universität wien

MASTERARBEIT

Titel der Masterarbeit

Die NSA-Affäre
und das System der globalen Massenüberwachung

Verfasserin

Oxana GEHL

angestrebter akademischer Grad

Master of Arts (MA)

Wien, 2015

Studienkennzahl lt. Studienblatt:	A 066 824
Studienrichtung lt. Studienblatt:	Politikwissenschaft
Betreuerin / Betreuer:	Ao. Univ.-Prof. i.R. DDr. Ingfrid Schütz-Müller

Inhaltsverzeichnis

Dokumentenverzeichnis

1 Vorwort

Im Juni 2013 wurde die Welt von dem wohl bisher größten Spionage-Skandal in der Geschichte der Geheimdienste erschüttert. Die Enthüllungen von Edward Snowden, einem ehemaligen Mitarbeiter des amerikanischen Geheimdienstes NSA, sorgten für weltweite Empörung und Aufschrei in der Politik und Zivilgesellschaft; denn sie belegten zum ersten Mal Schwarz auf Weiß das tatsächliche Ausmaß der weltweiten Überwachung durch den amerikanischen Geheimdienst NSA, die einer systematischen Überwachung gleich kommt. Die elektronische Überwachung und die Notwendigkeit von effizienterem Datenschutz werden im digitalen Zeitalter vor diesem Hintergrund zunehmend aktiv diskutiert.

In einer Zeit, in der elektronische Medien die weltweite Kommunikation beherrschen und gleichzeitig die Gefahr durch Terrorismus und organisierter Gewalt die politische Agenda bestimmt, drängt sich mehr und mehr die Frage auf: Was sind wir bereit aufzugeben, um Sicherheit zu bekommen?

2 Einleitung

2.1 Forschungsfrage

Der Schwerpunkt meiner Forschungsarbeit liegt auf der folgenden Fragestellung:

- *Kann man im Falle des gegenwärtigen Überwachungssystems der NSA von einer neuen Dimension der Überwachung sprechen?*

Ausgehend von meiner Forschungsfrage habe ich mich in meiner Arbeit eingehend mit der NSA-Affäre beschäftigt, indem ich die Geschehnisse zusammengefasst und die Auswirkungen der Affäre beschrieben habe.

Vor dem Hintergrund, dass die Enthüllungen des Whistleblowers Edward Snowden schwere Spionage-Vorwürfe gegenüber der geheimdienstlichen Arbeit der NSA erheben, erschien mir eine politische Aufarbeitung dringend erforderlich.

Untersucht habe ich in erster Linie den Status Quo der geheimdienstlichen Arbeit der NSA und die Entstehungsgeschichte der Agency. Mein Anspruch war es die Erkenntnisse der Enthüllungen von Edward Snowden möglichst umfassend aufzuarbeiten und ein ausführliches geschichtliches Bild von der Entwicklung elektronischer Überwachung im 20. Jahrhundert zu zeichnen.

Das Hauptaugenmerk lag auf der Analyse der letzten 20 Jahre, die geprägt waren von bedeutenden gesellschaftlichen und politischen Veränderungen, u.a. der digitalen Kommunikationsrevolution der 1990er Jahre und dem Sicherheitsdiskurs um 9/11 infolge der Terrornaschläge. Die Analyse schließt mit einer Zusammenfassung der Untersuchungsergebnisse und dem Versuch eine Antwort auf die Frage nach einem angemessenen Umgang mit den Erkenntnissen zu finden. Vor diesem Hintergrund wird die *neue Dimension* der (staatlichen) Überwachung im digitalen Zeitalter diskutiert.

Theoretisch habe ich mich der Thematik aus einer politikwissenschaftlichen Perspektive angenähert. Begonnen habe ich mit einer Analyse des Sicherheitsbegriffs in den internationalen Beziehungen, der für die Beantwortung meiner Forschungsfrage eine wesentliche Rolle spielt. Im Zuge dessen habe ich das

Paradigma 9/11 und den Krieg gegen den Terror untersucht, welche die gegenwärtige sicherheitspolitische Debatte in den internationalen Beziehungen prägen und zu einem wesentlichen Teil für die Überwachungs-Praktiken der NSA verantwortlich sind.

Dabei wurden diverse Fragen aufgeworfen, die ich versucht habe so weit wie möglich, mit den mir zugänglichen Informationen, zu beantworten:

- Wie operiert die NSA? und Welche Rolle spielen dabei ausländische (Partner-) Nachrichtendienste und private Sicherheitsunternehmen?

- Wie hat sich die staatliche (nachrichtendienstliche) Überwachung der NSA seit ihrer Gründung entwickelt? und Welche Rolle haben die Entwicklungen der letzten 20 Jahre, insbesondere die Terroranschläge von 9/11, dabei gespielt?

- Welche Auswirklungen hat die massenhafte Überwachung und Datenspeicherung?

2.2 Relevanz

Die Tatsache, dass es sich bei den Überwachungspraktiken der NSA um nichts Geringeres als die Verletzung informationeller Freiheitsrechte der Bevölkerung handelt, nämlich das Recht auf Privatsphäre jeder/s Einzelnen - ein fundamentales Grundrecht, welches unter dem Vorwand von Sicherheit maßgeblich eingeschränkt wird, macht eine Aufarbeitung der Thematik dringend erforderlich.

Die gesellschaftliche Relevanz liegt in der Aufklärung von Missständen im staatlichen Sicherheitsapparat; denn nur eine kritische Öffentlichkeit ist in der Lage die Gesellschaft vor einer willkürlichen Macht des Staates und der Geheimdienste zu schützen und antidemokratischen Entwicklungen entgegenzuwirken. Die Bevölkerung hat ein Anrecht darauf zu erfahren wie Geheimdienste arbeiten und wie hoch das Ausmaß der Überwachung durch sie tatsächlich ist. Die zaghaft stattfindende Aufarbeitung der NSA-Affäre macht umso mehr eine Bewusstseinsschaffung und Sensibilisierung für die Thematik der staatlichen Massenausspähung und Datenspeicherung notwendig.

Zu berücksichtigen ist hierbei insbesondere die neue Dimension der Überwachung, die seit der Erfindung des Internets und anderen Informations- und Kommunikationstechniken, eine zunehmende Rolle spielt.

In diesem Kontext ist es wichtig die Hintergründe der Affäre zu beleuchten, um damit einen Anstoß für den Umgang mit ihr zu geben. Die weltweite Debatte, die unmittelbar nach den Enthüllungen im Juni 2013 einsetzte und bis in die Gegenwart anhält, trägt zu einer kritischen Auseinandersetzung mit dem gegenwärtig existierenden Überwachungssystem der Geheimdienste bei. Die wissenschaftliche Relevanz besteht darin die NSA-Affäre zum Ausgangspunkt für eine weiterführende und tiefer gehende Betrachtung des Phänomens der weltweiten Überwachung zu nehmen. Aufgrund der Aktualität des Themas wurde die NSA-Affäre bisher kaum wissenschaftlich aufgearbeitet.

Relevant ist vor allem die Betrachtung des Zusammenspiels zwischen Sicherheit und Freiheit und in diesem Zusammenhang auch die Auswirkungen von 9/11 auf die Arbeit der Geheimdienste, insbesondere der NSA und des GCHQ.

Mein Anspruch war es, die Enthüllungen von Edward Snowden wissenschaftlich aufzuarbeiten. Bei der Analyse bin ich daher vorsichtig, systematisch und so objektiv wie möglich vorgegangen. Mir ging es vor allem darum der Öffentlichkeit ein reflektiertes Bild von der Thematik aufzuzeigen und den Menschen die Möglichkeit zu geben, sich eine eigene Meinung zu der Thematik zu bilden.

2.3 These

Die Kern-These, die meiner Arbeit zugrunde liegt ist, dass wir es gegenwärtig mit einer neuen Dimension der Überwachung durch die NSA, den größten Geheimdienst der Welt, zu tun haben.

Die Enthüllungen von Edward Snowden legen ein umfassendes Überwachungssystem offen, das sich durch eine komplexe technologische Struktur auszeichnet, die sich in den letzten Jahrzehnten des 20. Jahrhunderts manifestierte und primär auf zwei bedeutende Entwicklungen zurückgeht: die elektronische bzw. digitale Revolution der 1990er Jahre und die Anti-Terror Politik der westlichen Allianz infolge der Terroranschläge von 9/11.

Wie sich der Einfluss dieser beiden Faktoren konkret äußert, habe ich in meiner Arbeit unter Berücksichtigung historischer Gesichtspunkte genauer untersucht.

2.4 Methode

Um dem Erkenntnisinteresse gerecht zu werden, bedient sich diese Seminararbeit der Methode der Kritischen Diskursanalyse.

Der Fokus liegt dabei auf der qualitativen Dokumentenanalyse (Inhaltsanalyse) von Primär- und Sekundärliteratur, die diskursanalytisch beleuchtet, also unter Berücksichtigung des politischen und historischen Kontextes untersucht werden.

Als Grundlage für meine Untersuchungen dienten mir diverse offizielle Dokumente, wie das Enthüllungsmaterial von Edward Snowden (klassifizierte Dokumente der NSA), offizielle Stellungnahmen von Politikern, Analysen von Sicherheitsexperten, Sekundärliteratur zur Geschichte der NSA (Monographien, Zeitungs- bzw. Zeitschriftenartikel), insbesondere auch Erkenntnisse von sogenannten *Insidern*, also ehemaligen internen Angestellten des US-amerikanischen Sicherheitsapparats und diverse Gesetzestexte, wie der USA PATRIOT ACT, der FAA etc.

Alle diese Gesetze und Vereinbarungen wurden infolge der Terroranschläge von 9/11 formuliert und bestimmen seither die US-Politik und die europäische Politik in Sicherheitsfragen, insbesondere im Bereich der Terrorismusbekämpfung. Sie wirken sich unter anderem auf die Arbeit der Geheimdienste und der Regierungen weltweit aus, und bestimmen die Praktiken des US-Auslandsgeheimdienstes NSA maßgeblich.

Mein Anspruch war es, ein möglichst umfassendes Bild von der Problematik staatlicher Überwachung durch die Geheimdienste zu zeichnen. Die NSA-Affäre diente mir hierbei als Fallbeispiel für den Missbrauch staatlicher Gewalt und als Exempel zur Darstellung neuer Formen von Überwachung, die sich erst in den letzten Jahrzehnten infolge der digitalen Revolution entwickelt haben.

3 Der Sicherheitsbegriff in den internationalen Beziehungen

Eingangs sollen die zentralen Paradigmen der IB diskutiert werden, um auf Grundlage dessen, den gegenwärtig international vorherrschenden sicherheitspolitischen Diskurs verstehen und richtig einordnen zu können.

Als Leitgedanke bei der Analyse dient mir das Konzept Sicherheit. Es ist nicht nur ein zentrales Konzept in den internationalen Beziehungen (IB), sondern spielt auch eine Schlüsselrolle bei der Bearbeitung meiner Forschungsfrage. Die Konzeptualisierung von Sicherheit ermöglicht eine präzise Analyse des politischen Sicherheitsdiskurses.

Obwohl sich viele Forschungsbereiche mit *Sicherheit* auseinandersetzen und sie Bestandteil verschiedener Diskurse ist, bleibt sie begrifflich eine unklare Größe, die einem permanenten Wandel unterlegen ist.

Die sogenannten Sicherheitsstudien, die Sicherheit zum Gegenstand ihrer Analyse machen, sind eine Subdisziplin der IB und ursprünglich aus den Strategischen Studien im Kalten Krieg entstanden.

3.1 Klassische Theorien

3.1.1 Realismus

Die realistische Schule ist die erste und bedeutendste Schule in den IB. Sie etablierte sich in den 50er Jahren des 20. Jahrhunderts als Denkströmung und dominierte die IB bis in die 1980er Jahre. Sie bescherte den Sicherheitsstudien ein goldenes Zeitalter, mit einer Hochphase Mitte der 1960er Jahre.

Der klassische Realismus stützt sich auf den Begriff der *Macht*, wobei Macht als „die Fähigkeit, bestimmte Handlungen von Menschen oder ihren Organisationen durch Beeinflussung ihres Denkens oder Handelns zu kontrollieren oder zu lenken“ (Gu 2010: 59) verstanden wird.

Im internationalen System sind es die Nationalstaaten, die als zentrale Akteure auftreten und um ihre individuellen Interessen und ihren Machterhalt in der Welt kämpfen. Internationale Politik wird nach dieser Definition immer als Interessens- und

Machtpolitik begriffen. Grundannahme ist eine latente (militärische) Gefahr ausgehend von den Nationalstaaten des internationalen Systems, daher wird hauptsächlich auf militärische Abschreckung gesetzt. Man geht davon aus, dass Sicherheit nur durch militärische Mittel erreicht werden kann. (vgl. Morgenthau 1948)

Dieser Theorie liegt ein negatives Menschenbild zu Grunde, welches maßgeblich vom britischen Staatsphilosophen Thomas Hobbes geprägt wurde. In seinem bekanntesten Werk *Leviathan* beschreibt Hobbes einen Naturzustand, in dem die Menschen in absoluter Freiheit leben. Dieser Zustand ist laut Hobbes geprägt von Angst und Misstrauen gegenüber dem jeweils anderen, und kulminiert im Extremfall im *Krieg alle gegen alle*. Unmittelbare Folge ist die Überwindung dieses anarchischen, unsicheren Zustandes mittels der Einführung eines Gesellschaftsvertrages. Um ein friedliches Leben miteinander zu gewährleisten, geben die Menschen ihre Freiheiten auf und bekommen im Gegenzug dafür Sicherheit. Der König (Leviathan) ist als einziger von diesem Gesellschaftsvertrag ausgenommen, da er sich nur vor Gott allein rechtfertigen muss. (vgl. Hobbes 1651)

Dieser von Hobbes beschriebene Naturzustand ist nach Morgenthau vergleichbar mit den Beziehungen der Staaten im internationalen System. Da es in diesem keinen Weltstaat bzw. keine Weltregierung gibt, herrscht ein anarchischer Zustand und damit das Recht des Stärkeren.

Realpolitisch äußert sich die realistische Theorie in einem Machtspiel zwischen den Nationalstaaten; in der Zeit des Kalten Krieges in einer latenten atomaren Bedrohung der jeweils anderen Supermacht (UdSSR, USA) durch WMD (weapon of mass destruction), sodass die logische Folge eine militärische Aufrüstung ist. Die Folge waren sogenannten Stellvertreterkriege der Großmächte (z.B. Korea 1950-1953, Vietnam 1964-1975).

Die Gefahr dieser militärischen Aufrüstung liegt im sogenannten *Sicherheitsdilemma* – ein „Teufelskreis von Sicherheitsbedürfnis und Machtanhäufung in der Staatenwelt“ (vgl. Herz zit.n. Gu 2010: 61). Aufgrund der Abwesenheit einer übergeordneten Instanz mit Sanktionsgewalt müssen Staaten mit einer ständigen Bedrohung und Aggression seitens der anderen Staaten rechnen. Daher sind alle Nationalstaaten buchstäblich dazu gezwungen, immer mehr Macht anzuhäufen. Dies löst wiederrum

Misstrauen zwischen den Staaten aus. Es kommt zum Wettrüsten - doch statt mehr Sicherheit entsteht eine unsichere Konstellation in der internationalen Weltordnung.

Dieser klassische Sicherheitsbegriff, der die internationale Politik während des Kalten Kriegs prägte, stellt die militärische Kompetente in den Vordergrund der Sicherheitspolitik. Es geht in erster Linie um den Schutz der nationalen Souveränität durch militärische Mittel. Darunter sind alle Handlungen zu verstehen, die in den Bereich militärische Ressourcen, Militärdoktrin, Strategien etc. auf nationalstaatlicher Ebene fallen.

Neben dem klassischen Realismus (Morgenthau) hat die Schule zwei weitere bedeutende Denkströmungen hervorgebracht, den Neorealismus (Waltz) und den Post-Neorealismus (1990er Jahre).

Die Strömung des Neorealismus knüpft am klassischen Realismus an und entwickelte sich den 1960er Jahren. In der Tradition des klassischen Realismus konstatiert auch der Neorealismus eine im internationalen Staatensystem vorherrschende Anarchie und die Dominanz von Konflikten in zwischenstaatlichen Beziehungen. Die internationale Ordnung funktioniert, wie im klassischen anthropologischen Realismus, nach dem Machtprinzip. Im Gegensatz zum Realismus ist jedoch nicht die Macht an sich die Priorität des Staates, sondern die Wahrung der eigenen Sicherheit. (vgl. Waltz 1979)

Waltz unterscheidet zwischen den *high politics* und *low politics*. Seiner Ansicht nach verfolgen die Nationalstaaten primär die *high politics*, worunter unter anderem Sicherheit, Unabhängigkeit und Überleben fallen. Alles andere, also die *low politics*, sind zweitrangig (ebd.).

Das negative Menschenbild nach Hobbes wird im Neorealismus verworfen und durch den von Angst und Misstrauen geprägten Mensch, vom „economic man“ (vgl. Adam Smith 1776) ersetzt. Dieser wird als ein rationales und nutzenmaximierendes Individuum verstanden, das primär an der Durchsetzung seiner Interessen interessiert ist.

3.1.2 Liberalismus

Die zweite Tradition, auf die sich die Sicherheitsstudien gründen, ist der Liberalismus, eine politische Ideologie, die zurück geht ins 17. und 18. Jahrhundert. Sie ist als Kritik am feudalen System und am Merkantilismus zur Zeit der Aufklärung in Europa entstanden.

Der klassische Liberalismus stellt die Freiheiten des einzelnen Individuums in den Vordergrund und „(lehnt) jede Form des geistigen, sozialen, politischen und staatlichen Zwangs ab( )“ (Schubert/ Klein 2011).

Die wichtigsten Prinzipien des Liberalismus sind das Recht auf Selbstbestimmung auf der Basis von Vernunft und Einsicht, die Beschränkung politischer Macht, die Freiheit gegenüber dem Staat und die Selbstregulierung der Wirtschaft auf der Basis persönlichen Eigentums.

Als Urvater der liberalistischen Schule gilt der Philosoph und Vordenker der Aufklärung John Locke, der neben Thomas Hobbes und Jean-Jacques Rousseau die Lehre vom Gesellschaftsvertrag maßgeblich geprägt hat und mit seinem Werk *Two Treatises of Government (1689)* den Grundstein für die Ideen des Liberalismus legte.

> Darin entwirft John Locke zwei unterschiedliche Gesellschaftsbilder. Das erste Gesellschaftsbild geht von einem sogenannten Naturzustand der Menschen aus, in dem alle Menschen frei und gleich sind. Das zweite Gesellschaftsbild beschreibt einen Zustand, in dem der Mensch sich einer Gesellschaft anschließt und die individuelle Freiheit aufgibt; dieser Zusammenschluss wird als Gesellschaftsvertrag bezeichnet. Locke kommt zu dem Ergebnis, dass der Mensch im sogenannten Naturzustand nicht zu leben vermag, und sich daher einer höheren Gewalt - dem Staat - unterwerfe. Der Mensch verzichte damit auf seine Freiheit und die damit verbundenen Rechte zum Schutz und zur Erhaltung seines Eigentums, so Locke. Denn das Leben im Naturzustand ist gleichzeitig verbunden mit Ungewissheit, Furcht und Gefahr. Der Mensch ist in einem permanenten Zustand der Aufruhr und fürchtet sich vor der Unberechenbarkeit der anderen. Dies führt laut Locke zwangsläufig dazu, dass sich der Mensch einer Gemeinschaft anschließt. Er sucht in den Gesetzen der Regierung Zuflucht und Schutz zur Erhaltung seines Eigentums. (vgl. Locke zit. nach Gehl 2009: 3) […] Das endgültige Ziel dieser Form von Staatlichkeit ist Frieden, Sicherheit und das öffentliche Wohl des Volkes (ebd.).

Während Hobbes den Verzicht von Freiheit im Tausch gegen Sicherheit in den Vordergrund seiner Theorie über das Gemeinwesen eines Staates stellt, steht für

John Locke die individuelle Freiheit, die es vor dem Staat zu schützen gilt, im Fokus. Daraus ergeben sich unterschiedliche Ansichten über die Form der Ausgestaltung des gesellschaftlichen Lebens. Der Entwurf von Hobbes orientiert sich an einem absolutistischen Politikverständnis, es gibt einen Herrscher – den Leviathan, der für Recht und Ordnung sorgt. Locke hingegen entwirft eine liberalere Staatstheorie, die die Verteilung der Staatsgewalt auf mehrere Staatsorgane, die Legislative, Judikative und Exekutive vorsieht; und legt damit den Grundstein für das moderne Staatsverständnis (vgl. Hobbes 1651).

Neben Locke wurde der Liberalismus außerdem (grundlegend) von Immanuel Kant geprägt, der mit seinen Thesen zum ewigen Frieden, ein Konzept zur Ausgestaltung eines friedlichen Zusammenlebens von Staaten und Völkern im internationalen System entwarf. Kants Staatsverständnis ist vom Anspruch der Rechtsstaatlichkeit und Unveräußerlichkeit menschlicher Rechte geprägt, die es insbesondere auch in Krisenzeiten zu schützen gilt.

Der feste Glaube an die menschliche Vernunft und die Annahme, dass Menschen ihr Schicksal selbst formen können sind Grundelemente, auf denen die Ideologie des Liberalismus und des kantischen Idealismus fußt. Aufgrund dieser, den Menschen naturgegebenen Vernunft, sind sie laut Kant in der Lage, den Fatalismus zu besiegen und sich mittels sozialen Lernens weiterzuentwickeln. Mithilfe von Institutionen, der internationalen Diplomatie und internationalen Vereinbarungen und Verträgen kann die Anarchie im internationalen System überwunden werden. Der Leitgedanke dahinter ist, dass ökonomische Abhängigkeit die Staaten dazu zwingt, (im eigenen Interesse) friedlich miteinander umzugehen. (vgl. Jørgensen 2010: 57f.)

In der Realpolitik fand ab Mitte der 1960er Jahre eine Annäherung der beiden Supermächte UdSSR und USA statt. Sicherheitsfragen verloren in den IB, v.a. in Folge des Vietnamkriegs, zunehmend an Bedeutung, gleichzeitig entwickelten sich neue Konzepte, die die veränderte Weltordnung adäquater beschreiben konnten. Die wirtschaftlichen, politischen und sozialen Interessen der Weltgemeinschaft schienen sich anzugleichen, durch die steigende internationale Kooperation entstanden Interdependenzen, der Nationalstaat als Souverän verlor immer mehr an Bedeutung. Es kam zu strategischen Zusammenschlüssen, bedeutende internationale

Organisationen (z.B. die UNO, OSCE etc.) entstanden. Ab 1975 erlebten die Sicherheitsstudien eine regelrechte Renaissance. Die Zahl der Publikationen und der Lehrstühle im Fachbereich *Security Studies* stieg weltweit erheblich an.

Es entwickelten sich neue Denkströmungen, die alle der Tradition des Liberalismus zugeordnet werden, darunter der Interdependenz-Liberalismus, der Republikanische Liberalismus und der Neoliberale Institutionalismus.

3.2 Post-Positivismus

Mit dem Ende der Blockkonfrontation Anfang der 1990er fand ein breites Umdenken in der Gesellschaft statt. Zu beobachten war eine Abkehr vom reinen militärischen Sicherheitsbegriff hin zu einer differenzierteren Interpretation von Sicherheit (*erweiterter Sicherheitsbegriff*). Die *Security Studies* wurden zu einem interdisziplinären Fach (Psychologie, Geschichte, Friedensforschung, Dependenztheorie etc.); neben sicherheitspolitischen Aspekten, rückten auch gesellschaftliche, ökonomische und kulturelle Aspekte in den Mittelpunkt.

Zusammengefasst werden die verschiedenen Ansätze des erweiterten Sicherheitsbegriffs unter der Theorieschule des Post-Positivismus – eine Denkschule, die sich in den letzten zwei Jahrzehnten des 20. Jahrhunderts als Gegenströmung zu den traditionellen Ansätzen und Denkschulen in den IB entwickelte (vgl. Jørgensen 2010: 155).

Der Post-Positivismus fasst eine Reihe von unterschiedlichen Denkströmungen – Sozialkonstruktivismus, Post-Strukturalismus, Kritische Theorie – zusammen, die sich durch eine philosophische, (meta)-theoretische und empirisch-analytische Kritik an den Grundsätzen vorangegangener Theorien, wie beispielsweise der Staatszentriertheit des Neorealismus, auszeichnen (ebd.: 160).

Die bedeutendste und von den etablierten WissenschaftlerInnen anerkannte Strömung des Post-Positivismus ist der Sozialkonstruktivismus (ebd.: 158) – „eine Metatheorie, die die Möglichkeiten und Grenzen menschlicher (wissenschaftlicher und alltäglicher) Theoriebildung beschreibt“ (Siebert o.J).

3.2.1 Die Kopenhagener Schule

Die Kopenhagener Schule entstand in den 1980er Jahren als eine Theorieschule in den IB und steht in der Tradition des Konstruktivismus. Von den Wissenschaftlern Barry Buzan, Ole Wæver und Jaap de Wilde des Copenhagen Peace Research Institute (COPRI) entwickelt, kritisiert diese Theorieschule die traditionellen Sicherheitsstudien in ihren Ansätzen und Konzepten.

Sie prägt einen neuen differenzierteren Sicherheitsbegriff, der sich durch ein weites Sicherheitsverständnis auszeichnet. Neben dem rein militärischen Aspekt von Sicherheit rückt dieser Ansatz den ökonomischen, sozialen und umwelttechnischen Aspekt in den Mittelpunkt der politischen Sicherheitsagenda.

Ihren Ursprung hat die Theorieschule in drei theoretischen Hauptströmungen; in der Debatte um die Erweiterung des traditionellen staatszentrierten, militärischen Fokus von Sicherheitsstudien, in der Sprachtheorie und im klassischen Schmittischen (Carl Schmitt) Verständnis von Staat und Sicherheitspolitiken (vgl. Hansen/ Nissenbaum 2009: 1158).

Securitization (Versicherheitlichung) ist das Leitkonzept der Kopenhagener Schule, einer der bedeutendsten Theorieschulen des umfassenden Ansatzes von Sicherheit; und wurde als Begriff in den IB im Jahr 1995 von Ole Wæver geprägt.

Es wird im Allgemeinen als eine Kombination aus klassischem politischem Realismus und Konstruktivismus verstanden. Im Gegensatz zu den materialistischen Ansätzen der klassischen Sicherheitsstudien, ist *Securitization* ein prozess-orientiertes Konzept von Sicherheit. Kernaussage der Theorie ist, dass Sicherheitsprobleme in den IB sozial konstruiert werden. So heißt es im 1997 erschienen Hauptwerk *Security: A New Framework for Analysis*:

> The process of securitization is what in language theory is called a speech act. It is not interesting as a sign referring to something more real; it is the utterance itself that is the act. By saying words, something is done (like betting, giving a promise, naming a ship) (Buzan/ Waever/ de Wilde 1998: 26)

In der Praxis werden existenzielle Probleme in Szene gesetzt, sodass sie über der Politik als solches stehen; im Sicherheitsdiskurs werden sie dramatisiert und als höchste Priorität präsentiert. Mit dem Label *Security* versehen, fordert ein Akteur das Recht ein, außerordentliche Maßnahmen einzusetzen, um einem Problem adäquat zu begegnen. Es können unterschiedliche Bereiche versicherheitlicht werden, u.a. Politik, Wirtschaft, Gesellschaft, Umwelt etc. (vgl. ebd.: 23).

Mögliche Folge der Versicherheitlichung eines Bereichs oder eines Objekts ist die Aufhebung von bestehenden Vereinbarungen zwischen Einheiten bzw. Akteuren (ebd.: 26).

Ein erfolgreicher *Securitization*-Prozess vollzieht sich in drei Schritten: ein *Securitizing Actor* benennt ein bestimmtes Problem als existenzielle Bedrohung gegenüber dem der Öffentlichkeit (*Referent Object*), dessen Lösung sofortige Maßnahmen benötigt (*Securitizing Move*) und wird schließlich von ihr akzeptiert; wobei Akzeptanz nicht zwangsweise in einer zivilisierten, dominanzfreien Diskussion zu Stande kommen muss, sondern lediglich bedeutet, dass ein Befehl immer auf Zwang und Konsens beruht (ebd.: 25).

Process of Securitization:

existential threats → emergency action →

effects on interunit relations by breaking free of rules

(ebd.: 26)

Der *Securitization-Prozess* ist aufgrund seiner beträchtlichen Wirkung, vor allem also eine politisch relevante Kategorie. Die Theorie geht davon aus, dass jedes Politikfeld auf einem Spektrum von *nicht politisiert* (nicht existent auf der politischen Agenda), über *politisiert* (Teil öffentlicher Politik) bis hin zu *versicherheitlicht* verortet werden kann (ebd.: 23).

Letzteres ist für uns von besonderem Interesse. Ein bestimmtes Problem wird als existenzielle Bedrohung dargestellt, die dringliche Maßnahmen und gerechtfertigte

Aktionen, außerhalb der normalen Grenzen politischen Verhaltens, erfordert (Buzan/ Wæver/ de Wilde 1998: 23f.).

Das kann weitreichende Konsequenzen haben, denn wenn man etwas zu einem Sicherheitsproblem macht, ihm also den Status der Priorität verleiht, erklärt man etwas anderes automatisch für insignifikant und damit politisch irrelevant (vgl. Hansen/ Nissenbaum 2009: 1156).

Im Securitzing-Prozess spielen insbesondere auch die Medien eine entscheidende Rolle. Als Bindeglied zwischen der politischen und zivilgesellschaftlichen Sphäre sind sie für die Vermittlung von Inhalten zuständig und üben damit direkten Einfluss auf die öffentliche Meinungsbildung aus. Als Instrument der Verbreitung von Information werden sie mitunter auch für bestimmte politische Zwecke instrumentalisiert.

In meiner Ausarbeitung soll mir der Securitization-Ansatz als theoretisches Grundgerüst dabei helfen zu verstehen, wie es zum Ausbau der staatlichen Überwachung in der US-amerikanischen Sicherheitspolitik in der Post 9/11 Zeit kommen konnte.

Cyber-Security, dass erstmals Anfang der 1990er Jahre aufgrund geopolitischer Veränderungen und technologischer Innovationen Eingang in die politische Agenda fand, ist ein weiteres Grundkonzept der Kopenhagener Schule. Es beschreibt den Versuch einer Versicherheitlichung von digitalen Systemen (Internetinfrastrukturen) nach dem Vorbild des Securitization-Prozess (vgl. Buzan/ Waever/ de Wilde 1998: 25).

Die Entstehung neuer Informationstechnologien, insbesondere des Internets, revolutionierte nicht nur die weltweite Kommunikation, sie veränderte auch die Möglichkeiten der Überwachung für immer. Und selbstverständlich nutzen und missbrauchen auch Staaten und Sicherheitsbehörden die Möglichkeiten moderner Informationstechnik zur Überwachung und Informationsgewinnung.

Die wachsende Zahl der Internet-User hat auch zu einer Steigerung und zu einer erhöhten Komplexität der Kriminalität im Internet geführt.

Neue Risiken und Sicherheitsbedrohungen höchster Priorität entstehen, dazu zählen vor allem das Hacking, wobei man hierbei unterscheiden muss zwischen einem Angriff auf die staatliche nationale Sicherheit bzw. die Sicherheit eines Individuums.

Die Anschläge auf das World Trade Center am 11.09.2001 rückten insbesondere die Informationstechnologie und –sicherheit verstärkt in den Mittelpunkt, und nicht zuletzt Fragen zum Schutz digitaler Infrastruktur, elektronischer Überwachung, des Hackings durch Terroristen und des Internets als eine vernetzte Plattform für Kommunikation quer durch und gegen Staaten (vgl. Hansen/ Nissenbaum 2009: 1155f.).

Hierbei geht es in erster Linie um den Schutz der nationalen Sicherheit, einem formulierten Ziel mit bemerkenswerten Auswirkungen nicht nur auf den politischen Sicherheitsdiskurs, sondern damit einhergehend auch auf die Durchsetzung von politischen Reformen und Bestimmungen.

Unmittelbare Folgen des sicherheitspolitischen Diskurses um Cyber-Security und seiner erfolgreichen Versicherheitlichung waren unter anderem die Etablierung der *Commission on Critical Infrastructure Protection 1996* unter Präsident Clinton, die Formulierung einer *Cyber-Sicherheitsstrategie (2011)*, der *The National Strategy to Secure Cyberspace (2003)* unter Präsident Bush und die Errichtung eines von der NATO unterstützten Verteidigungszentrums in Estland im Jahre 2008 (ebd.: 1557).

So heißt es in der deutschen Cyber-Sicherheitsstrategie von 2011:

„Kriminelle, terroristische und nachrichtendienstliche Akteure nutzen den Cyber-Raum als Feld für ihr Handeln und machen vor Landesgrenzen nicht halt. Auch militärische Operatio-nen können hinter solchen Angriffen stehen“ (Cyber-Sicherheitsstrategie für Deutschland 2011: 3). Um dieser neuen latenten Gefahr begegnen zu können, setzt die Bundesrepublik auf enge Zusammenarbeit der weltweiten Strafverfolgungsbehörden (vgl. ebd.: 4), eine Anpassung des Strafrechts im Hinblick auf Cyber-Kriminalität auf der europäischen Ebene und auf internationale Abkommen (ebd.: 10).

Um die Ergebnisse der Entwicklungen in den Sicherheitsstudien noch einmal zusammenzufassen: man unterscheidet zwischen zwei wissenschaftlichen Grundkonzeptionen. Der erste Ansatz, auch *traditionelle Ansatz* genannt, definiert den militärischen Konflikt als Schlüsselfaktor in den internationalen Beziehungen. Als Hauptakteure im internationalen System gelten souveräne Nationalstaaten, die um Macht kämpfen.

Der zweite *umfassende Ansatz* hingegen versteht die Sicherheitsagenda, wie der Name schon sagt, umfassender und hierarchieloser. Die Hauptakteure sind in der Regel zwar nach wie vor Nationalstaaten, es rücken jedoch auch andere Akteure in den Mittelpunkt der Betrachtung. Zudem hinterfragt dieser Ansatz die Aussage, Sicherheit sei ein „good thing“ (Buzan/ Waever/ de Wilde 1998: 4), angestrebt wird vielmehr eine Entsicherheitlichung.

Mittlerweile ist der umfassende Sicherheitsbegriff elementarer Bestandteil der IB und des Post-Positivismus.Der aktuelle sicherheitspolitische Diskurs, der sich insbesondere auch infolge der Terroranschläge von 9/11 maßgeblich entwickelt hat, fügt sich ein in die Tradition des Post-Positivismus. Die politische Agenda wird nach 9/11 von der Diskussion um die neue sicherheitspolitische Bedrohung des *internationalen Terrorismus* bestimmt. In welcher Weise der Kampf gegen den internationalen Terrorismus von der US-Regierung instrumentalisiert wird, soll im nächsten Kapitel genauer erörtert genommen werden.

4 Der Krieg gegen den Terror

4.1 Das neue Paradigma

Das Ende des Kalten Krieges zwischen Sowjetunion und den Staaten des Warschauer Paktes und den USA und ihren westlichen Verbündeten (NATO-Staaten) leitete Anfang der 1990er Jahre einen Paradigmenwechsel in den internationalen Beziehungen ein.

Die bipolare Ordnung, die die internationalen Beziehungen seit 1945 bestimmt hatte, wurde abgelöst von einer neuen Weltordnung. Die USA blieben als einzige Supermacht im internationalen Staatensystem bestehen.

Damit wurde das Feindbild der jeweiligen Blöcke Kommunismus vs. Kapitalismus obsolet, und die Konfliktlinien im internationalen System formten sich neu; an die Stelle der alten Bedrohungen traten *neue Bedrohungen*.

Infolge der Terroranschläge auf das World Trade Center in New York und das Pentagon in Washington D.C. am 9. September 2001 kam es zu einem entscheidenden Einschnitt in der Disziplin der internationalen Beziehungen. Der *globale Terrorismus* – in diesem Fall als islamistischer Fundamentalismus verstanden – wurde als neue realpolitische Bedrohung definiert und der *asymmetrische Krieg* (vgl. Münkler 2002) als Krieg der Zukunft determiniert.

Der Krieg gegen den Terror wurde als neues Paradigma in den internationalen Beziehungen geboren und bestimmt seit jeher den weltweiten sicherheitspolitischen Diskurs.

Der bekannte deutsche Politikwissenschaftler Herfried Münkler formulierte im Jahr 2002 seine Theorie von den sogenannten *neuen Kriegen*, in der er die Kriege der Zukunft beschreibt. Laut Münkler zeichnen sich diese in erster Linie durch den Verlust des staatlichen Gewaltmonopols aus, d.h. im Falle eines Konflikts bzw. einer kriegerischen Auseinandersetzung treten asymmetrische Akteure, wie Banden und Gruppen, die keinem staatlichen Monopol unterliegen, dem staatlichen Heer als neue Konfliktparteien gegenüber. (vgl. Münkler 2004: 188)

Realpolitisch hatte diese Entwicklung gravierende Folgen, u.a. für die Arbeit der Geheimdienste. Mit der Umformulierung des Feindbildes verschoben sich die Prioritäten der Überwachung. Es standen nicht mehr nur bzw. primär *die Nationalstaaten* im Zentrum des Interesses der Geheimdienste, sondern vor allem auch *transnationale Akteure*, wobei *Terroristen* als die ultimative asymmetrische Bedrohung eingestuft wurden. Die Proliferation von konventionellen und nuklearen Waffen wurde zur Hauptsorge der USA und ihrer transatlantischen Bündnispartner und ihre Bekämpfung zum erklärten Ziel im Kampf gegen den internationalen Terrorismus. Der Präventivkrieg wurde zur neuen politischen Strategie und löste die konventionelle Kriegsführung ab. (vgl. USA's National Security Strategy 2002)

Aufgrund des größtenteils gestaltlosen, ortsunabhängigen und ungewissen Wesens des Terrorismus (vgl. Treverton 2009: 30), erweiterte sich der Überwachungsradius der Geheimdienste um ein Vielfaches. Ins Visier geheimdienstlicher Arbeit gerieten viele kleine, auch einzelne Individuen im In- und Ausland, wobei auch periphere Länder, wie Afghanistan zu Überwachungszielen wurden (ebd.: 22).

So kam der inländische Geheimdienst nicht umhin, mehr und mehr Informationen zu sammeln. Dabei gelangen auch vermehrt Informationen von zivilen Bürgerinnen und Bürgern ins Schleppnetz des Überwachungsapparats. Das Primat der Sicherheit geriet ins Zentrum, bürgerliche Freiheiten in den Hintergrund.

Diese Entwicklung belegen auch die von Edward Snowden enthüllten, und von mir in den kommenden Kapiteln diskutierten, geheimen Dokumente der NSA. Sie machen uns auf eine erschreckende Art und Weise bewusst, was der Staat bereit war aufzugeben, um nationale Sicherheit zu gewährleisten.

Obwohl inländischer Terrorismus kein *neues* Phänomen in den Vereinigten Staaten und weltweit ist, markierten die Terroranschläge vom 9. September 2001 eine neue Ära in der sicherheitspolitischen Geschichte der USA und weltweit. Sie hinterließen tiefe Spuren in der Psyche der US-amerikanischen Gesellschaft und veranlassten die US-Regierung ihre nationalen Geheimdienste grundlegend zu reformieren und auszubauen.

2002 wurde eine neue *National-Security-Strategy* formuliert. Sie legte den Fokus auf die Prävention terroristischer Aktivitäten und setzte die Geheimdienste zunehmend unter Druck, Bedrohungen frühzeitig zu erkennen und zu bekämpfen.

Der neue Anspruch verlangte nach neuen Methoden, die die staatlichen Sicherheitsbehörden vor neue Herausforderungen stellten. Die Beschaffung und Mobilisierung von Informationen, die im Ernstfall einem Terroranschlag verhindern könnten, rückte in den Mittelpunkt der geheimdienstlichen Arbeit. Hinzu kam die Notwendigkeit der Filterung relevanter Information aus der Masse an Desinformation. Denn im Zeitalter von BIG DATA mangelt es nicht am Zugang zur Information selbst, sondern am Zugang zu glaubwürdiger und nützlicher Information.

Um dieser Tatsache angemessen begegnen zu können, investierte die US-Regierung in den letzten Jahrzehnten viel in den Ausbau des staatlichen Sicherheitsapparates. Die Entwicklung neuer, moderner und leistungsfähiger Überwachungsprogramme war das Resultat dieser policy.

Der belgische Sozialwissenschaftler Armand Mattelart spricht in diesem Zusammenhang von einem „Techno-Security Paradigm“ (Mattelart 2010: 137) – einer neuzeitlich gesellschaftlich-politischen Entwicklung, die sich durch eine Versicherheitlichung technischer Infrastrukturen auszeichne.

Als maßgebliche Strategie dahinter sieht er den Versuch der USA ihre Vormachtstellung im internationalen System zu festigen. Neben der Sicherung der ökonomischen, militärischen und kulturellen Überlegenheit, geht es insbesondere auch um die Kontrolle von Information, genauer gesagt um die globale Informationsdominanz. (ebd.)

Tatsächlich sprechen viele ExpertInnen von einem Krieg der Information, der sich gegenwärtig abspielen soll. Seit den 1990er Jahren ist der Begriff Cyberwar wichtiger Bestandteil des öffentlichen Diskurses. Im wissenschaftlich-akademischen Bereich wird das Phänomen vor allem unter dem Begriff *sauberer Krieg* diskutiert.

4.2 Post 9/11 und die Anti-Terrorgesetzgebung

Die Terroranschläge vom 9. September 2001 läuteten eine neue Zeit in den internationalen Beziehungen und im Bereich der Sicherheitsstudien ein. Sie waren Auslöser einer Reihe grundlegender Veränderungen der US-amerikanischen und internationalen Gesetzgebung. Im Folgenden möchte ich nur einige wichtige Aspekte hervorheben.

Unmittelbar nach den Terroranschlägen von 9/11 wurden im UN-Sicherheitsrat die Resolutionen 1368 (12.09.2001) und 1373 (28.09.2001) verabschiedet. Beide verurteilten die Anschläge vom 9. September als einen Akt des Terrors und sprachen von einer Bedrohung des Weltfriedens und der internationalen Sicherheit (vgl. S.C. Res. 1368. para. 1). Sie riefen zu einer stärkeren Zusammenarbeit zwischen den Nationalstaaten im Kampf gegen den Terror auf (vgl. S.C. Res. 1368. para. 3).

Die Resolution 1373 verpflichtete die UN-Mitgliedsstaaten zu einem Vorgehen gegen den internationalen Terrorismus mit allen Mitteln, nach Kapitel VII der UN-Charta.

Es wurde das Einfrieren von Konten diverser Personen, die unter dem Verdacht standen in terroristische Aktivitäten verwickelt zu sein festgelegt (vgl. S.C. Res. 1373, para. 1). Außerdem wurde ein Waffenembargo für alle als terroristisch eingestuften Gruppierungen erlassen und die internationale Staatengemeinschaft wurde dazu aufgefordert, jegliche finanzielle oder sonstige Unterstützung für terroristische Gruppen zu unterbinden (ebd.: para.2). Der wohl wichtigste Punkt ist jedoch der Appell zur intensiveren Zusammenarbeit zwischen Nationalstaaten zur Erleichterung des Informationsaustausches von Sicherheitsbehörden (ebd.: para. 3).

Konkret bedeutete das, dass die Mitgliedsstaaten ihre nationale Gesetzgebung dahingehend anpassen mussten, dass die ihnen vorgegebenen Maßnahmen im Kampf gegen den internationalen Terrorismus entsprechend umgesetzt werden konnten. Zur Überwachung der Umsetzung der Resolution 1373 wurde eigens ein UN-Sicherheitsrats-Ausschuss eingeführt, das sogenannte *Counter-Terrorism Committee (CTC)*. Die UN-Mitgliedsstaaten wurden dazu verpflichtet den Ausschuss regelmäßig über die Fortschritte im Umsetzungsprozess zu unterrichten. (ebd.: para. 4)

Trotz des folgenschweren Beschlusses, der gravierende Auswirkungen auf die nationale Gesetzgebung der Staaten weltweit hatte, sucht man in dieser Resolution vergeblich nach einer klaren Definition des Begriffs Terrorismus. Folglich wird den Nationalstaaten und ihren Regierungen viel Spielraum in der Durchsetzung der Regelungen gegen vermeintliche Terroristen gelassen, und damit erhöht sich auch die Gefahr des Missbrauchs, beispielsweise durch die Instrumentalisierung der Maßnahmen gegen Oppositionelle und politische Gegner.

Ein weiterer Kritikpunkt ist das komplette Ausbleiben von menschenrechtlichen Gesichtspunkten bei der Implementierung der neuen Maßnahmen, die unter der Resolution für alle Staaten als verbindlich beschlossen wurden. Der Fokus liegt gänzlich auf der Wahrung sicherheitspolitischer Interessen, das Recht auf Sicherung der Privatsphäre ist irrelevant, und das obwohl die neuen Gesetze einen immensen Eischnitt in die Privatsphäre der Bürgerinnen und Bürger jedes Landes bedeuten.

Neben den Vereinten Nationen gab es auch seitens der EU (dem Europäischen Rat und dem Europäischem Parlament), großen Zuspruch zu einem stärkeren gemeinsamen Vorgehen im Kampf gegen den internationalen Terrorismus. Es wurden Konventionen, wie die *Council of Europe Convention on the Prevention of Terrorism (2005)* und die *Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (2005)* ratifiziert, die die Nationalstaaten zu einer aktive(re)n Zusammenarbeit in der Prävention, Investigation und Strafverfolgung krimineller Vergehen, insbesondere internationaler organisierter Gewalt, verpflichteten; und diverse Gesetze erlassen, die den staatlichen Autoritäten mehr Befugnisse in der Überwachung von Kommunikation erteilten.

Im Folgenden möchte ich mich auf die Analyse der wesentlichen Verordnungen kontenzentrieren, die bei der Beantwortung meiner Forschungsfrage eine Rolle spielen. Eine ausführlichere Behandlung aller erlassenen Gesetze würde den Rahmen der vorliegenden Arbeit sprengen.

Kurz nachdem der damalige US-amerikanische Präsident George W. Bush am 20. September 2001 den *Krieg gegen den Terror* erklärte, wurde am 25. Oktober 2001 der sogenannte *USA-PATRIOT-Act - Uniting and Strengthening America by*

Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 vom US-Kongress verabschiedet. Es ist das wohl wichtigste Antiterror-Gesetz, dass infolge der Anschläge von 9/11 bis dato beschlossen wurde – 363 Seiten starkes Dokument, dass zahlreiche Novellierungen im Bereich der nationalen und internationalen Sicherheit beinhaltet und weit reichende Einschränkungen in der Privatsphäre von Bürgerinnen und Bürgern mit sich bringt.

Es ist ein Gesetzespaket, das den nationalen Sicherheitsbehörden mehr Kompetenzen und Freiheiten bei der Fahndung nach Terroristen zugesteht, den Autoritätsbereich des US-Präsidenten hinsichtlich sicherheitsrelevanter Gebiete ausweitet, vor allem aber die Zusammenarbeit zwischen der Exekutive (den nationalen Verteidigungsinstitutionen), der Judikative (den Justizstrafvollzugsbehörden) und den US-amerikanischen Geheimdiensten stärkt.

Konkret bedeutet das, dass sich infolge der Gesetzesinitiative umfassende Umstrukturierungsmaßnahmen auf den verschiedensten Ebenen der staatlichen Strukturen vollzogen. Diese Reformen zeichneten sich insbesondere durch ihren zentralisierenden Charakter aus. Ihr primäres Ziel war die Förderung der Zusammenarbeit zwischen Militär, Geheimdiensten und Gesetzesvollzugsbehörden, u.a. in den Bereichen der Informationsgewinnung/-auswertung und im Informationsaustausch.

Wie später bekannt wird, wurden nach 9/11 diverse Überwachungskationen mit Berufung auf den USA-PATRIOT-Act durchgeführt, darunter Lauschangriffe auf den Email-, Telekommunikations- und Internetverkehr.

Zur Implementierung des USA-PATRTIOT-Acts wurde 2002 der sogenannte *Homeland Security Act* erlassen. Er begründete das Department of Homeland Security (DHS) – ein Ministerium, das die vormals unabhängigen Bundesbehörden und Programme, die im Zusammenhang mit dem Kampf gegen den internationalen Terrorismus existierten, in einem Bereich zusammenfasste. (vgl. Mattelart 2010: 141f.)

Auf seiner offiziellen Homepage formuliert das Department seine Mission, wie folgt:

> The Department of Homeland Security has a vital mission: to secure the nation from the many threats we face. This requires the dedication of more than 240,000 employees in jobs that range from aviation and border security to emergency response, from cybersecurity analyst to chemical facility inspector. Our duties are wide-ranging, but our goal is clear - keeping America safe. (U.S. Department of Homeland Security, 27.02.2014)

Die Hauptaufgabe des DHS besteht darin, Forschungs- und Entwicklungsprogramme für das Sicherheitsarsenal zu fördern. Dabei geht es in erster Linie um die Überwachung und Entschlüsselung von elektronischen Nachrichten und die Verschlüsselung von Datenübertragung (vgl. Mattelart 2010: 145).

Der belgische Soziologe Armand Mattelart spricht im Hinblick auf die Entwicklungen nach 9/11 von zwei grundlegenden Tendenzen: zum einen von der fortschreitenden Zentralisierung wirtschaftlicher und medialer Strukturen (ebd.: 148f.) und zum anderen von der Ausweitung der Zusammenarbeit zwischen dem Staat und privatwirtschaftlichen Organisationen (ebd.: 141).

So kam es im Jahre 2006 nach dem positiven Votum der *Federal Communications Commission (FCC)* zur Fusion der zwei großen US-amerikanischen Telekommunikationsunternehmen AT&T und Baby BellSouth (ebd.: 148). Diese Zusammenlegung vereinfachte den Geheimdiensten die Beschaffung von Kommunikationsdaten erheblich. Auch die nationale Medienlandschaft blieb von staatlichen Eingriffen nicht verschont. Der 2005 veröffentlichte Free Press Bericht konstatierte eine zunehmende staatliche Infiltrierung der US-Medien in der Zeit während der Bush-Administration (ebd.: 149).

Mattelart bezeichnet das Konzept, welches sich hinter dieser Strategie verbirgt als „network-centric warfare“ (Mattelart 2010: 141). Dabei handelt es sich um eine in den 1990er Jahren vom US-Verteidigungsministerium entwickelte militärische Doktrin, die auf die Vernetzung von Informationssystemen und –infrastrukturen zur Sicherung der (militärischen) Überlegenheit abzielt.

Ein anderes wesentliches Merkmal der Entwicklungen nach 9/11 war die vollständige Umstrukturierung des US-amerikanischen Sicherheitsapparates. Der Drang nach Vernetzung und Vereinheitlichung resultierte in der Standardisierung von Sicherheitssystemen und -strukturen (ebd.: 147). Es entstanden neue

Sicherheitsbehörden und die Befugnisse der nationalen Geheimdienste und Strafverfolgungsbehörden wurden ausgeweitet.

Ferner kam es zu einer zunehmenden Privatisierung von staatlichen Sicherheitsstrukturen. Die Entstehung von privaten Sicherheitsunternehmen, die sich auf Big Data spezialisierten, ist nur ein Beispiel für diese Entwicklung. Auch Edward Snowden war für ein solches privates Sicherheitsunternehmen tätig. In seiner Funktion als Systemadministrator in der IT-Abteilung von Booz Allen Hamilton, einem Zulieferanten der NSA, hatte er Zugriff auf die größten Geheimnisse der NSA.

Bevor ich genauer auf die relevanten Implikationen des USA-PATRTIOT-Acts im Hinblick auf (elektronische) Überwachung und ihre Auswirkungen auf bürgerliche Freiheiten zu sprechen komme, möchte ich kurz auf die sich im Zusammenhang mit 9/11 ergebenden Folgen für die Kompetenzen des US-Präsidenten eingehen.

Nachdem Präsident George W. Bush die Terroranschläge von 9/11 als einen terroristischen Akt einstufte und einen *State of Emergency*, einen nationalen Notstand ausrief, bemächtigter er sich neuer Befugnisse.

Seitdem beansprucht der US-Präsident die (Befehls-) Gewalt über die nationalen Streitkräfte, sowohl auf Bundes- als auch auf Landesebene. Genauer gesagt hat er die Autorität über die Einberufung von Reservetruppen und die Aufstellung von militärischen Einheiten, gemäß 14 U.S.C. § 331 (1994) und 10 U.S.C. § 12302 (1998) (vgl. Whitehead; Aden 2002: 1086). Was die Überwachung von (elektronischen) Kommunikationsströmen angeht, so autorisierte der USA-PATRIOT-Act erstmals das massenhafte Abhören ohne richterlichen Beschluss. Nach Paragraph 411, 412 des USA-PATRIOT-Act bedarf es für das Abhören von Telekommunikation, für Lauschangriffe auf Computer etc. durch die Strafverfolgungsbehörden nur mehr eines Verdachts und der In-Kenntnissetzung des/der zuständigen Richters/ Richterin des FISA-Gerichts. Das FISA-Gericht, das praktisch keiner Kontrolle unterliegt, hat die Aufsicht über Erlass oder Nicht-Erlass von Überwachungsbefugnissen an die Regierung und die Geheimdienste.

Ein Datengewinnungs-Programm, das für die Überwachungsaktionen der Regierung genutzt wird, ist zum Beispiel das das sogenannte „TIA – Total Information

Awareness“ bzw. „Terrorism Information Awareness“ (Mattelart 2010: 144), das als Teil des Homeland Security Acts im Jahr 2003 etablierte wurde. Es ist in erster Linie dafür zuständig, effektive Methoden der Datensammlung und -auswertung zu entwickeln und sie für die geheimdienstliche Arbeit zu nutzen. Genauer gesagt zielt das TIA-Programm darauf ab, eine möglichst umfassende Anti-Terror Datenbank zu erstellen und neue Verfahren und Modelle zur Füllung und Auswertung der Informationen in der Datenbank zu schaffen.

Nach Paragraph 215 des USA-PATRIOT-Act behält sich die US-Regierung außerdem vor auf die internen Informationen von Unternehmen zuzugreifen, wenn es laut Generalstaatsanwalt z.B. der Untersuchung zum Schutz vor internationalem Terrorismus oder verdeckten geheimdienstlichen Aktivitäten, gemäß dem FISA, dient. Es geht vor allem um den Zugang zu persönlichen Daten von KundInnen im Bereich der Internet- und Telekommunikation, bei Bank- und Kreditgeschäften etc. Um an diese Daten heranzukommen werden verschiedene Mittel der Informationsbeschaffung angewandt.

So sollen unter anderem Telefongesellschaften und Internetserviceprovider (ISPs) die Daten ihrer UserInnen an die US-Regierung und ihren Geheimdienst übermittelt haben. Außerdem soll dem FBI das Recht zur Einsicht in die finanziellen Transaktionen von Bankkunden zugesprochen worden sein. So standen u.a. die Reisedaten, Bankdaten, Kommunikationsdaten der Bevölkerung im Fokus der massenhaften Überwachungsaktionen, die mit dem Ziel der frühzeitigen Erkennung und Verhinderung von grenzüberschreitender Bedrohung der nationalen Sicherheit gerechtfertigt wurden.

High-tech Unternehmen in Silicon Valley haben diesen Bedarf an technischem Know-How in der Sicherheitsbranche längst für sich entdeckt. Sie arbeiten bei der Entwicklung von technischen Standards für die Sicherheit eng zusammen mit der Regierung und sind zu einem unerlässlichen Bestandteil des Systems geworden. (vgl. Mattelart 2010: 145)

Die Autorisierung von Überwachungsaktionen kann durch verschiedene nationale Behörden erfolgen. Nach Paragraph 808 des USA-PATRIOT-Act sind u.a. der Geheimdienst, der Justizminister bzw. Generalstaatsanwalt, die Küstenwache etc. in

der Lage die Befugnis zur Untersuchung nationaler Gewaltverbrechen, wie Straftaten gegen Beamte und öffentliches Eigentum, inklusive terroristischer Gewalttaten, zu erteilen. (vgl. Whitehead/ Aden 2002: 1088)

Strafverfolgungsbeamte und Regierungsmitglieder haben nach Paragraph 213 das Recht Haus- und Bürodurchsuchungen, ohne Wissen der Betroffenen, zu veranlassen.

Außerdem fällt die Investigation und Strafverfolgung nationaler Gewaltverbrechen immer mehr in den Zuständigkeitsbereich der Polizei. So kann diese, neben Staatsanwälten, Ermittlern etc. Überwachungskationen auf der nationalen Ebene autorisieren.

Diese umfangreichen Kompetenzen ergeben sich aus der Zentralisierung der nationalen und internationalen Strafverfolgung im Justizministerium. Die Bush-Administration übertrug die Befugnis des Justizministeriums zur Koordinierung der Inlandsnachrichtenbeschaffung an die CIA (ebd.: 1090) und behielt sich selbst (der Exekutive) vor zu bestimmen, welche Informationen sie dem Kongress in ihrer Position als Aufsicht bereitstellt bzw. vorenthält. Der CIA-Chef hat die Befehlsgewalt über die Sammlung geheimdienstlicher Information unter dem FISA von 1978 bekommen und sich gleichzeitig dazu verpflichtet diese Informationen mit dem Generalstaatsanwalt zu teilen (ebd.: 1091).

Die Definition von *Terrorismus* im Strafgesetzbuch wurde infolge des USA PATRIOT-Act um den *Inlands-Terrorismus* erweitert und der Generalstaatsanwalt bekam die Macht, Straftaten innerhalb des US-amerikanischen Territoriums, die als terroristisch eingestuft werden, also unter anderem Gewalttaten, die das US-amerikanische Strafrecht verletzen etc., zu verfolgen (USA-PATRTIOT-Act § 802)

So ist er u.a. in der Lage über die sofortige Abschiebung und Festnahme von als terroristisch eingestuften Personen bzw. Gruppen auf nationaler Ebene zu bestimmen. Die Festnahme kann ohne die Angabe von Gründen für eine Dauer bis hin zu 7 Tagen erfolgen (USA-PATRIOT-Act § 1226a).

Das US-amerikanische Justizministerium verstärkte ferner seine Zusammenarbeit mit ausländischen Geheimdiensten im Kampf gegen den internationalen Terrorismus (vgl. Whitehead/ Aden 2002: 1089).

Die Novellierungen des USA-PATRIOT-Acts hatten gravierende Folgen für die Freiheitsrechte von Bürgerinnen und Bürgern. Der IV. Grundsatz der US-amerikanischen Verfassung, der US-BürgerInnen vor Überwachung und Eingriffe in die Privatsphäre schützt, wurde mit dem neuen Gesetzespaket praktisch ausgehebelt. Gemäß dem Grundsatz muss ein/e neutrale/r und unbeteiligte/r RichterIn darüber entscheiden, ob jemand aufgrund eines schwerwiegenden Verdachts überwacht werden soll oder nicht.

Nun reicht aber auch ein unbegründeter Verdacht aus, um solche Überwachungsaktionen zu autorisieren (USA-PATRTIOT-Act § 411, 412), unter anderem das Belauschen von Telefonkonversationen (USA-PATRTIOT-Act §206-207) und die Überwachung von Emails und Computer Nachrichten (USA-PATRTIOT-Act §201-204).

Ein Beleg dafür ist das *Terrorist Surveillance Program*, eine von der Bush-Administration kurz nach den Terroranschlägen vom 9. September groß angelegte Überwachungsaktion. Der Präsident autorisierte damit das massenhafte Abfangen von Kommunikationsvorgängen, einschließlich der Kommunikation von US-AmerikanerInnen - die unter dem Verdacht stehen, Kontakte zu Terroristen zu haben - an. Die Lauschangriffe wurden teilweise ohne die Zustimmung vom zuständigen FISA-Gericht mit Berufung auf Paragraph 215 des 2001 erlassenen USA-PATRIOT-Acts autorisiert.

Trotz dieser und anderer gesetzlicher Initiativen, die infolge der Terroranschläge verabschiedet wurden und einen tiefen Einschnitt in die Freiheitsrechte der US-BürgerInnen bedeuteten, blieb eine kritische öffentliche Diskussion darüber, mit welchen Bedrohungen sich die USA wirklich konfrontiert sieht bzw. welche Maßnahmen zu ergreifen sind, um den Bedrohungen angemessen entgegentreten zu können, in der US-amerikanischen Öffentlichkeit aus.

Vielmehr war es eine klassische top-down Aktion, die den *Kampf gegen den internationalen Terrorismus* zur Priorität in der politischen Agenda machte. Die neue außenpolitische Orientierung der USA nach 9/11 sollte auch für Europa nicht ohne Konsequenzen bleiben. Seitdem wurde die sicherheitspolitische Zusammenarbeit zwischen den USA und der EU Schritt für Schritt ausgebaut.

Nach den Terroranschlägen von 9/11 erklärten sich die europäischen Staats- und Regierungschefs solidarisch mit den USA und verschrieben sich dem Kampf gegen den Terrorismus. Der Europäische Rat einigte sich auf einen *Gemeinsamen Standpunkt 2001/931/GASP über die Anwendung besonderer Maßnahmen zur Bekämpfung des Terrorismus* und beschloss einen Aktionsplan, der u.a. die Intensivierung der polizeilichen und justiziellen Zusammenarbeit, die Weiterentwicklung der internationalen Rechtsinstrumente, die Verhinderung der Finanzierung des Terrorismus und die Verstärkung der Flugsicherheit vorsah.

Seitdem hat die EU mehrere Maßnahmenpakete verabschiedet, die u.a. die Einführung eines Europäischen Haftbefehls (2002), Maßnahmen zur Bekämpfung der Finanzierung von terroristischen Gruppierungen und ein Rechtshilfeabkommen mit den Vereinigten Staaten (2009) etc. umfassen.

Darunter auch das SWIFT-Abkommen (2009) zwischen den USA und der EU, das im Zuge der Enthüllungen von Edward Snowden Bekanntheit erlangte. Demnach soll die NSA dieses als Grundlage für den Zugriff zur SWIFT-Genossenschaft genutzt haben, über das ein Großteil des europäischen und internationalen Geldverkehrs läuft. Somit hatte der Geheimdienst unberechtigten Zugang zu Banken- und Kreditkartentransaktionen. (vgl. Poitras/ Rosenbach/ Stark 2013: 81)

Die im Jahr 2003 formulierte Europäische Sicherheitsstrategie (ESS) untermauert die Vision der europäischen Einheit im Kampf gegen den Terrorismus. Darin ist die Rede von neuen Herausforderungen in der globalisierten Welt, wobei *Terrorismus,* neben der Proliferation von Atomwaffen, organisierter Gewalt, regionalen Konflikten etc., als eine der Hauptbedrohungen der Gegenwart klassifiziert wird (vgl. ESS 2003: 2).

Im Umgang mit den *neuen Bedrohungen*, die in ihrem Wesen *dynamischer Art* sind, wird im Rahmen der ESS die Forderung nach einer aktiveren Politik laut; einer

Politik, die auf Prävention statt nur auf Verteidigung ausgerichtet ist (ebd.: 3f.). Im Kampf gegen den internationalen Terrorismus soll die internationale Kooperation in den Bereichen Polizei, Justiz und Militär etc. ausgebaut werden (ebd.: 4), wobei vor allem auf die Bedeutung der transatlantischen Partnerschaft, und die Zusammenarbeit mit der NATO verwiesen wird (ebd.: 5).

Am 30. November 2005 formulierte die Europäische Kommission in Brüssel die sogenannte (*The) European Union – Counter-Terrorism Strategy*, in der sie ein vierstufiges Konzept zur Bekämpfung des internationalen Terrorismus vorstellte, beruhend auf den Pfeilern *prevent*, *protect*, *pursue* und *respond* (vgl. The European Union Counter-Terrorism Strategy 2005).

Darin wird die verstärkte Zusammenarbeit auf nationalem, europäischem und internationalem Level als zukünftige Notwendigkeit bestimmt (ebd.: 6), und das Ziel formuliert, Terrorismusbekämpfung als höchste Priorität im Dialog mit Schlüsselpartnern, wie z.B. der USA zu fördern (ebd.: 7).

Die Koordinierung, Transparenz und Flexibilität zwischen verschiedenen Behörden, auf dem nationalen und europäischen Level werden als Voraussetzungen einer effizienteren Sicherheitspolitik diskutiert (ebd.)

Datenspeicherung und Datenweitergaben, insbesondere der Austausch von (geheimdienstlichen) Informationen zwischen Staaten zur Stärkung der praktischen Kooperation der polizeilichen und juristischen Autoritäten (ebd.: 12) mittels neuer technischer Innovationen (ebd.: 10) werden als unabdingbar gesehen. In diesem Zusammenhang wird auch die Entwicklung neuer IT-Systeme, wie z.B. eines „Visa Information-System[s]“ oder eines neuen „Schengen Information-System[s]“ diskutiert (ebd.: 13).

Welche Bedeutung diese Zusicherung der Loyalität im Zusammenhang mit dem Informations- und Datenaustausch der Staaten, also vor allem auch der geheimdienstlichen Zusammenarbeit der Länder hat, gilt es im Weiteren genauer zu beleuchten und zu untersuchen.

Im Bericht über die Umsetzung der ESS aus dem Jahre 2008 wird noch einmal explizit auf die Bedeutung der „transatlantische[n] Partnerschaft“ (Bericht ESS 2008: 2), angesichts neuer globaler Bedrohungen hingewiesen.

Mit dem Vertrag von Lissabon, der am 1. Dezember 2009 in Kraft trat, wurde die Gemeinsame Sicherheits- und Verteidigungspolitik (GSVP) ausgeweitet, unter anderem durch den Ausbau der Europäischen Verteidigungsagentur und die Einführung eines Anschubfonds zur kurzfristigen Finanzierung militärischer Aktivitäten (an dem sich jedoch nur die Mitgliedstaaten beteiligen, die dazu bereit sind). Außerdem wurde die Einführung eines *EU-Außenministers* beschlossen (unter der Bezeichnung Hoher Vertreter für Außen- und Sicherheitspolitik), der vom Europäischen Rat ernannt wird und zugleich Vorsitzender des Außenministerrats und Vizepräsident der Kommission ist (EU-Vertrag, Titel III Art. 18).

Insbesondere die Gemeinsame Agrarpolitik und die polizeiliche und justizielle Zusammenarbeit in Strafsachen wurden in den Zuständigkeitsbereich des Europäischen Parlaments mit aufgenommen.

5 Die Entstehungsgeschichte des mächtigsten Geheimdienstes der Welt – der NSA

Um das Wesen des größten Geheimdienstes der Welt – der NSA – verstehen zu können, müssen wir seine Funktionsweise näher betrachten. Dazu gehört in erster Linie eine Analyse des juristischen Rahmens, in dem sich die Arbeit des Geheimdienstes bewegt (Status Quo) und die Betrachtung der Entstehungsweise des Geheimdienstes, um die Entwicklung nachvollziehen zu können.

Ich beginne mit einem kurzen historischen Rückblick und rbeite mich dann vor zum Status Quo. Dabei nehme ich eine Aufteilung in vier Unterkapitel vor, die chronologisch geordnet sind und mir im Hinblick auf die Entwicklung der NSA als sinnvoll erscheinen. Die erste Zeitspanne beschreibt die Anfänge nachrichtendienstlicher Arbeit im Allgemeinen, gefolgt von einer Analyse der Periode der unmittelbaren Nachkriegszeit bis zum Ende des Ost-West-Konflikts (1945-1980). Anschließend untersuche ich die 1980er und 1990er Jahre und schließlich die Zeit von den 2000 bis heute.

5.1 Staatliche Überwachung – Ein historischer Rückblick

5.1.1 Die Anfänge

Staatliche (nachrichtendienstliche) Überwachung, so wie sie gegenwärtig existiert, geht zurück ins 19. Jahrhundert, als die ersten nachrichtendienstlichen Institutionen entstanden.

Obwohl Spionage selbst – ein grundlegender Bestandteil der nachrichtendienstlichen Arbeit – bereits zu Zeiten des Römischen Reiches als Instrument der strategischen Kriegsführung gegen Feinde eingesetzt wurde, hat sich staatliche Überwachung im Rahmen nachrichtendienstlicher Arbeit erst in der späten Neuzeit entwickelt.

Den Grundstein dafür legte der Westfälische Friede von 1648, der das Konzept von Staaten als souveränen Subjekten des Völkerrechts erstmals etablierte und letztlich die Entstehung des Nationalstaats im 18. Jahrhundert bewirkte.

Mit der industriellen Revolution in der zweiten Hälfte des 18. Jahrhunderts und dem Einsetzten des technischen Fortschritts, brach ein neues Zeitalter an – das Zeitalter der Kommunikation. Die Kommunikationsrevolution, oft auch als zweite industrielle Revolution bezeichnet, reformierte die Methoden der Spionage grundlegend und öffnete die Türen für die technische und elektronische Aufklärung der Nachrichtendienste. Mit Erfindung des Telegraphs Anfang des 19. Jahrhunderts wurde die bis dahin ausschließlich auf physische Überwachung ausgelegte Form der nachrichtendienstlichen Spionage (Human Intelligence) ergänzt von mechanischer Überwachung (Spionageflugzeuge, Spionagesatelliten, Funkaufklärung), später kam dann das Anzapfen von Telefonleitungen und mit ihr die Überwachung der elektronischen Kommunikation durch SIGINT (Signals Intelligence) und IMINT (Imagery intelligence).

Bereits während des Amerikanischen Bürgerkriegs im 19. Jahrhundert wurden Lauschaktionen eingesetzt, um Bürgerinnen und Bürger zu überwachen (vgl. Landau 2010: 65). Im Rahmen kriminalpolizeilicher Arbeit wurden im Jahre 1895 in New York erstmals Lauschgriffe auf Telefone durchgeführt (ebd.) und während der Prohibition (1919-1933) fanden zum ersten Mal groß organisierte Überwachungsaktionen für investigative Zwecke statt (ebd.: 66).

Zu Zeiten des ersten Weltkriegs wurde das nachrichtendienstliche System weiter ausgebaut – 1919 entstand die sogenannte *Black Chamber*, eine beim US-Verteidigungsministerium assoziierte Behörde, die den Brief- und Telegraphenverkehr der Botschaften in Washington D.C. überwachte – die erste Codeknacker-Organisation der Welt; der Vorläufer der heutigen NSA. Bereits zu der Zeit pflegte die Behörde enge Beziehungen zu US-amerikanischen Telekommunikationsunternehmen (vgl. Schaar 2014: 118).

Der *Radio Communication Act of 1912*, der zum Schutz der Privatsphäre von Telegrammen erlassen wurde, wurde dabei zeitweise missachtet. Die US-Regierung verschaffte sich Zugang zu den Datensammlungen der gesamten US-amerikanischen Kabelindustrie.

Der *Radio Act of 1927* weitete das Gesetz von 1912 aus, sodass von da an nicht nur die Telekommunikationsunternehmen, die Informationen weitergeben, zur

juristischen Verantwortung gezogen werden konnten, sondern auch die Empfänger der Informationen (also z.B. die US-Regierung) (vgl. Bamford 2008: 164).

Der staatliche Missbrauch dauerte solange an, bis die Black Chamber 1929 auf Anweisung des damaligen Außenministers Henry Stimson geschlossen wurde.

5.1.2 1945-1980

Nachdem die Black Chamber Ende der 1920er Jahre geschlossen wurde, dauerte es nicht lange, bis die staatliche Überwachung im Zweiten Weltkrieg ihr Comeback feierte. Der Kampf ums Knacken von Chiffriersystemen, insbesondere die der Deutschen begann. Höhepunkt der amerikanischen und britischen geheimdienstlichen Arbeit war zu der Zeit unter anderem das Knacken der Chiffriermaschinen Enigma, Fish und Purple (vgl. Bamford 2001: 393). Außerdem überwachte die Signal Security Agency (SSA) – der Vorgänger der NSA – bereits in den 1940er Jahren u.a. erfolgreich die Konferenz in San Francisco, die zur Gründung der Vereinigten Nationen führte (ebd.: 421).

Im Jahre 1952 wurde dann die National Security Agency (NSA) gegründet – eine damals noch unscheinbare Behörde, die anfangs weder mit der CIA, noch dem FBI mithalten konnte, sich jedoch schnell zum Vorreiter geheimdienstlicher Arbeit im US-amerikanischen Sicherheitsapparat entwickeln sollte.

Die Situation in den IB begünstigte die Förderung und den schnellen Aufstieg der Behörde. Bereits zu Beginn des Kalten Krieges leitete Eisenhower den Bau von Großrechnern ein, die nun im Harvest-Komplex in Ford Mead beherbergt sind. Im Kampf um die Vorherrschaft im Kalten Krieg wurde die Behörde mit 25 Mio. US-Dollar vom US-Kongress ausgestattet. (ebd.: 581, 583, 592)

Zur Förderung dieser Entwicklung genehmigte Eisenhower 1958 die Errichtung eines NSA-Forschungsinstituts an der Universität Maryland, wo langfristig theoretische Forschung auf den Gebieten der Mathematik und Statistik betrieben werden sollte, und den Aufbau eines Labors für Physik (vgl. Bamford 2001: 599f.)

Insgesamt waren die Jahre des Kalten Krieges geprägt von der Grundeinstellung, dass die NSA eine Vorbildrolle im Wettrüsten gegen die Sowjetunion einnehmen

sollte, die Behörde wurde zum Sinnbild eines starken Amerikas und die Fernmeldeaufklärung zum wichtigsten Instrument im Kampf gegen den sowjetischen Block. Man baute die NSA nach und nach aus, investierte Millionen in Personal (Analytiker, Linguisten, Mathematiker), technisches Equipment (Supercomputer) und Abhörprogramme.

Zur Informationsbeschaffung via Fernmeldeaufklärung ließ die US-Regierung überall auf der Welt Horchposten (Satelliten) errichten und vorhandene aufrüsten, u.a. die uns im Zuge der NSA-Affäre bekannt gewordenen Horchposten in Bad Aibling, Deutschland und im englischen Yorkshire. Das Hauptüberwachungsziel war der Klassenfeind – die Sowjetunion. Doch der Geheimdienst hatte bis Ende der 1970er Jahre große Schwierigkeiten bei der Entschlüsselung der komplizierten sowjetischen Codes (ebd.: 364).

Stattdessen gelang es der NSA Erfolge in der Überwachung inländischer Kommunikation zu erzielen. Die 1960er und 1970er Jahre gingen vor allem aufgrund des Watergate-Skandals 1972, in die amerikanische Geschichte ein und sollten das Image der NSA nachhaltig prägen.

Zum ersten Mal seit der Entstehung der NSA und generell in der Geschichte der (amerikanischen) Geheimdienste kamen durch einen Leak des damaligen stellvertretenden Direktors des FBI William Mark Felt – bekannt geworden unter dem Codenamen *Deep Throat* – pikante Details über die massenhafte Überwachung der US-amerikanischen Zivilbevölkerung durch die US-Regierung an die Öffentlichkeit.

Die Überwachungsaktionen richteten sich gezielt gegen zivile Gruppierungen und Individuen. Besonders die zivilgesellschaftlichen Gruppierungen der 68er Jahre, unter anderem das Civil Rights Movement, die Anti-Vitnam-Kriegsbewegungen etc. gerieten ins Visier des Geheimdienstes. (ebd.: 68)

Die NSA hörte vorsätzlich die Telefonate und Nachrichten von amerikanischen BürgerInnen ohne richterlichen Beschluss und unter Missachtung existierender Gesetze ab. Bekannt wurde diese großangelegte, von Präsident Richard Milhous Nixon beauftragte, Überwachungsaktion unter dem Code-Namen *Minaret*.

Im Herbst 1967 wurden diese Mitschnitte von Gesprächen amerikanischer BürgerInnen von der US-Armee bei der NSA angefordert, aus Angst vor einem Bürgeraufmarsch zum Pentagon. Anschließend wurde eine Beobachtungsliste mit mehr als 600 Namen erstellt, die eine potenzielle Gefahr für die US-Regierung darstellten. In dieser sensiblen Angelegenheit arbeitete die NSA zusammen mit der CIA, dem FBI und der DIA. (vgl. Bamford 2008: 425, 431)

Außerdem wurde bekannt, dass die NSA ab 1970 die Auslandskommunikation von US-AmerikanerInnen ohne richterlichen Beschluss überwachte, d.h. alle aus den USA ausgehenden Telefonate und Telegramme konnten unter das Überwachungsraster der NSA fallen. Diese, unter dem Namen von der US-Regierung initiierte Aktion (*Houston-Plan*) lief über einen Zeitraum von vier Jahren, obwohl Nixon bereits kurz nach Erlass der NSA die Autorität für die Lauschangriffe entzog. (ebd.: 427f.)

Es begann mit einem Einbruch im Watergate-Gebäude in Washington - dem damaligen Hauptsitz der Demokratischen Partei - bei dem versucht wurde vertrauliche Dokumente sicherzustellen und Abhörwanzen zu installieren. Während der Ermittlungen zum Einbruch stellte sich heraus, dass die Auftraggeber enge Vertraute des amtierenden republikanischen Präsidenten Richard Nixon waren und dass die gesamte Aktion der Wiederwahl Nixons galt. Die Operation wurde von NSA und FBI durchgeführt.

Infolgedessen wurden zahlreiche Missbräuche von Regierungsvollmachten während der Amtszeit Nixons (1969-1974) aufgedeckt, unter anderem Verbrechen, die auf direkte Anweisung des Weißen Hauses begangen worden waren. Daraufhin erhöhte sich der öffentliche Druck und als sich der Präsident weigerte bei der Aufklärung der Affäre mit den Ausschüssen des Kongresses zu kooperieren, musste dieser im zweiten Jahr seiner zweiten Amtszeit (1974) zurücktreten.

Die Reaktion auf den Skandal kam prompt - im Januar 1975 erschuf der US-amerikanische Senat einen Ausschuss, der die Aufgabe hatte, die Operationen des staatlichen Geheimdienstes auf illegale, unangemessene und unethische Aktivitäten der Regierungsbehörden zu prüfen - das sogenannte *Church Committee* - benannt

nach dem US-Senator Frank Church, dem Vorsitzenden des Komitees (vgl. Landau 2010: 77).

Auf Druck von Frank Church und gegen den vehementen Widerstand der NSA stimmte der Ausschuss schließlich dafür, seinen Bericht zu veröffentlichen. Infolgedessen musste sich der damalige NSA-Direktor Lew Allen Jr. in einer öffentlichen Sitzung des Ausschusses zu den Vorwürfen, die gegen die NSA erhoben wurden, äußern, was bis dahin einmalig in der Geschichte des Nachrichtendienstes war. (vgl. Bamford 2001: 436)

Das Komitee enthüllte eine 40-jährige Geschichte der Abhöraktivitäten präsidentieller, exekutiver und nationaler Sicherheitsorgane. Überwachungsziele waren vor allem Oppositionelle, inklusive politische Gegner, Journalisten etc., da sie als potentielle Gefahr für die Regierung galten. (vgl. Landau 2010: 77)

Die ersten Missbräuche staatlicher Überwachung gingen gemäß den Ermittlungen bis in die 1940er Jahre, der Amtszeit Harry Trumans, zurück. Wobei unter anderem auch festgestellt wurde, dass bereits unter Franklin D. Roosevelt (1933-1945) in speziellen Fällen die Befugnis zur elektronischen Überwachung erteilt wurde. (ebd.: 69)

Die Operation *Shamrock* wurde beispielsweise unmittelbar nach Ende des Zweiten Weltkrieges, in der Amtszeit Harry S. Trumans, eingeleitet. Darunter wurde eine „Übereinkunft verstanden, der zufolge die großen US-amerikanischen Telefongesellschaften wie Western Union der NSA jeden Tag Kopien aller Telegramme schickten, die aus den USA ins Ausland gesandt und dort empfangen wurden“ (Bamford 2001: 431). Zu der Zeit war das Telegramm das bevorzugteste Kommunikationsmittel der meisten diplomatischen Vertretungen des Auslands in Washington D.C. und New York (vgl. Bamford 2001: 139).

Gemäß Louis W. Tordella, dem damaligen NSA-Direktor waren bei der Aktion alle großen internationalen Telefongesellschaften beteiligt (ebd.: 433)

Das Resultat der Enthüllungen war eine Reihe von Empfehlungen, die in Form von Gesetzten umgesetzt werden sollten. Die Grundidee war die Schaffung von

effizienten Kontrollmechanismen, die „Überwachung im Auftrag nationaler Sicherheit“ (Landau 2010: 77) unter Aufsicht stellen.

Ende der 1970er Jahre war die NSA zu einer so mächtigen (Geheimdienst-) Behörde geworden, dass sie den Einfluss der CIA immer mehr zurückdrängte und zu einem ernstzunehmenden Konkurrenten wurde (vgl. Bamford 2001: 378). Dies mündete in den 1980er Jahren schließlich im Spionagekrieg zwischen CIA und NSA (ebd.: 380).

5.1.3 1980-2000

Die 1980er und 1990er Jahre waren für die NSA ein Wendepunkt in vielerlei Hinsicht.

Ende der 1980er Jahre setzte die Informationsrevolution ein. Auf der ganzen Welt wurden kommerzielle Bodenstationen errichtet, um die Kommunikationsströme via Kommunikations-Satelliten zu übermitteln und zu empfangen.

Mit der neuen Schaltungstechnik telefonischer Kommunikation, die in den 1980er Jahren zur Anwendung kam, erlebte die (staatliche) Telefonüberwachung einen Wendepunkt. Die neue Kommunikationstechnologie sollte die Natur der Fernmeldeaufklärung für immer verändern.

Das Einfangen telefonischer Daten vereinfachte sich mit der neuen Technik um ein Vielfaches (vgl. Landau 2010: 79f.) Während zu Beginn des Telefons ein Operator für die Verbindung der Anrufe zuständig war, automatisierte sich die Kommunikation mittels direkter Zugänge. Damit konnte ein unverzögerter Zugriff auf die Anrufe erfolgen.

Um die elektronische Kommunikation, die dadurch ermöglicht wurde angemessen zu schützen, verabschiedete der Kongress *1986* den sogenannten *Electronic Communications Privacy Act (ECPA),* eine Verordnung, die das Abfangen mündlicher, verkabelter und elektronischer Kommunikation von privaten und öffentlichen Akteuren untersagte, sofern nicht ausdrücklich von Gesetz oder per Gerichtsbeschluss genehmigt. (ebd.: 21f.)

ECPA fügte Sicherheitsbestimmungen für gespeicherte Kommunikationsdaten hinzu als Reaktion auf die Entstehung von ISPs, die solche Dienste zur Verfügung stellten.

Der Zugang und die Benutzung dieser Daten wurde für private BürgerInnen verboten, und für die Regierung unter bestimmter Voraussetzung - die Existenz einer Suchbefugnis - erlaubt, wobei es deutlicher einfacher ist, an Daten zu kommen, die älter als 180 Tage sind oder bereits gelesen wurden. (ebd.: 80)

Unabhängig von dem erlassenen Gesetz zum Schutz der Kommunikation, ließ die NSA in Zusammenarbeit mit ihren Partnern ausbauen.

Nach dem Ende des Kalten Krieges, ging auch die Blütezeit des Geheimdienstes zu Ende – zumindest hatte es für eine kurze Zeit den Anschein. Bei seinem Amtsantritt 1993, sah sich Bill Clinton einem hohen Haushaltsdefizit gegenüber und reagierte mit umfangreichen Einsparungen und Kürzungen, wovon auch der nationale Sicherheitsapparat betroffen war. Die NSA musste das erste Mal seit ihrer Entstehung sämtliche MitarbeiterInnen entlassen. Von 1990-1997 verzeichnete die NSA einen Personalrückgang von bis zu 17,5% (ebd.: 548), also rund 1/3 der bei Beginn ihrer Entstehung zählenden MitarbeiterInnen (vgl. Bamford 2008: 106).

Die zahlreichen Horchposten bzw. Lauschstationen, die während des Kalten Krieges weltweit errichtet worden waren, wurden geschlossen und Antennen stillgelegt (vgl. Bamford 2001: 545). Es fand eine Verlagerung von Geldern statt, die Förderung von Satelliten und technischen MitarbeiterInnen ging über zur Förderung von Analyse und Sprachwissenschaft. Zur Förderung von qualifiziertem Fachpersonal begann die NSA in Colleges, Sommerschulen zu investieren (vgl. Bamford 2001: 556f.)

„In den wenigen Jahren von 1991-1994 ging die Zahl der Spionagesatelliten um fast die Hälfte zurück“ (Bamford 2001: 548).

Die traditionellen Ziele des Geheimdienstes, die Sowjetunion und die Satellitenstaaten, wurden abgelöst von Krisenherden, die überall auf der Welt aus dem Boden schossen (vgl. ebd.: 552). Der Kampf gegen die Verbreitung von Kernwaffen und konventionellen Waffen rückte auf die politische Agenda der USA. Der Drang nach Erkenntnissen und der Fachkräftemangel in der Behörde, förderten die Zusammenarbeit der NSA mit CIA, FBI und anderen Vertragspartnern (ebd.: 405). Die genaue Zusammensetzung der Partner bzw. Kunden der NSA wird später im Kapitel 6.4 erläutert.

Neben weitreichenden Umstrukturierungen in der NSA, u.a. Personalaustausch - die russischen Linguisten wurden größtenteils ersetzt von Dari und Arabisch sprechenden Linguisten. Ferner wurde in interne (Weiter-) Bildungseinrichtungen investiert.

Mit dem Zusammenfall der sozialistischen Blocks und der Entstehung einer multinationalen Welt entwickelten sich auch viele neue transnationale Probleme und Gefahren. Polizeiliche Arbeit begann sich immer mehr mit Fällen der nationalen Sicherheit zu überschneiden und es entstanden Zentren der Kooperation zwischen Geheimdienstmitarbeitern und Polizeibeamten, wie z.B. Zentren zur Drogenbekämpfung. (ebd.: 448)

5.1.4 1999-2005 (Die Hayden Ära)

Ab 2000 befand sich die Fernmeldeaufklärung gewissermaßen in einer Krise. Ein Jahr nach dem Amtsantritt von Hayden brachen die Computersysteme der NSA zusammen. Sie hielten der extremen Belastung der Masse an gesammelter Information nicht mehr statt. (vgl. Bamford 2001: 456)

Trotz dieser anfänglichen Schwierigkeiten schaffte es Hayden die NSA bald wieder auf Erfolgskurs zu bringen, mehr noch, er machte sie zu dem, was sie heute ist.

Am 12. April 2000 sagte er als Zeuge in einer offenen Sitzung des *House Intelligence Committee* aus und rechtfertigte die Aktionen der NSA als rechtmäßig und angemessen. Er betonte, dass die NSA unter der Wahrung des Rechts auf Privatsphäre US-amerikanischer BürgerInnen in Einklang mit dem IV Amendement der US-Verfassung handele. Am Ende schienen die Mitglieder des Ausschusses und die Öffentlichkeit von der Unschuld der NSA überzeugt. (vgl. Bamford 2008: 36ff.)

Die Terroranschläge von 9/11 leiteten einen neuen Kurs in der sicherheitspolitischen Diskussion ein. Unter der Administration von George W. Bush wurde das bisher größte Überwachungsaktion in der Geschichte der NSA, das *Warrantless Surveillance Program* autorisiert, das dem Geheimdienstdirektor Hayden dazu berechtigte das FISA-Gericht bei der Durchführung von Lauschangriffen zu umgehen. Damit trat das Programm in die Fußstapfen seiner Vorgänger aus den 1940er und 1960er Jahren – den Operationen Shamrock und Minaret.

Die Lauschangriffe des Geheimdienstes richteten in erster Linie gegen eingehende und ausgehende internationale Kommunikation von US-AmerikanerInnen (ebd.: 118). Die Operation *Highlander* weitete die Befugnisse dieses illegalen Abhörprogramms weiter aus, indem sie die Grundsatzregel – das eine Kommunikation von einer/m US-AmerikanerIn nur dann überwacht werden dürfe, wenn der Verdacht bestehe, er/sie würde mit einem Al Qaeda Mitglied kommunizieren, aufhob (ebd.: 131).

Der Ansatz war so viele Informationen wie möglich zu sammeln, statt sich bei der Überwachung auf die wichtigsten und potenziell produktivsten Ziele zu konzentrieren.

Unter Hayden rückte insbesondere die Standortermittlung von Personen, die unter dem Verdacht standen in Kontakt mit Terroristen zu stehen, in den Vordergrund (ebd.: 138). Zusätzlich intensivierte Hayden die Überwachung der UN in, insbesondere des UN-Sicherheitsrats und Kofi Annans.

Außerdem schaffte es Hayden noch im selben Jahr (2001) einen Großteil der nationalen Telekommunikationsunternehmen dazu zu bewegen, im Rahmen des Warrantless Surveillance Program mit der NSA im Geheimen zu kooperieren (ebd.: 181).

Die umfangreichen Maßnahmen in der Hayden-Ära konnten u.a. nur durch die Fördermittel des Staates realisiert werden. Das Budget der Behörde stieg nach 9/11 um ein Vielfaches an und Hayden nutzte es für einen technischen Ausbau seiner Behörde (ebd.:124).

5.1.5 2005-2014 (Die Alexander Ära)

Am 1. August 2005 wurde der Vier-Sterne-General Keith Alexander in seinen Dienst als neuer Geheimdienstchef der NSA inauguriert – vor ihm neun lange Dienstjahre, Jahre die den Geheimdienst grundlegend verändern sollten. Als General der US Army entsprang er aus den Reihen der Militärelite und trat die Nachfolge von Hayden an.

Die größte Errungenschaft seiner langjährigen Amtszeit (2005-2014) war die Schaffung des größten und einflussreichsten Geheimdienstes der Welt. Unter seiner

Leitung wurde der Sicherheitsapparat konsequent ausgebaut, die Kompetenzen des Geheimdienstes großzügig erweitert und der Einfluss der Behörde stark vergrößert. Sein Ansatz – ALLES sammeln! (vgl. Greenwald 2014: 143f.)

Ende 2005 enthüllte die New York Times, dass die US-Regierung kurz nach dem 9. September 2001 die transnationale Kommunikation von bis zu 500 US-amerikanischen BürgerInnen ohne richterlichen Beschluss überwachen ließ (vgl. Landau 2010: 88).

Damals versicherten die staatlichen Autoritäten, dass die Überwachung wieder eingestellt wurde. In Wirklichkeit weitete sie sich aus, wie aus den Enthüllungen von Edward Snowden hervorgeht.

Wie aus den geleakten Dokumenten hervorgeht, werden zu jedem beliebigen Zeitpunkt seit Beginn des von Hayden eingeleiteten Überwachungsprogramms um die 500 Ziele im Inland (vgl. Landau 2010: 88) und im Ausland bis zu 5000-7000 an einem beliebigen Tag, überwacht (vgl. Bamford 2008: 121f.).

Einige Monate später veröffentlichte die USA Today einen Bericht darüber, wie die NSA die Datenbanken diverser US-amerikanischer Telefonanbieter nutze, um gewisse Anruf-Muster auszumachen. Betroffen waren 3 von den 4 größten Langstrecken-Providern (AT&T, BellSouth und Verizon), insgesamt wurden mehr als 100 Mio. Berichte gesammelt. Dies widersprach klar der Behauptung vom damaligen US-Präsidenten George W. Bush, die Überwachung würde sich lediglich auf internationale Anrufe beschränken. (vgl. Landau 2010: 88)

Nach den Enthüllungen von Edward Snowden im Sommer 2013 verteidigte Alexander vehement die Überwachungsprogramme der NSA in der Öffentlichkeit. So berichtet Guardian Reporter Carroll über folgende Aussage von Alexander auf einem Kongress in Las Vegas:

„Our job is defending this country, saving lives, supporting our troops in combat. It's our responsibility to provide the information that they need to survive [and] to go after the enemy." (Carroll 31.07.2013)

5.2 Der Status Quo

5.2.1 NSA – No Such Agency

Der unter seinen MitarbeiterInnen neckisch als *No Such Agency* bezeichnete Geheimdienst, der als militärische Abteilung dem Pentagon untersteht, ist innerhalb von ein paar Jahrzehnten zum größten und mächtigsten Geheimdienst der Welt geworden.

Heute zählt er um die 40.000 MitarbeiterInnen, darunter die weltbesten MathematikerInnen und LinguistInnen, ein Jahresbudget von 10 Mrd. US-Dollar (vgl. Stock 2013: 51) und die größte Sammlung an datenverarbeitenden Großrechnern bzw. Supercomputern.

Diese hochentwickelten, extrem leistungsfähigen technischen Geräte werden auch als das Gehirn bzw. Gedächtniszellen der NSA bezeichnet. Als Knotenpunkt der Überwachungsmaschine sammeln, verarbeiten und speichern sie Millionen von Daten. (vgl. Bamford 2001)

Die Zentrale der NSA liegt in Fort Mead, Maryland, auch bekannt als Crypto-City, Geheimstadt (vgl. Bamford 2001: 487f.). Im Zentrum der City befindet sich das großzügig angelegte Hauptquartier und Operationszentrum der NSA (ebd.: 487), in den anderen (Gebäude-) Komplexen, die diversen Unterabteilungen der Agency. Zu den wichtigsten zählen u.a. das Directorate of Operations (DO) – das Zentrum der Fernmeldeaufklärung mit dem Auftrag zur Analyse von Chiffriersystemen, das Directorate of Technology and Systems (DT) – das für alle technischen Angelegenheiten, u.a. für den Entwurf, die Entwicklung und den Einsatz von Fernmeldeaufklärungssystemen (ebd.: 522), zuständig ist (ebd.: 499) und die System Security Organization (SSO) – die Abteilung, die Code- und Chiffriermaterial für die Kommunikation der Regierung produziert (ebd.: 521).

Aufgrund der Überkapazitäten der NSA hat der Geheimdienst ein zusätzliches Rechenzentrum, zur Unterbringung von Servern (Datenspeicher), in Utah errichten lassen – ein riesiges Areal mit vier Server-Hallen zu jeweils 2.300 m², das 2013 in Betrieb genommen wurde (vgl. Stock 2013: 52).

Erwähnenswert ist zudem, dass die NSA ihre eigenen Streitkräfte – den Central Security Service (CSS) (bestehend aus Heer, Marine und Luftwaffe) hat (ebd.: 497), eine eigene Zeitung namens SIGINT Digest besitzt (ebd.: 515) und ein Intranet, das sie unter anderem auch mit anderen Diensten verbindet, dazu aber später noch mehr.

Das Regelgesetzbuch der NSA ist das *United States Signals Intelligence Operations of the United States Sigint Systems (USSID 18)*. Es wurde 1976 verfasst und legt seither die Vorschriften und Verfahren der NSA fest.

Offiziell geschützt vor der Überwachung durch die NSA sind US-amerikanische BürgerInnen, die sich in den USA aufhalten. Laut der Verordnung *U.S. Identities in Sigint (1994)* müssen alle US-amerikanischen Namen in den Berichten der Fernmeldeaufklärung entfernt werden. Dies gilt jedoch nicht in Notfällen, wie z.B. einer Entführung, einem terroristischen Angriff oder einem hinreichenden Verdacht auf ein Verbrechen. (vgl. Bamford 2001: 440)

Außerdem sind US-BürgerInnen, die sich außerhalb der USA befinden und ausländische Botschaften und Diplomaten im Inland vom Rechtsschutz ausgeschlossen. Um diese auszuspähen bedarf es nur einer Genehmigung des amerikanischen Justizministeriums, die ein Jahr Gültigkeit hat. (ebd.: 438)

Außerdem ist der Zugriff auf die Kommunikation von Regierung und Verwaltung ist strengstens untersagt und muss im Falle eines zufälligen Mitschnitts umgehend gelöscht werden (ebd.: 47).

5.2.2 Der legislative Rahmen der geheimdienstlichen Arbeit der NSA

Im folgenden Kapitel möchte ich einen kleinen Exkurs in die US-amerikanische Gesetzgebung machen, die den legislativen Rahmen für die Arbeit der US-Geheimdienste im Bereich der Fernmeldeaufklärung ausmacht.

Die Analyse versteht sich nicht als umfassende Prüfung aller Aspekte, sondern als sorgfältige und aussagekräftige Skizzierung der zentralen gesetzlichen Bestimmungen, zu denen u.a. der FISA (1974), USA-PATRIOT Act (2001) und der FISA Amendement Act (FAA) (2008) zählen.

Die Autorität der US-amerikanischen Sicherheitsbehörden zur Durchführung (elektronischer) Überwachung im Rahmen geheimdienstlicher Arbeit fußt in erster Linie auf zwei Statuten, dem *Foreign Intelligence Security Act of 1978 (FISA)* und dem *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FAA)*.

Das FISA-Gesetz von 1978 ist ein Gesetz zur Regulierung staatlicher Abhöraktivitäten für ausländische nachrichtendienstliche Zwecke. Es wurde nach Bekanntwerden des Watergate-Skandals erlassen und sollte dem staatlichen Machtmissbrauch bei der Durchführung von Lauschangriffen Einhalt gewähren. Mithilfe des Gesetzes wurde eine strikte Trennung zwischen Lauschaktionen im Rahmen polizeilicher Arbeit und inländischer geheimdienstlicher Arbeit zum Schutz der nationalen Sicherheit festgelegt. Ziel war es die Überwachung US-amerikanischer BürgerInnen, die unter Richard Nixon massiv betrieben wurde, zu stoppen. (vgl. Bamford 2008: 67)

Gemäß dem FISA muss sowohl inländische als auch ausländische elektronische Überwachung entweder durch (a) einen richterlichen Beschluss des FISA-Gerichts (vom zuständigen Richter ermächtigt) (FISA, 50 U.S.C. § 1881b) oder durch (b) eine Vollmacht des Generalstaatsanwalts bei einem vorangegangenen Ersuch des Präsidenten ohne einen Gerichtsbeschluss für die Dauer von bis zu einem Jahr (FISA, 50 U.S.C. § 1802), autorisiert werden.

Die Antragstellung für einen (elektronischen) Lauschangriff erfolgt mit einem offiziellen Ersuch des Justizministeriums oder eines FBI-Beamten beim FISA-Gericht (FISA, 50 U.S.C. Sec. 301.).

Voraussetzung für die Ermächtigung ist ein hinreichender Verdacht, dass es sich bei der der überwachten Person, Gruppe oder Institutionen um eine ausländische Macht, also z.B. eine ausländische Regierung, einen Geheimagenten, eine terroristische Gruppierung oder eine/n TerroristIn etc., handelt (FISA, 50 U.S.C. § 1801). Ferner muss sich mindestens eine Person der angezapften Unterhaltung außerhalb der USA befinden, und die Überwachungsaktion darf nicht dafür missbraucht werden, bestimmte Personen in den Vereinigten Staaten von Amerika zu überwachen (FISA, 50 U.S.C. § 1802).

Die Umgehung des Gerichts und des Prozesses der richterlichen Autorisierung bei einem Ersuch zur Überwachung wird laut 50 U.S.C. § 1809 des FISA offiziell mit einer Geldbuße von 10,000 US-Dollar und einer Gefängnisstrafe von 5 Jahren gefahndet.

Die Einhaltung des rechtlichen Rahmens, der die Arbeit der NSA bestimmt, wird von zwei Kontrollinstanzen überwacht, den Geheimdienstausschüssen (*Intelligence Committees*) des Repräsentantenhauses (*House of Representatives*) und des US-Senats (*Senate*) und dem *Foreign Intelligence Surveillance Court (FISC*). Die beiden Ausschüsse sind für die Kontrolle der Finanzen und die Nominierung der Geheimdienstführung zuständig.

Das FISA-Gericht bzw. FISC ist ein eigens zur Kontrolle des FISA-Gesetzes eingeführtes Bundesgericht, das über die Genehmigung der Anträge der US-Regierung in einem geheimen Gerichtsverfahren entscheidet. Es besteht aus 11 Bundes(verfassungs) richtern, die vom obersten Richter des Obersten Gerichtshofs ernannt werden (FAA, 50 U.S.C. § 1881a).

Paragraph 218 des USA-PATRIOT-Acts, 50 U.S.C. ändert das FISA-Gesetz dahingehend ab, dass bereits ein hinreichender Verdacht ausreicht, um Überwachungsanträge im Rahmen des Gesetzes einzuleiten. Das gilt sowohl für die Ermächtigung elektronischer Überwachung, als auch für die Durchsuchung von Eigentum.

Nach 50 U.S.C. § 1807 des FISA ist der Generalstaatsanwalt dazu verpflichtet dem Verwaltungsamt des Gerichtshofs der USA und dem Kongress Rechenschaft über

die Gesamtzahl der Anträge zur Genehmigung elektronischer Überwachung abzulegen, und zwar in Form eines jährlichen Berichts.

Die Tatsache, dass die Standards des FISA-Gerichts zum Feststellen eines hinreichenden Verdachts vergleichsweise niedrig sind, erklärt wieso das Gericht so anfällig ist für Missbräuche. Es besteht vor allem die Gefahr, dass die Lauschangriffe für investigative Fälle der nationalen Strafverfolgungsbehörden genutzt werden und nicht, wie eigentlich vorgesehen für Fälle, die die nationale Sicherheit betreffen.

Was die Glaubwürdigkeit des Gerichts angeht, muss mit Ernüchterung festgestellt werden, dass es seine Funktion als Kontrollinstanz nur unzureichend erfüllt. Ein Großteil der Überwachungsanträge der NSA wird ohne weiteres genehmigt. Da das Gericht unter Ausschluss der Öffentlichkeit tagt und die Entscheidungen des Gerichts streng geheim sind, existiert de facto keine rechtsstaatliche Kontrolle seitens der Zivilbevölkerung.

Laut James Bamford stehen die FISA RichterInnen der NSA oder dem FBI praktisch 24 Stunden am Tag zur Verfügung, wenn es um ein dringliches Ersuchen zu einer Überwachungsbefugnis geht (vgl. Bamford 2008: 113).

Infolge der Terroranschläge von 9/11 und der Anti-Terrorgesetzgebung (USA PATRIOT-Act) wurde im Jahr 2008 der *FISA Amendements Act (FAA)*, eine modifizierte Form des FISA, verabschiedet.

Das Gesetz vereinfachte die massenhafte Überwachung, indem es sämtliche legale Beschränkungen zum Zugriff auf Kommunikation aufhob.

Mit dem FAA legalisierte die Bush-Administration Überwachung ohne richterlichen Beschluss. Damit weitete sich insbesondere die Überwachung von privaten Personen, einschließlich US-AmerikanerInnen, aus. Laut 50 U.S.C. § 1881a des FAA kann die Überwachung einer Einzelperson ohne richterliche Anordnung erfolgen, vorausgesetzt diese hat Kontakt zu einer/m unter Beobachtung stehende/n AusländerIn. Diese Ausnahmeregelung wurde schon bald zum Regelfall und blieb auch in der Amtszeit von Obama bestehen, wie die geleakten Dokumente belegen.

Die US-Regierung verschaffte sich mit Berufung auf den FAA (2008) direkten Zugang zu den persönlichen Kommunikationsdaten von ausländischen und US-amerikanischen BürgerInnen, indem sie die Telekommunikations- und IT-Unternehmen zur Herausgabe dieser Daten zwang. Damit war sie in der Lage auf Telefonate, Emails, Google-Suchanfragen etc. zuzugreifen. (vgl. Greenwald 2014:166)

Gleichzeitig wurde den Unternehmen, die im Auftrag der Regierung zur Herausgabe von Daten gezwungen werden, Immunität vor Strafverfolgung zugesichert (vgl. Mattelart 2010: 148).

Mit der Entstehung von Glasfaserkabeln und der steigenden transnationalen Kommunikationsströmen, die über Satellit gesendet wurden, eröffneten sich für den Geheimdienst neue Möglichkeiten der Überwachung.

Die US-Regierung und die NSA wussten die neue Kommunikationstechnologie, zusammen mit ihren erweiterten Befugnisse für ihre Zwecke zu nutzten.

Charakteristisch für die Zeit nach 9/11 war neben der Erweiterung staatlicher Überwachungskompetenzen die Beschränkung bzw. Reformierung diverser Gesetze zum Schutz der Privatsphäre, darunter: des *Federal Communications Act of 1934 (FCA)* bzw. des *Telecommunications Act of 1996*, des *Electronic Communications Privacy Act of 1986 (ECPA)* etc.

Der *Federal Communications Act of 1934 (FCA*) war die erste bundesgesetzliche Regelung zur Regulierung der US-amerikanischen Kommunikation via Telefon, Telegraf und Radio (später auch Fernseher), die u.a. das unautorisierte Abfangen und die Preisgabe von Kommunikation für illegitim erklärte (47 U.S.C. § 605). Er wurde im Zuge des USA-PATRTIOT-Acts korrigiert.

6 NSA-Affäre 2013-2014: Die Enthüllungen von Edward Snowden

6.1 Die NSA – der mächtigste Geheimdienst der Welt

Der Amerikaner Edward Joseph Snowden überraschte die Welt Anfang Juni 2013, als er geheime Dokumente der National Security Agency (NSA), dem Auslandsgeheimdienst der USA enthüllte und damit den wohl bisher größten Geheimdienstskandal in der jüngsten Geschichte auslöste.

Der aus Crofton, Maryland stammende IT-Spezialist und ehemalige CIA-Agent fasste nach einer langjährigen beruflichen Laufbahn als treuer Staatsdiener und überzeugter US-Patriot, den Entschluss aus dem Sicherheitsapparat auszutreten. Nachdem er seinen Dienst bei der CIA kündigte, heuerte er als Systemadministrator bei DELL an. Dort war er für die Wartung der NSA-Rechner zuständig, was ihm die Möglichkeit verschaffte auf geheime interne Informationen des Geheimdienstes zuzugreifen. (vgl.: Rosenbach; Stark 2014: 27,38)

Zum ersten Mal beschäftigte er sich ausführlich mit den Inhalten der Dokumente und war nach eigenen Angaben geschockt von den Methoden des Geheimdienstes. Später gibt er an, dass vor allem ein Dokument ihn beunruhigte und aufrüttelte. Es ist ein vom Generalinspekteur der NSA am 24. März 2009 verfasster Report, der ausführlich darlegt, „wie das Weiße Haus die Nachrichtendienste dazu drängt, die Grenzen des Rechtsstaats zu verschieben, u.a. auch wie die Behörde im inländischen Telefonbestand nach Terroristen sucht“ (ebd.: 47).

Nach eigenen Angaben war dieses Dokument der Tropfen, der das Fass zum Überlaufen brachte. Snowden war dermaßen enttäuscht vom staatlichen System, dass er sich dazu entschloss so viel Material wie möglich aus dem Computernetzwerk der NSA zu saugen und damit an die Öffentlichkeit zu gehen. (ebd.: 48)

Nachdem ihm bewusst wurde, dass er bei DELL nur einen begrenzten Zugang auf die internen Dokumente der NSA hat, nahm er im März 2013 einen Job bei der privaten Sicherheitsfirma Booz Allen Hamilton in Honolulu, Hawaii an. Dort war er in der Lage auf ein breites Spektrum an Informationen zuzugreifen und er sammelte so

viel Material wie möglich. Mit den gesammelten Geheimdokumenten machte sich Snowden auf den Weg nach Hong Kong, wo er auf den freien Journalisten Glen Greenwald, den Guardian-Journalisten Ewen MacAskill und die Dokumentarfilmerin Laura Poitras traf, um mit deren Hilfe die das gesammelte Material zu veröffentlichen. (ebd.: 51) Die Motivation des Whistleblowers:

> I think that the public is owed an explanation of the motivations behind the people who make these disclosures that are outside of the democratic model. […] I'm no different from anybody else. I don't have special skills. I'm just another guy who sits there day to day in the office, watches what's happening and goes, 'This is something that's not our place to decide, the public needs to decide whether these programs and policies are right or wrong.' And I'm willing to go on the record to defend the authenticity of them and say, 'I didn't change these, I didn't modify the story. This is the truth; this is what's happening. You should decide whether we need to be doing this. (Gallagher 2013: 4:04-5:20)

Es geht ihm nicht um die Sabotage des US-amerikanischen Sicherheitsapparates oder der NSA, wie er im Interview ausdrücklich betont, sondern vielmehr darum die illegitime Massenüberwachung anzuprangern und die Gesellschaft darüber entscheiden zu lassen, ob das was gegenwärtig im Namen der Sicherheit geschieht, richtig ist oder nicht.

Im Zuge der Veröffentlichung von Geheimdokumenten der NSA wurden dann eine Reihe von zum Teil sehr komplizierten, Überwachungsprogrammen des amerikanischen und britischen Geheimdienstes bekannt.

Bei den geleakten Dokumenten handelt es sich größtenteils um als „streng geheim“ (Greenwald 2014: 138) klassifiziertes Material das entweder nur für die Five Eyes – der Nachrichtendienste der USA, UK, Kanadas, Australiens und Neuseelands – bestimmt oder aber gar nicht zur Weitergabe an Ausländer vorgesehen ist: „NOFORN“ – „no foreign distribution“ (ebd.).

Das Material besteht überwiegend aus internen Power Point Präsentationen der NSA und anderen Geheimdiensten, in denen diverse Überwachungsprogramme vorgestellt werden, unter anderem PRISM, Tempora und XKeyscore.

Neben der klassischen menschlichen Spionage, die ihre Informationen aus menschlichen Quellen gewinnt, dem sogenannten HUMINT (Human Intelligence),

bedient sich der Geheimdienst vor allem technischer Mittel bei der Beschaffung von Information; wobei vorrangig IMINT (Imagery Intelligence) – die technische Sammlung von Satellitenbildern und anderen Bildern und SIGINT oder das Sammeln von Informationen von (Satelliten-) Bodenstationen und anderen Plattformen, die (staatliche) Signale abfangen, zur Anwendung kommen. (vgl. Treverton 2009: 17)

Die geheimen Dokumente belegen die technischen Möglichkeiten der Geheimdienste zur Überwachung der weltweiten Kommunikation, die ein schier unendliches Ausmaß erreicht haben.

Zu den gängigen Methoden der Überwachung der NSA zählen:

- das direkte Anzapfen von international genutzten Glasfaserkabeln für Datenübertragung (auch Unterseekabel), das sogenannte „upstream surveillance“ (Greenwald 2014: 160) und die Umleitung der Daten von Glasfaserkabeln, die über die US-amerikanischen Systeme laufen, in die NSA-Archive (Kooperation mit anderen Ländern),
- der Zugriff auf die Computer und Server von IT- und Telekommunikationsunternehmen durch Hacking (ebd.: 151),
- der direkte Datenaustausch zwischen der NSA und IT- und Telekommunikationsunternehmen und zwischen der NSA und ihren Partnerdiensten, aufgrund von geheimen Vereinbarungen, die zur geheimdienstlichen Kooperation verpflichten (ebd.),
- das Einschleusen von Schadprogrammen in einzelne Computer, um deren Benutzer auszuspähen (CNE – Computer Network Exploitation), Abteilung TAO –Tailored Access Operation (ebd.: 173)
- die Beobachtung der Kommunikation im Internet (soziale Netzwerke, Blogs, Skype usw.)
- die Unterwanderung von Verschlüsselungsprogrammen (Biermann 2013: 23)

  etc.

Die günstige geografische Lage der USA – die meisten Überseekabel laufen über die Vereinigten Staaten, wie Abbildung 3 zeigt – kommt der Überwachungsmaschine der NSA zu Gute.

Der Geheimdienst nutzt die dominante Rolle der USA zur umfassenden Überwachung, indem er die Unterseekabel an ihren Landestationen (blau eingezeichnet) an der Ostküste (für den Datenverkehr aus Europa, Südamerika, Afrika) und an der Westküste (für den Datenverkehr aus Asien und Südamerika) anzapft und überwacht.

Zum Teil laufen die Transatlantik-Leitungen über Knotenpunkte in Großbritannien, wo der britische Geheimdienst GCHQ Kommunikationsdaten abgreift und sie an die NSA weiterleitet. Das wohl bekannteste und umfassendste britische Überwachungsprogramm ist *Tempora* – es hat Zugriff auf mehr als 200 internationale und interkontinentale Glasfaserkabel zu, darunter auch das Transatlantik-Glasfaserkabel TAT-14 mit Knotenpunkt im britischen Bude-Haven, durch das ein Großteil der europäischen Übersee-Kommunikation fließt (vgl. Bamford 2008: 177).

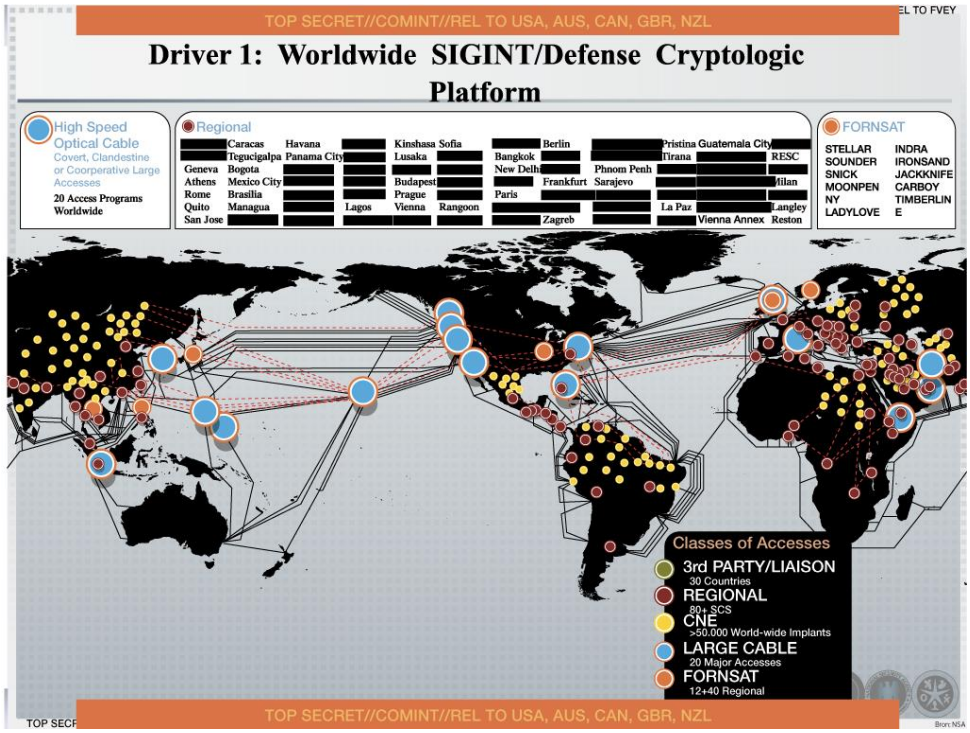

Abb. 1: USA – Transitland der internationalen Kommunikation
(Quelle: NSA, zit.n. Greenwald 2014: 173)

Die USA sind aufgrund technischer Überlegenheit, ökonomischer Stärke und politischer Macht zentraler Knotenpunkt der weltweiten Kommunikation. Die größten und wichtigsten Internet Service Provider (ISP), unter anderem auch die größten

Email-Provider der Welt (wie Yahoo Mail, Hotmail, Gmail etc.) und Telekommunikationsunternehmen (wie AT&T, Verizon, etc.) sind in den Vereinigten Staaten ansässig. (Landau 2010: 87)

Allein AT&T, das größte US-amerikanische Telekommunikationsunternehmen und eines der größten weltweit, bietet Fernverkehr-Dienstleistungen für insgesamt 34.4 Mio. KundInnen weltweit an (vgl. Bamford 2014: 186). Für die Geheimdienste ergeben sich daraus neue umfassende Möglichkeiten und Formen der Überwachung.

Konkret bedeutet das, dass sogar Emails, die auf der lokalen Ebene von A nach B verschickt werden, möglicherweise über die USA laufen, vorausgesetzt es wird ein US-amerikanischer Email Server, wie z.B. Gmail benutzt. Dies gilt auch für ISP und Dienste, wie z.B. Cloud-Services, die von US-Unternehmen in weiten Teilen der Welt angeboten werden.

Relevant sind neben den Inhalten der Kommunikation, vor allem auch die sogenannten Metadaten bzw. Verbindungsdaten – also Informationen darüber, wer mit wem wie lange kommuniziert. Sie gelten zum Teil sogar als aufschlussreicher als die konkreten Inhalte von Kommunikationen, da sie ein umfassenderes Bild vom/von der NutzerIn und seinem/ihrem Personenkreis zeichnen können. Sie lassen sich im Gegensatz zu Inhaltsdaten nicht verschlüsseln und altern auch weniger schnell. Dies bestätigt die folgende ins Deutsch übersetzte Aussage von Edward Snowden aus einem Interview mit dem Spiegel:

> Gegenwärtig altert im Volltext gesammeltes Material sehr schnell, innerhalb von ein paar Tagen, vor allem durch seine gewaltige Masse. Es sei denn ein Analytiker markiert ein Ziel oder eine bestimmte Kommunikation. In dem Fall wird die Kommunikation bis in alle Ewigkeit gespeichert, eine Berechtigung dafür bekommt man immer. Die Metadaten […] altern weniger schnell. Die NSA will, dass wenigstens alle Metadaten für immer gespeichert werden können. Meistens sind die Metadaten wertvoller als der Inhalt der Kommunikation. Denn in den meisten Fällen kann man den Inhalt wieder besorgen, wenn man die Metadaten hat. (Rosenbach/ Stark 2014: 76)

Dieses Potenzial haben auch die Geheimdienste für sich entdeckt. Die NSA sammelt Meta-Daten und erstellt mithilfe von ihnen detaillierte (Bewegungs-) Profile von Personen.

Das mitunter wichtigste Kommunikationsmedium, das von der NSA zur Überwachung eingesetzt wird, ist das Mobiltelefon. Die Überwachung läuft entweder über das Anzapfen von Zielen im oder aber mithilfe von sogenannten Verfolgungs-Technologien, wie z.B. Triggerfish. Die elektronischen Werkzeuge für einen Lauschangriff reichen von Mikrofonen, die in der unmittelbaren Umgebung installiert werden (z.B. der benachbarten Wohnung), bis hin zu Wanzen, die in den Telefonreceiver eingebaut werden etc. 2009 liefen insgesamt 96 % der Abhörpraktiken der NSA über das Abhören von Mobilgeräten (Mobiltelefonen und Pagern), autorisiert durch Gesetze, wie den USA-PATRTIOT-Act und den FAA. (vgl. Landau 2010: 248f.)

Das Sammelvolumen der NSA ist gigantisch, wie folgendes Dokument belegt. 2012 übersteigt der Wert aller gesammelten Daten 20 Milliarden pro Tag. Das ist weit mehr als die NSA tatsächlich bearbeiten kann, wie der folgende Power-Point Chart aus dem Snowden-Archiv zeigt.

Das belegen auch diverse Insider – ehemalige Mitarbeiter und ranghohe Beamte der CIA, NSA und FBI, die auf das Problem der NSA hinweisen, nicht alle gesammelten Daten tatsächlich auch auswerten zu können (vgl. Bamford 2001: 521).

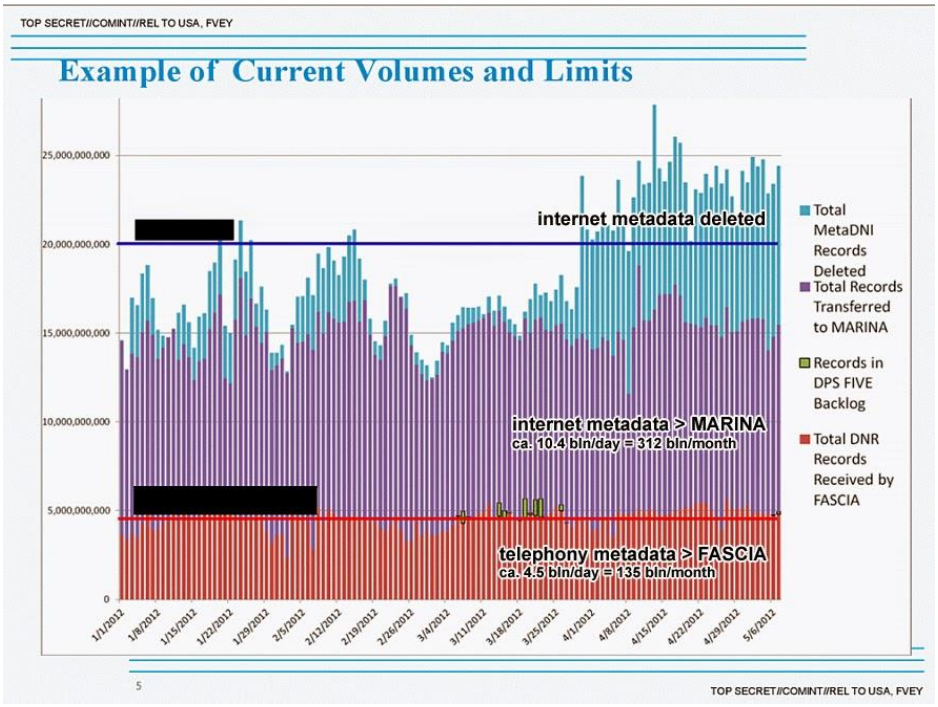

Abb. 2: Die Kapazitäten der NSA und der Umfang der Überwachung
(Quelle: NSA, zit.n. Greenwald 2014: 148)

Das Verständnis der eigenen Mission ist nicht beschränkt auf die Sammlung sicherheitsrelevanter Informationen. Nach dem Motto *Um die Nadel zu finden, braucht man erstmal den Heuhaufen,* wie der NSA-Direktor Keith Alexander während eines Interviews beim Aspen Security Forum 2013 betonte, wird eine schleppnetzartige Überwachung betrieben. Aus der gesammelten Menge an Daten werden Informationen nach bestimmten Kriterien herausgefiltert. Ein gutes Beispiel für ein derartiges Analyseinstrument der NSA ist *XKeyscore* (vgl. Greenwald 2014: 221). Ein Programm, das mithilfe von Algorithmen die vollen Datenbanken des Geheimdienstes nach ausgewählten Merkmalen, wie z.B. IP-Adressen, Namen, Schlüsselwörtern etc. durchsucht und anhand dessen ein komplettes Profil zu einer Person – mit allen auffindbaren Daten – in Echtzeit erstellt (ebd.: 228).

Nach Angaben von BND-Chef Gerhard Schindler und BfV-Chef Hans-Georg Maßen besitzen auch der BND und der BfV das Programm, angeblich zu Testzwecken (vgl. Gebauer et.al. 2013: 21).

Die NSA sucht u.a. auch nach Auffälligkeiten, die sich vom konventionellen Kommunikationsverhalten unterscheiden, so speichert sie beispielsweise verschlüsselte Emails für einen längeren Zeitraum (vgl. Roth 2013: 48).

Was die rechtlichen Einschränkungen bezüglich der Überwachung von Kommunikation angeht, z.B. das Verbot der Überwachung von US-AmerikanerInnen, so kommen diese erst nach der Sammlung der Informationen zur Anwendung (vgl. Heumann/ Scott 2013: 153).

Dieser Aspekt der allumfassenden Sammlung ist ein entscheidender Faktor, der die Überwachungsinfrastruktur der NSA als höchst undemokratisch entlarvt.

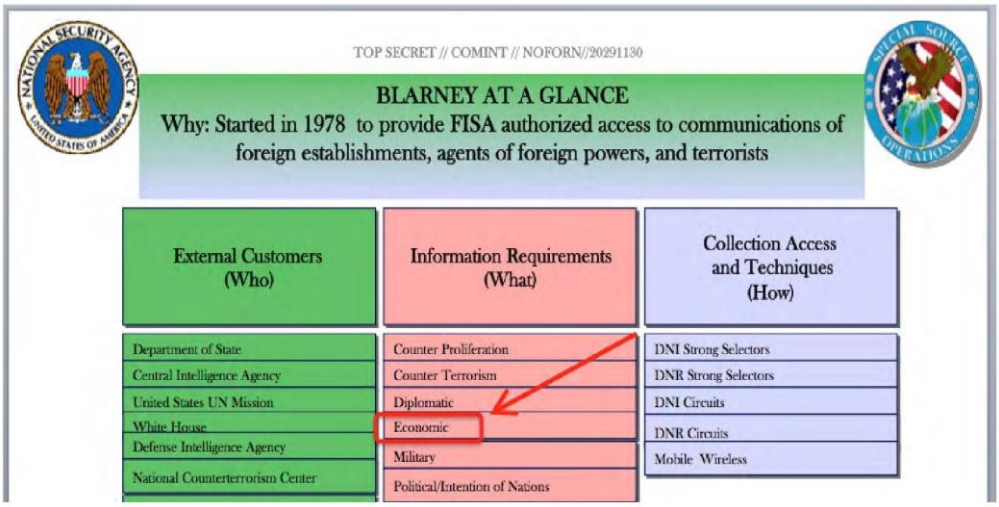

Abb. 3: Das Überwachungsprogramm BLARNEY und seine Abnehmer
(Quelle: NSA, zit.n. Greenwald 2014: 197)

Abgesehen von der Überwachung krimineller Organisationen und Terroristen bzw. verdächtiger Staaten zum Schutz der nationalen Sicherheit, wie von der US-Regierung stets behauptet, betreibt die NSA, eindeutig auch Wirtschaftsspionage, wie in der Abb. 3 zu sehen ist. Zu den Überwachungszielen zählen neben Counter Proliferation, Counter Terrorism, Military auch die Bereiche Economic, Diplomatic, Political Intention of Nations. Auch demokratisch gewählte Regierungschefs verbündeter Staaten (ebd.: 201f.), darunter auch die deutsche Bundeskanzlerin, und gewöhnliche Bürgerinnen und Bürger (FISA Secondary Order 2013) sind strategische Ziele der NSA, wie geheime Dokumente belegen.

Das formulierte Ziel der NSA ist es alle verfügbaren Kommunikationsdaten weltweit zu sammeln und zu speichern. Es geht um die Wahrung eines lückenlosen Systems der Geheimdienste NSA und GCHQ.

Dies geschieht unter anderem im Auftrag der US-Regierung, das White House steht zusammen mit andern Ministerien auf der Liste der sogenannten *Customers*, also KundInnen, die den Dienst der NSA in Anspruch nehmen, wie folgender Slide verdeutlicht.

Abb. 4: Die KundInnen und PartnerInnen der NSA
(Quelle: NSA, zit.n. Greenwald 2014: 197)

Weitere Kooperationspartner sind nationale und internationale Sicherheitsorganisationen bzw. -institutionen, wie die NATO, das Verteidigungsministerium diverse militärische Einheiten etc.

6.2 Die Überwachungsprogramme der NSA und des GCHQ

Alles beginnt am 6. Juni 2013, als in der linksliberalen britischen Tageszeitung The Guardian die erste Enthüllung des 30-järigen Systemadministrators Edward Snowden veröffentlicht wird. Der Artikel beschreibt, wie das US-amerikanische Telekommunikationsunternehmen *Verizon* auf Anfrage des FBI zur regelmäßigen Herausgabe von Telefon-Metadaten seiner KundInnen, unter anderem von Millionen von US-BürgerInnen gezwungen wurde, und zwar auf der Grundlage einer geheimen Verfügung des FISA-Gerichts vom 25. April 2013. (vgl. The Guardian, 6.06.2013).

Diese beruft sich auf den Paragraphen 1861 (50 U.S.C) des USA-PATRIOT-Act (vgl. United States Foreign Intelligence Surveillance Court 2013: 1), der den Zugriff zu bestimmten „business records“ im Rahmen geheimdienstlicher Arbeit und im Rahmen von Ermittlungen zu internationalem Terrorismus regelt.

Laut der geheimen Verfügung wird dem FBI und der NSA der Zugriff auf die KundenInnendaten des Unternehmens im Jahr 2013 für die Dauer von bis zu drei Monaten gewährt (FISA Secondary Order 2013: 3f.).

Dies ist ein klarer Beweis dafür, dass die NSA entgegen der Behauptung von James Clapper - dem nationalen Geheimdienstdirektor Vereinigten Staaten - vor dem US-Senat im März 2013 (vgl. Wyden 2013: 6:43-7:06), Millionen von Daten US-amerikanischer BürgerInnen sammelt.

Später wird bekannt, dass die Zugriffsberechtigung für die letzten 7 Jahren galt und alle 3 Monate vom FISA-Gericht erneuert wurde (vgl. Heumann; Scott 2013: 154).

Die zweite große Enthüllung ist das Überwachungsprogramm *PRISM*, ein Programm, das Kommunikationsdaten direkt von den Servern der US-amerikanischen Internetdienstleister Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple sammeln soll, wie in der Abbildung angegeben. Bei dem gesammelten Material handelt es sich überwiegend um private Emails, Fotos, Videos etc., die in den Datenbanken der Internet-Unternehmen gespeichert werden (vgl. Greenwald; MacAskill 07.06.13)

Autorisiert wird das Programm durch Abschnitt 702 des FAA-Gesetzes von 2008, das die Richtlinien für die geheimdienstliche Überwachung festlegt. Demnach sind Überwachungsziele Personen, die sich zur Zeit der Überwachung im Ausland befinden und keine US-BürgerInnen sind (FAA 2008: 3).

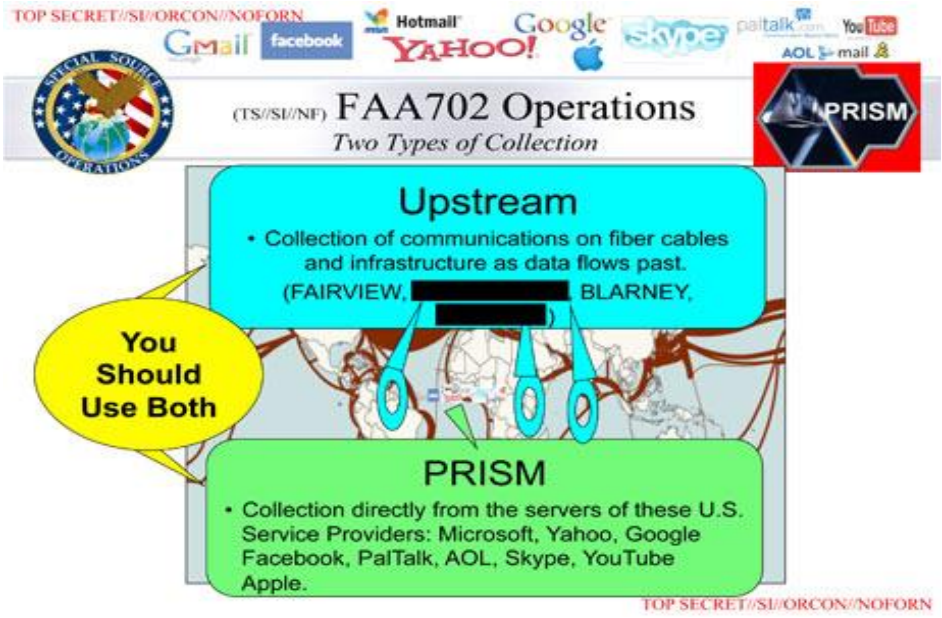

Abb. 5: Überwachungsmethoden – Upstream und das Programm PRISM (Quelle: NSA, zit.n. Greenwald 2014: 160)

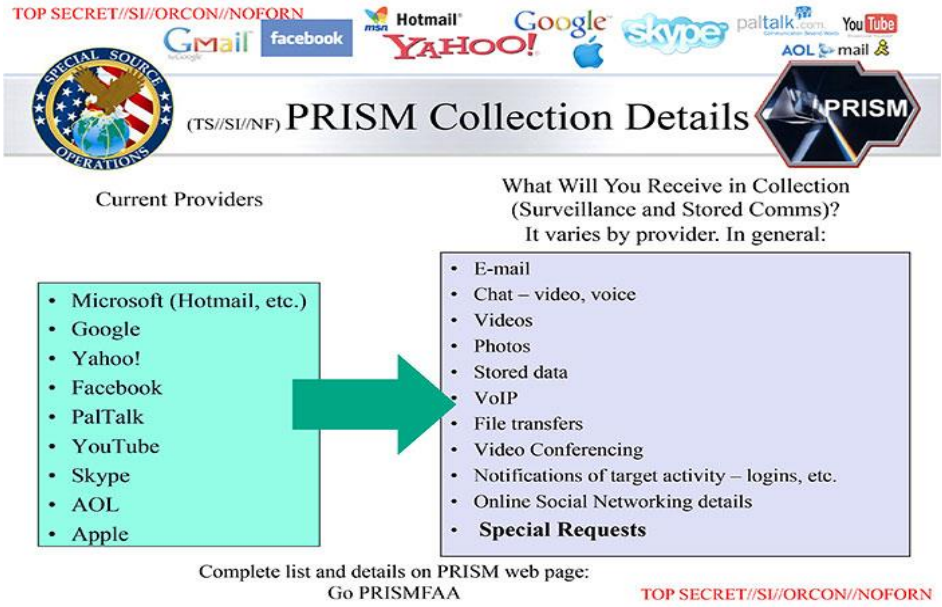

Abb. 6: Das Überwachungsprogramm PRISM (Quelle: NSA, zit.n. Greenwald 2014: 162)

Es ist ein Schock für alle Kundinnen und Kunden der angesehenen Internetdienstleister. Trotz diverser Datenschutzbestimmungen geben sie detailliertes personenbezogenes Datenmaterial an die NSA weiter.

Die Reaktion der Firmen nach der Veröffentlichung des Programms PRISM war verhalten, einige Unternehmen, wie z.B. Facebook und Google stürzten sich in wirre Formulierungen, letztendlich bestritten sie aber nicht die Zusammenarbeit mit der NSA. (Greenwald 2014: 161)

Am 8. Juni 2014 folgt die Veröffentlichung von *Boundless Informant*, eines Programms, das für die Sammlung von Datensätzen aus Telefonaten (DNR, Dialed Number Recognition) und internetbasierten Kommunikationsformen, wie E-Mail und Chats (DNI, Digital Network Intelligence) zuständig ist. Es greift auf die Kommunikation der Menschen weltweit quasi in Echtzeit zu, sammelt ihre Meta-Daten und erstellt anhand dessen Benutzerprofile von den Userinnen und Usern. Aus folgender Graphik geht hervor, dass die Abteilung *Global Access Information* insgesamt mehr als 200 Milliarden Datensätze monatlich aus Tele- und Internetkommunikation sammelt.

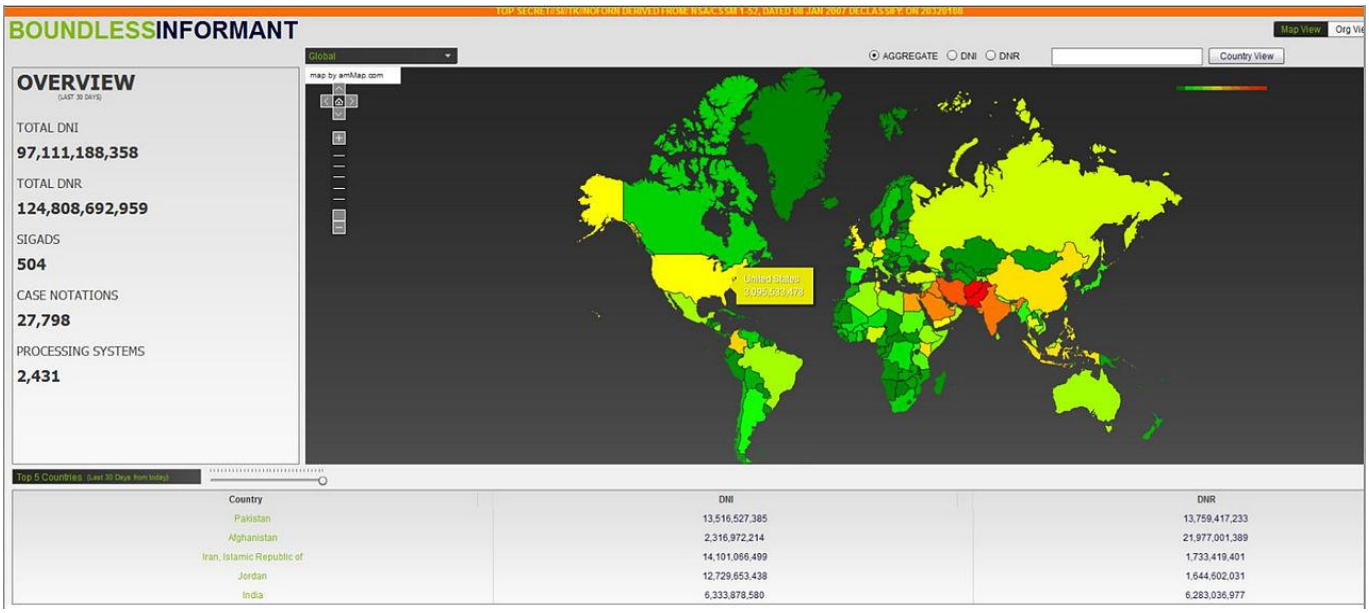

Abb. 7: Das Programm Boundless Informant
(Quelle: NSA, zit.n. Greenwald 2014: 141)

Allein in Deutschland werden rund 500 Millionen Datensätze in einem Zeitraum von nur 30 Tagen gesammelt, wie das Programm Boundless Informant bestätigt (vgl. ebd.: 140).

Entgegen der Behauptung Keith Alexanders vor dem Untersuchungsausschuss des US-Kongress die NSA würde ihre gesammelten Daten nicht zählen, zeigt die Graphik, dass sie genau das mithilfe des Programms Boundless Informant tut.

Am 9. Juni 2013 wird dann ein Video publik, das die Person hinter den Enthüllungen zeigt, den Whistleblower Edward Snowden wie er von zwei Journalisten in seinem Hotelzimmer in Hong Kong befragt wird. Auf Youtube wird das Video binnen kürzester Zeit wird es mehr als 1 Mio. Mal angeklickt, mittlerweile hat es schon mehr als 3 Mio.

Als Reaktion auf die Veröffentlichungen erhebt die US-Regierung am 21. Juni 2013 eine Anklage gegen Edward Snowden wegen Spionage, Diebstahl und Weitergabe von Regierungseigentum. Anschließend wird ein Haftbefehl gegen ihn erlassen und sein Pass annulliert.

Am 23. Juni beschließt Snowden nach Moskau zu fliegen und verbringt mehr als fünf Wochen im Transitbereich des Flughafens Scheremetjewo, bis er schließlich am 1. August für ein Jahr Asyl in Russland bekommt. Dieses wird im Sommer 2014 auf drei Jahre verlängert.

Bis dato folgten weitere Veröffentlichungen von Geheimdokumenten, die u.a. auch die Überwachung von Staats- bzw. Regierungschefs und diplomatischer Vertretungen enthüllen.

6.3 Der Auftrag der NSA

Der Auftrag der NSA teilt sich im Wesentlichen in zwei Bereich auf: die Fernmeldeaufklärung und die Informationssicherheit.

Letzteres gewinnt insbesondere mit der Informationsrevolution zunehmend an Bedeutung. Im Zeitalter der neuen Informationstechnologien soll die NSA neben der klassischen Fernmeldeaufklärung, deren Aufgabe es ist Datenflüsse (mit technischen Mitteln) Abzufangen, zu Filtern und zu Analysieren, vor allem auch eine Vorreiterrolle im Schutz staatlicher kritischer Infrastrukturen vor Cyber-Angriffen einnehmen. So ist sie nach dem *Computer Security Act (1987)* u.a. für die Entwicklung (kryptographischer) Standards für den Schutz von Daten zuständig (vgl. Landau 2010: 244).

In ihrem Strategiepapier formuliert die NSA ihre Mission wie folgt:

> The National Security Agency/Central Security Service (NSA/CSS) leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances (NSA/CSS 2010:1).

Der allumfassende Anspruch der Behörde lässt sich aus dem folgenden Geheimdokument der NSA (Abb. 8) schlussfolgern, darin heißt es: Know It All, Collect It All, Process It All, Exploit It All, Partner It All, Sniff It All. Diesem Selbstverständnis liegt ein zutiefst herrschsüchtiger Gedanke zu Grunde.

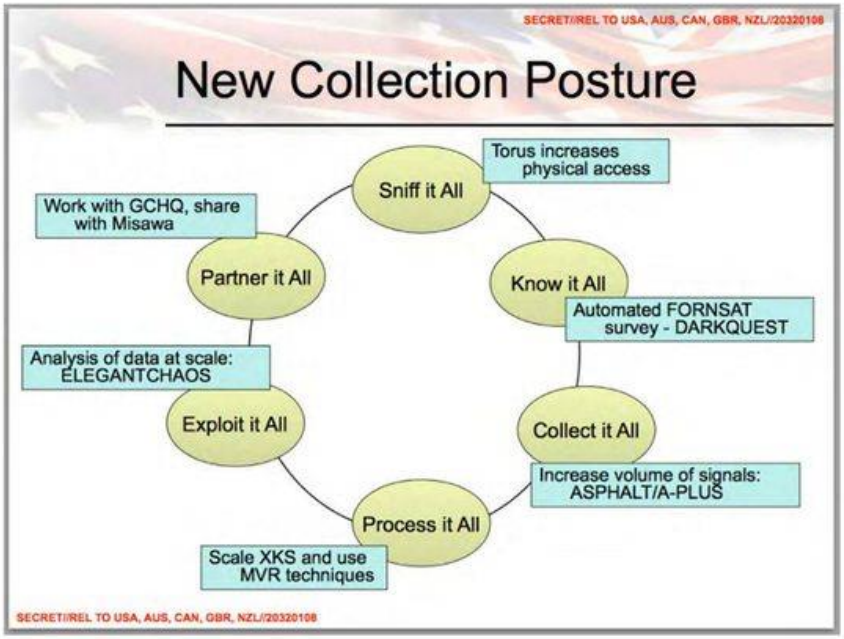

Abb. 8: Der Anspruch der NSA
(Quelle: NSA, zit.n. Greenwald 2014: 146)

Das Primat der geheimdienstlichen Arbeit liegt in der Bekämpfung dieser Bedrohungen, wobei diese bereits bei der Prävention ansetzt.

6.4 Die Partner der NSA

Die Liste der NSA-Partner ist lang, und lässt sich in verschiedene Kategorien einteilen. Zunächst einmal sind da die nationalen Geheimdienste (CIA, FBI etc.), aber auch die internationalen Geheimdienste, die je nach Vertrauensverhältnis mehr oder weniger eng mit der NSA zusammenarbeiten.

Eine besondere, fast freundschaftliche Beziehung pflegt die NSA zu der Gruppe der sogenannten „FVEY“ (Greenwald 2014: 138), den Geheimdiensten der Staaten Großbritanniens, Kanadas, Australiens und Neuseelands. Das geht aus den geleakten Dokumenten hervor, in denen die genannten Länder als „Second Parties“ (ebd.: 181) gekennzeichnet sind, was so viel bedeutet wie eine enge Beziehung und Kooperation, aufgrund ähnlicher Interessen.

Der Datenaustausch zwischen den Diensten findet durch eigens dafür eingerichtete Netzwerke statt. Zu den bedeutendsten zählen *Interlink* – ein Intranet für die Kommunikation der NSA mit dem FBI, der CIA und den Geheimdiensten der Partnerländer Großbritannien, Kanada und Australien, in dem die NSA regelmäßig Dokumente veröffentlicht und das *Advanced Technology Demonstration Network* – das die NSA mit dem Pentagon, der DIA, der NSA etc. verbindet. (Bamford 2001: 514f.)

Die enge Zusammenarbeit der NSA mit der Gruppe der FVEY geht zurück auf die Nachkriegszeit. Diese strategische Partnerschaft hatte in erster Linie den Zweck der Sicherung westlicher Interessen und der Ausweitung der westlichen Einflusssphäre.

Das *UKUSA Communications Intelligence Agreement* vom 5. März 1946 – ein Abkommen zwischen den Geheimdiensten Großbritanniens, Kanadas, Australiens Neuseelands und der NSA diente der Ausweitung der Kooperation im Bereich der Fernmeldeaufklärung dieser Länder. Überall in den Partnerländern wurden Abhörposten errichtet, zum Teil Ableger der NSA, aber auch nationale Stationen der Partnerländer (vgl. Bamford 2001: 389).

Mittlerweile sind die UKUSA-Partner zu einer Supermacht unter den Geheimdiensten geworden mit eigenen Regeln und Gebräuchen, verbunden durch ein umfassendes

Computernetz mit dem Codenamen *Platform* (Bamford 2001: 399f.) – ihr Ziel: die Beherrschung des Cyberspace.

Sie haben auch ein eigens zur Überwachung und Auswertung der Satellitenkommunikation eingerichtetes System entwickelt – das sogenannte ECHELON- System (vgl. Rosenbach/ Stark 2014: 107). Bereits im Jahr 2001 verabschiedete das EU-Parlament einen kritischen Bericht zu diesem System, in dem sie auf die besorgniserregende Überwachung von europäischer Kommunikation durch die NSA hinwies.

Aus der Gruppe der FVEY hat die NSA eine noch engere Beziehung zum britischen Geheimdienst, dem Government Communications Headquarters (GCHQ). So geht aus den geleakten Dokumenten hervor, dass der GCHQ zusammen mit der NSA an der Überwachung internationaler Politikerinnen und Politkern beim G20-Treffen in London im Jahr 2009 beteiligt war. Es wurden unter anderem Emails und Computer ausspioniert. Außerdem sollen während des Meetings in London, die über die Mobilfunkverbindungen laufende, Kommunikation der anderen TeilnehmerInnen nahezu in Echtzeit an die britischen PolitikerInnen übermittelt worden seien. (vgl. Rosenbach/ Stark 2014: 158f.)

Es sind also nicht nur unter dem Verdacht des Terrorismus agierende Personen, die unter das Überwachungsraster der NSA fallen, sondern auch internationale Staatsoberhäupter, wie Angela Merkel und staatliche Institutionen, wie die ständige Vertretung der EU bei den Vereinten Nationen in New York und Washington D.C.. Das allein verstößt schon gegen sämtliche internationale Abkommen.

Außerdem ist der GCHQ an der Überwachung der weltweiten Zivilbevölkerung beteiligt. Wie die Enthüllungen von Edward Snowden zeigen, sammelt der britische Geheimdienst massenhaft Kommunikationsdaten aus Unterseekabeln. Das wohl umfangreichste britische Überwachungsprogramm ist Tempora – ein Instrument, das nach dem „full take“ (Rosenbach/ Stark 2014: 12) Prinzip operiert. Es greift auf sämtliche Informationen zu, die über britische Server oder Glasfaserkabeln in Großbritannien laufen und speichert diese bis zu 3 Tage (Ewen MacAskill et al. 2013).

Als rechtliche Grundlagen für die Sammlung der Informationen, die über die Glasfaserkabeln Großbritanniens laufen, dienen der britischen Regierung in erster Linie der *Intelligence Surveillance Act* von 1994 und der *Regulation of Investigatory Powers Act 2000 (RIPA)*.

Letzteres ist verantwortlich für die umfassenden Befugnisse des GCHQ beim Zugriff auf Informationsströme innerhalb Großbritanniens. Das Gesetz wurde im Jahr 2000 verabschiedet und erteilt dem britischen Geheimdienst die Befugnis, auf die Kommunikation des gesamten Landes und auf die durch Großbritannien geleiteten Kommunikationsströme in transatlantischen Glasfaser-Kabeln zuzugreifen.

Zur Autorisierung von (umfangreichen) Spähaktionen bedarf es in Großbritannien lediglich einer Generalvollmacht des britischen Außenministers, die für die Dauer von 6 Monaten gewährt wird. Eine richterliche Instanz, vergleichbar mit dem FISA Gericht in den USA gibt es in England nicht. (vgl. Leisegang 2014: 135)

Nach der Gruppe der FVEY, kommen die Partner der sogenannten „Third Parties“ (Greenwald 2014: 181) Partner, zu denen u.a. Länder, wie Deutschland, Israel, Indien und Pakistan zählen etc. (vgl. ebd.). Im Gegensatz zu den FVEY, sind diese Staaten Abhörziele der NSA.

Wie intensiv die Geheimdienste teilweise zusammenarbeiten wird an den geleakten Dokumenten zum deutschen Geheimdienst BND deutlich. Am 22.07.2013 veröffentlicht der Spiegel erstmals einen Artikel, der von der bewussten Weitergabe deutscher Verbindungsdaten an die NSA handelt. Ein in dem Artikel veröffentlichtes Geheimdokument der NSA, vom 17.01.2013 belegt, dass der BND die Bundesregierung gezielt dazu aufforderte, bestehende Datenschutzrechte, im Interesse einer besseren Zusammenarbeit (im Austausch von Geheimdienstinformationen) zwischen BND und NSA, zu umgehen (vgl. Pfister et. al. 2013: 17). Ein anderes Dokument, vom 29.04.2013, beweist den Erfolg dieser Bemühungen, darin heißt es wörtlich:

„The German government modified its interpretation of the G-10 Privacy Law, protecting the communications of German citizens, to afford the BND more flexibility in sharing protected information with foreign partners” (ebd. 2013: 19).

Auch BND-Chef Gerhard Schindler räumte im Zuge der Ermittlungen der Bundesregierung zur NSA-Affäre im Parlamentarischen Kontrollgremium des Bundestages, die Zusammenarbeit mit der NSA ein.

Tatsächlich hat die Zusammenarbeit zwischen BND und NSA eine lange Tradition. Sie geht zurück bis in die Nachkriegszeit, als sich die Alliierten, insbesondere die US-Amerikaner, ihre politische und wirtschaftliche Hegemonie in Westdeutschland, im Tausch gegen Sicherheit, sicherten. Aus dieser Zeit stammt das *NATO-Truppenstatut Zusatzabkommen (1959)*, das die BRD zur Zusammenarbeit mit den USA verpflichtete (zum Schutz US-amerikanischer Truppen in Westdeutschland), und bis heute den Aufenthalt von NATO--Streitkräften in Deutschland regelt.

Nach 9/11 wurde diese langjährige Zusammenarbeit auf der Grundlage des *Memorandum of Agreement* vom 28. April 2002 ausgedehnt, das die Einrichtung einer Basis für die gemeinsame Fernmeldeaufklärung im bayrischen Bad Aibling vorsah. Seither findet eine intensive Zusammenarbeit beider Nachrichtendienste auf deutschem Boden statt. So soll der BND regelmäßig Metadaten (Telefonnummern, Email Adressen, IP-Anschlüsse etc.) aus der eigenen Fernmeldeaufklärung an die NSA liefern, wie die geheimen Dokumente belegen.

Auch der deutsche Inlandsgeheimdienst BfV – Bundesamt für Verfassungsschutz – arbeitet intensiv mit der NSA zusammen. Wie aus einem am 29.07.2013 im Spiegel veröffentlichten Geheimdokument der NSA hervorgeht.

Außerdem wurde am 22.07.2013, in einem im Spiegel veröffentlichten Artikel bekannt, dass der deutsche Inlandsgeheimdienst BfV – Bundesamt für Verfassungsschutz – im Jahr 2012 insgesamt 180 Mio. Datensätze aus der nationalen Aufklärung – also Daten von deutschen BürgerInnen – an die NSA übermittelte; die er durch das Überwachungsprogramm XKeyscore erfasst hatte (vgl. Pfister et.al. 2013: 18).

Die Zusammenarbeit der beiden Dienste findet u.a. im Dagger-Complex, einem ehemaligen US-Stützpunkt statt. Der Spiegel bestätigte in seiner Ausgabe vom 12.08.2013, dass der im hessischen Griesheim ansässige Dagger-Complex „das **Europäische kryptologische Zentrum** [Hervorhebung der Verf.] des Dienstes [der

NSA]“ (Poitras/ Rosenbach/ Stark 2013: 23) ist. Er berief sich dabei auf Geheimdokumente der NSA, die er in der Ausgabe 31 veröffentlichte.

Tatsache ist, dass die Kooperation zwischen den deutschen Geheimdiensten und der NSA in den letzten Jahren, also in der Amtszeit von Angela Merkel, deutlich gestiegen ist. Das lässt sich anhand der veröffentlichten Geheimdokumente der NSA belegen. Es scheint fast so, als habe die Bundesregierung ihre Absage an die USA am Irak Krieg teilzunehmen, mit einer aktiven Zusammenarbeit der Geheimdienste wettgemacht.

Neben der nachrichtendienstlichen Kooperation zwischen BND/BfV und NSA, hat auch auf der gesetzlichen Ebene eine Annäherung Deutschlands an die Anti-Terrorpolitik der US-Amerikaner stattgefunden. Zu den wichtigsten Reformen in Deutschland zählen u.a. die 2001 und 2002 erlassenen Anti-Terror-Sicherheitspakete.

Das Anti-Terror-II Paket beinhaltet Änderungen des Gesetzes über den Militärischen Abschirmdienst, des Bundeskriminalamtsgesetzes, Bundesverfassungsschutzgesetzes, Gesetzes über den Bundesnachrichtendienstes, Ausländergesetzes, Sozialgesetzbuches X – Verwaltungsverfahren und des Gesetzes zu Artikel 10 des Grundgesetzes (vgl. Classen 2001: 1).

Relevant sind insbesondere die Erweiterungen der Kompetenzen der Strafverfolgungsbehörden. So wird dem BKA die Durchführung von „Ermittlungen zu schweren Fällen der Datennetzkriminalität gemäß §§ 303a und 303b StGB“ (Classen 2001: 3) innerhalb der Bundesrepublik überlassen. Dabei muss nicht einmal ein begründeter Verdacht vorliegen (vgl. ebd.), womit praktisch die Überwachung von jedem/r beliebigen BürgerIn autorisiert und die Trennung zwischen Exekutivorganen und Geheimdiensten quasi aufgehoben wird.

Auch den nationalen Geheimdiensten (BfV, BND) wurden gemäß des Anti-Terrorgesetzes II zusätzliche Befugnisse in der Überwachung zugesichert, u.a. das Einholen von KundInneninformationen bei „Postunternehmen, Banken, Luftverkehrsunternehmen [und Telekommunikationsunternehmen]“ (Classen 2001: 5) und die Durchführung von „große[n] Lauschangriff[en]“ (ebd.), u.a. wenn es um

begründete Verdachtsfälle geht, die gegen Art. 9 Absatz 26 des Grundgesetzes verstoßen (vgl. ebd.: 4).

Damit wird das Grundrecht auf individuelle Freiheit, das im Artikel 10 des Grundgesetzes verankert ist, erheblich eingeschränkt. Dies wirkt sich natürlich beträchtlich auf die Privatsphäre der Bundesbürgerinnen und Bundesbürger aus.

Die langzeitliche Speicherung von Telefon- und Internetverbindungsdaten, die sogenannte *Vorratsdatenspeicherung*, wurde auf der europäischen Ebene im 2006 durchgesetzt. In Deutschland wurde die neue Regelung jedoch 2010 vom Bundesverfassungsgericht für verfassungswidrig erklärt und verboten.

Die enge Kooperation der Dienste ermöglicht das Finden von Schlupflöchern in der jeweils anderen nationalen Gesetzgebung, sodass die gesammelten Daten des einen Nachrichtdienstes im Tausch gegen Quellen und Informationen des anderen Nachrichtendienstes erkauft werden.

Neben der rein staatlichen Zusammenarbeit mit anderen Geheimdiensten und Sicherheitsinstitutionen, hat die NSA auch zahlreiche Partnerschaften mit privatwirtschaftlichen Unternehmen. Da sind zum einen private (Sicherheits-) Unternehmen, wie DELL und Booz Allen Hamilton, die Überwachungs- und nachrichtendienstliche Tätigkeiten für die NSA erledigen. (vgl. Greenwald 2014: 151)

Zum anderen gibt es enge Kooperationen des Geheimdienstes mit privaten IT- und Telekommunikationsfirmen, wie die geleakten Dokumente beweisen. Dazu zählen Unternehmen, wie Verizon, Microsoft, Google, Yahoo etc. – sie spielen eine essentielle Rolle bei der Informationsbeschaffung. Zuständig für die geheimdienstliche Kooperation mit den Unternehmen ist die Abteilung Special Sources Operations (SSO) der NSA. Der Zugriff erfolgt durch spezielle SSO-(Überwachungs-) Programme, wie BLAIRNEY, FAIRVIEW, OAKSTAR und STORMBREW (ebd.: 153), die mittels Anzapfen von Glasfaserkabeln und anderen Infrastrukturen an die Daten der UserInnen gelangen (ebd.: 160).

Abb. 9: Die strategischen Partner der NSA
(Quelle: Greenwald 2014: 153)

Die Zusammenarbeit zwischen Nachrichtendiensten und privatwirtschaftlichen Unternehmen regelt das sogenannte CALEA Gesetz - *Communications Assistance for Law Enforcement Act of 1994*. Es verpflichtet die Tele- und Internetkommunikationsunternehmen dazu, ihre Systeme (Kommunikationsgeräte, Internetrouter etc.) in einer Weise zu gestalten, dass ihre Netze bei Bedarf überwacht werden können. Das Gesetz veranlasst sogar die Unternehmen, wenn nötig, selbst Abhörgeräte zu installieren und ihre Existenz geheim zu halten. (vgl. Bamford 2008: 210f.)

Datenschützer und Verfassungsrechtler sprechen von einem Verfassungsbruch, die Bundesregierung und der BND verteidigen ihre Arbeit als rechtmäßig und notwendig. Doch die Enthüllungen sprechen eine andere Sprache. Mittels PRISM etwa greift der US-amerikanische Geheimdienst NSA auf die Server diverser US-amerikanischer Unternehmen zu und hat so Einblick in die persönlichen Daten von Userinnen und Usern weltweit.

Das Beunruhigende dabei ist die Tatsache, dass die nationale Gesetzgebung der Staaten kaum Einfluss auf die Einhaltung von Datenschutzregeln hat. Sobald der

Server, über den die Kommunikationsdaten laufen, im Ausland steht, unterliegt er nur mehr der dortigen Gesetzgebung und den dortigen Datenschutzregeln, unabhängig davon aus welchem Land der User oder die Userinnen kommen, die den Internetdienst nutzen.

Die Enthüllungen, die in der britischen (The Guardian), amerikanischen (The Washington Post, The New York Times) und der deutschen Presse (Der Spiegel) veröffentlicht werden, lösen weltweit eine hitzige Diskussion über Überwachung, Speicherung und die Weitergabe von Daten aus.

7 Die Digitale Revolution des 20. Jahrhunderts

Die digitale Revolution, die sich in der zweiten Hälfte des 20. Jahrhunderts vollzog, zählt neben der landwirtschaftlichen und industriellen Revolution zu den bedeutendsten Entwicklungen der neuzeitlichen Geschichte. Sie markiert den Beginn des Informationszeitalters und leitete eine neue Epoche in der gesellschaftlichen Entwicklung ein. In vielerlei Hinsicht hat sie zu einem tiefgreifenden gesellschaftlichen Wandel geführt.

Genauer gesagt handelt es sich bei der (technischen) Revolution um einen Wechsel von analoger, mechanischer und elektronische Technologie zur digitalen Technologie. Diese Entwicklung ist auf einen rasanten technischen Fortschritt in den letzten Jahrzehnten zurückzuführen. Es veränderten sich die Kommunikationsmittel und –wege und mit ihnen die Reichweite von Information. Die Erfindung von digitalen Computern Ende der 1950er Jahre, ihre massenhafte Verbreitung und Nutzung für digitale Datenverarbeitung revolutionierte nicht nur das Kommunikationsverhaltens der Menschen, sie hatte auch gravierende Auswirkungen auf die gewerbliche und private Mediennutzung. So wurden verstärkt Computer im wirtschaftlichen Bereich eingesetzt, bei der Produktion, im Büro etc.

Diese Kommunikationsrevolution vollzog sich hauptsächlich in drei Phasen: Kommunikation über elektromagnetische Wellen (1920-1960), Satellitenkommunikation (1960-1990), Kommunikation über Glasfaserkabel (ab 1990er - heute).

Heute wurde die Kommunikation über elektromagnetische Wellen und die Satellitenkommunikation größtenteils abgelöst von der Kommunikation über Glasfaserkabel. Die Verwendung von komplexeren Informationssystemen (digitalen Handys und Internet) machte den Einsatz von Glasfaserkabeln, die im Boden vergraben wurden, erforderlich.

Als dann Ende der 1980er, Anfang 1990er Jahre die Telekommunikation digitalisiert wurde, stellten die Kommunikationsunternehmen weltweit ihre Netzwerke von Satelliten zu Glasfaserkabeln um.

Mittlerweile findet ein Großteil der weltweiten Kommunikation, der Telefonverkehr miteingeschlossen über durch das Internet bereitgestellte Infrastruktur statt. Im Jahr 2000 lief bereits 80% der weltweiten Kommunikation über Glasfaserkabeln (vgl. Bamford 2008: 175).

Eines der bekanntesten Netzwerke ist das US-amerikanische Qwest, bestehend aus Hardware, Engineering, Communications Services und Network Management. Es ist eines der größten weltweit und erstreckt sich durch die gesamte USA und Europa. (vgl. Bamford 2008: 172f.)

Die Vorteile der Kommunikation über Glasfaserkabeln gegenüber der Mikrowellen- und Satellitenkommunikation sind die geringeren Kosten, die höhere Reliabilität und die schnellere Übertragung (ebd.: 176).

Wie aus den geleakten Geheimdokumenten hervorgeht, greift die NSA sowohl auf Satellitenkommunikation, als auch auf die Kommunikation, die via Glasfaserkabel läuft, zu. Die nachrichtendienstliche Informationsbeschaffung via Satelliten, bei der die Signale, die zwischen den Bodenstationen auf der Erde und den (Kommunikations-) Satelliten im All fließen, in der Luft abgefangen werden, war bis in die späten 1980er Jahre gängige Praxis der NSA. (vgl. Bamford 2001: 458)

Dabei wurden mithilfe von Horchposten, Frühwarnsatelliten, Seismographen etc. Signale empfangen und die sammelten Daten dann in großen Rechenzentren gespeichert. Der codierte Nachrichtenverkehr lief direkt von der Quelle in die wichtigste Dienststelle der NSA – dem *Defense Special Missile and Astronautics Center* (DEFSMAC) und wurde dort analysiert und entschlüsselt. Anhand der Befunde wurde dann eine Art Frühwarnsystem erstellt. (ebd.: 502f., 506)

Der weltweite Wandel im Gebrauch von Technologien stellte den Geheimdienst Ende des 20. Jahrhunderts vor neue Herausforderungen. Die Methoden der Überwachung änderten sich. Die neue Technologie, die die Information via Glasfaserkabel leitete, erschwerte den Zugriff auf Informationen aufgrund technischer und juristischer Hindernisse. So ist Kommunikation, die über mobile Signale (Mobiltelefone) läuft beispielsweise viel schwieriger abzufangen als die, die über analoge Signale geht. Hinzu kommt, dass digitale Signale (Internet, Handys) nicht mehr aus Stimmen,

sondern Datenpäckchen bestehen, die zerlegt und auf unterschiedlichste Weise übermittelt werden können. (vgl. Bamford 2001: 461) Dies machte das Eindringen in die neuen Systeme kostspieliger, schleppender und vom technischen Aufwand her intensiver.

Für das Anzapfen eines Kabels brauchte die NSA nun einen Beschluss des FISA-Gerichts, den sie bei der Überwachung von Satellit-Signalen früher nicht benötigte (vgl. Bamford 2008: 162).

Daher begann die NSA schnell nach anderen Alternativen zu suchen. Sie verstärkte ihre geheime Kooperation mit den Telekommunikationsunternehmen. Die 1980 gegründete Organisation *Security Affairs Support Association (SASA)*, seit 2003 *Intelligence and National Security Alliance (INSA)* ist dient als Verbindung zwischen den privatwirtschaftlichen Unternehmen und dem nachrichtendienstlichen Apparat (vgl. Bamford 2008: 201).

Der wichtigste Kommunikationskanal, den die digitale Revolution hervorgebracht hat, ist zweifellos das Internet – ein globales System von miteinander verbundenen Computernetzen, das diverse Dienstleistungen und Anwendungen umfasst. Die wohl bekannteste ist das sogenannte World Wide Web (WWW), ein über das Internet zugängliches (Informations-) System, das sich aus elektronischen Hypertext-Dokumenten (Webseiten) zusammensetzt.

Es hat unser Leben revolutioniert. Das Web hat einen Raum der Kommunikation und Vernetzung geschaffen, in dem Informationen verbreitet, geschaffen und ausgetauscht werden. Seit den 2000er Jahren gewinnt insbesondere das interaktive Web, das im Allgemeinen unter dem Begriff Web 2.0 bezeichnet wird, zunehmend an Bedeutung. Soziale Netzwerke, Blogs und Foren schaffen eine neue Plattform des Austausches mit einer großen Reichweite.

Diese auf den ersten Blick durchaus positiven Entwicklungen, die das Internet hervorbrachte, täuschen jedoch nicht über die Risiken des Webs hinweg.

Während die einen von unglaublichen Chancen für die Demokratie sprechen und den Untergang des klassischen politischen Systems prognostizieren, warnen andere vor einem Missbrauch des Internets für machtpolitische Zwecke. Sie sehen im Internet

ein Instrument zur Sicherung von Macht und befürchten sogar eine Vergrößerung der Ungleichheit durch das Internet.

Über die Argumente lässt sich streiten. Tatsache ist jedoch, dass die wesentlichen Bestandteile des Internets, also die grundlegenden technischen Komponenten, wie Router, Leitwegprogramme etc. größtenteils von US-amerikanischen Unternehmen, wie Cisco Systems etc. produziert bzw. betrieben werden. Fast der gesamte Internet-Verkehr durchläuft das System des Unternehmens Cisco Systems (vgl. Bamford 2001: 463), was den USA eine enorme Macht verleiht.

Edward Snowden hat uns die Möglichkeiten elektronischer Überwachung vor Augen geführt und uns die Gefahren von Machtmissbrauch im digitalen Zeitalter bewusst gemacht. Vor allem aber hat er auf die gegenwärtigen Machtstrukturen aufmerksam gemacht und die Frage nach dem Machtmonopol im Falle der neuen Medien, insbesondere des Internets, aufgeworfen.

IT-Unternehmen konkurrieren um die Vormachtstellung im digitalen Netzwerk, wobei die Konzentration der Macht in nur wenigen Händen liegt; überwiegend bei US-amerikanischen ISP, wie Google, Yahoo etc. Sie kontrollieren das Internet oder zumindest den Teil des Internets, der für uns UserInnen sichtbar ist, das sogenannte World Wide Web. Es ist ein Irrglaube anzunehmen, das Internet wäre ein *freies Internet*. Tatsächlich ist es eine Ansammlung an bereits selektierten Foren und Inhalten und ist unter der Kontrolle einiger weniger IT-Unternehmen.

Das enorme Machtpotenzial des wichtigsten Kommunikationsmediums des digitalen Zeitalters, führt zu einem Machtkampf im Cyberspace, bei dem es um die Sicherung der Informationsvorherrschaft geht. Es ist ein Kampf um die Hoheitsgewalt über die elektronischen Medien, der gegenwertig zwischen den Nationalstaaten stattfindet.

Fakt ist auch, dass die NSA das Internet zur Überwachung von Kommunikation nutzt. Nachdem wir uns die Funktionsweise der NSA genauer angesehen und ihre Kapazitäten ergründet haben, steht außer Frage, dass die NSA die Fähigkeit besitzt riesige Datenmengen abzufangen und zu speichert. Eine der gängigsten Methoden, um in die Internet- und Glasfaserkabelkommunikation einzudringen, ist ein Angriff auf einen Router (vgl. Bamford 2008: 195).

Die NSA-Affäre hat gezeigt, welche Möglichkeiten der Überwachung im elektronischen Zeitalter existieren. Die Fülle an neuen Kommunikationsträgern hat nicht nur die Kommunikation verändert, sondern auch die Arbeit der Geheimdienste revolutioniert. Das Internet ist zum wichtigsten Medium der Massenkommunikation und gleichzeitig wichtigsten Instrument der Überwachung geworden. Die Verbreitung von Smartphones und die zunehmende Nutzung von digitalen Anwendungen (Applikationen, Android, BlackBerry) die nur über eine Verbindung zum Internet benutzbar sind, haben das Internet zu einem alltäglichen Bestandteil unserer Kommunikation gemacht und die massenhafte Überwachung der Bevölkerung erst ermöglicht. Sie sind zu wichtigen Zielobjekten geworden, denn sie speichern so gut wie alles von ihren NutzerInnen (Fotos, Details über das Nutzungsverhalten/ Aufenthaltsort, Kontakte etc.).

Der Spiegel veröffentlichte am 9.09.2013 ein Dokument, das den Zugriff auf eine BlackBerry-Email beweist (Poitras/ Rosenbach/ Stark 2013: 146).

Mittlerweile ist elektronische Überwachung zum festen Bestandteil strafrechtlicher Verfolgung geworden. Sie wird sowohl in Fällen der nationalen Sicherheit, als auch für gewöhnliche polizeiliche Arbeit verwendet; und wird als solche auch größtenteils widerspruchslos akzeptiert.

7.1 Big Data - Big Business

Ein zentraler Aspekt der digitalen Revolution ist die Digitalisierung von Daten, Informationen und von Kommunikation in Bits und Bytes, eine Entwicklung die in den letzten Jahren explosionsartig fortgeschritten ist und zur Entstehung eines einzigartigen Phänomens geführt hat, das in der öffentlichen Diskussion unter dem Begriff Big Data diskutiert wird. Dabei geht es um das exponentielle Wachstum von elektronischen bzw. digitalen Daten.

Das Oxford English Dictionary definiert *Big Data* als „data of a very large size, typically to the extent that its manipulation and management present significant logistical challenges; (also) the branch of computing involving such data" (OED).

Eines der wichtigsten Wachstumsgebiete für Big Data Anwendungen ist der Bereich *Sicherheit*. Vor allem die Geheimdienste haben das Potenzial von Big Data – einer unversiegbaren Quelle (an Information) – für sich entdeckt und setzen es für ihre Zwecke ein. Die Auswertung und Analyse von Daten ist zu einem zentralen Bestandteil der geheimdienstlichen Arbeit geworden, die mithilfe von Algorithmen konkrete Vorhersagen über menschliches Verhalten machen können.

Big Data hat die nachrichtendienstliche Informationsbeschaffung revolutioniert. Die Menge an bereits vorhandenen zugänglichen Daten hat sich durch die digitale Revolution um ein Vielfaches vergrößert. Diese Entwicklung haben wir vor allem der Entstehung des Internets und seiner massenhaften Verbreitung zu verdanken. Durch die Nutzung von sozialen Netzwerken, Online-Chats, IP-Telefonie, Emails, Online-Banking etc. produzieren wir immer mehr sogenannter Online-Daten, die im virtuellen Gefüge des Internets zu verschwinden scheinen, tatsächlich aber auf Servern, in Clouds etc. gespeichert werden.

Eigens dafür entwickelte Überwachungsprogramme der Geheimdienste saugen diese Online-Daten aus dem riesigen Datenpool und nutzen sie für ihre Zwecke.

Die untere Graphik (Abb. 10) thematisiert die Erzeuger von Big Data – die neuen Technologien der (Massen-) Kommunikation, die seit den 1990er Jahren massenhaft in Betrieb sind und immer mehr neuer Online-Daten produzieren. Es sind vor allem Smartphones und Computer, die über diverse Anwendungen (Internetinfrastrukturen,

Applikationen etc.) Daten von ihren UserInnen beanspruchen. Fakt ist, dass wir es gegenwärtig mit einer bisher nie dagewesenen Menge an Informationen bzw. Daten zu tun haben.

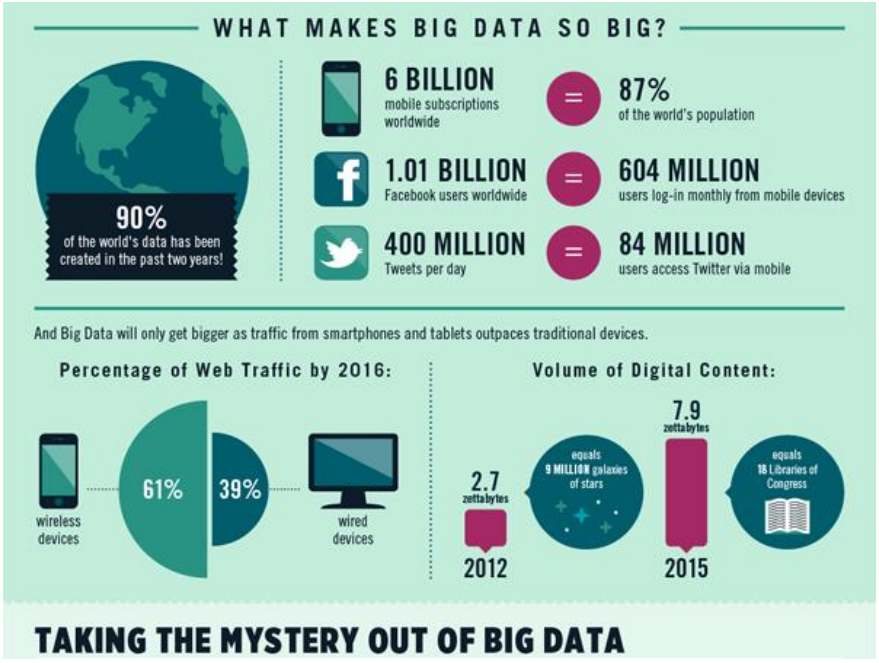

Abb. 10: Was ist Big Data?
(Quelle: Rocheleau, 22.01.2013)

Als wichtigste Mittel (Massen-) Kommunikation haben sie längst Eingang in unseren Alltag gefunden. Laut offizieller Statistik hatten im Jahr 2014 weltweit 43,6 Haushalte Internetzugang (vgl. Statista 2015).

Abbildung 11 zeigt, wie stark die Menge an weltweit verfügbaren Daten in den letzten Jahren angewachsen ist, Tendenz steigend. Während sie 2009 noch 1 Zettabyte betrug, stieg sie 2015 bereits auf fast 8 Zettabyte an. Für das Jahr 2020 wird eine Summe von 30 Zettabyte prognostiziert.

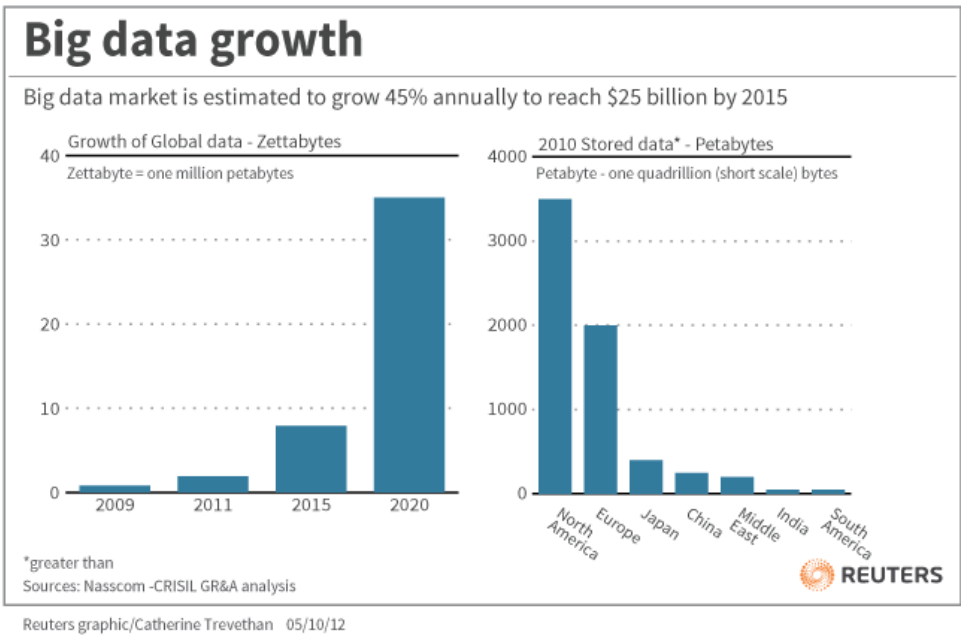

Abb. 11: Das Wachstum von Big Data
(Quelle: Trevethan, 05.10.2012)

Die riesige Menge an Informationen macht den Einsatz von leistungsstarken Computern notwendig. Aufgrund der starken Belastung versucht die NSA möglichste viele abgefangene Informationen bereits am Punkt des Mitschnitts (z.B. an den diversen Horchposten) zu filtern (vgl. Bamford 2001: 457). Hier kommen diverse Analyseinstrumente zur Anwendung, die im System nach Mustern suchen und anhand der Ergebnisse entscheiden, welche Informationen für einen längeren Zeitraum im Computer gespeichert werden.

Die geleakten Dokumente belegen die NSA sammelt weit mehr, als sie verarbeiten kann. „Mitte 2012 bearbeitete die NSA über 20 Milliarden Kommunikationsereignisse (im Internet und per Telefon) auf der ganzen Welt – pro Tag!“ (Greenwald 2014: 148). Auch der britische GCHQ hat ein enormes Sammelvolumen, laut eigenen Angaben erhält er bis zu 50 Milliarden Fälle pro Tag, Tendenz steigend (vgl. ebd.: 150).

Dabei geht es nicht nur um die enorme Datenmenge, die gespeichert wird, sondern in erster Linie auch um die Tatsache, dass eben diese Daten strukturell ausgewertet werden, und zwar sowohl von Geheimdiensten (NSA und GCHQ) als auch von Unternehmen (u.a. von IT- und private Sicherheitsunternehmen) und

WissenschaftlerInnen. Mittels Algorithmen werden Muster im Kommunikationsverhalten der Menschen entdeckt und für kommerzielle, politische und andere Zwecke genutzt. Das ist die wirklich neue Dimension, die es so vorher nie gegeben hat.

Im Rahmen der Enthüllungen ist bekannt geworden, dass sowohl die NSA als auch der GCHQ direkten Zugriff auf Kommunikationsinfrastrukturen (Glasfaserkabeln von US-Unternehmen etc.) und damit auf die persönliche Daten von UserInnen („upstream surveillance“) haben (vgl. Greenwald 2014: 160).

Außerdem können sie offenbar gängige Verschlüsselungssysteme für Online-Datenverkehr ohne Probleme knacken, und zwar mittels diverser Entschlüsselungsprogramme, wie PROJECT BULLRUN, MUSCULAR etc. (ebd.: 142).

„Der heutige Überwachungsapparat ist technologisch und historisch unvergleichbar. Nie zuvor in der Geschichte hatten wir eine ähnlich weitreichende und mächtige Überwachungsstruktur wie jetzt“ (Coleman 2014: 109).

7.2 Fifth Estate – Die Fünfte Macht

Das Konzept der *Fünften Macht* – „Fifth Estate“ (vgl. Dutton, 2007) erlangt im gegenwärtigen digitalen Zeitalter immer mehr an Bedeutung und soll im Folgenden näher erläutert werden.

Als Grundlage soll mir der Ansatz von William H. Dutton, einem anerkannten Professor der Oxford Universität, dienen. In seiner Ausarbeitung *The Fifth Estate emerging through the Network of Netwerks (2007)* beschreibt er das Aufkommen einer neuen Institution im 21. Jahrhundert, die mit der Entwicklung und Verwendung von ICTs zusammenhängt (vgl. Dutton H. 2007: 2).

Das Konzept der *Fünften Macht* erweitert den Begriff der *Vierten Macht*, der in vielen liberalen demokratischen Gesellschaften die klassische Presse (Radio, Fernsehen, Printmedien etc.) beschreibt, um den Aspekt des individuellen Zugangs zu alternativen Informationsquelle, Menschen, Diensten und anderen Quellen. Die Entwicklung von neuen *information and communication technologies (ICTs)*,

insbesondere des Internets, schafft laut Dutton einen neuen Raum der Vernetzung und des Informationsaustausches zwischen Individuen, der es möglich macht, bestehende Institutionen zu umgehen und aufgrund seiner Reichweite (das Erreichen einer großen kritischen Masse an NutzerInnen), eine größere soziale Rechenschaftspflicht der Politik, Presse etc. gegenüber der Öffentlichkeit zu bewirken. (ebd.: 3)

Als Fünfte Macht werden digital vernetzte Individuen verstanden aus den unterschiedlichen Fachbereichen, u.a. Presse, Politik, Wirtschaft etc. (ebd.: 14f.). In unserem Fall sind die sogenannten nicht-professionellen Medienakteure und –aktivistInnen, also Blogger, Informationsplattformen wie Wikileaks, Community Medien etc. von besonderer Relevanz, denn sie schaffen nicht nur eine alternative Presse abseits der bestehenden Institutionen, sondern auch eine kritische alternative Öffentlichkeit. Der Fall Edward Snowden zeigt, wie wichtig diese Instrumente der kritischen Öffentlichkeit für die Allgemeinheit sind, etwa bei der Aufdeckung von Missständen im staatlichen System. Sogenannte *Insider* – Eingeweihte, aus dem System stammende Akteure, und *Whistleblower* – Enthüller, gewinnen in Zeiten intransparenter staatlicher Kontrollmechanismen und einer sich am (politischen) Mainstream orientierenden und zum Teil unkritischen Medienlandschaft, zunehmend an Bedeutung. Sie sind zu einem wesentlichen „Bestandteil des Systems der **Checks und Balances** [Hervorhebung der Verf.]“ (Mühlberg 2013: 46) geworden und damit Garanten der Demokratie. Umso wichtiger ist ihr Rechtsschutz.

Tatsächlich werden Whistleblower gegenwärtig immer noch unter dem *Official Secrets Act (1889)* und dem *Espionage Act (1917)* angeklagt, Tendenz steigend.

Allein während der Präsidentschaft von Barack Obama (2009 – heute) wurden insgesamt 7 Informanten (in der Geschichte Amerikas insgesamt zehn Menschen) nach dem Espionage-Act angeklagt (vgl. York 2013: 117), darunter Bradley Manning Thomas Drake etc. und das obwohl Obama noch zu Beginn seiner Amtszeit ausdrücklich betonte, sich für die Rechte von Whistleblowern und für den Schutz des kritischen Investigativjournalismus einzusetzen, wie folgendes Zitat zeigt:

> Often the best source of information about waste, fraud, and abuse in government is an existing government employee committed to public integrity and willing to speak out. Such acts of courage and patriotism, which can sometimes save lives and often save taxpayer

> dollars, should be encouraged rather than stifled. We need to empower federal employees as watchdogs of wrongdoing and partners in performance. Barack Obama will strengthen whistleblower laws to protect federal workers who expose waste, fraud, and abuse of authority in government. Obama will ensure that federal agencies expedite the process for reviewing whistleblower claims and whistleblowers have full access to courts and due process.
> (The Obama-Biden Plan 2009)

Doch statt die Whistleblower tatsächlich zu schützen, bezeichnet sie die US-Regierung als Landesverräter und bestraft sie unverhältnismäßig. Ein Paradebeispiel dafür ist der Fall von Bradley Manning, der durch die Weitergabe von Geheimdokumenten der US-Army zum Irak an die Enthüllungsplattform Wikileaks traurige Bekanntheit erlangte. Er wurde in den USA wegen Spionage schuldig gesprochen und zu einer lebenslangen Haftstrafe verurteilt, und das obwohl seine Enthüllungen nicht viel mit Spionage zu tun haben.

Sollten der Wikileaks Gründer Julian Assange und Edward Snowden an die USA ausgeliefert werden, würde ihnen höchstwahrscheinlich dasselbe, wie ihrem Vorgänger Manning, bevorstehen.

Die Willkür eines Staates wird insbesondere an seinem Umgang mit Whistleblowern deutlich. Der Fall Edward Snowden und der andere Kritikern offenbart die prekäre Situation von Whistleblowern im heutigen System, auch demokratischer Staaten. Er zeigt eine von Intoleranz geprägte Stimmung gegenüber Systemkritikern.

8 Fazit

8.1 Die Auswirkungen der NSA-Affäre

Edward Snowden hat die Ausspähprogramme der NSA und des GCHQ öffentlich gemacht und eine weltweite Debatte über die Überwachung der weltweiten elektronischen Kommunikation durch die Geheimdienste ausgelöst.

Seine Enthüllungen haben gezeigt, dass die Überwachung der digitalen Kommunikation umfassender und folgenschwerer ist, als bisher angenommen. Zum ersten Mal hat man handfeste, von seriösen Investigativ-JournalistInnen geprüfte Beweise für die massenhafte Überwachung durch die NSA – dem größten und mächtigsten Geheimdienst der Welt.

Die Fakten, die dank Edward Snowden öffentlich gemacht wurden, belegen – es geht um viel mehr als die Überwachung von Terroristen. Im Namen der nationalen Sicherheit werden große Teile der weltweiten Bevölkerung ausspioniert. Jede noch so kleine und scheinbar unwichtige Information wird gesammelt, ausgewertet und für eigene Zwecke gebraucht; ganz nach dem Prinzip je mehr Daten desto besser. Zudem wird politische Spionage und Wirtschaftsspionage im großen Stil betrieben.

Der britische Journalist Glenn Greenwald, der die von Edward Snowden übermittelten Dokumente der NSA aufbereitete und veröffentlichte, spricht von einem komplexen Überwachungssystem mit allumfassenden Anspruch (vgl. Greenwald 2014: 139).

Die geleakten Dokumente enthüllen Überwachungsprogramme, die sich bisher nie dagewesener technischer Mittel bedienen. Sie ermöglichen die Überwachung der Kommunikation auf den unterschiedlichsten Ebenen, je nach dem welcher elektronische Kanal (z.B. Telefon oder Internet) genutzt werden. Angezapft werden so gut wie alle Wege der Kommunikation: Internetserver, Satelliten, Unterseekabel, nationale und internationale Telefonsysteme und private Computer.

Außerdem setzt die NSA bei der Informationsbeschaffung auf strategische Partnerschaften mit anderen Geheimdiensten und die aktive Kooperation mit privaten Internetunternehmen bzw. –dienstleistern, wie Google, Yahoo etc.

Die NSA und der GCHQ überwachen, sammeln und analysieren systematisch einen Großteil der weltweiten Kommunikation (Inhalte und Metadaten), ohne Rechenschaft abzulegen.

Ermöglicht wird die massenhafte Überwachung von Bürgerinnen und Bürgern in erster Linie durch zwei bedeutende Ereignisse in den letzten 20 Jahren – die digitale Revolution in den 1990er Jahren und die Terroranschläge vom 9. September 2001 und die Gesetzesreformen infolgedessen.

Letztere leiten einen neuen Kurs in der Sicherheitspolitik der USA und der europäischer Staaten ein – das Motto: Sicherheit um jeden Preis. Die bestehenden Sicherheitsstrukturen, die wie 9/11 demonstriert deutlich versagt haben, werden weder zur Verantwortung gezogen, noch kritisch hinterfragt.

Stattdessen findet ein *Securitization*-Prozess statt. Die US-Regierung bestimmt den Kampf gegen den internationalen Terrorismus zur Staatsdoktrin und versicherheitlicht damit große Bereiche der Politik. Die Medien schaffen ein öffentliches Bewusstsein.

Die Folge ist eine massive Aufrüstung des Militärs (Rüstungsindustrie) und der Geheimdienste (Sicherheitsindustrie). Die Prioritätensetzung ist klar. Nur wenige Tage nach den Terroranschlägen werden die ersten Anti-Terrorgesetzte erlassen, die Einrichtung eines Ausschusses zur Aufklärung der Terroranschläge hingegen dauert über ein Jahr.

Es werden Gesetzesreformen verabschiedet, die die richterliche Kontrollinstanz bei der Überwachung von telefonischer Kommunikation und Internet-Kommunikation faktisch aufheben. Der von der Bush-Regierung verabschiedete *FISA Amendement Act von 2008* modifiziert das ursprüngliche FISA-Gesetz dahingehend, dass keine richterliche Zustimmung mehr erforderlich ist, um Massenüberwachung zu autorisieren. Damit wird das brüchige System der Checks und Balances endgültig aufgehoben.

Es ist eine Politik, die die Entstehung eines umfassenden Überwachungssystems fördert und somit die demokratische Ordnung gefährdet. Denn Überwachung ohne jeglichen Verdacht ist höchst anti-demokratisch und widerspricht dem rechtsstaatlichen Prinzip. Wir sehen uns mit den Fragen konfrontiert: Was sind wir bereit aufzugeben, um Sicherheit zu bekommen? und Wie weit darf der Staat (bei der Überwachung) gehen, ohne demokratische Grundrechte, wie die informationelle Freiheit und Meinungsäußerung zu gefährden?

Die NSA-Affäre zeigt eindringlich, wie groß die Gefahr von Machtmissbrauch bei unzureichend funktionierenden Kontrollmechanismen ist.

Über die Folgen und Konsequenzen der NSA-Affäre lässt sich viel spekulieren. Vor allem die langfristigen Folgen sind noch kaum abzuschätzen. In diesem Kapitel möchte ich daher in erster Linie die sich bisher abzeichnenden Tendenzen, die als unmittelbare Folge der NSA-Enthüllungen zu sehen sind, beschreiben. Außerdem möchte ich den Versuch unternehmen potentielle langfristige Auswirkungen der NSA-Affäre zu diskutieren.

Die wichtigsten Schlussfolgerungen aus der NSA-Affäre sind meiner Ansicht nach die Folgenden:

Das Internet in seiner jetzigen Form ist weit davon entfernt, ein freier und unabhängiger Kommunikationsraum zu sein. Tatsache ist, dass das für uns sichtbare Cyberspace bereits eine gefilterte Variante des Internets ist und die staatliche Überwachung, die online stattfindet, die Grenzen des Internets aufzeigt.

Die Anti-Terrorpolitik infolge von 9/11 hat die sich bereits seit den 1990er Jahren abzeichnenden Tendenzen in Richtung Massenüberwachung nur noch verstärkt und die Ausbreitung neuer Technologien, diesen Trend beschleunigt.

Die Befürworter staatlicher Überwachung, wie z.B. argumentieren damit, „wer nichts zu verbergen hat, hat auch nichts zu befürchten“ (Biermann 2014: 21). Dies bedeutet jedoch nichts Geringeres, als dass die Suche nach der Nadel im Heuhaufen, die Überwachung der Allgemeinheit rechtfertigt. Die Menschen werden unter Generalverdacht gestellt, und es bedarf nicht einmal mehr eines begründeten

Verdachts oder Gerüchts, um Überwachungsaktivitäten auszuführen. Es wird einfach alles gesammelt, gefiltert und gespeichert. (Biermann 2014: 22)

Die Kritiker argumentieren hingegen, dass die Existenz von solchen Überwachungsmethoden schon ausreichen würde, um Oppositionelle einzuschüchtern; denn wer beobachtet wird, ändert automatisch sein Verhalten.

Außerdem trügt die Argumentation der Befürworter nicht darüber hinweg, dass es einen großen Unterschied macht, ob man freiwillig entscheidet, Informationen über sich weiterzugeben oder ob man dazu gezwungen wird. Das Problem dabei ist, dass das Wissen von den Überwachungsprogrammen langfristig Misstrauen in der Bevölkerung hervorrufen kann. Die Folge wäre die Angst vor einer möglichen Fehlinterpretation bestimmter Kommunikationsinhalte, was wiederrum zu einer vorsichtigeren Artikulation bzw. Selbstzensur führen würde. Zudem besteht bei Speicherung auf Dauer die Gefahr des Missbrauchs durch zukünftige Regierungen (vgl. Hintz 2014: 98f.).

Es ist also ein tiefer Einschnitt in die Privatsphäre der Personen und bedroht die Demokratie in ihren Grundelementen, denn sobald man an einem Grundrecht zu schaben beginnt, gerät das System aus dem Gleichgewicht und bricht irgendwann zusammen.

Beängstigend ist auch die Art und Weise mit welcher Härte gegen Whistleblower vorgegangen wird, also Menschen, die auf Missstände im System (z.B. staatlichen Behörden, privatwirtschaftlichen Unternehmen etc.) hinweisen und dabei ihr eigenes Wohl riskieren. Ihr Handeln im Interesse der Allgemeinheit macht sie zu mächtigen Gegnern des Systems und erfordert daher einen angemessen Schutz.

Das zeigen neben Edward Snowden, auch die Fälle Bradley Manning und Julian Assange. Manning wurde für seine Enthüllungen geheimer Akten der US-Armee zu Vergehen im Irak-Krieg vor das Kriegsgericht gestellt und zu lebenslanger Haft verurteilt. Julian Assange, der unter anderem mehrere tausende klassifizierte Dokumente der US-Regierung auf der Enthüllungsplattform Wikileaks veröffentlicht hat, versteckt sich bis heute vor den US-Behörden und einem von der US-Regierung initiierten internationalen Haftbefehl in der ecuadorianischen Botschaft in London.

Die Obama Administration geht unerbittlich gegen Whistleblower vor. Unter Obama wurden bisher die meisten Whistleblower, insgesamt 7 verurteilt; mehr als unter allen bisherigen US-Regierungen. Das ist sehr beunruhigend und ein Armutszeugnis für die Demokratie.

Die NSA-Affäre hat eine Reihe unterschiedlicher Reaktionen hervorgerufen. Neben zahlreichen Reaktionen auf staatlicher Ebene, kam auch viel Resonanz aus der Zivilgesellschaft. Im Großen und Ganzem kann man sagen, dass die Enthüllungen von Edward Snowden eine breite Debatte zum Thema staatliche Überwachung und zum Schutz der Privatsphäre ausgelöst haben, eine Debatte, die im elektronischen Zeitalter längst überfällig ist.

Die Gefahr des Machtmissbrauchs ist allgegenwärtig und die Existenz von funktionierenden Kontrollmechanismen (internationalen Abkommen bzw. Gesetzen) umso notwendiger.

Der Abhörskandal ist bisher weder politisch noch rechtlich aufgearbeitet worden. Die fehlende Aufarbeitung auf politischer Ebene hängt unter anderem mit der Vormachtstellung der USA im internationalen System zusammen und der sich daraus ergebenden politischen Abhängigkeiten. Auf der gesellschaftlichen Ebene ist man vor allem konfrontiert mit der Abstraktheit und Nicht-Fassbarkeit der Enthüllungen bzw. fehlendem technischem Wissen, um die konkreten Folgen für jede/n Einzelne/n BürgerIn ermessen zu können. Es besteht also ein großer Aufklärungsbedarf in der Öffentlichkeit im Hinblick auf die Risiken digitaler Kommunikation.

8.2 Die neue Dimension der Überwachung

Die Analyse des Status Quo der NSA-Überwachungskapazitäten unter Berücksichtigung der geschichtlichen Entwicklungen, lässt mich zu der Schlussfolgerung kommen: Wir haben es tatsächlich mit einer neuen Dimension (staatlicher) Überwachung zu tun.

Staatliche (nachrichtendienstliche) Überwachung ist an sich nichts Neues. Neu ist jedoch das Ausmaß staatlicher Überwachung, das gegenwärtig existiert und sich aufgrund des technischen Fortschritts, immer weiter ausdehnt. Die digitale Revolution des 20. Jahrhunderts hat dazu einen wesentlichen Beitrag geleistet. Mit der Digitalisierung von Daten, Information und Kommunikation hat eine Verschiebung der alltäglichen Kommunikation in den digitalen Raum stattgefunden.

Mit den Enthüllungen von Edward Snowden wurde diese Problematik erstmals einer breiten Öffentlichkeit ins Bewusstsein gerufen. Der heutige Überwachungsapparat ist mit nichts in der Historie vergleichbar, er ist in politischer, technischer und ökonomischer Hinsicht allen früheren (Infra-) Strukturen deutlich überlegen.

Im Zeitalter des Internets und anderer Medien der Massenkommunikation (Telefone, Handys, Notebooks und PCs) sind die Möglichkeiten des Zugriffs auf Informationen schier unendlich. Die modernen elektronischen Medien, denen wir uns Tag täglich bedienen, erleichtern nicht nur die Kommunikation und Vernetzung, sie bärgen auch neue Gefahren und Risiken. Insbesondere die Gefahr des Missbrauchs solcher Techniken macht sie äußerst gefährlich.

Ein großes Problem ist die zunehmende Verbreitung persönlicher Informationen in Form von Daten mittels diverser elektronischer Medien, z.B. Online-Bankgeschäfte, Emails, Online-Chats und Kommunikation in Sozialen Netzwerken etc. Zu den analogen Daten (offline-Daten) eines/r jeden Bürgers/in kommen die elektronischen Daten (online-Daten) hinzu. Unser Leben spielt sich immer mehr in der digitalen Welt ab – eine Entwicklung, die in Anbetracht der Enthüllungen von Edward Snowden, zu Bedenken gibt. Denn als UserInnen dieser besagten Medien vergrößern wir unsere persönliche Angriffsfläche, indem wir unsere persönlichen Daten online stellen, also

aus dem offline-Bereich herausnehmen und damit sichtbar machen, und zwar auf einem Kanal, welcher für verschiedene Akteure zugänglich ist.

Neben der Überwachung von AusländerInnnen, wird auch das bewusste und unbewusste Ausspähen von US-BürgerInnen mit dem technischen Fortschritt immer wahrscheinlicher.

Die NSA-Affäre mit all ihren Implikationen zeigt sehr anschaulich wie sich der Staat die Informationen auf diesen Kanälen zu nutzen macht. Die Überwachungsprogramme, mit denen der größte Nachrichtendienst der Welt – die NSA – arbeitet, setzten die verschiedenen Medien der Massenkommunikation zur Überwachung ein. Das formulierte Ziel ist es alle verfügbaren Kommunikationsdaten einer beliebigen Person, zu jeder Zeit sammeln und speichern zu können.

Der Geheimdienst agiert in einem breiten Akteursnetzwerk, das sich aus (Partner-) Geheimdiensten, privatwirtschaftlichen Unternehmen, nationalen Sicherheitsbehörden etc. zusammensetzt. Das Verhältnis ist geprägt von einem regen Kommunikations- und Informationsaustausch, der sich infolge des technischen Fortschritts intensiviert hat.

8.3 Konsequenzen aus der NSA-Affäre

Die Frage nach einem angemessenen Umgang mit der NSA-Affäre ist essentiell und soll im Folgenden kurz beleuchtet werden.

Meine Untersuchungsergebnisse lassen mich zu der Schlussfolgerung kommen, dass wir es derzeit mit einer sehr gefährlichen Situation zu tun haben, die sich einerseits aus der Verletzung von Gesetzen seitens der Gesetzgeber und andererseits aus einem unzureichenden Rechtsschutz für Leute, die auf Verstöße des staatlichen Systems aufmerksam machen, ergibt. Hinzu kommen die nur sehr unzureichenden Gesetze zur Verteidigung bürgerlicher Freiheiten vor (Massen-) Überwachungen.

In Anbetracht dessen sind in erster Linie eine vollständige Aufklärung der Sachverhalte und eine rechtliche und politische Aufarbeitung notwendig. Beides ist bisher nur unzureichend geschehen. Wenn man sich die Reaktionen auf die Affäre ansieht, so muss man ernüchternd feststellen, dass Konsequenzen auf der politischen und rechtlichen Ebene weitgehend ausgeblieben sind.

Notwendig wäre meiner Ansicht nach zu allererst eine umfangreiche Untersuchung aller gegen die NSA erhobenen Vorwürfe und die Bestimmung der juristischen Verantwortlichkeit von allen involvierten Personen und Institutionen. Derzeit kann von einer solchen Aufklärung seitens der staatlichen Akteure, nicht die Rede sein. Die Befragung der Geheimdienstchefs der NSA, des GCHQ und des BND in den jeweiligen nationalen parlamentarischen Kontrollgremien, ohne weitreichende Konsequenzen ist alles andere als ausreichend und zufriedenstellend.

Im zweiten Schritt sollte dann die Überprüfung und gegebenenfalls das Aussetzten bestehender Überwachungsprogramme und internationaler Abkommen kommen, die Überwachung auf der globalen Ebene erst ermöglichen.

Die Überwachungsprogramme der NSA, die durch Edward Snowden an die Öffentlichkeit gelangt sind und klar gegen sämtliche Gesetze verstoßen, sollten umgehend stillgelegt werden. Analog sollte man über die Aufhebung oder zumindest die Beschränkung des *Safe-Harbor Abkommens (2000)*, das zu einem beträchtlichen

Teil für die Weitergabe von persönlichen Daten europäischer BürgerInnen an die USA verantwortlich ist. Genauer gesagt ermöglicht es europäischen Unternehmen personenbezogene Daten legal in die USA zu übermitteln und entkräftet damit faktisch das europäische Datenschutzrecht.

Auf der bilateralen Ebene sollte man im Falle Deutschlands, wenn schon kein No-Spy-Abkommen erreicht werden konnte, dann doch zumindest die Aufhebung des NATO-Truppenstatut Zusatzabkommens, der die Zusammenarbeit der Geheimdienste beider Staaten bestimmt, in Erwägung ziehen. Dies wäre jedenfalls ein klares Zeichen in Richtung Washington, dass Überwachung von Partnern nicht einfach hingenommen wird.

Auch auf der zivilgesellschaftlichen Ebene sollte man Konsequenzen aus der Affäre ziehen und aktiv gegen die Überwachung unserer Kommunikation vorgehen. Die Verwendung von Verschlüsselungsprogrammen scheint zumindest im Moment die schnellste und effektivste Lösung zu sein, um sich selbst vor Angriffen auf die eigene Kommunikation zu schützen.

Auf langfristige Sicht wäre es meiner Meinung nach zielführend, eine breite öffentliche Debatte über einen verantwortungsvollen Umgang mit Privatsphäre im elektronischen Zeitalter zu führen. So sollte man u.a. über effektive Kontrollmechanismen diskutieren, die z.B. in Form von verbindlichen internationalen Vereinbarungen ausgehandelt werden könnten. Dabei sollten engere Grenzen zur Beschränkung der staatlichen Macht (Geheimdienste etc.) diskutiert werden, zur Eindämmung eines unkontrollierten staatlichen Gewaltmonopols. Transparenz muss hierbei an erster Stelle stehen.

Das 2008 vom Bundesverfassungsgericht verabschiedete IT-Grundrecht, das die Integrität und Vertraulichkeit informationstechnischer Systeme sichern soll, ist ein Schritt in die richtige Richtung. Es beruft sich auf das Recht auf informationelle Selbstbestimmung, das 1983 verabschiedet wurde und den geheimen Zugang zu informationstechnischen Systemen für verfassungswidrig erklärt.

Ein interessanter Ansatz ist auch der Vorschlag diverser Bürgerrechtsvereinigungen, die 13 internationale Grundsätze zur Gewährleistung von Menschenrechten in der

Überwachung von Kommunikation formuliert haben, wie den Grundsatz LEGALITY, ADEQUACY und COMPETENT JUDICIAL AUTHORITY etc. (International Principles on the Application of Human Rights to Communications Surveillance 2014)

Viele Kritiker, wie Georg C.F. Greve, Mitgründer der Free Software Foundation Europe, fordern eine freie bzw. offene Software, die unabhängig ist von Unternehmen und dem Gemeinwohl dient. Sie weisen insbesondere auf die Problematik hin, dass viele IT- (Internet) Unternehmen von Think Tanks finanziert werden, die ihre (politischen) Interessen auch im Netz durchzusetzen versuchen und damit ihre politische Macht festigen (vgl. Greve 2014: 30).

Wie die Enthüllungen von Edward Snowden belegen, hat sich das Internet, das anfangs als Meilenstein der Demokratie galt, zur größten Plattform für Überwachung entwickelt.

Die Vorstellung einer freien Software mag zwar utopisch sein, ist tatsächlich aber gar nicht so abwegig. Diskutiert werden verschiedene Formen der Umsetzung. So spricht beispielsweise Annette Mühlberg, die Leitetin des Referats eGovernment, Neue Medien, Verwaltungsmodernisierung beim ver.di Bundesvorstand in Deutschland von der Möglichkeit regionale Hosting- und Routingdienste aufzubauen, mithilfe von Partnerschaften aus Politik, Wirtschaft etc. (vgl. Mühlberg 2013: 43fff.)

Der Kampf für ein unabhängiges und freies Internet wird zu den zentralen Streitfragen der Zukunft gehören.

9 Nachwort

The greatest fear that I have regarding the outcome for America of these disclosures is that nothing will change. People will see in the media all of these disclosures. They'll know the lengths that the government is going to grant themselves powers unilaterally to create greater control over American society and global society. But they won't be willing to take the risks necessary to stand up and fight to change things to force their representatives to actually take a stand in their interests. (Gallagher 2013: 10:47-11:31)

10 Bibliographie

Monographien

Bamford, James (2001): NSA. Die Anatomie des mächtigsten Geheimdienstes der Welt. München: C. Bertelsmann Verlag.

Bamford, James (2008): The Shadow Factory. The Ultra-Secret NSA from 9/11 to the Eavesdropping on America. New York: Anchor Books, A Division of Random House, Inc.; Toronto: Random House of Canada Limited.

Buzan, Barry; Wæver, Ole (2003): Regions and powers. The Structure of International Security. Cambridge (u.a.): Cambridge University Press.

Buzan, Barry; Wæver, Ole; de Wilde, Jaap (1998): Security: A New Framework for Analysis. Boulder; London: Lynne Rienner Publi shers, Inc.

Gu, Xuewu (2010): Theorien der internationalen Beziehungen. München: Oldenbourg Wissenschaftsverlag GmbH.

Greenwald, Glenn (2014): Die globale Überwachung. Der Fall Edward Snowden, die amerikanischen Geheimdienste und die Folgen. München: Droemer Verlag.

Hobbes, Thomas (1651): Leviathan or The Matter, Forme and Power of a Common Wealth Ecclesiasticall and Civil. London: Printed for Andrew Crooke.

Jørgensen, Knud Erik (2010): International Relations Theory. A New Introduction. London: Palgrave Macmillan.

Landau, Susan (2010): Surveillance or Security? The Risks Posed by New Wiretapping Technologies. Cambridge; London: The MIT Press.

Locke, John (1998). Zwei Abhandlungen über die Regierung. Suhrkamp, Frankfurt/a.M. S. 277-281. [englische Version des Textes Locke, John (1997). Two Treatises of Government. Cambridge UP, Cambridge. p. 349-53]

Mattelart, Armand (2010): The Globalization of Surveillance. The Origin of the Securitization Order. Paris; Malden; Cambridge: Polity Press.

Morgenthau, Hans (1948): Politics Among Nations: The Struggle for Power and Peace. New York: Knopf.

Münkler, Herfried (2002): Die neuen Kriege. Lizenzausgabe. Bonn: Bundeszentrale für Politische Bildung.

Münkler, Herfried (2004): Die neuen Kriege. Reinbek bei Hamburg: Rowohlt-Taschenbuch-Verl.

Rosenbach, Marcel; Stark, Holger (2014): Der NSA-Komplex. Edward Snowden und der Weg in die totale Überwachung. München: Deutsche Verlags-Anstalt; Hamburg: SPIEGEL-Verlag.

Schieder, Siegfried; Spindler, Manuela (2003): Theorien der Internationalen Beziehungen. Opladen: Leske+Budrich.

Smith, Adam (1776): An Inquiry into the Nature and Cause of the Wealth of Nations. London: W. Strahan and T. Cadell.

Terry, Col. James P. (2013): The War on Terror: The Legal Dimension. Lanham (u.a.): Rowman & Littlefield Publishers, Inc.

Treverton, Gregory F. (2009): Intelligence for an Age of Terror. Cambridge (u.a.): Cambridge Univ. Press.

Waltz, Kenneth (1979): Theory of International Politics. New York: McGraw-Hill.

Aufsätze, Beiträge in Sammelbänden:

Hansen, Lene; Nissenbaum, Helen (2009): Digital Disaster, Cyber Security, and the Copenhagen School. In: International Studies Quarterly, Jg. 53, Nr. 4, 1155-1175.

Heumann, Stefan; Scott, Ben (2013): Rechtsrahmen für geheimdienstliche Überwachung im Internet: USA, Großbritannien und Deutschland im Vergleich. In: Beckedahl, Markus; Meister, Andre (Hrsg.): Überwachtes Netz. Edward Snowden und der größte Überwachungsskandal der Geschichte. Berlin: newthinking communications, S.149-171.

Mühlberg, Annette (2013): Der Ausspähskandal – Weckruf für die Demokratie. In: Beckedahl, Markus; Meister, Andre (Hrsg.): Überwachtes Netz. Edward Snowden und der größte Überwachungsskandal der Geschichte. Berlin: newthinking communications, S.37-46.

Schaar, Peter (2013): Welche Konsequenzen haben PRISM und Tempora für den Datenschutz in Deutschland und Europa? In: Beckedahl, Markus; Meister, Andre (Hrsg.): Überwachtes Netz. Edward Snowden und der größte Überwachungsskandal der Geschichte. Berlin: newthinking communications, S.118-127.

Walt, Stephen M. (2012): The Renaissance of Security Studies. In: International Studies Quarterly, Jg. 35, Nr. 2, 211-239.

Whitehead John W.; Aden, Steven H. (2002): “Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA Patriot Act and the Justice Department's Anti-Terrorism Initiatives.” American University Law Review 51, No.6, 1081-1133.

Artikel aus Zeitschriften:

Gebauer, Mathias (u.a.) (2013): Tricks und Finten. Sieben Wochen nach Beginn der Spähaffäre bricht die Regierung ihr Schweigen. Kanzleramtsminister Ronald Pofalla soll das Thema im Wahlkampf neutralisieren. Doch die wirklich heiklen Fragen kann auch er nicht beantworten. In: Der Spiegel (2013), Nr. 31, 20-22.

Poitras, Laura; Rosenbach, Marcel; Stark, Holger (2013): Shrimps aus Griesheim. Deutschland ist für die NSA Partner und Angriffsziel zugleich, wie eine Aufgabenliste der amerikanischen Aufklärung zeigt. Von Hessen aus operiert der Nachrichtendienst mit dem Schnüffelwerkzeug XKeyscore – die Ergebnisse werden dem US-Präsidenten vorgetragen. In: Der Spiegel (2013), Nr. 33, 23-25.

Pfister, René (u.a.) (2013): Der fleißige Partner. Die NSA-Affäre rückt an die Kanzlerin heran. Angela Merkel will erst aus der Presse von der Abhörmanie der US-Regierung erfahren haben – dabei nutzen deutsche Geheimdienste eines der ergiebigsten NSA-Schlüsselwerkzeuge selbst. In: Der Spiegel (2013), Nr. 30, 16-21.

Poitras, Laura (u.a.) (2013): Angriff aus Amerika. Geheimdokumente zeigen, wie umfassend die USA in Deutschland und Europa spionieren. Jeden Monat überwacht die NSA dabei eine halbe Milliarde Kommunikationsvorgänge, EU-Gebäude werden verwanzt. Die Affäre bedroht die diplomatischen Beziehungen. In: Der Spiegel (2013), Nr. 27, 76-82.

Poitras, Laura; Rosenbach, Marcel; Stark, Holger (2013): iSpy. In: Der Spiegel (2013), Nr. 37,144-147.

Stock, Jonathan (2013): Thomas Drake galt als loyaler Mitarbeiter der National Security Agency, des weltgrößten Geheimdienstes. Dann fand er heraus, dass sein Arbeitgeber US-Bürger ausspionierte, und wurde zum Staatsfeind. In: Der Spiegel (2013), Nr. 20, 50-56.

Hochschulschriften:

Gehl, Oxana (2009): Essay zu der Ring-Vorlesung: Sozialwissenschaften und gesellschaftlicher Wandel – aktuelle Debatten (STEP I), WS 2008/09. Hausarbeit, Universität Wien.

Amtliche Quellen:

<u>Nationale Sicherheitsstrategien</u>

Cyber-Sicherheitsstrategie für Deutschland, Februar 2011. Bundesministerium des Innern (BMI). [online] Verfügbar unter: <http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf;jsessionid=3F70440A7E10B4B609BC005942A0A41F.2_cid364?__blob=publicationFile> [Zugriff: 13.04.15].

NSA/CSS Strategy, Juni 2010. [online] Verfügbar unter: <https://www.nsa.gov/about/_files/nsacss_strategy.pdf> [Zugriff: 13.04.15].

The National Security Strategy of the United States of America, September 2002. The White House Washington. [online] Verfügbar unter: <http://www.state.gov/documents/organization/63562.pdf> [Zugriff: 13.04.15].

EU Dokumente

A Secure Europe in a Better World: European Security Strategy (ESS), 12.December 2003. Council of the European Union. [online] Verfügbar unter: <https://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf > [Zugriff: 13.04.15].

Bericht über die Umsetzung der Europäischen Sicherheitsstrategie, 11. Dezember 2008. Council of the European Union. [online] Verfügbar unter: <http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/de/reports/104634.pdf> [Zugriff: 13.04.15].

The European Union Counter-Terrorism Strategy, 30. November 2005. 14469/4/05 REV 4. Council of the European Union [online] Verfügbar unter: <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST+14469+2005+REV+4> [Zugriff: 13.04.15].

Nationale Rechtsvorschriften

Communications Act of 1934, 19.06.1934. Public Law 73-416, 73 rd Congress. [online] Verfügbar unter: <http://transition.fcc.gov/Reports/1934new.pdf / http://www.legisworks.org/congress/73/publaw-416.pdf> [Zugriff: 13.04.15].

Foreign Intelligence Surveillance Act of 1978 (FISA), 25.10.1978. Public Law 95-511, 95th Congress. [online] Verfügbar unter: <http://legcounsel.house.gov/Comps/Foreign%20Intelligence%20Surveillance%20Act%20Of%201978.pdf> [Zugriff: 13.04.15].

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FAA), 10.07.2008. Public Law 110-261, 110th Congress. [online] Verfügbar unter: <http://www.gpo.gov/fdsys/pkg/STATUTE-122/pdf/STATUTE-122-Pg2436.pdf / http://www.gpo.gov/fdsys/pkg/BILLS-110hr6304pcs/pdf/BILLS-110hr6304pcs.pdf > [Zugriff: 13.04.15].

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA-PATRIOT-ACT) of 2001, 26.10.2001. Public Law 107-54, 110th Congress. [online] Verfügbar unter: <www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf /

http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf> [Zugriff: 13.04.15].

United States Foreign Intelligence Surveillance Court, Secondary Order (2013): In Re Application of the Federal Bureau of Investigation for an order requiring the production of tangible things from Verizon Business Network Services, Inc. on behalf of MCI Communication Services, Inc. D/B/A Verizon Business Services. [pdf] Washington, D.C. Verfügbar unter: <https://s3.amazonaws.com/s3.documentcloud.org/documents/709012/verizon.pdf > [Zugriff: 13.04.15].

UN Resolutionen

S.C. Res. 1368 (2001)
S.C. Res. 1373 (2001)

Online-Quellen:

Carroll, Rory (2013): NSA director Keith Alexander defends surveillance tactics in speech to hackers. *The Guardian*. [online] 31.07.13. Verfügbar unter: <http://www.theguardian.com/world/2013/jul/31/nsa-keith-alexander-black-hat-surveillance> [Zugriff: 13.04.15].

Chane.Gov. The Office of the President-Elect (2009): The Obama-Biden Plan. [online] Verfügbar unter: <http://change.gov/agenda/ethics_agenda/> [Zugriff: 13.04.15].

Greenwald, Glenn; MacAskill, Ewen (2013): NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. [online] 07.06.13. Verfügbar unter: < http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> [Zugriff: 13.04.15].

MacAskill, Ewen (u.a.) (2013): GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian*. [online] 21.06.13. Verfügbar unter: <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> [Zugriff: 13.04.15].

International Principles on the Application of Human Rights to Communications Surveillance (2014) [online] Verfügbar unter: <https://necessaryandproportionate.org/> [Zugriff: 13.04.15].

Oxford English Dictionary (OED): Big Data. [online] Verfügbar unter: <http://www.oed.com/view/Entry/18833> [Zugriff: 13.04.15].

Rocheleau, Jake (2013): Top 10 Internet & Tech-Related Infographics from 2012. *SpyreStudios*. [online] 22.01.13. Verfügbar unter: <http://spyrestudios.com/top-10-internet-tech-related-infographics-from-2012/> [Zugriff: 13.04.15].

Schubert, Klaus; Klein, Martina: Das Politiklexikon. 5., aktual. Aufl. Bonn: Dietz 2011. *bpb* [online] Verfügbar unter: <http://www.bpb.de/nachschlagen/lexika/politiklexikon/17794/liberalismus> [Zugriff: 13.04.15].

Siebert, Horst (o.J.): Sozialkonstruktivismus. Gesellschaft als Konstruktion. [online] Verfügbar unter: <http://studienseminar.rlp.de/fileadmin/user_upload/studienseminar.rlp.de/bb-nr/fl-grafik/Sozialwissenschaften/Sozialkonstruktivismus-HorstSiebert.pdf> [Zugriff: 13.04.15].

Statista (2015): Anteil der Haushalte weltweit mit Internetzugang von 2002 bis 2014. [online] Verfügbar unter: <http://de.statista.com/statistik/daten/studie/187116/umfrage/anteil-der-haushalte-mit-internetzugang/> [Zugriff: 13.04.15].

The Guardian (2013): NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. [online] 6.06.13. Verfügbar unter: <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> [Zugriff: 13.04.15].

Trevethan, Catherine (2012): The Knowledge Effect. *Reuters graphic. Thomson Reuters Blog*. [online]. Verfügbar unter: <http://blog.thomsonreuters.com/index.php/big-data-graphic-of-the-day/> [Zugriff: 13.04.15].

U.S. Department of Homeland Security (2014): Official website of the Department of Homeland Security. [online] Verfügbar unter: <http://www.dhs.gov/about-dhs> [Zugriff: 13.04.15].

Videos:

Gallagher, Kevin M. (2013): NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things'. [YouTube-Video]. 09.06.2013. Verfügbar unter: <https://www.youtube.com/watch?v=5yB3n9fu-rM> [Zugriff: 13.04.15].

Wyden, Ron (2013): DNI Clapper tells Wyden the NSA does not collect data on millions of Americans. [YouTube-Video]. 12.03.2013. Verfügbar unter: <https://www.youtube.com/watch?v=QwiUVUJmGjs> [Zugriff: 13.04.15].

Abstract

The following master thesis represents a comprehensive investigation into the Leaks of Edward Snowden, which became known as the NSA surveillance scandal. The thesis focuses on the question: “Does the current NSA surveillance-apparatus constitute a new dimension of surveillance?” Two main aspects are discussed as the key elements which led to the establishment of the status quo: the digital revolution (laying the technical groundwork) and the post-9/11 policy (creating the legal framework conditions for mass surveillance). By investing massively in the security infrastructure (especially in the intelligence services) in the aftermath of 9/11, the US-government shaped a new broad security-apparatus. Its existence is proved by the secret documents of the National Security Agency (NSA) which reveal the comprehensive surveillance programs of the Agency. The main conclusion of my analysis is that the security-system in its current form is historically unique and represents a new dimension of surveillance.

Die vorliegende Master-Arbeit ist eine umfassende Untersuchung der Enthüllungen von Edward Snowden, bekannt geworden unter dem Begriff NSA-Affäre. Die Analyse konzentriert sich auf die Frage: „Kann man im Falle des gegenwärtigen Überwachungssystems der NSA von einer neuen Dimension der Überwachung sprechen?“ Zwei (Haupt-) Aspekte werden als Schlüsselfaktoren diskutiert, die zur Etablierung des Status Quo der NSA geführt haben: die digitale Revolution, die die technischen Grundlagen legte, und die Anti-Terrorpolitik nach 9/11, die die rechtlichen Rahmenbedingungen für die Massenüberwachung schuf. Die massiven Investitionen der US-Regierung in die Sicherheitsinfrastruktur (insbesondere in die Geheimdienste) nach den Terroranschlägen vom 11. September 2001, führten zu der Errichtung eines neuen umfassenden Sicherheitsapparates. Das belegen die Geheimdokumente der National Security Agency (NSA), die die umfassenden Überwachungsprogrammen des Geheimdienstes enthüllen. Die wichtigste Schlussfolgerung meiner Analyse ist, dass das Sicherheitssystem in seiner jetzigen Form historisch einzigartig ist und eine neue Dimension von Überwachung darstellt.

Lebenslauf

Oxana Gehl

Neugrabener Allee 35
21147 Hamburg
Germany
Tel: +49-176-5756 0128
Email: gehl.oxana@gmail.com

Ausbildung

10/2011 – 01/2015	**Universität Wien, Wien, Österreich** Politikwissenschaft, Master of Arts Master-These: Die NSA-Affäre 2013 – Die neue Dimension der Überwachung Studienschwerpunkte: Internationale Politik und Entwicklung: Friedens- und Konfliktforschung, Internationales Völkerrecht, Demokratisierung; Kultur und Politik: Erinnerungspolitik, Politische Symbolik
02/2013 – 06/2013	**Université de Genève, Genf, Schweiz** Erasmus Austausch-Semester
10/2008 – 06/2011	**Universität Wien, Wien, Österreich** Politikwissenschaft, Bachelor of Arts (Abschlussnote: 1.8) Bachelor-These: Gewalt in Mexiko – Eine Studie zu dem Phänomen nicht-häuslicher Gewalt gegen Frauen in Ciudad Juárez, Chihuahua unter Betrachtung der Rolle des mexikanischen Staatsapparates Studienschwerpunkte: Internationale Politik: Sicherheit, Globalisierung, Menschenrechte, EU; Osteuropastudien: Post-Sowietische Ära – Transformation Erweiterungscurricula: Internationale Entwicklung, Psychologie, Philosophie
09/1999 – 06/2008	**Friedrich-Ebert-Gymnasium, Hamburg, Deutschland**

Berufserfahrung

04/2013 – 07/2013	**OHCHR, Vereinte Nationen, Genf** Fachbereich: Europa und Zentralasien Länderreferentin für 5 europäische Länder
seit 04/2014	**Cinnamon GmbH, Hamburg** Eventplannung- und Koordination

seit 04/2014	**Universität Hamburg Marketing GmbH, Hamburg** Projektbetreuung
10/2013	**Viennafair 2013, Wien** Galerie Andreas Binder Organisation und Consulting
04/2012 – 01/2013	**CGK Communication Group/ Media&Mehr/ Styria Multi Media AG & Co KG, Wien** Eventplanung- und Koordination Organisation
07/2009 – 09/2009	**Persönliche Assistenz der GAL Bürgerschaftsfraktions-Abgeordneten Nebahat Güclü** Fachbereich Soziales, Migration und Frauen
10/2008 – 05/2012	**Privater Sprachunterricht** in Deutsch und Russisch
05/2007 – 08/2008	**HSH Nordbankarena, Hamburg** Gästebetreuung und Service
01/2005 – 02/2005	**DER Reisebüro, Hamburg** Kundenbetreuung, Telefonistin

Zusätzliche Studien

08/2012	**IS Institut International de Langue, Aix-en-Provence, Frankreich** Französisch Intentivkurs, Diploma A2 - Level
02/2012	**Bildungsreise nach New York/ Washington D.C.**, organisiert vom Institut für Politikwissenschaft der Universität Wien, Österreich
12/2011	**Model UN Sicherheitsrat zur Palästina-Frage**, UN Wien, Österreich
06/2011 – 08/2011	**Escuela Mediterráneo, Barcelona, Spanien** Spanisch Sprach- und Kulturkurs, Mittleres Niveau
01/2011	**Model UNIDO "Delivering as One"** am Beispiel von Mosambik, UN Wien, Österreich

Persönliche Daten

Geburtsdatum	20.09.1988
Geburtsort	St. Petersburg, Russland
Sprachen	Englisch, Deutsch, Russisch, Spanisch, Französisch
Familienstand	ledig

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides Statt, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe.

Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Wien, am 17.04.15

(Oxana Gehl)