



Institut für Politische Wissenschaft und Soziologie
Proseminar BMIB
Neue Entwicklungen und Herausforderungen in der internationalen Politik
Dozent: Dr. Kai Hirschmann
Wintersemester 2013/2014

**“So are we living in 1984?” –
Die Enthüllungen des Whistleblowers
Edward Snowden und ihre Folgen**

von

Tamara Nepicks

Gliederung:

	Seite
1. Einleitung	1
2. Die Enthüllungen des „Whistleblowers“ Edward Snowden und ihre Folgen	2
2.1 Die NSA-Affäre – Die Akteure und worum es geht	2
2.1.1 Die Hintergründe – Edward Snowden	2
2.1.2 Die Chronologie und Akteure des Skandals	4
2.2 Die Reaktionen in den USA und in Deutschland	7
2.3 Die politische Herausforderungen an die EU	11
3. Schlussfolgerung	13
Literaturverzeichnis	III
Eidesstattliche Versicherung	XII

1. Einleitung

„*So are we living 1984?*“ – der Vergleich, den der Online-Publizist des „The New Yorker“, Ian Crouch, im Juni letzten Jahres anstellte, hat in den weltweiten Diskussionen um den sogenannten „NSA-Skandal“ massiv Konjunktur.¹ Ausgelöst durch die Enthüllungen des informationstechnischen Experten und Geheimdienstmitarbeiters Edward Snowden, erlangt der bereits über sechzig Jahre alte Klassiker von George Orwell, „Nineteen Eighty-Four“, über den Schrecken eines totalitären Überwachungsstaates, neue Aktualität. Nicht nur, dass der Roman im letzten Jahr wieder in den Amazon-Bestsellerlisten war, auch inhaltlich werden in den Medien und internationalen sicherheitspolitischen Debatten Parallelen gezogen – *Big Brother is watching you*. Dabei geht es im Kern um die Frage, wie viel Überwachung notwendig und akzeptabel ist. Und ob diese Art der bekanntgewordenen Datensammlung überhaupt noch mit dem gemeinsamen Verständnis von Demokratie und dem Leben in einer freien Gesellschaft vereinbar ist, oder ob wir schon in einer „orwell’schen Dystopie“ leben?

Im Zeitalter von Globalisierung, Internet und weltweiter Vernetzung zu glauben, dass die Daten, die wir freizügig durch die Nutzung digitaler Medien selbst ins World Wide Web stellen, privat sind und bleiben, und man im Internet keine digitalen Spuren hinterlässt, ist wohl naiv. Wir leben in einer digitalen Gesellschaft. Dabei sind weder geheimdienstliche Überwachung noch Spionage, auch nicht im Cyberraum, neu. Ungeahntes Ausmaß hingegen haben die Quantität und die Qualität der Überwachung und der Analyse von Daten durch die NSA und den GCHQ erreicht – sie betreffen jeden. Doch ist es wirklich die große Überraschung oder gab es schon vorher Anzeichen? Bekannt ist, dass die Datenüberwachung und der Markt für IT-Sicherheit seit dem amerikanischen Trauma von 9/11 zugenommen haben.² Kurz nach den Anschlägen wurde der „Patriot Act“ verabschiedet, der die Bürgerrechte einschränkt und die Befugnisse der Geheimdienste und Ermittlungsbehörden erweitert.³ Das erklärte Ziel ist der Kampf

1 Auch der ehemalige deutsche BND-Chef Geiger zieht diese Metapher heran.

2 Seit 2004 gibt es eine Erweiterung der Aufgaben und Kapazitäten von Nachrichtendiensten bei der Abwehr von Terroristen und anderen internationalen Aufgaben, ausgehend von den Empfehlungen der „9/11 Kommission.“ IP, Jan./Feb. 2014, S. 108.

3 Aufweichung der richterlichen Aufsicht über Abhörmaßnahmen und der Aufzeichnung von Verbindungsdaten, Aufhebung des Verbots, US-Bürger zu bespitzeln, Erlaubnis für massive Überwachung von E-Mails und Internetverbindungen. Auch US-Firmen mit Firmensitz in Europa sind zur Datenweitergabe verpflichtet, das verstößt jedoch gegen europäisches Recht. Vgl. Price, David: *Le Monde*, S. 3-4.

gegen den Terror.⁴ Eine weitere Initiative, die offiziell ebenfalls auf dieses Ziel ausgerichtet ist, scheitert am öffentlichen Widerstand und dem Kongress. Das “Total Information Awareness”-Projekt aus dem Jahr 2002 sah die Sammlung und Auswertung sämtlicher elektronischer Metadaten vor, um sie auf verdächtige Muster zu prüfen.⁵ 2006 berichtet die Zeitung USA Today jedoch, dass die NSA bei den drei größten amerikanischen Telefonkonzernen Telefonverbindungsdaten im großen Umfang abfragt und diese in Datenbanken zusammenträgt.⁶ Experten befürchteten damals schon, dass diese Sammlung nur ein Teil der Wahrheit und der Anfang von mehr ist. Und auch in Deutschland warnt das Bundesinnenministerium 2012 in einem vertraulichen Bericht vor der Gefahr zunehmender Informationsabschöpfung.⁷

Im Folgenden wird sich diese Hausarbeit näher mit der größten, globalen Überwachung der Geschichte befassen und den Fragen nachgehen, worum es in dem „NSA-Skandal“ geht, wie die USA und Deutschland auf die Enthüllungen reagieren und welche politischen Herausforderungen sich daraus an die EU ergeben. Abschließend wird eine Schlussfolgerung gezogen. Auf Grund des beschränkten Umfangs, wird primär ein Überblick gegeben, weitergehende Informationen finden sich zum Teil in den Fußnoten. Da das Thema aktuell ist und ständig neue Informationen bekannt werden, beruht diese Hausarbeit vor allem auf elektronischen Nachrichten und Aufsätzen. Vier Bücher, die sich mit dieser Thematik beschäftigen, erscheinen erst im April und Mai diesen Jahres.⁸

2. Die Enthüllungen des „Whistleblowers“ Edward Snowden und ihre Folgen

2.1 Die NSA-Affäre – Die Akteure und worum es geht

2.1.1. Die Hintergründe – Edward Snowden

Am 6. Juni 2013 wurde durch den neunundzwanzigjährigen Edward Snowden die brisanteste Geheimdienstenthüllung seit dem Whistleblower Daniel Ellsberg öffentlich.⁹

4 “The PATRIOT Act is essential to protecting the American people against the terrorists.” George Bush am 22.12.2005. Vgl. Department of Justice. Dazu gehören die Bekämpfung von transnationalen terroristischen Netzwerken, organisierter Kriminalität, illegalem Waffenhandel und Proliferation von Massenvernichtungswaffen. Vgl. IP Jan./Feb. 2014, S. 112.

5 Das Projekt wurde später heimlich in Form des PRISM-Programms umgesetzt. Vgl. Price, Le Monde, S. 3-4.

6 Cauley, Leslie: USA Today, 11.05.2006.

7 Vgl. Wirtschaftswoche: Schutz vor dem Datenstaubsauger, 17.06.2013, S. 44.

8 Ein in der Bibliothek der Hochschule Rhein-Sieg bestelltes Buch, „Überwachtes Netz“, ist leider nicht vor Fertigstellung der Hausarbeit vom Händler geliefert worden.

9 Daniel Ellsberg übergab der New York Times 1971 Kopien der „Pentagon Papers“, das die Beziehungen zwischen den USA und dem Vietnam dokumentiert.

Edward Joseph Snowdens Lebenslauf ist bis dahin eher unauffällig. 1983 in North Carolina geboren,¹⁰ bricht Snowden mit 15 die Highschool in Maryland ab. Von 1999 bis 2005 besucht er College-Kurse, vor allem im Bereich IT, und erwirbt herausragende Computerkenntnisse. Er macht jedoch nie einen akademischen Abschluss.¹¹ Mit zwanzig tritt er der US-Army bei, um für die US Special Forces ausgebildet zu werden. Ein Trainingsunfall, bei dem er sich beide Beine bricht, führt zur Entlassung.¹² 2005 ist er nach kurzer Arbeitslosigkeit als Wachmann für eine geheime Einrichtung der National Security Agency (NSA) an der Universität von Maryland angestellt. Ein wichtiger Schritt in seiner Karriere ist die Einstellung für die Central Intelligence Agency (CIA), wo er im Bereich IT-Sicherheit tätig ist und seit 2007 für drei Jahre am Konsulat in Genf arbeitet.¹³ Dort bekommt er Zugang zu geheimen Dokumenten. Weitere berufliche Stationen sind der US-Computerkonzern Dell¹⁴ und die Unternehmensberatungsfirma und Sicherheitsspezialisten Booz Allen Hamilton, einem privaten Sub-Unternehmen der NSA, wo Snowden bis 2013 als Systemadministrator in Japan und auf Hawaii tätig ist.¹⁵ Nach anfänglicher Begeisterung, ohne Abschluss und nur durch Talent so weit gekommen zu sein,¹⁶ zweifelt Snowden 2010 eigenen Angaben nach zunehmend an den Überwachungsprogrammen, mit denen er täglich konfrontiert ist – „I realised that I was part of something that was doing far more harm than good.“¹⁷ 2012 entschließt er sich, die Öffentlichkeit über die Spähprogramme zu informieren und beginnt die brisanten Daten mittels Webcrawlern zu kopieren.¹⁸ Nach Angaben der Ermittler wurde der massive Datenabfluss von der NSA-Zentrale zwar sofort bemerkt, der kritische Verdacht

Vgl. Süddeutsche, 11.07.2013.

10 Seine Eltern und Schwester stehen im Staatsdienst. Welt, 11.06.2013.

11 Brauer, Ulla: NDR, 24.01.2014.

12 Abc-News, 13.06.2013. Angaben der US-Army nach, hat Snowden die Ausbildung nicht bestanden. Brauer, Ulla: NDR, 24.01.2014.

13 Abc-News, 13.06.2013.

14 Dell äußert sich nicht zu der Anstellung Snowdens.

15 Blau, John: Deutsche Welle, 11.06.2013. Es kann in Frage gestellt werden, ob Snowden sich schon im Hinblick auf die geplante Veröffentlichung von Booz Allen Hamilton anstellen lässt, um an noch mehr Beweise zu gelangen. Brauer, Ulla: NDR, 24.01.2014.

16 “His understanding of the internet and his talent for computer programming enabled him to rise fairly quickly for someone who lacked even a high school diploma.” The Guardian, 09.06.2013.

17 The Guardian, 09.06.2013.

18 Nach eigenen Angaben sind auch die Enttäuschung über die Präsidentschaft Barack Obamas, von der sich Snowden verfassungsrechtliche Schritte gegen die zunehmende Überwachung erhofft hatte und das Ignorieren seiner Bedenken durch die Vorgesetzten, ausschlaggebend. 2012 unterstützte er die Präsidentschaft von Ron Paul mit einer kleineren Spende.

von Snowden jedoch plausibel entkräftet.¹⁹ Nach seiner Ausreise nach Hongkong am 20. Mai 2013 übergibt Snowden die strenggeheimen Daten, wohl wissend um die Sprengkraft dieser hochsensiblen Informationen, dem Guardian-Journalisten Glenn Greenwald und der Filmemacherin Laura Poitras, mit denen er bereits seit Anfang des Jahres in Kontakt steht. Eigenen Angaben nach hat er eine sorgfältige Auswahl getroffen²⁰ und nur das kopiert, was seiner Einschätzung nach im öffentlichen Interesse liegt, „[...] because harming people isn't my goal. Transparency is.“²¹ Nach seinen Enthüllungen wird Edward Snowden wegen Geheimnisverrats und Spionage angeklagt, sein Pass annulliert.²² Am 23. Juni gelingt ihm jedoch die Ausreise nach Moskau, wo ihm später auch Asyl gewährt wurde. Sein Bleiberecht dort ist jedoch befristet, wie es danach weitergeht, ist unklar. Snowdens Rolle wird bei den Diskussionen um den Skandal ambivalent bewertet – für die einen ist er ein Held, für die anderen ein Verräter.

2.1.2 Die Chronologie und Akteure des Skandals

Am 6. Juni 2013 veröffentlicht der britische Guardian erstmals einen Artikel, in dem der Zugriff der NSA auf die Verbindungsdaten des Telekomkonzerns Verizon enthüllt wird. Am 7. Juni folgen weitere Veröffentlichungen im Guardian und der „Washington Post“ über das seit 2007 bestehende, hoch geheime Überwachungsprogramm PRISM. Unter Rückgriff auf die Dienste und Nutzerdaten von den neun größten US-Internetunternehmen,²³ werden Daten wie Audios, Videos, Fotos, E-Mails, Dokumente und Verbindungsdaten gesammelt und gespeichert.²⁴ Schon seit 2008 sind die Unternehmen verpflichtet, dem FBI und der NSA, bei einem entsprechenden Beschluss des Foreign Intelligence Surveillance Court (Fisc), unter Geheimhaltung die gewünschten Daten zu übergeben. Darüber hinaus soll es aber auch einen direkten Zugriff der NSA auf die Server gegeben haben. Die Unternehmen bestreiten dies und lehnen es ab, Kenntnis von der Datensammlung gehabt zu haben. Dem widerspricht am 19.03.2014

19 Ihm kamen veraltete Systeme und rudimentäre Sicherheitsvorkehrungen für den Datendiebstahl „von innen“ zu Gute. Vgl. FAZ, 09.02.2014.

20 Auffällig ist, dass es in den (bisher veröffentlichten) Dokumenten keine Informationen über chinesische oder russische Geheimdienstaktivitäten gibt.

21 The Guardian, 09.06.2013.

22 Süddeutsche, 27.01.2014, Teil 1.

23 Google, Facebook, Microsoft, Apple, YouTube, Skype, AOL, PalTalk und Yahoo.

24 Tagesschau: Chronologie, Teil 1.

der NSA-Anwalt Rajesh De.²⁵ In einer Stellungnahme vom 7. Juli verteidigt der US-amerikanische Präsident Barack Obama PRISM als durch ein geheimes Gericht genehmigt und damit rechtsstaatlich und verfassungskonform. Von der Regierung und den Geheimdiensten wird in den folgenden Monaten immer wieder darauf verwiesen, dass die Überwachung legal und wichtig sei – sie gewährleiste erfolgreich den Schutz und die Sicherheit der eigenen Nation und die der amerikanischen Verbündeten.²⁶ Widerlegt wurde jedoch, dass PRISM nur Daten im Ausland erhebt und sich nicht gegen US-Bürger richtet, wie anfangs behauptet wurde.²⁷

Drei Tage nach der ersten Veröffentlichung bekommt die Affäre ein Gesicht. Wohl durch den Druck der amerikanischen Ermittler zu dem Whistleblower, gibt Edward Snowden in einem Guardian-Interview seine Identität preis und erklärt seine Motivation.

*„I have no intention of hiding who I am because I know I have done nothing wrong," [...] I can't in good conscience allow the US government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building. [...] "I am not afraid, because this is the choice I've made."*²⁸

Am 21. Juni 2013 veröffentlicht der Guardian, dass es auch durch den britischen Geheimdienst, das Government Communications Headquarters (GCHQ), eine umfangreiche Internetüberwachung gibt. Mittels „Tempora“ wurden an transatlantischen Glasfaserkabeln Kommunikationsdaten abgeschöpft und gespeichert. Davon betroffen sind fast der gesamte weltweite Internetverkehr und Telekommunikationsstrom. Ein neues Ausmaß bekommt die Überwachung durch die Veröffentlichung der Folien zu „XKeyScore“²⁹ – einem "System zur Ausnutzung von Digital Network Intelligence / Analysestruktur".³⁰ Es ermöglicht die umfangreiche Analyse von Metadaten, vor allem aber die Verfolgung von Netzbewegungen einer Zielperson in Echtzeit.³¹ XKeyScore stellt

25 The Guardian, 19.03.2014. Ebenfalls kritisch: Schiller, Dan: Le Monde, 11.10.2013, S. 9.

26 Tagesschau, 18.06.2013.

27 Süddeutsche, 27.01.2014, Teil 1.

28 The Guardian, 09.06.2013.

29 Documentcloud: Dokumente zu XKeyScore.

30 Spiegel, 31.07.2013.

31 Zeit: Überwachung, Seite 1, 22.07.2013.

die größte Sammlung von Kommunikationsdaten der NSA dar. Die Daten dafür kommen aus Tempora,³² Sammlungen der NSA und der Kooperation mit der CIA.³³

Neben Prism, Tempora und XKeyScore gibt es weitere Programme, um große Datenmengen zu sammeln, auszuwerten oder in den NSA-Datenbanken auffindig zu machen.³⁴ Nach Angaben der NSA werden aber nur 1,2 % des gesamten Datenverkehrs erfasst, noch weniger davon zur Kenntnis genommen – nur etwa 0,0004%.³⁵ Jüngst wurde bekannt, dass die NSA eine automatisierte, auf Algorithmen basierende Schadsoftware plant, die eine flächendeckende Überwachung ermöglicht.³⁶ Zudem soll der amerikanische Geheimdienst mit „Mystic“ und „Retro“ ein Überwachungsprogramm entwickelt haben, das auch die Namen und Inhalte von Telefongesprächen aufzeichnet. Demnach werden ganze Telefonate eines Landes zu 100% mitgeschnitten und bis zu einem Monat gespeichert.³⁷ Eine solch gravierende Überwachung hatte die US-Regierung bisher offiziell immer dementiert. Bekannt wiederum ist, dass die NSA auch „klassische“ Wanzen einsetzt,³⁸ um gezielt die Kommunikation einzelner Personen oder Gruppen zu überwachen. Im Juni wurde enthüllt, dass eben diese Wanzen in den EU-Vertretungen in Washington und den EU-Repräsentanzen in New York und Brüssel eingesetzt wurden. Darüber hinaus kann die NSA unter anderem Netzwerke, Betriebssysteme und Software infiltrieren und Verschlüsselungen umgehen.³⁹ Doch nicht nur die Geheimdienste der USA und Großbritanniens, die im Zentrum des Skandals stehen, auch die kanadische Regierung räumt ein, weltweit auf Telekommunikations- und Internetverbindungsdaten zuzugreifen.⁴⁰ Es ist damit das dritte Land der „Five Eyes“-Partnerschaft,⁴¹ unter denen eine gegenseitige Spionage eigentlich ausgeschlossen ist.⁴²

32 GCHQ nutzt die Daten aus PRISM und stellt der NSA ihrerseits die Daten aus Tempora zur Verfügung. Süddeutsche, 27.01.2014, Teil 1.

33 Zeit: Überwachung, Seite 1: 22.07.2013.

34 Dazu gehören die „Brüder“ von PRISM, die Überwachungsprogramme Mainway, Marina, Nucleon und Pinewal, aber auch Dishfire, Blarney, Fairway, Stormbrew, Bullrun, Dropmire, Boundless Informant, Muscular, Squeaky Dolphin. Vertiefend dazu: Golem: Glossar zur NSA-Affäre. Die Enthüllung weiterer Programme ist wahrscheinlich.

35 IP Jan./Feb. 2014, S. 114.

36 So zum Beispiel ein Angriff über manipulierte Facebook-Seiten. Spiegel, 12.03.2014.

37 Tagesschau, 19.03.2014.

38 Wanzen in Räumen, Computern und Smartphones. Auch Raumüberwachung mit Radar ist möglich.

39 In Folge dessen gelten auch SSL-Verschlüsselungen, mindestens zu US-amerikanischen Webseiten, nicht mehr als sicher. Ein umfassender Überblick über die Programme und Quellen der NSA auf Zeit: Alles Wichtige zum NSA Skandal, S. 2.

40 Zeit, 11.06.2013.

41 Zum „Five Eyes“-Bündnis gehören die USA, GB, Kanada, Australien und Neuseeland. Es besteht seit dem Kalten Krieg und tauscht auch mit anderen Ländern Informationen aus.

Betroffen von der globalen Überwachung sind Staatsoberhäupter, Politiker und Privatpersonen fast jeden Landes,⁴³ ebenso wie Repräsentanten, Diplomaten, Journalisten, Unternehmen, internationale Organisationen wie die Weltbank, der IWF und die OPEC, aber auch internationale Konferenzen wie die UN-Klimakonferenz 2007 auf Bali, der Klimagipfel in Kopenhagen 2009 und der G-20 Gipfel in Großbritannien.⁴⁴

Eine umfassende und abschließende Chronologie des Skandals ist bisher nicht möglich. Insgesamt handelt es sich um geschätzt 1,7 Millionen Daten, die Snowden Greenwald, Poitras und dem Enthüllungsreporter Jeremy Scahill überlassen hat.⁴⁵ Auf ihrer Webseite „The Intercept“ gibt es fast täglich neue Enthüllungen.

2.2 Die Reaktionen in den USA und in Deutschland

Die immer neuen Enthüllungen sorgen weltweit für Empörung. Der US-amerikanische und britische Geheimdienst geraten zunehmend in die Kritik und müssen sich rechtfertigen.⁴⁶ Die Forderungen nach einer umfassenden Aufklärung werden lauter. Bis auf wenige Ausnahmen, bleiben die politischen Reaktionen in der Welt aber eher aus.⁴⁷

Die USA reagieren gespalten auf die Enthüllungen – jedoch nicht entlang der konventionellen Linie. Demokraten und Republikaner sind sich einig, mehrheitlich werfen sie Snowden Vorrat vor. Er gefährde die Sicherheit Amerikas und die der US-Truppen im Einsatz, mit potentiell tödlichen Konsequenzen.⁴⁸ Gegen Snowden wird ein Straf- und Auslieferungsverfahren angestrebt. In einer ersten Reaktion hatte die US-Regierung die Vorwürfe des Guardian noch zurückgewiesen. Die Arbeit der NSA und anderer Geheimdienste habe einer stetigen Kontrolle durch den Kongress und der Bundesgerichte unterlegen und es gäbe keine Datensammlung und Speicherung dieses Um-

42 Am 20.11.2013 enthüllt der Guardian, dass sich die Five-Eye-Allianz gegenseitig ausgespäht hat und auch die NSA jahrelang die britische Bevölkerung ausgespäht hat – mit Duldung der britischen Regierung. The Guardian, 20.11.2013.

43 Vgl. Boundless Informant: The Guardian, 08.06.2013. Sogar der Vatikan soll betroffen sein.

44 Tagesschau: PRISM, “Tempora” und viele Wanzen.

45 FAZ, 09.02.2014.

46 Auf Grund des beschränkten Umfangs der Arbeit kann nicht auf die vergleichsweise geringe Resonanz in Großbritannien eingegangen werden. Dort gab es in erster Linie Kritik am Guardian, der nach Meinung der Regierung, des GCHQ und den konservativen Medien die britische Sicherheit gefährdet und Terroristen in die Hände gespielt hat. Der Druck der Behörden auf den Guardian wächst bis hin zur Vernichtung von Dokumenten. Vertiefend: Tagesschau, 20.08.2013.

47 Eine Ausnahme bildet das Land Brasilien, das zusammen mit Deutschland bei der UN eine Datenschutz-Resolution eingebracht hat, die einstimmig verabschiedet wurde.

48 Die von Snowden kopierten Daten enthalten unter anderem auch Hinweise auf Militärstrategien, eine Veröffentlichung gefährdet die amerikanischen Streitkräfte. „Snowden’s actions are likely to have lethal consequences for our troops in the field.” Presseerklärung, H.o.R., 09.01.2014.

fangs.⁴⁹ Die Spionage-Vorwürfe an sich werden jedoch nicht widerlegt oder dementiert. Der Präsident, die Regierung und die Geheimdienste verteidigen die Spähprogramme, insbesondere PRISM, als legale und wichtige Mittel im Kampf gegen den Terrorismus. Im Vordergrund stehe die Sicherheit der US-Bürger. So habe PRISM bereits weltweit mehr als fünfzig Anschläge verhindert.⁵⁰ Linksliberale und liberale Tea-Party-Politiker wie Senator Ron Paul hingegen wollen eine Verfassungsklage prüfen.⁵¹ Von ihrer Seite erhält Snowden Zuspruch und Lob. Die amerikanische Bevölkerung akzeptiert die Überwachung mehrheitlich, wie eine Umfrage des Meinungsforschungsinstituts Pew im Auftrag der Washington Post ergab.⁵² 62% stimmen einer Einschränkung der Privatsphäre zu Gunsten der Ermittlungsarbeit zum Schutz vor Terror zu, 56% finden eine Überwachung durch die NSA „akzeptabel“ und 45 % der Befragten sind sogar der Meinung, die Regierung sollte sämtliche online Aktivitäten und E-Mails überwachen.⁵³ Trotz der öffentlichen Unterstützung im eigenen Land wächst der weltweite Druck. Anfang 2014 stellt Obama eine Geheimdienstreform vor. Die Vorschläge einer offiziell unabhängigen Expertengruppe finden dabei nur wenig Eingang.⁵⁴ Das Ergebnis bringt keine inhaltliche Wende – die Datensammlung der NSA bleibt bestehen, nur die Ziele und Bedingungen werden neu formuliert. Rechtlich gesehen, stehen die Aktivitäten der NSA bisher offiziell noch im Einklang mit der amerikanischen Verfassung und dem Völkerrecht. Trotz zahlreicher Klagen kam es bisher nicht zu einer eindeutigen Verurteilung.⁵⁵ Ein gegenteiliges Urteil ist bisher nur vorläufig, das Justizministerium reichte Berufung ein.⁵⁶ Ein anderes Urteil erklärt die Telefonüberwachung für legal.⁵⁷

49 Präsident Barack Obama äußert sich erst über eine Woche später zu den Vorwürfen. Tagesschau, 26.12.2013.

50 Tagesschau: Chronologie, Teil 1.

51 Tagesschau: Zwischen Verrat und Heldentum, 11.06.2013. Am 12.02.2014 erhebt Paul Klage.

52 Die Statistik muss jedoch im Hinblick auf den Auftraggeber, die Washington Post, kritisch gelesen werden, da sie auf Grund ihrer Veröffentlichungen in die Kritik der Regierung und der Geheimdienste geraten sind. Es ist davon auszugehen, dass die Washington Post eher regierungskritisch eingestellt ist.

53 Majority say NSA tracking of phone records “acceptable” – Washington Post-Pew Research Center poll, 10.06.2013. Zum Vergleich: Noch vor 9/11 standen die Geheimdienste in der Kritik, das Vertrauen war gering. Abhörmaßnahmen wurden als Verletzung des Persönlichkeitsrechts empfunden und mit Hinblick auf den 4. und 5. Verfassungszusatz abgelehnt. Price, Le Monde, S. 3-4.

54 Obama hatte das Gremium für Bürgerrechte und den Schutz der Privatsphäre im Juni als Reaktion auf die weltweite Empörung eingesetzt. Es sollte die Spähprogramme überprüfen. Die Änderungsvorschläge sind aber nur nicht bindende Empfehlungen. Vgl. Zeit: Alles Wichtige zum NSA-Skandal, S. 3.

55 Tagesschau, 13.02.2013.

56 Vgl. The New York Times, 16.12.2013 und Handelsblatt, 03.01.2014.

57 Zeit, 27.12.2013.

Die Bundesregierung und die deutschen Geheimdienste regieren überrascht auf das Ausmaß der globalen Datensammlung – sie betonen, keine Kenntnis von PRISM gehabt zu haben.⁵⁸ Innenminister Friedrich schließt aber nicht aus, dass deutsche Sicherheitsbehörden indirekt von dem umstrittenen Programm profitiert haben könnten, da die Bundesbehörden regelmäßig Informationen von den US-Geheimdiensten erhalten.⁵⁹ Er gehe aber davon aus, dass die geltenden rechtlichen Grundlagen gewahrt worden seien.⁶⁰ Auch die Bundeskanzlerin rechtfertigt die Überwachung bei einem Treffen mit dem US-Präsidenten in Berlin – „Das Internet ist für uns alle Neuland.“ Gleichzeitig mahnt sie jedoch, dass die Verhältnismäßigkeit zwischen Freiheit und Sicherheit gewahrt bleiben muss.⁶¹ Insgesamt ist die Reaktion aus Regierungskreisen verhalten,⁶² auch als der Spiegel Ende Juni enthüllt, dass Deutschland stärker als jedes andere europäische Land überwacht wurde. Der öffentliche Druck wächst,⁶³ als bekannt wird, dass auch der deutsche Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz die Spähsoftware der NSA (XKeyScore) nutzen.⁶⁴ Gleichzeitig wurden umfangreiche Verbindungsdaten aus Deutschland an die NSA weitergeleitet.⁶⁵ Es gab damit eine wechselseitige Kooperation mit der NSA – Informationen wurden bezogen und der NSA verschafft. Die Regierung verteidigt diesen Austausch von Informationen und Infrastruktur mit der Aufklärung im Ausland.⁶⁶ Die Diskussion um den Datenschutz erhitzt zunehmend die Öffentlichkeit und wird Wahlkampfthema, Regierung und Opposition machen sich gegenseitig Vorwürfe.⁶⁷ Gleichzeitig scheint es, dass es allgemein noch kein Bewusstsein für das ganze (drohende) Ausmaß und die tiefere Problematik des

58 Tagesschau: Chronologie, Teil 1.

59 Tagesschau: Bundesregierung von PRISM überrascht, 11.06.2013. Friedrichs Bemühen, sich den USA über die Ausspähprogramme zu informieren, bleibt erfolglos. Welt: Chronik, 27.10.2013, S. 2.

60 Tagesschau: Bundesregierung von PRISM überrascht. Stand: 11.06.2013. Am 16.08 meldet die Washington Post, dass die NSA in großem Umfang gegen US-Datenschutzlinien verstößt. Tagesschau: Chronologie, Teil 2.

61 Auch Bundespräsident Gauck warnt in einer Rede am 26.07.2013 vor den Gefahren für die Freiheit.

62 Eine Übersicht von Zitaten der Bundesregierung: Süddeutsche, 24.10.2013.

63 Vgl. z.B. Demonstrationen („Freiheit statt Angst am 7.9) und Internetinitiativen wie „antiprism.de.“

64 Das Bundesamt für Verfassungsschutz betont jedoch, dass XKeyScore nur am Computer und ohne Verbindung mit dem Internet getestet werden würde. Welt: Chronik, 27.10.2013, S. 2.

65 Noch im Juli hatte Roland Pofalla zugesichert, dass der Datenschutz eingehalten werde. Vgl. Spiegel, 20.07.2013. Die USA hingegen bezeichnen Deutschland sogar ihren „Schlüsselpartner“. Vgl. Zeit : Überwachung, Seite 2, 22.07.2013.

66 Die Zusammenarbeit besteht seit 2002 und beschränke sich auf die Fernmeldeaufklärung. Die Daten stammen aus der Aufklärungsarbeit in Krisengebieten wie Afghanistan oder Nordafrika. Vgl. Tagesschau, 05.08.2013.

67 Die Opposition wirft der Regierung die Zusammenarbeit mit der NSA vor. Diese hingegen verweist auf eine verstärkte Kooperation unter Steinmeier. Der Protest der Opposition lässt nach, andere Parteien protestieren weiter. Vgl. Welt: Chronik, 27.10.2013, S. 2.

schon Bekannten gibt – zumindest offiziell. So erklärt Kanzleramtschef Roland Pofalla die Affäre am 12. August für beendet. „Der Vorwurf der vermeintlichen Totalauspähung in Deutschland ist vom Tisch. Es gibt in Deutschland keine millionenfache Grundrechtsverletzung.“⁶⁸ Ähnlich äußern sich Friedrich und Merkel. Und auch das Interesse der Bevölkerung an dem Thema sinkt.⁶⁹ Erst nachdem enthüllt wird, dass auch ein Handy der Bundeskanzlerin Gegenstand der Überwachung war,⁷⁰ kehrt der Skandal ins öffentliche Bewusstsein zurück und kommt (erstmal richtig) auf die politische Agenda. Regierung, Opposition und Bürger sind in ihrer Empörung geeint. Die Bundesregierung fordert Obama zu einer umfassende Aufklärung der Spionage in Deutschland auf und bestellt als Signal der Kritik den US-Botschafter in das Auswärtige Amt ein.⁷¹ Ein bilaterales No-Spy-Abkommen wird jedoch voraussichtlich an Zugeständnissen der Amerikaner scheitern.⁷² Ersatzweise wird ein grundsätzlicher Cyber-Dialog angestrebt.⁷³ Dennoch, die Enttäuschung auf deutscher Seite ist groß, das transatlantische Verhältnis schwer belastet. Einer ARD-Umfrage zu Folge, wächst auch in der deutschen Bevölkerung das Misstrauen gegenüber Obama und den USA.⁷⁴ Edward Snowden wird mehrheitlich als Held gesehen.⁷⁵ Trotzdem entscheidet sich die Regierung aus Rücksicht auf die USA weiterhin gegen ein Asyl für Snowden.⁷⁶ Und auch der Generalbundesanwalt sieht aus diplomatischer Rücksicht von einem Ermittlungsverfahren gegen den US-Geheimdienst ab.⁷⁷ Die politischen, wirtschaftlichen und kulturellen Verflechtungen sind zu hoch, die großen Aufgaben in der Zukunft bedürfen einer transatlantischen Kooperation.⁷⁸ Zur Aufarbeitung der Abhöraffaire beschließt der neue Bundestag

68 Vgl. Tagesspiegel, 12.08.2013.

69 Vgl. Welt: Chronik, 27.10.2013, S. 2.

70 Nach Meldungen der New York Times und des Spiegels werden deutsche Politiker seit 2002 (wieder) abgehört. So auch das alte, nicht abhörsichere Partei-Handy der Bundeskanzlerin. Ihr aktuelles Handy sei nicht betroffen. Medienberichte, ob Obama davon wusste, sind widersprüchlich. Der Guardian meldet, dass insgesamt 35 Staats- und Regierungschefs betroffen seien. Süddeutsche, 27.01.2014, Teil 5.

71 Süddeutsche, 27.01.2014, Teil 5.

72 Die USA wollen nicht auf die Überwachung der Deutschen und der Bundesregierung verzichten. Vgl. Tagesschau, 28.02.2014.

73 Tagesschau, 28.02.2014.

74 Vgl. ARD-DeutschlandTREND, Nov. 2013.

75 Sympathien werden Snowden auch von Vertretern aller Parteien bekundet.

76 Bereits im Juli war Asyl für Snowden in Deutschland abgelehnt worden. Und auch künftig ist es nicht zu erwarten.

77 Vgl. Zeit, 19.11.2013.

78 Auch das geplante Freihandelsabkommen soll nicht gefährdet werden. Peter Beyer (CDU) findet deshalb auch den Besuch von Ströbele bei Snowden in Moskau kontraproduktiv. Vgl. Politik und Kommunikation: Schön war die Zeit, Nov. 2013, S. 18.

im Januar die Einsetzung eines Untersuchungsausschusses, wo auch Snowden als Zeuge gehört werden soll.⁷⁹ Schon Ende Oktober hatte der Grünen-Politiker Hans-Christian Ströbele Snowden unter strenger Geheimhaltung in Moskau zu einem Gespräch getroffen. Snowden erklärte sich zu einer Aussage bereit, stellte aber Bedingungen.⁸⁰ Die Reaktion der Regierung gegenüber den Amerikanern ist hingegen vielen zu schwach – „Empört, aber kraftlos“ titelt die Süddeutsche online im November.⁸¹ In dem Bemühen, den öffentlichen Druck zu erhöhen, erstattet der Chaos Computerclub im Februar zusammen mit der Internationalen Liga für Menschenrechte und dem Verein Digitalcourage Strafanzeige gegen die Bundesregierung und die Geheimdienste des Bundes und der Länder.⁸² Der Vorwurf der verbotenen Kooperation mit der NSA wird vom Generalbundesanwalt geprüft, ein Ermittlungsverfahren wurde bisher nicht eingeleitet.

2.4 Die politischen Herausforderungen an die EU

Die Enthüllungen und ihre Folgen stellen vor allem an Europa eine große Herausforderung. Die Affäre hat Europas Schwäche enthüllt – dem Angriff von außen konnten Europa und die EU politisch, juristisch und technisch nur sehr wenig entgegensetzen.⁸³ Was nun folgen muss, ist ein differenzierter Dialog und Verhandlungen mit den USA. Dieser darf nicht moralischer, sondern muss politischer Natur sein. Auf diplomatischer Ebene muss, wie bereits angesprochen, das beschädigte Vertrauen in den transatlantischen Partner wieder hergestellt werden.⁸⁴ Im Hinblick auf die gegenwärtigen und künftigen transnationalen Herausforderungen besteht eine gegenseitige Abhängigkeit, so dass eine funktionierende und vertrauensvolle Kooperation essentiell ist.⁸⁵ Dafür ist eine ebenbürtige Kooperation der Geheimdienste der EU-Mitgliedsstaaten notwendig. Ebenso wichtig ist aber eine gemeinsame, europäische Regelung zum Datenschutz. Schon seit zwei Jahren arbeitet die EU an einem solchen strengen Datenschutzabkommen in

79 Vgl. Welt, 19.03.2013. Die Opposition hatte der neuen Bundesregierung zuvor Versäumnisse vorgeworfen.

80 Vgl. Tagesschau, 31.10.2013 und Zeit, 01.11.2013.

81 Süddeutsche, 03.11.2013.

82 Die Anzeige richtet sich zudem auch gegen die US-amerikanischen und britischen Geheimdienst. CCC, 03.02.2014. Die Opposition begrüßt diese Entscheidung.

83 Es darf nicht vergessen werden, dass es auch ein Angriff von innen war. Durch die Überwachung der GCHQ, jedoch in enger Kooperation mit dem Hauptakteur USA.

84 Der vom Parlament eingesetzte LIBE-Ausschuss stellte die Legalität und das Ausmaß der NSA-Überwachungsprogramme in Frage.

85 Zu diesen Herausforderungen gehören Bereiche wie die Außen- und Sicherheitspolitik, Verteidigung, Terrorbekämpfung und Wirtschaft.

Form einer Datenschutzreform, das durch die Enthüllungen Snowdens eine neue Dringlichkeit erfährt. In der Theorie sind sich dabei die Mitgliedsländer und die EU-Institutionen einig, dass sie ihre Kräfte bündeln müssen, um ein ernstzunehmendes Gegengewicht zu den USA zu bilden.⁸⁶ Die Datenschutzreform der EU soll einen eindeutigen juristischen Rahmen schaffen, der ein ausgewogenes Verhältnis zwischen dem Schutz der privaten Daten und der Verwertung der Daten zu Sicherheitszwecken festlegt.⁸⁷ Ziel des Gesetzes ist es, die Datensammlung zu minieren und damit die Rechte der Bürger zu schützen, gleichzeitig aber den europäischen Binnenmarkt für Unternehmen zu öffnen.⁸⁸ Um den Herausforderungen der technischen Globalisierung gerecht zu werden, sollen nur grundlegende Regeln verankert werden, die Spielraum für Anpassungen lassen.⁸⁹ Künftige Verletzungen des Gesetzes sollen nach dem Vorbild des europäischen Wettbewerbsrechts geahndet werden – mit Strafen von bis zu 100 Millionen Euro oder 5% des weltweiten Jahresumsatzes des Unternehmens.⁹⁰ Das geplante Freihandelsabkommen (TTIP) ist dabei aber nicht Gegenstand der Verhandlungen.⁹¹ Die Reformvorschläge sollten vor der Europa-Wahl im Mai 2014 verabschiedet werden, scheitern aber an einer politischen Einigung der EU-Innenminister; zu umstritten sind die Themen.⁹² Verzögerungen gibt es vor allem durch Großbritannien und die deutsche Bundesregierung.⁹³ Der Grünen Europaabgeordnete Jan Philipp Albrecht rechnet mit einer Einigung erst in drei bis vier Jahren.⁹⁴ Des Weiteren führt die EU mit den USA Verhandlungen über ein Datenschutz-Rahmenabkommen, das ebenfalls vor dem Sommer 2014 abgeschlossen sein soll, dazu verpflichtet sich im November der US-Justizminister.⁹⁵ Zugleich soll das Datenschutzabkommen „Safe Harbour“ von den USA

86 IP Sep./Okt. 2013, S. 46.

87 Unternehmen sollen nur Daten von zentraler Bedeutung speichern und das nicht länger als notwendig. Es bedarf Regeln für die Unternehmen und die Strafverfolgung, sowie Sicherheitsvorkehrungen, um Eingriffe zu minimieren. IP Sep./Okt. 2013, S. 49.

88 Nur über die Einhaltung und das Respektieren der EU-Datenschutzstandards, bekommen und behalten die amerikanischen Unternehmen Zugang zum europäischen Markt mit 500 Millionen potentiellen Kunden. Der Firmensitz ist dabei unerheblich, solange die Waren und Dienstleistungen am europäischen Markt angeboten und Daten von EU-Bürgern verarbeitet werden. Vgl. IP Sep./Okt. 2013, S. 50/51.

89 IP Sep./Okt. 2013, S. 49.

90 Europäisches Parlament, 12.03.2014.

91 IP Sep./Okt. 2013, S. 47.

92 Umstritten ist beispielsweise, wo Verbraucher sich bei Datenschutzverstößen beschweren können.

93 Vgl. Süddeutsche, 06.12.2013.

94 Tagesspiegel, 24.01.2014.

95 Brok, Elmar: Ein „Sputnik-Moment“, S. 15.

nachgebessert werden, andernfalls wird es von der EU ausgesetzt. Ziel der EU und der USA sollte es sein, hohe Standards global festzulegen.⁹⁶

Neben den politischen Verhandlungen ist es auch wichtig, Europa künftig durch technologische Investitionen gegenüber den USA zu stärken – „das ist eine Frage der Selbstachtung und der Souveränität.“⁹⁷ Ein Schritt zur Unabhängigkeit ist die Entwicklung europäischer Clouds. In Europa erhobene und verarbeitete Daten werden dabei nur in Clouds gespeichert, in denen das europäische Recht mit den EU-Datenschutzregeln Anwendung findet.⁹⁸ Faktisch ist aber bei dem Aufbau einer digitalen europäischen Infrastruktur noch fast nichts passiert.

3. Schlussfolgerung

Im Ergebnis lässt sich festhalten, dass die Enthüllungen Edward Snowdens eine internationale, sicherheitspolitische Debatte über Überwachung, Cyber- und Datensicherheit, Privatsphäre und die Rolle der Nachrichtendienste in Gang gesetzt haben. Seine Rolle wird dabei ambivalent bewertet – Held oder Verräter. Außer Frage steht, dass die enthüllten Informationen eine weltweite Relevanz haben – jeder ist von der Überwachung der NSA und der GCHQ betroffen, auch wenn allein aus technischen Gründen eine vollumfassende Überwachung des kompletten täglichen Datenverkehrs (zum Glück) nicht möglich ist. Dennoch hätte Snowden andere Wege der Veröffentlichung wählen können.⁹⁹ Es kann dabei jedoch in Frage gestellt werden, ob und inwieweit die Welt davon Kenntnis erlangt hätte, wie es aktuell der Fall ist, und wie es um den öffentlichen Druck für eine umfassende Aufklärung und bessere Kontrolle bestellt wäre. Doch trotz aller Empörung weltweit muss differenziert werden. Bisher hat nur Edward Snowden geltendes amerikanisches Recht verletzt. Die Überwachung der NSA bewegt sich bisher, da es noch kein eindeutiges juristisches Urteil amerikanischer Gerichte gibt, im Rahmen bestehender amerikanischer Gesetze und dem Völkerrecht.¹⁰⁰ Anders als in Europa, dürfen in den USA Daten verarbeitet werden, solange es nicht explizit verboten

96 Viviane Reding. Vgl. IP Sep./Okt. 2013, S. 48.

97 Müller, Reinhard: Freunde und Feinde der Freiheit, S. 29.

98 IP Sep./Okt. 2013, S. 51.

99 Internes Beschwerdeverfahren, Petition an den Kongress mit Immunitätszusage oder Freedom of Information Act. Vgl. IP Jan. Feb. 2014, S. 116.

100 Entsprechende Änderungen bestehender Gesetze, die die Überwachung ermöglichen sind z.B. der Patriot Act von 2001 oder die Änderungen im Foreign Intelligence Surveillance Act 2008. Und auch das Völkerrecht verbietet Spionage nicht. Jedoch ist kein Staat verpflichtet, diese zu dulden.

ist.¹⁰¹ Es kann jedoch wohl gesagt werden, dass die NSA die bestehenden Gesetze großzügig interpretiert und auch technisch alle Möglichkeiten genutzt hat. Eine Debatte über die Angemessenheit der Mittel ist deshalb dringend notwendig – dient die Abfrage und Speicherung von Metadaten und die Auswertung von Kommunikationsinhalten in diesem Maße sachlich und effektiv der transnationalen Terrorprävention? Ein politisches Forschungsinstitut in den USA verneint einen erkennbaren Einfluss, ebenso Geoffrey Stone, ein Berater des Präsidenten.¹⁰² Demnach werden Terroranschläge durch den Erfolg anderer Programme verhindert, Metadaten leisten nur einen bescheidenen Anteil zur Sicherheit der Nation.¹⁰³ Das gezielte Ausspähen von Privatpersonen ohne begründeten Verdachtsmoment, Politikern befreundeter Länder und Unternehmen lässt sich demnach vorrangig mit den eigenen politischen und wirtschaftlichen Interessen der USA erklären.¹⁰⁴ Und nicht für alle ist dieses Vorgehen mit dem Verständnis einer liberalen, repräsentativen Demokratie konform. Dass Amerika damit seine sich aus der Weltmachtstellung ergebene Vorbildfunktion missbraucht, erkennt auch Obama: „Amerikas Führung in der Welt hängt vom Beispiel amerikanischer Demokratie und Offenheit ab.“¹⁰⁵ Gleichwohl ist Deutschland, ebenso wie Europa, in sicherheitspolitischer Hinsicht auf die Zusammenarbeit mit den USA angewiesen. Deshalb wurde das Ausmaß der vorangegangenen intensiven Zusammenarbeit bisher politisch hingenommen.

Der Skandal zeigt, dass die USA Sicherheit, Freiheit und Privatsphäre anders als Europa bewerten.¹⁰⁶ Eine Ausnahme stellt wohl Großbritannien dar.¹⁰⁷ Ob die Diskussion in Europa, vor allem in Deutschland, auch so geführt wurde wie es ihr gebührt, sei dahin gestellt. In jedem Fall wird deutlich, dass es an klaren Regelungen fehlt – sowohl völkerrechtlich, als auch in und zwischen den einzelnen Ländern. Doch neben generellen Regelungen bedarf es auch eines neuen, digitalen Bewusstseins und Sensibilität der Bürger. Einer Umfrage von Infratest Dimap nach, haben nach den Enthüllungen ledig-

101 Deshalb ist auch die Äußerung Merkels: „Auf deutschem Boden gilt deutsches Recht“ nicht ohne weiteres richtig. Vertiefend: Müller: Freunde und Feinde der Freiheit, S. 26.

102 So konnten beispielsweise der Anschlag auf den Boston-Marathon nicht verhindert werden. Washington Post, 13.01.2014 und New America Foundation, 13.01.2014.

103 Anders bei der internationalen Telekommunikationsüberwachung, diese habe „eindrucksvolle Resultate“ gebracht. Heise, 23.12.2013.

104 Das Ziel, sich Wettbewerbsvorteile zu verschaffen ist weder nachgewiesen noch widerlegt. Vgl. Ip Jan./Feb. 2014, S. 117.

105 Vgl. Müller: Freunde und Feinde der Freiheit, S. 26.

106 Es fehlt an international anerkannten Definitionen für Begriffe aus dem Cyber-Bereich.

107 „Der Feind im eigenen Haus“ – Großbritannien als Verbündeter der USA erschwert ein einheitliches Auftreten der EU.

lich zehn Prozent der Deutschen ihr digitales Verhalten überdacht.¹⁰⁸ Der Mehrheit der Bevölkerung sind die Folgen der neuen, digitalen Zeit (Stichwort: Der gläserne Bürger und Manipulation) trotz aller Technik- und Netzaffinität noch nicht hinreichend bewusst. Trotzdem war die öffentliche Empörung groß – doch was heißt der Ruf nach Datenselbstbestimmung noch in Zeiten sozialer Netzwerke?¹⁰⁹ Die EU zielt mit einer reformierten internationalen Datenschutzvereinbarung auf die Wahrung und Einhaltung elementarer Grundrechte ab, vor allem auf das Recht der Privatsphäre. Der Ansatz ist lobenswert, doch bleibt es abzuwarten, wie er in Zukunft wirksam umgesetzt und eingehalten wird.

Zurückgehend auf den Titel dieser Arbeit und das einleitende Zitat, ist ein Vergleich des NSA-Skandals mit George Orwells dystopischen „Nineteen Eighty-Four“ nachvollziehbar, muss jedoch differenziert betrachtet werden. In beiden Fällen geht es um einen Eingriff in die Privatsphäre von erschreckender Quantität und Qualität. Während es bei Orwell Mikrofone und Kameras in jedem Haus gibt und das Ziel die Verinnerlichung und Kontrolle der Umsetzung einer herrschaftlichen, totalitären Ideologie ist, vor allem in den Gedanken („Gedankenverbrechen“), überwacht die NSA Daten. Eine Gedankenpolizei wie bei Orwell hat und ist die NSA nicht, zumindest nicht unmittelbar. Durch die umfangreiche Überwachung hat die NSA aber die Möglichkeit, jedwede Kommunikation zu kontrollieren. Dies führt zu einer Selbstkontrolle über das, was man dem Internet und anderen Kommunikationsmedien noch „anvertrauen“ möchte. Denn selbst Verschlüsselungen kann die NSA umgehen. Der totalitäre Herrschaftsanspruch wie er bei Orwell zu finden ist, ist im Fall der USA eher ein Machstreben, verbunden mit Idealismus und kommerziellen Interessen aus einem aufgeklärten Eigeninteresse. Der Grund, warum der Vergleich so gerne herangezogen wird, ist die zentrale Bedeutung des Internets und der globalen Internetkommunikation in der heutigen Zeit. Die Hoffnung, dass diese neue technische Möglichkeit nur Gutes bringt, namentlich Demokratisierung und Freiheit, wurde enttäuscht. Die einstige Utopie ist einer Ernüchterung und Unsicherheit gewichen, die neue Herausforderungen an uns alle stellt.

Ende der Bearbeitung

108 ARD-DeutschlandTREND, Nov.2013. Andere Zahlen nennt Reding, Vgl. IP Sep./Okt. 2013, S. 47.

109 IP Sep./Okt. 2013, S. 55.

Literaturverzeichnis

Aufsätze und Zeitungen

Alexander, Nicole: Schön war die Zeit, in: Politik und Kommunikation, November 2013, S. 16-21.

Berke, Jürgen/ Kroker, Michael: Schutz vor dem Datenstaubsauger, in: Wirtschaftswoche, 17.06.2013, S. 44-49.

Bewarder, Manuel/ Nagel, Lars-Marten: Die Welt: Die Chronik der großen NSA-Affäre, 27.10.2013, S. 2.

Brok, Elmar: Ein „Sputnik-Moment“ – Die Europäische Sicherheit und der NSA-Skandal, in: Die Politische Meinung, Januar/Februar 2014, S. 12-15.

Kraus, Prof. Dr. Joachim: Diskutieren statt moralisieren – Was in der deutschen Debatte über die NSA-Affäre wichtig wäre, in: Internationale Politik, Januar/Februar 2014, S. 108-119.

Müller, Reinhard: Freunde und Feinde der Freiheit – Die NSA-Affäre, in: Die Politische Meinung, November/Dezember 2013, S. 25-29.

Price, David: Absolut unamerikanisch – Die schleichende Enteignung der Privatsphäre in den USA, in: Le Monde diplomatique, 09.08.2013, Seite 3-4.

Rinke, Dr. Andreas: „Europas Antwort: strenger Datenschutz“ – Interview mit der Eu-Kommissarin Viviane Reding, in: Internationale Politik, September/Oktober 2013, S. 46-57.

Schiller, Dan: Google und die anderen Heuchler, in: Le Monde diplomatique, 10.11.2013, S. 9.

Internetquellen

Alle Quellen wurden am 24. März 2014 nochmals aufgerufen und überprüft.

Die Ordnung ist alphabetisch und chronologisch erfolgt.

ABC-News:

Mosk/ Matthew/ Meek, James Gordon u.a.: Timeline: Edward Snowden's Life As We Know It, 13.06.2013, in: <http://abcnews.go.com/Blotter/timeline-edward-snowdens-life/story?id=19394487>.

Chaos Computer Club:

Chaos Computer Club erstattet Strafanzeige gegen die Bundesregierung, 03.02.2014, in: <http://www.ccc.de/de/updates/2014/complaint>.

Department of Justice:

Statement of President George W. Bush on the importance of the USA PATRIOT Act in combatting terrorism, December 22, 2005, in: <http://www.justice.gov/archive/ll/archive.htm>.

Deutsche Welle:

Blau, John: Spionage – Snowden, Booz Allen und die NSA, 11.06.2013, in: <http://www.dw.de/snowden-booz-allen-und-die-nsa/a-16874642>.

Documentcloud:

XKEYSCORE, 25.02.2008, p. 1-32, contributed by Charles Savage, The New York Times, in: <https://www.documentcloud.org/documents/743244-xkeyscore-slidedeck.html>.

Europäisches Parlament:

Parlament verschärft Regeln zum Schutz persönlicher Daten im digitalen Zeitalter, 12.03.2014, in: <http://www.europarl.europa.eu/news/de/news-room/content/20140307IPR38204/html/Parlament-versch%C3%A4rft-Regeln-zum-Schutz-pers%C3%B6nlicher-Daten-im-digitalen-Zeitalter>.

Frankfurter Allgemeine Zeitung:

Greenwald und Omidyar starten “The Intercept” – Am Anfang stehen die Snowden-Dokumente, 09.02.2014, in: <http://www.faz.net/aktuell/politik/greenwald-und-omidyar-starten-the-intercept-am-anfang-stehen-die-snowden-dokumente-12793591.html>.

The Guardian:

Boundless Informant: the NSA’s secret tool track global surveillance data, 08.06.2013, in: <http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining#>.

Edward Snowden: the whistleblower behind the NSA surveillance revelations, 09.06.2013, in: <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.

US and UK struck secret deal to allow NSA to ‘unmask’ Britons’ personal data, 20.11.2013, in: <http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data>.

US tech giants knew of NSA data collection, agency’s top lawyer insists, 19.03.2014, in: <http://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de>.

Golem:

Glossar zur NSA-Affäre: Marina, Prism, Noforn, Scissors, Pinwale, Sigad US984XN, 25.07.2013, in: <http://www.golem.de/news/glossar-zur-nsa-ffaere-marina-prism-noforn-scissors-pinwale-sigad-us-984xn-1307-100428.html>.

Handelsblatt:

US-Regierung geht gegen NSA-Urteil in Berufung, 03.01.2014, in: <http://www.handelsblatt.com/politik/international/spaechprogram-us-regierung-geht-gegen-nsa-urteil-in-berufung/9287028.html>.

Heise:

Obama-Berater: NSA-Vorratsdatenspeicherung hat keine Anschläge verhindert, 23.12.2013, in: <http://www.heise.de/newsticker/meldung/Obama-Berater-NSA-Vorratsdatenprogramm-hat-keine-Anschlaege-verhindert-2072184.html>.

Infratest Dimap:

ARD-DeutschlandTREND, November 2013, in: <http://www.infratest-dimap.de/umfragen-analysen/bundesweit/ard-deutschlandtrend/2013/november/>.

NDR:

Brauer, Ulla: Vom Schulabbrecher zum Whistleblower, Stand: 24.01.2014, in: <http://www.ndr.de/ratgeber/netzwelt/snowden215.html>.

New America Foundation:

Bergen, Peter/ Stermann, David u.a.: Do NSA's Bulk Surveillance Programm Stop Terrorists? 13.01.2014, in: http://www.newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1_0_0.pdf.

The New York Times:

Savage, Charlie: Judge Questions Legality of N.S.A. Phone Records, 16.12.2013, in: http://www.nytimes.com/2013/12/17/us/politics/federal-judge-rules-against-nsa-phone-data-program.html?hp&_r=0.

Spiegel:

Schnüffelsoftware XKeyscore: Deutsche Geheimdienste setzen US-Spähprogramm ein, 20.07.2013, in: <http://www.spiegel.de/politik/deutschland/bnd-und-bfv-setzen-nsa-spaehprogramm-xkeyscore-ein-a-912196.html>.

Lischka, Konrad/ Stöcker, Christian: NSA-System XKeyScore: Die Infrastruktur der totalen Überwachung, 31.07.2013, in:

<http://www.spiegel.de/netzwelt/netzpolitik/xkeyscore-wie-die-nsa-ueberwachung-funktioniert-a-914187.html>.

Snowden-Enthüllungen: NSA plant Schadsoftware für die Massen, 12.03.2014,
in: <http://www.spiegel.de/netzwelt/netzpolitik/snowden-enthuellungen-nsa-setzt-auf-automatisierte-ueberwachung-a-958324.html>.

Süddeutsche:

Vereinigte Stasi von Amerika. Whistleblower Daniel Ellsberg über Prism, 11.07.2013, in: <http://www.sueddeutsche.de/kultur/whistleblower-daniel-ellsberg-ueber-prism-vereinigte-stasi-von-amerika-1.1718578>.

Obama verteidigt Spähprogramm Prism, 18.07.2013, in:
<http://www.sueddeutsche.de/politik/datensammlung-durch-us-geheimdienst-nsa-obama-verteidigt-spaehprogramm-prism-1.1699086>.

Obama-Regierung bedroht Pressefreiheit, 11.10.2013, in:
<http://www.sueddeutsche.de/politik/journalisten-in-den-usa-obama-regierung-bedroht-pressefreiheit-1.1792284>.

König, Michael: Vom Tisch? Von wegen! 24.10.2013, in:
<http://www.sueddeutsche.de/politik/zitate-von-unionspolitikern-zur-nsa-ffaere-vom-tisch-von-wegen-1.1802410>.

Klasen, Oliver: Empört, aber kraftlos 03.11.2013, in:
<http://www.sueddeutsche.de/politik/deutschlands-protest-wegen-nsa-ffaere-empoert-aber-kraftlos-1.1809338>.

Cáceres, Javier: Besserer Datenschutz kommt frühestens Ende 2014, 06.12.2013,
in: <http://www.sueddeutsche.de/digital/neue-eu-verordnung-besserer-datenschutz-kommt-fruehestens-ende-1.1837931>.

Chronik des NSA-Geheimdienstskandals – Affäre ohne Grenzen, 27.01.2014
[Als Datum ist der 27.01.2013 vermerkt, bei der Jahresangabe muss es sich jedoch um einen Fehler handeln, so dass hier bei den Angaben das Jahr 2014 verwendet wird.]

Teil 1: Affäre ohne Grenzen: in:

<http://www.sueddeutsche.de/politik/chronik-des-nsa-geheimdienstskandals-ffaere-ohne-grenzen-1.1807106>.

Teil 5: Oktober 2013: Das abgehörte Merkel-Handy, in:

<http://www.sueddeutsche.de/politik/chronik-des-nsa-geheimdienstskandals-ffaere-ohne-grenzen-1.1807106-5>.

Tagesschau:

Ganslmeier, Martin: Zwischen Verrat und Heldentum, 11.06.2013, in:
<http://www.tagesschau.de/ausland/prism-nsa106.html>.

Bundesregierung von PRISM überrascht, 11.06.2013, in:
<http://www.tagesschau.de/inland/prism-bundesregierung100.html>.

NSA verteidigt Überwachungsprogramm – PRISM – legal und erfolgreich?
Stand: 18.06.2013, in: <http://www.tagesschau.de/ausland/prism-terrorabwehr100.html>.

Kooperation mit US-Geheimdienst – Regierung nimmt BND in Schutz,
05.08.2013, in: <http://www.tagesschau.de/inland/bnd170.html>.

Wessel, Barbara: „Wir wollen das Snowden-Material“, 20.08.2013, in:
<https://www.tagesschau.de/ausland/guardian-gchq104.html>.

Ströbele trifft Snowden in Moskau, Stand: 31.10.2013, in:
<http://www.tagesschau.de/ausland/snowden260.html>.

Chronologie des Überwachungsskandals

Teil 1: PRISM, „Tempora“ und viele Wanzen, Stand: 31.10.2013, in:
<http://www.tagesschau.de/ausland/chronologie-prism-tempora100.html>.

Teil 2: „Tempora“: Die Briten lesen mit, Stand: 31.10.2013, in:
http://www.tagesschau.de/ausland/chronologie-prism-tempora100~_page-2.html.

Büllmann, Rolf: Verräter, Hacker oder Held? 26.12.2013, in:
<http://www.tagesschau.de/ausland/snowden340.html>.

Fritz, Sabrina: US-Senator verklagt Obama-Regierung, 13.02.2014, in:
<http://www.tagesschau.de/ausland/nsa-klage100.html>.

No-Spy-Abkommen vor dem Aus, 28.02.2014, in:
<http://www.tagesschau.de/ausland/steinmeier-kerry100.html>.

Büllmann, Rolf: Alle Telefonate eines Landes gespeichert, 19.03.2014, in:
<http://www.tagesschau.de/ausland/nsa-skandal120.html>.

Der Tagesspiegel:

Birnbaum, Robert/ Monath, Hans: Pofalla: Es gibt keinen Datenskandal,
12.08.2013, in: <http://www.tagesspiegel.de/politik/nsa-ffaere-pofalla-es-gibt-keinen-datenskandal/8629534.html>.

Ziedler, Christopher: Neue EU-Datenschutzregeln kommen erst nach Europawahl, 24.01.2014, in: <http://m.tagesspiegel.de/politik/aufgeschobene-reform-neue-eu-datenschutzregeln-kommen-erst-nach-europawahl/9377498.html>.

USA Today:

Cauley, Leslie: NSA has massive database of Americans' phone calls, 11.05.2006, in: http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

U.S. House of Representatives

Permanent Select Committee on Intelligence: Press Release: HPSCI Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger – “Snowden’s acts of betrayal truly place America’s military man and woman in greater danger around the world.”, 09.01.2014, in: <http://intelligence.house.gov/press-release/hpsci-chairman-mike-rogers-and-ranking-member-ca-dutch-ruppersberger-%E2%80%9Csnowden%E2%80%99s-acts>.

Washington Post:

Majority say NSA tracking of phone records “acceptable” – Washington Post-Pew Research Center poll, 10.06.2013, in: http://www.washingtonpost.com/page/2010-2019/WashingtonPost/2013/06/10/National-Politics/Polling/release_242.xml.

NSA phone record collection does little to prevent terrorist attacks, group says, 13.01.2014, in: http://www.washingtonpost.com/world/national-security/nsa-phone-record-collection-does-little-to-prevent-terrorist-attacks-group-says/2014/01/12/8aa860aa-77dd-11e3-8963-b4b654bcc9b2_story.html?hpid=z4.

Die Welt:

Bykowicz, Julie/ Giroux, Greg: Informant Snowden war schüchterner Teenie und Computer-Liebhaber, 11.06.2013, in: <http://www.welt.de/newsticker/bloomberg/article117028715/Informant-Snowden-war-schuechterner-Teenie-und-Computer-Liebhaber.html>.

NSA-Untersuchungsausschuss soll Snowden und Merkel hören. Bundestag will Gremium am Donnerstag einsetzen, 19.03.2014, in:

<http://www.welt.de/newsticker/news2/article125961963/NSA-Untersuchungsausschuss-soll-Snowden-und-Merkel-hoeren.html>.

Zeit:

Spionage – Auch Kanada sammelt weltweit Onlinedaten, 11.06.2013, in:
<http://www.zeit.de/digital/datenschutz/2013-06/kanada-daten-spionage-prism>.

Beuth, Patrick: Überwachung – Das Wichtigste zu Prism und XKeyscore, 22.07.2013,

Teil 1: Das Wichtigste zu Prism und Xkeyscore, in:

<http://www.zeit.de/digital/datenschutz/2013-07/faq-nsa-skandal>.

Teil 2: Deutschland, ein „Schlüsselpartner“ der USA, in:

<http://www.zeit.de/digital/datenschutz/2013-07/faq-nsa-skandal/seite-2>.

Snowden will in Deutschland aussagen, 01.11.2013, in:

<http://www.zeit.de/politik/deutschland/2013-11/stroebele-snowden-briefe>.

Der Generalbundesanwalt knickt in NSA-Affäre ein, 19.11.2013, in:

<http://www.zeit.de/politik/deutschland/2013-11/generalbundesanwalt-nsa-ermittlungsverfahren>.

US-Bundesrichter erklärt NSA-Telefonüberwachung für legal, 27.12.2013, in:

<http://www.zeit.de/digital/2013-12/nsa-richter-urteil>.

Snowden-Enthüllungen: Alles Wichtige zum NSA-Skandal.

<http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal/seite-1>.

Stand: 24.03.2014.

<http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal/seite-2>.

<http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal/seite-3>.