschuss drohten als Konsequenz mit Klage und forderten, die geschwärzten Passagen wieder lesbar zu machen.

[14] Vgl. (Biermann, 2017)
[15] Vgl. (Bundestag, 2014)
[16] Vgl. (Caspari, 2014)
[17] Vgl. (Goertz, Leyendecker, Mascolo, & Obermaier, 2014)
[18] (Biermann, Spähskandal: Regierung enthält dem NSA-Ausschuss wichtige Akten vor, 2014)

Da einige geheimen Informationen aus dem NSAUA an die Öffentlichkeit gelangten, zeigte das Bundeskanzleramt sich am Oktober 2014 empört. Die Empörung ging sogar soweit, dass sie den Mitgliedern des NSAUA mit Strafanzeige drohten, wenn weitere Veröffentlichungen stattfinden würden. Dabei bezog das Bundeskanzleramt sich speziell auf die Berichte des Spiegel, der Süddeutschen Zeitung und Meldungen von Netzpolitik.org. Die Vorwürfe des Geheimnisverrates weisen sowohl die Mitglieder des NSAUA als auch die genannten Medien zurück. „Schließlich sei es Aufgabe der Aufklärer, während der laufenden Untersuchung politische Einschätzungen zu geben und die Öffentlichkeit zu informieren.“[19]

Durch die öffentlichen Anhörungen und Vernehmungen, welche im Jahr 2014 anfingen, wurden eine Reihe von BND-Mitarbeitern und ehemalige NSA-Angestellte bzw. auch Whistleblower zur Rede gestellt. Dabei wurde die Vermutung der Zusammenarbeit zwischen der NSA und BND gefestigt. Der Austausch zwischen BND und NSA basiere auf einem Vertrag zwischen den beiden Organisationen aus dem Jahr 2002 und ist eigentlich streng geheim. Dabei bestätigte sich, dass nicht die Bundesregierung Verhandlungen führte, welche Daten der BND an die NSA übergibt werden, sondern der BND selbst entschied. „Das allein ist bedenklich, da so keine demokratische Kontrolle über diese Amtshilfe bei der Spionage existiert.“[20]

3.1.1 Diskussion über Befragung von Snowden

Ein großer Streitpunkt wurde die Zeugenbefragung von Edward Snowden. Am 8. Mai 2014 beschloss der Ausschuss Edward Snowden als Zeugen zu befragen. Nachdem der Whistleblower in einem Interview damit warb, noch viel mehr Informationen zu besitzen, als er schon veröffentlich habe, u.a. über die Spionage der deutschen Kommunikation, in die er involviert gewesen sein soll, warf der Vorsitzende der NSAUA ihm vor „nie speziell mit der massenhaften Ausspähung deutscher Bürger in Deutschland befasst“[21] gewesen zu sein und dass er seine Glaubwürdigkeit ohne die Aushändigung der Originaldokumente verliere. Die Ansichten stießen bei den meisten Mitgliedern der NSAUA, der Koalition und selbst bei Mitgliedern seiner eigenen Fraktion auf Kritik. "Wir müssen Snowden testen, ob er weitere Erkenntnisse hat, die über das Bekannte hinausgehen. Ich rate dazu, dass wir ihn nicht schon

[19] (Gude & Meiritz, 2014)
[20] Vgl. (Biermann, 2014)
[21] Patrick Sensburg

im Vorfeld abqualifizieren"[22] [23] Zudem stellte sich die Frage, wo das Interview stattfinden solle. Wie sich im März 2015 herausstellte, hatte die USA der Bundesrepublik stark mit Sanktionen gedroht. Wenn Deutschland Snowden Asyl gewähren würde, würden die US-Geheimdienste Deutschland keine Geheimdienstinformationen in Sachen Terrorabwehr mehr liefern, d.h. falls es erste Anzeichen für einen terroristischen Anschlag in Deutschland gäbe, würden die US-Behörden keine Warnung nach Berlin übermitteln. Dies galt auch für einen kurzzeitigen Aufenthalt Snowdens in der BRD, wodurch die Koalition eine Befragung von Snowden in Deutschland ablehnte.[24] Nachdem Snowden eine Befragung via Videoübertragung strikt verweigerte, nahm die Opposition im September 2014 die Ablehnung der Befragung von Snowden in Deutschland seitens der Koalition zum Anlass, vor dem Bundesverfassungsgericht zu klagen. Demnach warfen sie der Bundeskanzlerin vor, dass sie keine „Rechts- und Amtshilfe“[25] im Falle des Untersuchungsausschusses mit ihrer Regierung leiste.[26] Zwei Jahre später wurde vom Bundesgerichtshof beschlossen, dass Snowden persönlich einzuladen sei. Jedoch verpflichtete der Beschluss den NSAUA ein Ersuchen an die Bundesregierung stellen zu dürfen, aber nicht, dass die Bundesregierung dem nachkommen muss.[27] Dies ist wahrscheinlich auch der Grund, warum es bis dato zur keiner Zeugenbefragung von Edward Snowden kam.

3.1.2 Operation Eikonal und die Zusammenarbeit zwischen NSA und BND

Durch Zeugenvernehmungen diverser BND-Leiter und ehemaliger Angestellter der NSA wurde durch den NSAUA festgestellt, dass Deutschland selbst sogar zur Datensammlung in Europa beitrug. Dabei konnte aus den vorliegenden Dokumenten entnommen werden, wie die genaue Zusammenarbeit der NSA und BND von 2004 bis 2008 aussah. Unter dem Namen Operation Eikonal wurden in Frankfurt am Main in dem am Datendurchsatz gemessen weltweit größten Netzknoten „DE-CIX“ der Deutschen Telekom Telefon- und Internetdaten von der BND gefiltert und über eine Leitung zum BND-Sitz in Pullach transportiert. Der Zugriff auf die Server wurde vertraglich zwischen der BND und der Deutschen Telekom geregelt. Von Pullach aus gelangten die Daten ins bayrischen Bad Aibling.

[22] Roderich Kiesewetter, CDU-Obmann und Sensburgs Fraktionskollege
[23] Vgl. (Meiritz, Zeuge Snowden: NSA-Aufklärer stellen sich gegen ihren Vorsitzenden, 2014)
[24] Vgl. (heb, 2015)
[25] Artikel 44 des Grundgesetzes
[26] Vgl. (Meiritz, 2014)
[27] Vgl. (Biermann, 2016)

Der BND suchte mit Hilfe ihrer Computer in ihrer Abhörstation in Bad Aibling alle Mail-Endungen mit „.eu“ sowie Begriffe wie "diplo", "gov" und "Bundesamt". Dabei handelt es sich um sogenannte Selektoren. Mit diesen festgelegte Suchmerkmalen ist es für Geheimdienste möglich, für sie relevante Informationen aus Datenströmen abzugreifen. Ein Selektor kann Metadaten[28] wie einzelne Telefonnummern, E-Mail-Adressen, Keywords, URL etc. betreffen oder die Kommunikation eines ganzen Landes. Durch die Schenkung der Antennen der Anlage und dem Bezug von modernster Technik hatte sich der BND dazu verpflichtet, die Rohdaten der 13 abgehörten Kommunikationssatelliten an die NSA weiterzuleiten. Mit der neuen Technik konnte der BND auch ihre eigene Internetüberwachung verbessern.

Durch den Einsatz des BND von dem zu starken Filter „Dafis“, um die Daten der deutschen Bürger herauszufiltern, wurden die übriggebliebenen Daten für die NSA uninteressant und beendeten 2008 vermeintlich die Operation. Obwohl die Zusammenarbeit für beendet galt, deckten die veröffentlichten Dokumente von Snowden das Fortbestehen der Datenlieferung durch den BND auf.[29]

So suchte bis zum 14. August 2013 die NSA durch die BND und ihren darauf programmierten Computern nach den festgelegten Selektoren. Pro sogenannter „Session“, die stündlich stattfand, wurden 23 Millionen Rohdaten erfasst. Dabei galt durch das G10-Gesetz bei den Daten der deutschen Bürger strenge, vertraglich festgelegte Regeln. Alle E-Mail-Adressen mit der Endung „.de“ sowie alle Telefonnummern mit der Landeskennung „+49“ seien ausgefiltert worden. Die Daten anderer Europäer, egal ob Mitglied der EU-Kommission oder normaler Bürger, wurden ohne Einschränkungen gespeichert, wenn die Kommunikation über Satellit ging und sie eines der 12.000 Suchbegriffe der Selektorenliste verwendet haben. Zudem seien auch Unternehmen, wie Airbus betroffen gewesen, da die NSA nach Hinweisen für illegale Exportgeschäfte suchte. Die Aufdeckung kam durch einen Unterabteilungsleiter der Abteilung "Technische Aufklärung" der Abhörstation in Bad Aibling zustande, der herausfinden wollte, wonach die NSA noch suche außer des ursprünglichen Zwecks der Abhörstation – nämlich der Beschaffung von Informationen aus Afghanistan und den Krisenregionen im Norden Afrikas.[30]

[28] Unter Metadaten sind Verbindungsdaten zu Telefonaten, E-Mails, SMS und Chatbeiträgen zu verstehen, z.B. wann welcher Anschluss mit welchem Anschluss wie lange verbunden war
[29] Vgl. (Greis, 2014)
[30] Vgl. (Moscolo & Goetz, 2015)

Abbildung 2: Abhörstation in Bad Aibling[31]

Die Operation Eikonal und allgemein die Spionageaktivitäten der BND sind im Hinblick auf die Rechtsgrundlage und die in Deutschland herrschende Demokratie ziemlich fragwürdig. Denn Absatz 1, Artikel 10 des Grundgesetzes der Bundesrepublik Deutschland sagt aus, dass „das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis […] unverletzlich“ sind. Jedoch kann eine gesetzliche Beschränkung in Kraft treten (Absatz 2), wenn „[die] freiheitliche demokratische Grundordnung“ gefährdet ist oder “[die] Sicherung des Bundes oder eines Landes“ davon abhängt. Zudem heißt es, dass „sie dem Betroffenen nicht mitgeteilt“ und der Rechtsweg ausgeschlossen wird, d.h. Bürger dürfen ausspioniert werden, ohne informiert werden zu müssen und ohne die Möglichkeit zu klagen.[32]

Durch das G10-Gesetz, welches aussagt, dass deutsche Geheimdienste „Überwachungsmaßnahmen gegen einzelne Personen beim begründeten Verdacht auf schwere Straftaten wie Hoch- oder Landesverrat, Gefährdung des demokratischen Rechtsstaats oder der äußeren Sicherheit, Terrorismus oder Sabotage von IT-Infrastrukturen“ anwenden dürfen, wird der Absatz 1 des Artikel 10 des Grundgesetzes für Geheimdienste eingeschränkt. Außerdem sagt der zweite Teil des G10-Gesetzes – die „strategische Fernmeldeaufklärung“ – aus, dass der BND ohne einen Verdacht internationale Telekommunikation abfangen und durchsuchen darf. Beim Abfangen dieser sogenannten Ausland-Ausland-Verkehre genießt der BND Freiheit, solange keine deutschen Staatsbürger betroffen seien. Außerdem darf der BND nach §7a des

[31] Nach (Niesen, 2017)
[32] Vgl. (Deutscher Bundestag)

„Gesetz(es) zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10, G10-Gesetz)“ die erhobenen Daten an ausländische öffentliche Behörden, wie im Fall der Operation Eikonal die NSA, nach Zustimmung des Bundeskanzleramtes weitergeben.[33] Durch dieses Gesetz betrachtet sowohl die Bundesregierung als auch der BND diese Form der Spionage als legitim an, auch wenn Staats- und Verfassungsrechtler das Gesetz stark kritisieren.[34] Da die eingesetzten Filter von der BND nie komplett alle Daten der deutschen Bürger herausgefiltert haben bzw. herausfiltern, stelle dies einen Gesetzesbruch des G10-Gesetzes dar, wodurch eine Legitimation der Weitergabe der Daten an die NSA seitens Staats- und Verfassungsrechtler angezweifelt wird. Man geht davon aus, dass 95% der Daten herausgefiltert wurden. Nichtsdestotrotz sind 5% der Daten gesetzeswidrig.[35]

3.1.3 Ausspionierung des Untersuchungsausschusses

Am 4. Juli 2014 wurde veröffentlicht, dass ein BND-Mitarbeiter von der Bundesanwaltschaft wegen des Verdachts der geheimdienstlichen Agententätigkeit festgenommen wurde. Der 31-jährige Deutsche arbeitete in der Abteilung Einsatzgebiete/Auslandsbeziehung. Seine Aufgaben beim BND waren u.a. das Entgegennehmen und Einscannen von Dokumenten. Seit Ende 2012 wurde er von den US-Geheimdiensten als Agent registriert. Er habe sich selbst der US-Botschaft in Berlin per Mail als Agent angeboten. Neben der Anschuldigung der Spionage an dem BND, soll er für die CIA auch die NSAUA ausspioniert haben. Er soll mehr als 200 Dokumente des BND beschafft und an die amerikanischen Geheimdienste verkauft haben. Davon würden drei Dokumente einen direkten Bezug zur NSAUA aufweisen. Nicht nur dass der BND offensichtlich ein Sicherheitsproblem in seiner Archiv- und Dokumentationsabteilung hat, sondern soll die Aufdeckung des Spions auch nur durch Zufall geschehen sein. Nachdem der Spion seine Dienste auch dem russischen Geheimdienst anbot, flog er auf, da die Russen im Gegensatz zu den Amerikanern von der deutschen Spionageabwehr überwacht werden. So wurde die Mail vom Bundesverfassungsschutz abgefangen. Bis dato profitiert der Spion davon, dass verbündete Staaten nicht ausspioniert werden. Er habe durch den Verkauf der Dokumente rund 25.000€ verdient.[36]

[33] Vgl. (Bundesministerium für Justiz und für Verbraucherschutz)
[34] Vgl. (Krempl, Geheimakte BND & NSA: Operation Eikonal – das Inland als "virtuelles Ausland", 2017)
[35] Vgl. (Greis, 2014)
[36] (Schwarze, 2014)

Durch die Spionage des BND und des Untersuchungsausschusses wurde der ehemalige BND-Mitarbeiter zu acht Jahren Haft verurteilt. Dabei sprach man ihn „des Landesverrats und der Verletzung von Dienstgeheimnissen“ schuldig. Als Motivation nannte der Beschuldigte Langeweile und Geld.[37]

Am 9. Juli 2014 konnte ein zweiter US-Spion entlarvt werden. Es handelte sich dabei, um einen Mitarbeiter des Bundesverteidigungsministeriums, der ausgerechnet bei der Aufarbeitung des Spionageverdachte des ehemaligen BND-Mitarbeiters mitwirkte.[38]

In der Zeit des Bestehens des NSAUA kam des Öfteren die Vermutung auf, dass Mitglieder ausspioniert wurden. Oftmals betraf es die Krypto-Handys, die entweder monatelang abgehört oder manipuliert worden sein sollen. Konkrete Beweise bzw. Täter konnten dabei nicht identifiziert werden.[39]

3.1.4 Ergebnis des NSAUA und Folgen

„Kein Ausschuss oder Kontrollgremium hat sich bisher so intensiv damit beschäftigt, wie elektronische Kommunikationsüberwachung im 21. Jahrhundert funktioniert."[40] Wie man anhand dieses Zitats von Christian Flisek, SPD-Vertreter des NSAUA, erkennen kann, war das Interesse und der Drang nach der Aufklärung der Spionageaktivitäten seitens des NSAUA enorm. Trotz diverser Schwierigkeiten und Einschränkungen, wie bspw. Schwärzen oder gar nicht aushändigen von Dokumenten durch das Bundeskanzleramt, konnte der Ausschuss einige Erkenntnis aufdecken, die bis dato nicht angenommen wurden, und einiges erreichen.

Wie sich im Laufe der Ermittlungen feststellte, stellte der BND sich in den Dienst der NSA und lieferte große Datenmengen an jene. Durch diese Recherche konnte der NSAUA das Verständnis im Bereich der Internetüberwachung durch Geheimdienste offen darlegen. Außerdem konnten sie beweisen, dass der BND und das Bundeskanzleramt Gesetze wissentlich übergangen und es riskiert haben, Bürgerrechte zu missachten, um an möglichst viele Ergebnisse zu gelangen. Ebenfalls fand der Ausschuss Belege für die Spionage an befreundeten Politikern der Bundesrepublik Deutschland durch den BND, wie z.B. hochrangiger Beamter des französischen Außenministeriums, des Präsidentenpalastes in Paris und der EU-

[37] Vgl. (jog/dpa, 2016)
[38] Vgl. (fued, 2014)
[39] Vgl. (Juh, 2014)
[40] Vgl. (mh/pxt/dpa, 2017)

Kommission in Brüssel.[41] Eine der wichtigsten Erkenntnisse war, dass alle Kontrollen des Geheimdienstes in Deutschland gescheitert sind. Zeugenbefragungen ergaben, dass Verstöße weder durch interne Kontrollen der Nachrichtendienste, der Fachaufsicht des Bundeskanzleramtes noch durch externe Kontrollen der Datenschützer bemerkt oder beendet werden konnten. Daraus erschließt sich, dass Geheimdienste auch in einem demokratischen Staat schwer zu kontrollieren sind.

Neben all jener positiven Erkenntnis des NSAUA gibt es diverse Misserfolge und Fragen, die nicht geklärt werden konnten. Die Person, durch dessen Aufdeckung der Ausschuss überhaupt konstruiert wurde, konnte nicht befragt werden, auch wenn Snowden zum Hauptzeugen benannt wurde. Ebenso konnte kaum Transparenz bei den Ermittlungen geschaffen werden, obwohl dies ein wichtiges Anliegen für den NSAUA war. Ohne Berichte diverser Medien, wie von „Netzpolitik.org“ hätte die Öffentlichkeit viele Informationen nicht bekommen, da Zeugen und Akten oftmals als streng geheim eingestuft wurden. Außerdem konnten keine Erkenntnisse und Untersuchungen zu weiteren Projekten der BND, wie bspw. „Wharpdrive“, und anderen ausländischen Geheimdiensten, wie vorab angekündigt, vorgenommen werden, da das Bundeskanzleramt wegen der fehlenden Zustimmung der Länder die Ausgabe der Dokumente an den NSAUA verweigerte. Ebenfalls konnte auch nicht bewiesen werden, ob das Handy der Bundeskanzlerin abgehört wurde, da das NSA-Dokument nicht als Original vorlag und die Bundeskanzlerin ihr Handy nicht zur Analyse freigab.[42]

Auch wenn diverse Probleme und Fragen nicht beantwortet werden konnten, war die Berufung des NSAUA wichtig, da er bewiesen hat, dass die Kontrolle von Geheimdiensten verbessert werden muss. Dadurch hat die Regierung neue präzisere Gesetzespakete erlassen. Jedoch werden diese von der Opposition beklagt, da die Gesetze eine Legalisierung der Auslandsüberwachung darstellen sollen. Durch die Befürchtung von Terrorangriffen, wie bspw. islamistisch-motivierten Anschlägen, kann die einst angestrebte strikte Geheimdienstreform nicht umgesetzt werden, sondern nur eine abgeschwächte Form. Dabei soll die bisherigen „Ausland-Ausland-Fernmeldeaufklärung“, die auch aus dem deutschen Inland erfolgen darf, klar definiert werden. Ziel ist dabei „Erkenntnisse über das Ausland zu gewinnen, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind“. Dafür wird die „Rechtssicherheit und damit die Handlungsfähigkeit des BND gestärkt“. Zudem soll durch das Bundeskanzleramt und ein Gremium aus den Richtern

[41] Vgl. (dpa, 2015)
[42] Vgl. (Biermann, 2017)

des Bundesgerichtshofs die Fernmeldeaktivitäten geprüft werden. Für EU-Bürger sowie Einrichtungen der Europäischen Union und öffentliche Stellen ihrer Mitgliedstaaten sollen ab sofort besondere Schutzvorgaben gelten. Künftig erhofft sich die Bundesregierung mit dem Gesetz, bei der Weitergabe der Daten an ausländische Geheimdienste mehr Rechtssicherheit und Achtung der Privatsphäre von privaten Daten der Menschen zu schaffen.[43]

Gegner dieser neuen Regelung kritisieren, dass die BND seine Internet-Überwachung dadurch massiv ausbauen kann und dass die Taten der Vergangenheit, die durch den NSAUA aufgedeckt wurden, einfach legalisiert und ausgeweitet werden dürfen. Im Folgenden werden die Meinungen wichtiger Politiker, Juristen und Leuten aus der Wirtschaft zu dem Gesetzerlass des Bundestages aufgezeigt:

Linke: „Ausspionieren unter Freunden geht jetzt doch“

„Es ist letztlich das eingetreten, was wir befürchtet haben: Anstatt dem BND klare rechtliche Grenzen aufzuzeigen und Grauzonen zu beseitigen, soll nun fast alles nachträglich gesetzlich legitimiert werden, was sich im NSA-Untersuchungsausschuss als unzulässig und rechtswidrig, mindestens aber fragwürdig herausgestellt hat. Mit dem Entwurf soll die Massenüberwachung durch den BND nunmehr auf eine gesetzliche Grundlage gestellt werden. Uns stört aber nicht in erster Linie das Fehlen einer gesetzlichen Grundlage, sondern die Massenüberwachung selbst. Diese lehnen wir ganz grundsätzlich ab.“[44]

Nešković: „Mit Schein des Rechts das Recht betrügen“

Mit dem Gesetzentwurf will das Bundeskanzleramt einen verfassungswidrigen Zustand beseitigen: Das ist rechtlich und politisch misslungen. Durch die Verwendung einer Fülle von unbestimmten Rechtsbegriffen erfüllt der Gesetzentwurf nicht den verfassungsrechtlich gebotenen Grundsatz der Normenklarheit. So versucht er, mit dem Schein des Rechts das Recht zu betrügen. Das zeigt sich insbesondere bei der Schaffung des so genannten ‚Unabhängigen Gremiums‘. Wer Mitglied wird, entscheidet allein die Bundesregierung. Mit anderen Worten: der zu Kontrollierende entscheidet über den Kontrolleur. Damit muss die Regierung im Gesamtsystem der Kontrolle ihre Kontrolleure nicht fürchten: Im Parlamentarischen Kontrollgremium haben die Regierungsfraktionen eine verlässliche Mehrheit und beim

[43] Vgl. (Bundesregierung, 2016)
[44] André Hahn, Abgeordneter der Linksfraktion und Mitglied des Parlamentarischen Kontrollgremiums,

„Unabhängigen Gremium" haben sie es in der Hand, wer berufen wird. Damit bleibt die Kontrolle das, was sie bislang war – ein makaberer Witz."[45]

Internet-Knoten DE-CIX: „Gesetzentwurf ist ein absolutes Debakel"

„Alles, was NSA und GCHQ vorgeworfen wurde, soll dem BND jetzt auch erlaubt sein – die Bundesregierung legalisiert die Praxis sozusagen im Nachhinein. Wenn der Gesetzentwurf so verabschiedet wird, wird erstmalig in voller Absicht eine anlasslose Massenüberwachung im Inland gezielt erlaubt. Auch die Kommunikation deutscher Staatbürger wird dem Dienst dabei zugeleitet, der einzige Schutz unserer Grundrechte besteht in einem obskuren, geheimen Filter welcher – wie bereits in der Gesetzesbegründung ausgeführt – schlicht nicht in einem ausreichenden Masse funktional ist."[46] [47]

Die Aussagen dieser Personen zeigen teils unterschiedliche Perspektiven auf, jedoch ist bei allen der gemeinsame Tenor klar: Die Erschütterung vor der rechtlichen Legitimation der Massenüberwachung im Inland und die Furcht vor der Spionage eigener Daten ohne das Wissen und das Recht der gerichtlichen Klage.

3.1.5 Keine Spionage in Deutschland

Nach der Legalisierung und Ausweitung der Massenüberwachung der BND folgte im Herbst 2017 eine weitere Enttäuschung für Bürgerrechtler und Gegner der Vorratsdatensammlung. Sowohl nach den Ermittlungen der Bundesanwaltschaft in Karlsruhe als auch denen der NSAUA seien keine Anhaltspunkte vorhanden, die belegen, dass der NSA „deutsche Telekommunikations- und Internetdaten rechtswidrig, systematisch und massenhaft überwacht haben soll und beenden somit die Ermittlungen. Der Grund für den Beschluss sei, dass die von Snowden veröffentlichten Dokumente zwar als authentisch eingestuft wurden, sie jedoch nur „allgemein die Möglichkeiten und Maßnahmen der strategischen Fernmeldeaufklärung" durch die amerikanischen Geheimdienste darlegen. Darunter sei festzuhalten, dass der anfängliche Verdacht auf Aktivitäten im Hinblick auf Deutschland sich nicht bestätigt hätte und dass in den Dokumenten ausschließlich von den technischen Möglichkeiten berichtet wurde, aber nicht von konkreten Handlungen, Tatzeiten oder -orten. Zudem lasse sich aus den NSA-Dokumenten ableiten, dass die NSA zwar wie alle weltweit großen Nachrichtendienste Kommunikation

[45] Wolfgang Nešković, ehemaliger Richter am Bundesgerichtshof,
[46] Klaus Landefeld, Beirat der DE-CIX Management GmbH,
[47] Vgl. (Meister, 2016)

erfassen, jedoch nicht eigenmächtig den deutschen Telekommunikations- und Internetverkehr überwacht haben. Die Gründe ähneln denen des Abhörskandales der Bundeskanzlerin.[48]

Nach Aussage des Grünen-Fraktionsvize Konstantin von Notz sei das Verwehren der Erkenntnisse vom NSAUA von Seitens des Generalbundesanwalts ein „Schlag ins Gesicht für die Bürgerrechte" und zollte dadurch keine Achtung der jahrelangen Arbeit des NSAUA. Nach dreieinhalb Jahren endete der NSAUA sogar im Streit. Während die SPD und CDU die Ansicht der Bundesanwaltschaft teilten, hielt die Opposition an der These der anlass- und unterschiedslosen Massenüberwachung – auch der deutschen Bevölkerung – durch die NSA fest. Als Reaktion darauf lehnte die Opposition den beschönigenden Abschlussbericht im Juni ab und verfasste selbst ein Sondervotum[49], indem sie den Vorwurf der Massenüberwachung der NSA deutlich unterstrichen.[50] Jedoch wurde nach Angabe der Regierungsfraktion das Sondervotum nicht nur zu spät eingereicht, sondern enthielt noch Passagen mit geheimen Inhalt, die noch nicht veröffentlicht werden durften. Daraufhin verweigerte die Opposition die Unterschrift unter dem Abschlussbericht. Ohne die Unterschriften aller Mitglieder des Untersuchungsausschusses könne der Bericht nicht dem Bundestag vorgelegt werden. Um dies zu verhindern, entzog der Ausschussvorsitzende Sensburg von der CDU den Mitgliedern der Linkspartei und den Grünen ihre Ämter als Berichterstatter per Vorsitzenden-Diskret, was bis dato in Deutschland in einem Untersuchungsausschuss noch nie vorgefallen sei. Die Oppositionsmitglieder reagierten und wollen rechtliche Schritte prüfen und einreichen. "Ein Untersuchungsausschuss ist Instrument der Minderheit zur Kontrolle der Regierung"[51]

3.2 ZITiS – Zentrale Stelle für Informationstechnik im Sicherheitsbereich

Angesichts der Legalisierung und Legitimation der Massenüberwachung von ausländischen Daten durch die BND hat das Bundesministerium am 6. April 2017 den Beschluss zur Eröffnung einer deutschen Bundesoberbehörde mit dem Namen „Zentrale Stelle für Informationstechnik im Sicherheitsbereich“, kurz ZITiS, erlassen. Die ZITiS stellt einen Dienstleister für die Sicherheitsbehörden in Deutschland dar, dessen Aufgaben sich am Bedarf

[48] Vgl. (Biselli, 2017)
[49] Mit einem Sondervotum können Minderheiten in einem Ausschuss ausdrücken, dass sie in bestimmten Punkten des Abschlussberichts inhaltlich anderer Meinung sind.
[50] Vgl. (ZEIT ONLINE, AFP, kg, 2017)
[51] Vgl. (tagesschau, 2017)

der Sicherheitsbehörden orientieren und die Bereiche der digitalen Forensik[52], der Telekommunikationsüberwachung, die Krypto-[53] und Big-Data-Analyse[54] umfassen. Zudem helfen sie bei technischen Fragen der Kriminalitätsbekämpfung und der Gefahren- und Spionageabwehr. Im Gegensatz zum BND hat die ZITiS keine Eingriffsbefugnisse und ist keine Beschaffungsorganisation. Dementsprechend dürfen sie selbst keine Daten erheben oder sammeln. Sie gehen lediglich dem anwendungsbezogenen Forschungsauftrag, über den auf der Jahreshauptversammlung mit den verschiedenen Behörden abgestimmt wird, nach. Zur Umsetzung des Forschungsauftrags entwickeln sie Strategien und technische Lösungen, testen Werkzeuge mit Cyberbezug und koordinieren gemeinsame Projekte für deutsche Sicherheitsbehörden. Sinn und Zweck der Berufung war es die Abhängigkeit der deutschen Geheimdienste von ausländischen Geheimdiensten bzw. Dienstleistern beim Bezug von technischen Werkzeugen zur Datensammlung zu beenden. Zudem die bislang 40 verschiedenen Behörden, die sich mit cyberbezogenen Lösungen auseinandersetzen, zu bündeln und das Know-how zu kanalisieren.

Das Ziel der ZITiS ist „nicht das technisch Machbare, sondern das technisch Notwendige“. Im Bereich der Erforschung und Entwicklung von Lösungen mit Cyberbezug bekleiden sie eine zentrale Rolle und sind damit ein wichtiger Teil der Cyber-Sicherheitsstrategie Deutschlands. Mit ihrer Arbeit möchte die ZITiS die zuständigen Behörden bei der effektiven Gefahrenabwehr und Strafverfolgung unterstützen und damit einen Beitrag zum Schutz der deutschen Bürgerinnen und Bürger leisten.[55]

Die ZITiS ist heutzutage noch wichtiger im Bereich Datensammlung und Ermittlung für deutsche Geheimdienste geworden, da er technische Werkzeuge zum Abhören und Mitlesen neben der üblichen Telekommunikation über Glasfaserkabel auch von verschlüsselter Kommunikation[56], wie z.B. Handygespräche über Skype oder Chatverläufe von WhatsApp, ermöglicht.[57]

Von Kritikern wird die ZITiS als „Heimat der Bundeshacker“ tituliert, da sie systematisch nach Schwachstellen in der von Millionen von Menschen täglich benutzten Technik suchen sollen.

[52] Digitale Forensik behandelt die Untersuchung von verdächtigen Vorfällen im Zusammenhang mit IT-Systemen
[53] Krypto-Analyse ist die Methode und Technik, um Informationen aus verschlüsselten Texten zu gewinnen
[54] Big-Data-Analyse ist die systematische Auswertung großer Datenmengen mit Hilfe neu entwickelter Software
[55] Vgl. (ZITiS, 2017)
[56] Bei verschlüsselter Kommunikation handelt es sich um Daten, die nur auf den Geräten von Sendern und Empfängern entziffert werden kann
[57] Vgl. (Beuth, 2017)

Dabei werden sie sogar von der Bundesrepublik finanziell unterstützt. Im Vergleich zu der ZITiS sind andere Unternehmen in dieser Branche privatwirtschaftlich organisiert und profitorientiert. Durch das Entdecken und den Verkauf von den Sicherheitslücken an Dritte erzielen diese Unternehmen mehr Gewinn als es dem jeweiligen Hersteller zu melden, der nur eine einmalige Prämie auszahlen würde, wie z.B. beim Bug-Bounty-Programm von Apple[58]. So muss jeder einzelne Interessent für die Informationen der Sicherheitslücke zahlen, um diese ausnutzen zu können.

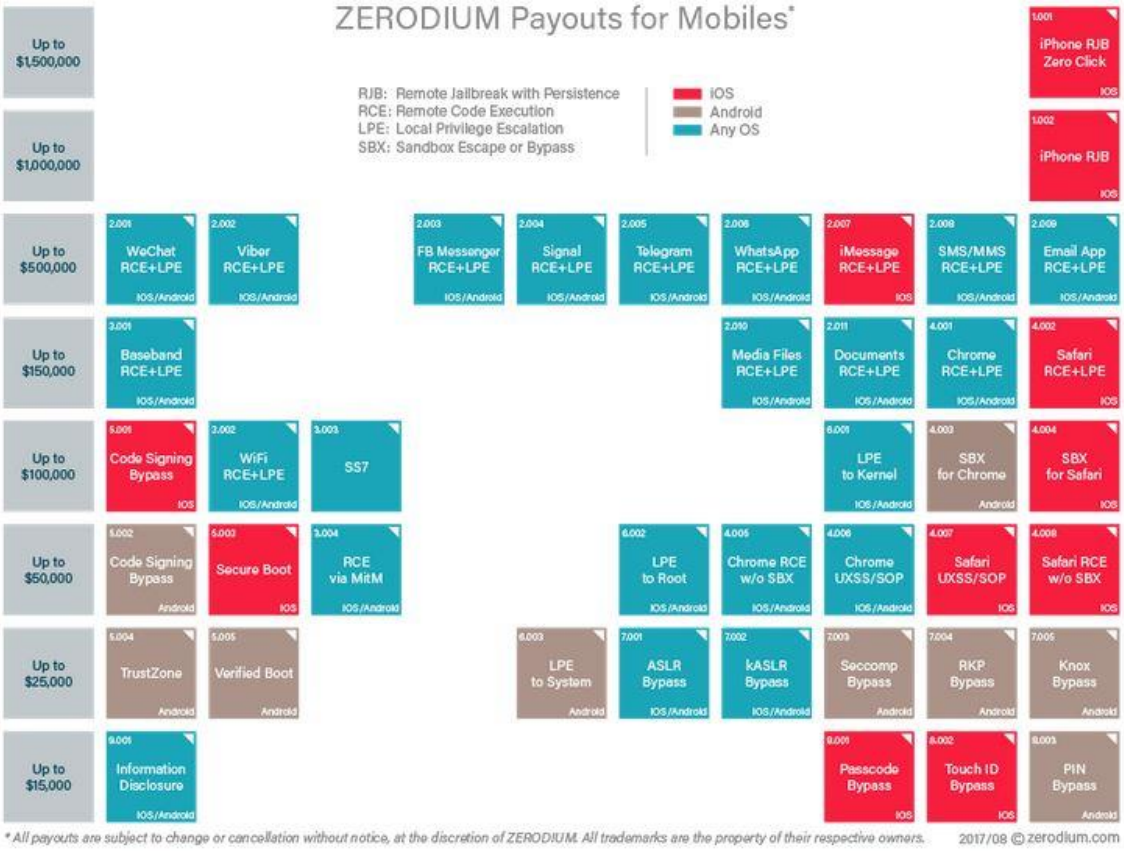

Abbildung 3: Übersicht der Bezahlungen von Zerodium für Mobile-Programme[59]

[58] Ein Programm, welches Apple initiiert hat, um Hacker für das Aufzeigen von Sicherheitslücken zu belohnen (200.000 US-Dollar).

[59] Nach (ZERODIUM, 2018)

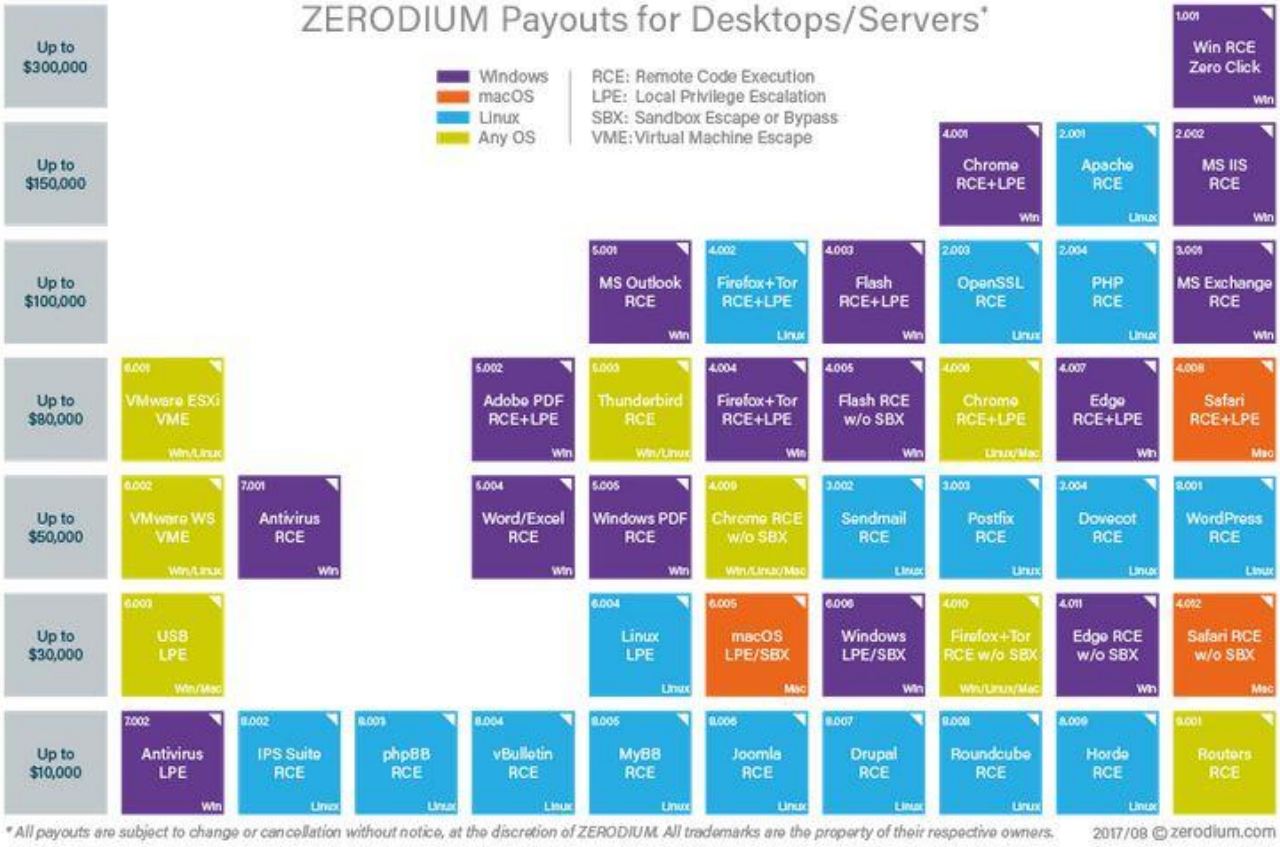

Abbildung 4: Übersicht der Bezahlungen von Zerodium für PC-Programme[60]

Wie man Anhand von Abbildung 3 sehen kann, zahlt das Unternehmen Zerodium[61] für bisher unbekannte Sicherheitslücken und das dazugehörige Exploit[62] bis zu 1,5 Millionen US-Dollar, was im Vergleich zu den Herstellern, die die Sicherheitslücke in ihrer Software haben, deutlich mehr ist. Außerdem fällt bei der Betrachtung von Abbildung 3 und Abbildung 4 auf, dass die Prämien für die Sicherheitslücken und dem dazugehörigen Exploit für Mobile-Programme, wie z.B. „Facebook-Messenger“ oder „WeChat“, höher ausfallen als für PC-Programme, wie bspw. Microsoft. Daran wird ersichtlich, dass das Eindringen in mobile Geräte in der heutigen Zeit wichtiger bzw. lukrativer ist als in Computer, da zu den Käufern Geheimdienste und Staaten gehören, die diese Informationen zur Strafverfolgung und zum Aufdecken von terroristischen Aktivitäten verwenden. „Leitungen transportieren häufig nur noch unbrauchbare Daten, also sind die Endgeräte das neue Ziel.“

Um die Kommunikation in Deutschland für private Nutzer von Mobilegeräten zu sichern, hat die Bundesregierung beschlossen, dass die Verschlüsselung der privaten Kommunikation zur Regel werden soll. Jedoch heißt im Entwurf zur Cybersicherheitsstrategie der Bundesregierung:

[60] Nach (ZERODIUM, 2018)
[61] Zerodium ist ein Händler für Sicherheitslücken und Exploits.
[62] Ein Exploit ist ein der Sicherheitslücke angepasstes Werkzeuge, mit der man jene auszunutzen kann.

„Die deutsche Kryptostrategie umfasst Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung."[63] Wie man anhand dieses Zitates erkennen kann, entsteht ein Widerspruch in der Vorstellung der Bundesregierung. Würde die ZITiS ihre Kenntnisse über die Sicherheitslücken ad hoc mit den betroffenen Herstellern teilen, so könnte dieser die Sicherheitslücke schließen und man würde Millionen von Nutzer schützen. Indes sollen die Kenntnisse zum Entwickeln von Exploits für die deutschen Nachrichtendienste dienen. Dadurch akzeptiert die Bundesregierung das Risiko, dass andere die gleichen Sicherheitslücken finden und ebenfalls zur Überwachung von Menschen nutzen. Folglich kann man aus der Berufung der ZITiS erkennen, dass die Bundesregierung Innere Sicherheit und IT-Sicherheit als gegensätzlich erachtet.

3.3 Anstieg der Tor-Nutzerzahlen in Deutschland

Nachdem durch Edward Snowden bekannt wurde, dass Nachrichtendienste die Daten von normalen Bürgern sammeln und die Kommunikation im Internet verfolgen, wurde durch die Berichterstattung größerer Medien die Bekanntheit des Tor-Netzwerkes in Deutschland rasant größer. Das Tor-Netzwerk ist ein Netzwerk im Internet zur Anonymisierung von Verbindungsdaten und kann für Browsing, Instant Messaging, E-Mail-Verkehr etc. eingesetzt werden. Dabei beruht das Prinzip auf dem sogenannten „Onion-Routing“[64] und ermöglicht dem Nutzer den Schutz vor der Analyse des persönlichen Datentransfers. Wenn ein Nutzer über Tor surfen möchte, wird im ersten Schritt durch eine zuvor heruntergeladene Software („Client“) eine Liste von allen verfügbaren und aktiven Tor-Knoten erstellt. Im zweiten Schritt wird eine Route über drei verschiedene Knoten zum Empfänger kreiert, die sich alle zehn Minuten verändert. Der ständige Wechsel von den Tor-Knoten bzw. Servern führt zur Verschleierung des Standorts des Nutzers. Dies ermöglicht der Bevölkerung von Staaten, die einer Zensur unterliegen, den Zugriff auf die vom Staat zensierten Webseiten, bspw. der Zugriff auf Facebook in China.

[63] Vgl. (Beuth, 2017)

[64] Onion Routing ist eine Anonymisierungstechnik im Internet. Dabei werden die übertragenden Daten mehrmals verschlüsselt. Auf die Daten wird Innerhalb jedes Knotens ein Ent- bzw. Verschlüsselungsschritt angewendet. Welches angewendet wird, hängt davon ab, ob die Daten gesendet oder empfangen werden. Durch den Client wird jedes zu sendende Paket verschlüsselt und jedes empfangene Paket entschlüsselt.

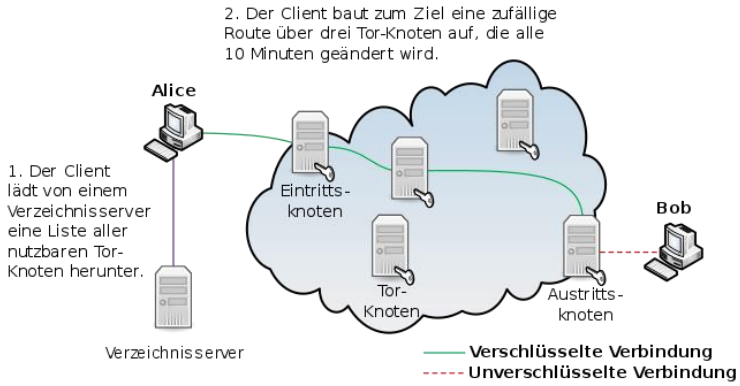

Abbildung 5: Graphische Darstellung der Funktionsweise vom Tor-Netzwerk[65]

Durch die mediale Präsenz stieg das Interesse der Bevölkerung für anonymes Surfen im Internet und führte zur Verdopplung der Nutzerzahl des Tor-Netzwerkes in Deutschland im Jahr 2013 (siehe Abbildung 6).

Seit Ende 2014 bietet Facebook den Zugang über die Tor-Domain „https://www.facebookcorewwwi.onion/“ an („Hidden Service“), um den Nutzern Sicherheit und Privatsphäre zu gewähren und Dritten, wie etwa Telefonanbietern, Hackern oder Geheimdiensten, das Mitlesen und den Zugriff auf das jeweilige Konto zu erschweren. Jedoch muss man dabei beachten, dass dennoch eine Anonymität des Nutzers nicht gewährleistet wird, da Facebook weiterhin persönliche Daten, wie bspw. Bilder und Videos, speichert und zur freien Verfügung erhält. Der primäre Nutzen ist hierbei der Kampf gegen die Zensur von Staaten.[66]

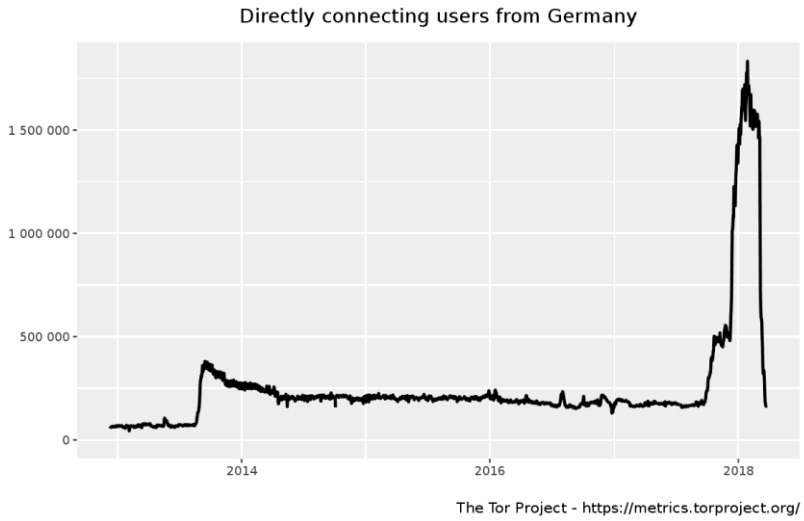

Abbildung 6: Diagramm der Nutzer des Tor-Browsers aus Deutschland (Stand:27.03.2018)[67]

[65] Nach (File:TOR Arbeitsweise.svg, 2016)
[66] Vgl. (Kühl, 2016)
[67] Nach (Tor Metrics, 2018)

Wie man anhand der Abbildung 6 sehen kann, gab es nicht nur einen sprunghaften Anstieg der direkten Verbindungen mit dem Tor-Netzwerk in Deutschland im Jahr 2013, sondern auch am Ende des Jahres 2017. Jedoch war der Fall genauso schnell wie der rasantere Anstieg. Warum es zu solch einem Anstieg kam, können Experten noch nicht erklären, da der Anstieg der Nutzerzahlen in Deutschland in dem Zeitraum ein Einzelfall war. Oft lässt sich solch eine Situation durch eine vom Staat umgesetzte Zensur erklären, jedoch trifft dieser Fall für Deutschland nicht zu.[68] Möglicherweise resultiert das gestiegene Interesse an der Datensicherheit aus dem Hype des Bitcoins, dessen Wert im gleichen Zeitraum stieg (Höchststand am 17.12.2017: 1 Bitcoin = 16.892,34€)[69], und der allgemeinen Funktionsweise des Blockchain.

Um die gestiegene Relevanz des Tor-Netzwerk in Deutschland zu verdeutlichen, kann man auf der Website des Unternehmens „Uncharted“ eine TorFlow-Karte sehen, die Datenströme von 2007 bis 2016 zeigen (siehe Abbildung 7).

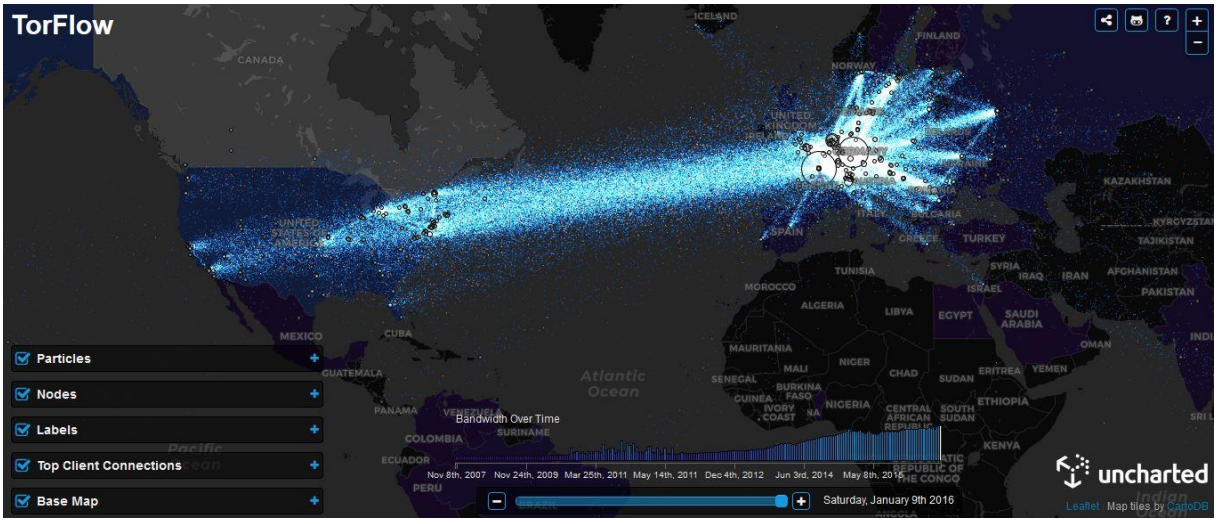

Abbildung 7: TorFlow-Karte (Stand: 09.01.2016)[70]

Bei der Betrachtung der Abbildung 7 fällt auf, dass sich die Bandbreite bzw. Signalverbreitung in den letzten Jahren weltweit erhöht hat und dass die meisten Datenpakete (dargestellt als blaue Punkte) aus Europa bzw. Deutschland transportiert werden.

[68] Vgl. (Hayon, 2017)
[69] Nach (Finanzen.net, 2018)
[70] Nach (Uncharted, 2016)

4. Digitalisierung und Datenschutz: Datensammlung in der deutschen Wirtschaft

Ein wichtiges Thema heutzutage sowohl für die Wirtschaft als auch für das Bildungssystem ist die Digitalisierung[71]. Das Thema, welches in den Medien zurzeit hohe Wellen schlägt, wurde durch die am 14. März 2018 neuernannte Staatsministerin für Digitalisierung, Dorothee Bär, wieder publik. Vor ihrem Amtsantritt prangerte sie an, dass die Digitalisierung Deutschlands „viel, viel zu langsam" voranschreite. Außerdem kritisierte sie, dass der Datenschutz „wie im 18. Jahrhundert" sei. Damit möchte sie ausdrücken, dass der Schutz der Daten ziemlich streng und zu stark sei. Ein starker Datenschutz sei zwar ein Vorteil für Unternehmen, die geheime Daten in einer Cloud[72] speichern wollen und analysieren lassen, jedoch bestehe bei einem zu starken Datenschutz die Gefahr, dass deutsche und auch europäische Unternehmen in ihrer internationalen Wettbewerbsfähigkeit zu sehr geschwächt werden würden.[73] Genau dies befürchtet sie mit der Umsetzung der neuen europaweitgeltenden Datenschutzgrundverordnung, die zwar einen einheitlichen Datenschutz in Europa gewährleistet und somit die Verlagerung der Firmensitze, z.B. nach Irland – schwächsten Gesetze im Bereich der Privatsphäre in Europa – verhindert, jedoch auch gleichzeitig das Sammeln der Daten für die Big-Data-Analyse erschwert. Die neue Datenschutzgrundverordnung sagt aus: „Unternehmen dürfen Daten, die sie für einen bestimmten Zweck bekommen, nicht ungefragt weitergeben oder für andere Zwecke nutzen." Erst „durch [ein] eindeutiges Handeln" des Nutzers, welches eine Zustimmung aussagt, dürfen die Daten verwendet werden.[74] Derzeit steht Facebook durch den Verstoß dieses Gesetzes in der Kritik. Durch die britische Datenanalysefirma Cambridge Analytica sollen Daten von mehr als 50 Millionen Facebook-Nutzern abgeschöpft und für den Wahlkampf des heutigen US-Präsidenten Donald Trump ausgewertet worden sein. So konnten gezielt Anzeigen für den Präsidentschaftskandidaten Trump geschaltet werden. Dorothee Bär fordert schwerwiegende Konsequenzen für die Taten.[75]

Ein wichtiges Credo für Bär ist, dass die Digitalisierung zum Top-Thema für alle Bürger, Unternehmen und Politiker werden muss. Dabei solle der Staat als „Vorreiter" agieren, indem

[71] Die Digitalisierung bezeichnet das Umwandeln von analogen Werten in digitale Formate bzw. Daten, welche informationstechnisch verarbeitet werden können.
[72] Unter Cloud (deutsch: Rechnerwolke oder Datenwolke) versteht man die Bereitstellung von IT-Infrastruktur als Dienstleistung über das Internet, wie z.B. für Speicherplatz, Rechenleistung oder Anwendungssoftware
[73] Vgl. (Krempl, 2017)
[74] Vgl. (Krempl, 2015)
[75] Vgl. (lob/AFP, 2018)

Fachministerien und Behörden, soweit digitalisiert sind, dass Bürger nicht mehr allzu viel Zeit auf Ämtern verschwenden, nur um bspw. sich umzumelden. Man dürfe auch durch „bürokratische Hürden“ die Chance von Start-up Unternehmen in Deutschland nicht schmälern. Außerdem ist ein wichtiges Anliegen für sie die Digitalisierung des Bildungssystems. Nicht nur durch das Ersetzen von Büchern durch Tablets, sondern auch durch die Integration von Programmiersprachen in den Lehrplan solle die Digitalisierung vorangetrieben werden. Genauso sei die Gründung von „Digitalgymnasien“, die sich noch ausführlicher mit der Vermittlung der IT beschäftigen sollen, – wie im Vergleich Musikgymnasium mit der Musik – wichtig. Das Beherrschen von Programmiersprachen sei heutzutage „so wichtig wie [das] Lesen und Schreiben".[76]

Durch die Beschleunigung der Digitalisierung von Unternehmen in Deutschland, möchte sie in der Branche der Digitalisierung ein Standing Deutschlands ähnlich wie in der Logistik und im Fußball schaffen: „Wir wollen auch Digital-Weltmeister werden!“[77] Laut der Studie „Digital Europe“ des McKinsey Global Institute, welches der McKinsey&Company – eine der weltweitführenden Unternehmens- und Strategieberatungen – gehört, nutze Deutschland derzeit lediglich 10% des wirtschaftlichen Nutzens der Digitalisierung und läge damit unter dem EU-Durchschnitt (12%). Im Vergleich weist der weltweitführende Staat, die USA, einen Wert von 18% auf. Den EU-Spitzenwert stellt Großbritannien mit 17%. Durch diesen geringen Wert des wirtschaftlichen Nutzens der Digitalisierung entgehen Deutschland Einnahmen im Milliardenbereich. „Wenn Deutschland sein digitales Potenzial optimal nutzen würde, könnte das Bruttoinlandsprodukt bis 2025 um einen Prozentpunkt jährlich zusätzlich wachsen – das sind umgerechnet insgesamt rund 500 Milliarden Euro"[78] Die stärksten digitalisierten Branchen in der EU seien die Informations- und Telekommunikationsbranche sowie Medien und Finanzdienstleistungen und die schwächsten vor allem kapitalintensive Branchen wie die Fertigungsindustrie, überwiegend staatliche Sektoren wie Gesundheits- und Bildungswesen sowie lokale Branchen wie die Bauwirtschaft und das Hotelgewerbe. Speziell in Deutschland ist die Digitalisierung in den Branchen Dienstleistung, Transport und Logistik äußerst schwach. Zudem besteht ein besonderer Nachholbedarf in Europa im Vergleich zu den USA laut der McKinsey&Company in dem Bereich der Start-ups: „Unter den „Unicorns“ – Start-ups mit einer Bewertung über 1 Milliarde Dollar – stammen lediglich fünf aus Europa.“[79]

[76] Vgl. (ZEIT ONLINE, AFP, dpa, mp, 2018)
[77] Vgl. (spo. /dpa, 2018)
[78] Karel Dörner, McKinsey-Seniorpartner
[79] Vgl. (McKinsey&Company, 2017)

Einen Befürworter in ihrem Anliegen findet die Staatsministerin für Digitalisierung in Stephan Noller. Der Psychologe, Unternehmer und Experte für Digitalisierung führt in seinem Gastbeitrag in der ZEIT die ungenutzten Vorteile der Digitalisierung in der Gesundheitsbranche auf. Dabei geht er beispielhaft auf ein unter den Menschen weitverbreitete Krankheit, dem Bluthochdruck, und die medikamentöse Behandlung ein. Die Frage, wie stark und in welchen Abstand das Medikament eingenommen werden soll, wird derzeit auf Basis einer 24-Stunden-Messung eingestellt. Auf Grundlage dieser Werte wird seiner Meinung nach eine sehr grobe Einteilung der Medikamente vorgenommen. „(…) alle bekommen eine Standardmedikation: einmal täglich fünf oder eben zehn Milligramm." Durch das Tragen eines „Wearables"[80] und einer App könne er selbst feststellen wie volatil der Wert seines Bluthochdruckes sei. „Bei manchen Leuten ist der Blutdruck morgens hoch, bei anderen abends. Manche reagieren empfindlich auf Stress, andere auf Lärm. Bei einigen gehen die Werte nach dem Sport runter, bei anderen nach dem Baden." Durch die Umsetzung einer Digitalisierung, wie bspw. durch eine Smartwatch, könne man die Dosierung auf jeden Patienten individuell anpassen und dadurch die Lebenserwartung durch weniger Nebenwirkungen steigern. Zudem auch langfristig die Kosten für das Gesundheitssystem senken. Ein Aspekt, der aufgrund des harten Datenschutzes und der damit verbundenen Auflagen in Deutschland und auch in der EU, nicht durchsetzbar sei, wäre der Abgleich der Messdaten und der Dosierung der Medikamente mit anderen Patienten. Dies würde eine eigene Medikation vereinfachen und transparent gestalten.[81]

Trotz der möglichen Vorteile der Digitalisierung gibt es viele Kritiker – darunter auch Politiker der SPD und der Grünen –, die die Haltung von Dorothee Bär zum Datenschutz als fragwürdig empfinden und ihr den Versuch eines Affronts gegen den Datenschutz vorwerfen. Dabei gehe es für die Kritiker nicht um „irgendwelche Daten, sondern [um die] Menschenwürde und individuelle Freiheit". Unternehmen, wie bspw. Facebook und Google, hätten schon mehr Informationen über die Menschen gesammelt als jeder Geheimdienst.[82]

[80] Ein Armband, welches Werte, wie bspw. für die Fitness, messen kann
[81] Vgl. (Noller, 2018)
[82] Vgl. (Krempl, 2018)

5. Fazit: Meinung des Autors

Als Autor der Seminararbeit möchte ich die Chance nutzen, meine persönliche Meinung zu der Thematik der Vorratsdatensammlung und den damit verbundenen Geschehnissen in Deutschland darzulegen und bediene mich bewusst des Schreibens aus der Ich-Perspektive. Dabei geht es mir nicht, um die Überzeugung des Lesers von meiner Meinung, sondern lediglich um die Publikation der eigenen Erkenntnisse und Überlegungen, die mir während der Recherche begegnet sind.

Die Ansicht des Whistleblowers Edward Joseph Snowden, dass jeder Mensch selbst über seine Daten frei entscheiden dürfen sollte, teile ich ganz und gar, da dies zu den demokratischen Grundstrukturen eines Rechtsstaates gehört. Dadurch empfinde ich die rücksichtslose Vorratsdatensammlung seitens der Geheimdienste als Verletzung dieser Strukturen. Ohne die Erlaubnis des einzelnen Bürgers sollten Kommunikationen bzw. Daten nicht abgehört oder gar gespeichert werden, solange jener Bürger keinen Gesetzesbruch begeht. Man sollte die Privatsphäre des Menschen respektieren, wobei ich auf Artikel 10 des Grundgesetzes erinnern möchte, der aussagt, dass „das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis […] unverletzlich“ sind. Eine für mich mögliche Legitimation der Datensammlung eines Bürgers wäre der erwähnte Gesetzesbruch, wie bspw. das Abrufen von Kinderpornographie oder der Verdacht der Terrorgefahr. Falls solch ein Fall vorliegt, sollte der Geheimdienst nicht freientscheiden dürfen, sondern erst durch die Zustimmung eines beauftragten Gremiums, wobei Transparenz zwischen Gremium und Bundesamt unabdingbar ist. Selbst in einer Demokratie sollte man darauf achten, dass Geheimdiensten nicht allzu viele Freiheiten gelassen werden. Denn zu viele Freiheiten für Geheimdienste, wie bspw. im Fall der BND und der Operation Eikonal, kann die Handlungen für die Regierung intransparent gestalten, sodass die Entscheidungsfähigkeit nicht mehr der Regierung obliegt und im Wohle der Mehrheit gehandelt werden kann. Um festzustellen, ob User im Internet solche Seiten abrufen, sollte der Zugriff auf diese Seiten beobachtet oder Filter zur Identifizierung jener genutzt werden.

Die Berufung eines parlamentarischen Untersuchungsausschusses empfinde ich als einen richtigen Schritt. So konnten viele Delikte und Unklarheiten aufgedeckt werden, wie z.B. die Zusammenarbeit der BND und NSA. Jedoch finde ich, dass das Bundeskanzleramt und der Bundestag vollste Unterstützung für die Ermittlung leisten hätten müssen und nicht die Ermittlungen behindern hätten sollen, wie durch bspw. Schwärzen oder gar nicht aushändigen von Dokumenten oder durch das nicht genehmigen der Befragung des Hauptzeugens Edward Snowden. Nicht nur die Vorratsdatensammlung konnte der NSAUA aufdecken – auch wenn

durch die Bundesanwaltschaft in Karlsruhe gerichtlich entschieden wurden, dass keine stattfand – sondern auch die Macht, die seitens der USA über die Bundesrepublik Deutschland bis heute herrscht. Belege hierfür sind u.a. die Verhinderung des Asylantrags zur Befragung von Edward Snowden in Deutschland und die allgemeine Datensammlung von internationalen Kommunikationsdaten durch die BND. Dies ging sogar soweit, dass auch Daten von EU-Mitgliedsstaaten gesammelt wurden, was in meinen Augen einen Vertrauensbruch und eine Gefährdung der europäischen Beziehungen für Deutschland darstellt. Zudem riskierte der BND auch, dass Daten der deutschen und in Deutschland lebenden Bürger in die USA überliefert werden, da eine hundertprozentige Datenfreiheit der deutschen Daten trotz der Verwendung von Filtern vielen Meinungen nach nicht möglich sei.

Obwohl die Gründung der ZITiS den Versuch einer autarken Handlungsfähigkeit Deutschlands bei der Investigation von Terrorismus und Internetkriminalität darstellt, betrachte ich die Aufgaben jener Bundesbehörde für kritisch. Sollte man wirklich Sicherheitslücken unter Verschluss halten, um Terrorismus frühzeitig entdecken zu können? Dabei wird riskiert, dass die Daten von Millionen von Menschen in die Hände von Hackern gelangen könnten. Der damit verbundene Schaden wäre enorm. Vielleicht wäre eine mögliche Kooperation mit den Software-Herstellern wohlmöglich der bessere Weg.

Die Spionageaktivitäten der Geheimdienste zeigen meines Erachtens diverse parallelen zur jüngeren deutschen Geschichte auf, in der DDR-Bürger vom Ministerium von Staatssicherheit ausspioniert und teils unschuldig inhaftiert wurden. Ein freies Bewegen in der Gesellschaft oder eine freie Meinungsäußerung war nur unter Vorbehalt möglich, da die Angst vor Konsequenzen durch mögliche Spitzel stets präsent war. Dies ist heutzutage mit dem Surfen oder die Kommunikation im Internet zu vergleichen. Durch die Befürchtung, dass die eigenen Daten gefiltert und gespeichert werden könnten, wird die freie Meinungsäußerung gehemmt und man muss selbst bei privater Kommunikation darauf achten, dass keine Äußerungen getätigt werden, die den Geheimdiensten negativ auffallen könnte und man selbst zu einem möglichen Verdächtigen wird. Selbst bei der Recherche über die Internetsuchmaschine Google könnte man durch die Verwendung von bestimmten Suchbegriffen, wie bspw. „IS“, den Verdacht erregen, terroristisches Gedankengut zu hegen, obwohl man eventuell nur versucht, sich über die Geschehnisse im Nahen Osten zu informieren. Außerdem kann der Missbrauch von erfassten Daten dazu führen, dass Meinungen gezielt beeinflusst werden, wie z.B. bei der aktuellen Facebook-Debatte zu sehen.

Nichtsdestotrotz finde ich nicht, dass die Vorratsdatensammlung komplett schlecht oder gar gefährlich sein muss. Wie im Beispiel von Stephan Noller aufgeführt (Kapitel 4), kann sie auch positive Aspekte für den Menschen bergen. Dabei sollten die Daten der Patienten jedoch nur unter Einwilligung gespeichert und abgeglichen werden. Auch der wirtschaftliche Nutzen darf nicht unter Acht gelassen werden. Auch hier gilt: Vorratsdatensammlung nur unter der Permisse der Zustimmung jedes Einzelnen!

Zum Abschluss meiner Seminararbeit möchte ich noch beifügen, dass die Sensibilisierung und Schulung der Menschen, wie z.B. durch Seminare an Universitäten oder durch die Berichterstattung von Medien und Organisationen, wie bspw. Netzpolitik.org, zum Thema Vorratsdatensammlung ein guter Weg ist, um diesen den bewussten Umgang mit den eigenen Daten nahezubringen. Dabei sollte man sowohl die positiven als auch die negativen Seiten der Vorratsdatensammlung berücksichtigen und sich bewusst zur oder gegen die Weitergabe und Sammlung der persönlichen Daten entscheiden. Auch das gestiegene Interesse am Tor-Netzwerk ist für mich ein positives Zeichen, das zeigt, dass die Menschen sich mehr mit dem Umgang der eigenen Daten im Internet auseinandersetzen.

6. Literaturverzeichnis

Antrag der Fraktionen CDU/CSU, SPD, Die Linke. und Bündnis 90/Die Grünen: Einsetzung eines Untersuchungsausschusses. (18. 03 2014). Abgerufen am 16. 03 2018 von Deutscher Bundestag: http://dip21.bundestag.de/dip21/btd/18/008/1800843.pdf

Biermann, K. (25. 09 2014). *BND-Zeuge im NSA-Ausschuss: "Dazu darf ich öffentlich nichts sagen".* Abgerufen am 16. 03 2018 von Zeit Online: http://www.zeit.de/politik/deutschland/2014-09/bnd-nsa-ausschuss-zeuge-bad-aibling/komplettansicht

Biermann, K. (23. 09 2014). *Spähskandal: Regierung enthält dem NSA-Ausschuss wichtige Akten vor.* Abgerufen am 16. 03 2018 von Zeit Online: http://www.zeit.de/politik/deutschland/2014-09/nsa-bnd-akten-geheim-konsultation

Biermann, K. (21. 11 2016). *BGH: NSA-Ausschuss darf Snowden vorladen.* Abgerufen am 16. 03 2018 von Zeit Online: http://www.zeit.de/politik/deutschland/2016-11/bgh-nsa-ausschuss-darf-edward-snowden-vorladen

Biermann, K. (28. 06 2017). *Überwachungsaffäre: Was der NSA-Ausschuss erreicht hat und was nicht.* Abgerufen am 16. 03 2018 von Zeit Online: http://www.zeit.de/politik/deutschland/2017-06/ueberwachungsaffaere-nsa-untersuchungsausschuss-abschlussbericht-faq

Bundesministerium für Justiz und für Verbraucherschutz. (kein Datum). *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10).* Von https://www.gesetze-im-internet.de/g10_2001/__7a.html abgerufen

Bundestag, D. (18. 03 2014). *Einsetzung eines Untersuchungsausschusses.* Abgerufen am 13. 03 2018 von dip21.bundestag.de: http://dip21.bundestag.de/dip21/btd/18/008/1800843.pdf

Caspari, L. (09. 04 2014). *NSA Ausschuss: Ein seltsamer Rücktritt.* Abgerufen am 16. 03 2018 von Zeit Online: http://www.zeit.de/politik/deutschland/2014-04/nsa-ruecktritt-binninger-ausschuss-fragen/komplettansicht

Deutscher Bundestag. (kein Datum). *I. Die Grundrechte.* Von Deutscher Bundestag: https://www.bundestag.de/parlament/aufgaben/rechtsgrundlagen/grundgesetz/gg_01/245122 abgerufen

dpa, AFP, sdo. (12. 06 2015). *NSA-Affäre: Ermittlungen zu Merkels Handy eingestellt.* Abgerufen am 13. 03 2018 von Zeit Online: http://www.zeit.de/politik/deutschland/2015-06/nsa-affaere-handy-ueberwachung-angela-merkel-ermittlungen-eingestellt

fued. (11. 07 2014). *Kuriose Verbindung zwischen Spionagefällen.* Abgerufen am 19. 03 2018 von Süddeutsche Zeitung: http://www.sueddeutsche.de/politik/geheimdienst-affaere-in-deutschland-kuriose-verbindung-zwischen-spionagefaellen-1.2041674

Goertz, J., Leyendecker, H., Mascolo, G., & Obermaier, F. (04. 07 2014). *NSA-Untersuchungsausschuss: Zur Sicherheit Musik.* Abgerufen am 16. 03 2018 von Süddeutsche Zeitung: http://www.sueddeutsche.de/politik/nsa-untersuchungsausschuss-zur-sicherheit-musik-1.2031158

Goetz, J., Kempmann, A., & Baars, C. (09. 05 2015). *US-Spionage in Deutschland: No-Spy-Abkommen war nie in Sicht.* Abgerufen am 13. 03 2018 von Tagesschau ARD: https://web.archive.org/web/20150509195945/http://www.tagesschau.de/inland/nospy-101.html

Greenwald, G. (2014). *Die globale Überwachung - Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen.* Droemer Knaur.

Greenwald, G., & MacAskill, E. (11. 06 2013). *Boundless Informant: the NSA's secret tool to track global surveillance data.* Abgerufen am 15. 03 2018 von The Guardian: https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

Greis, F. (08. 10 2014). *Operation Eikonal: NSA wollt die DE-CIX-Daten des BND nicht mehr.* Abgerufen am 20. 03 2018 von golem.de: https://www.golem.de/news/operation-eikonal-nsa-wollte-die-de-cix-daten-des-bnd-nicht-mehr-1410-109715.html

Gude, H., & Meiritz, A. (16. 10 2014). *Schriftliche Warnung: Kanzleramt droht NSA-Aufklärern mit Strafanzeige.* Abgerufen am 16. 03 2018 von Spiegel Online: http://www.spiegel.de/politik/deutschland/nsa-affaere-kanzleramt-droht-ausschuss-mit-strafanzeige-a-997468.html

Hamm, S. (Hrsg.). (18. 06 2013). *Big Boss is watching you*. Abgerufen am 12. 03 2018 von Deutschlandradio: https://web.archive.org/web/20140302121313/http://www.deutschlandfunk.de/big-boss-is-watching-you.724.de.html?dram:article_id=250267

Harding, L. (2014). *Edward Snowden // Geschichte einer Weltaffäre.* Weltkiosk.

heb. (15. 03 2015). *Asyl für Edward Snowden: USA sollen Deutschland "aggressiv" gedroht haben .* Von Spiegel Online: http://www.spiegel.de/politik/ausland/snowden-asyl-usa-sollen-deutschland-gedroht-haben-a-1024841.html abgerufen

jog/dpa. (17. 03 2016). *Urteil wegen Landesverrats:CIA-Spion beim BND muss acht Jahre in Haft.* Abgerufen am 19. 03 2018 von NTV: https://www.n-tv.de/politik/CIA-Spion-beim-BND-muss-acht-Jahre-in-Haft-article17244151.html

Juh. (03. 07 2014). *Spionageverdacht: Geheimdienst-Kontrolleure melden Cyberangriffe auf ihre Handys.* Abgerufen am 19. 03 2018 von Spiegel Online: http://www.spiegel.de/netzwelt/netzpolitik/spionageverdacht-steffen-bockhahn-und-roderich-kiesewetter-betroffen-a-980718.html

Krempl, S. (09. 04 2017). *Geheimakte BND & NSA: Operation Eikonal – das Inland als "virtuelles Ausland".* Abgerufen am 20. 03 2018 von heise online: https://www.heise.de/newsticker/meldung/Geheimakte-BND-NSA-Operation-Eikonal-das-Inland-als-virtuelles-Ausland-3677151.html

Medick, V. (11. 05 2015). *Ex-Ministerin Leutheusser-Schnarrenberger: "Das Kanzleramt hat die Menschen hinter die Fichte geführt".* Abgerufen am 13. 03 2018 von Spiegel Online: http://www.spiegel.de/politik/deutschland/no-spy-schnarrenberger-fuehlt-sich-von-merkel-betrogen-a-1033171.html

Meiritz, A. (28. 09 2014). *Einblick in NSA-Klageschrift: Grüne und Linke werfen Merkel Missachtung des Grundgesetzes vor.* Abgerufen am 16. 03 2018 von Spiegel Online: http://www.spiegel.de/politik/deutschland/nsa-spaehaffaere-opposition-verklagt-merkel-wegen-snowden-a-994029.html

Meiritz, A. (28. 05 2014). *Zeuge Snowden: NSA-Aufklärer stellen sich gegen ihren Vorsitzenden.* Abgerufen am 16. 03 2018 von Spiegel Online: http://www.spiegel.de/politik/deutschland/snowdens-selbstmarketing-sorgt-fuer-streit-im-nsa-ausschuss-a-972179.html

Moscolo, G., & Goetz, J. (1. 05 2015). *Die Überwachungsfabrik.* Abgerufen am 15. 03 2018 von SüddeutscheZeitung: http://www.sueddeutsche.de/politik/bnd-die-ueberwachungsfabrik-1.2460526

Niesen, C. (02. 16 2017). *Abhörskandal: Alles Wichtige zur NSA-Affäre.* Abgerufen am 15. 03 2018 von Spiegel Online: http://www.spiegel.de/politik/deutschland/nsa-affaere-worum-geht-es-a-1134779.html

Reuters. (28. 02 2014). *NSA-Affäre: Steinmeier rückt von Anti-Spionage-Abkommen ab.* Abgerufen am 13. 03 2018 von Zeit Online: http://www.zeit.de/politik/ausland/2014-02/usa-kein-no-spy-abkommen

Schwarze, T. (08. 07 2014). BND Affäre: In den Archiven liegt die Macht. Abgerufen am 19. 03 2018 von Zeit Online: http://www.zeit.de/politik/deutschland/2014-07/bnd-spionage-usa-cia-ermittlungen/komplettansicht

7. Abbildungsverzeichnis