Geheimdienstliche Telekommunikationsüberwachung als Mittel sozialer Kontrolle

NSA, GCHQ und BND in der Disziplinar- und Sicherheitsgesellschaft

Schriftliche Arbeit zur Erlangung des Akademischen Grades
Magister Artium
im Studiengang Politikwissenschaft an der
Eberhard Karls Universität Tübingen

eingereicht im Sommersemester 2016

Erstgutachter: Dr. Rolf Frankenberger
Institut für Politikwissenschaft, Eberhard Karls Universität Tübingen

Zweitgutachter: Prof. Dr. Daniel Buhr
Institut für Politikwissenschaft, Eberhard Karls Universität Tübingen

Die vorliegende Arbeit wurde in möglichst gendergerechter Schreibweise verfasst. Um eine bessere Lesbarkeit zu gewährleisten wurde auf das Gendern von Pronomen verzichtet und stattdessen (vor gegenderten Begriffen) die weibliche Schreibweise verwendet.

Inhaltsverzeichnis

1 Einleitung

Wenn Sie ihre Freund_innen und Verwandten per E-Mail zu Ihrem Geburtstag einladen, wird dies überwacht. Schreiben Sie darin umgangssprachlich, dass die Party „bombe“ wird, kann dies schon ausreichen, dass sich geheimdienstliche Überwachungsprogramme genauer mit dieser E-Mail beschäftigen. Haben Sie, eine Ihrer Freund_innen oder Verwandten, einen Migrationshintergrund oder Kontakt zum Islam - in welcher Form auch immer - kann dies schnell zu einem Terrorismusverdacht führen.

Streamen Sie Abends einen Film über das Internet, kaufen irgendwelche Dinge, die Sie dringend oder eigentlich gar nicht benötigen, wird dies registriert. Telefonieren Sie mit Ihrem Kind, wird auch das erfasst. Schreiben Sie Ihren Liebsten private oder intime SMS-Nachrichten, landen auch diese in den Datenbanken der Geheimdienste. Tauschen Sie sich mit Kolleg_innen per Skype aus und besprechen dabei wichtige Details eines anstehenden Projekts, wird auch dieses Videotelefonat überwacht. Lesen Sie die vorliegende Arbeit oder tauschen sich darüber im Internet oder mit anderen Telekommunikationsmitteln aus, wird auch dies registriert. Das Thema „geheimdienstliche Telekommunikationsüberwachung als Mittel sozialer Kontrolle“ dürfte den Geheimdiensten reichen, um ihr Interesse daran oder gar einen Verdacht zu wecken. Lesen Sie jedoch nur die gedruckte Variante der Arbeit und tauschen sich nicht telekommunikativ darüber (oder über das behandelte Thema geheimdienstliche Überwachung) aus, wird dies - zumindest von der Telekommunikationsüberwachung - nicht erfasst.

Es schützt aber nur bedingt vor einer geheimdienstlichen Überwachung, welche eine unsichtbare Omnipräsenz in den Telekommunikationsmedien erlangt hat. Sie sammelt alles was sie kriegen kann. Dabei ist das Ziel, jeden Telefonanruf, jede Textnachricht, jeden (Video-)Chat, jede E-Mail, jeden Webseitenbesuch, jede in der Cloud abgelegte Datei, jede Forendiskussion und vieles mehr in die Datenbanken der Geheimdienste zu kopieren. Auch wenn diese Praxis bis Juni 2013 weitgehend im Geheimen stattfand und dem Großteil der Bevölkerung unbekannt war, änderte sich das mit den Snowden Leaks. Viele geheimdienstliche Überwachungsprogramme sind nun weithin bekannt.

Die geheimdienstliche Telekommunikationsüberwachung wird seitdem in Medien und der Öffentlichkeit diskutiert. Es gibt (parlamentarische) Untersuchungsausschüsse, etliche Bücher, Dokumentationen und vieles mehr, die sie thematisieren.

Eine spannende Frage wird allerdings meist nicht gestellt: Wie wirken diese geheimdienstlichen Telekommunikationsüberwachungsprogramme auf die Menschen ein? Wie findet die Kontrolle statt? Halten sie die Menschen zu einer Normeinhaltung an und sind damit Mittel sozialer Kontrolle? Diesen Fragen möchte die Arbeit mit Theorien der sozialen Kontrolle nachgehen und beantworten.

1.1 Fragestellung

Diese Arbeit befasst sich mit den normativen Wirkungen geheimdienstlicher Telekommunikationsüberwachung. Diese sollen anhand ausgewählter Theorien zur sozialen Kontrolle analysiert werden. Unter dem Begriff der sozialen Kontrolle versteht man staatliche und private Mechanismen und Techniken, mit welchen eine Gesellschaft oder eine soziale Gruppe ihre Mitglieder dazu anhält, sich entsprechend der von ihr aufgestellten Normen zu verhalten.[1]

Soziale Kontrolle ist einem Wandel unterworfen und hängt von den herrschenden gesellschaftlichen Bedingungen ab. Bis in die zweite Hälfte des 20. Jahrhunderts dominierten disziplinargesellschaftliche Elemente und Techniken die soziale Kontrolle. Durch einen ökonomischen, kulturellen und sozialen Wandel der gesellschaftlichen Bedingungen geriet die Disziplinargesellschaft in eine Krise und wurde seitdem von Elementen und Techniken der Sicherheitsgesellschaft abgelöst. In der Disziplinargesellschaft galt ein fester Normenkatalog, dessen Einhaltung überwacht und bei Abweichung (normierend) sanktioniert wurde. In der Sicherheitsgesellschaft hingegen findet eine Orientierung an einem empirischen Mittelwert statt, der Abweichungen bis zu einem gewissen Grad zulässt, während das Subjekt durch Techniken der Selbstführung, der Kontrolle oder bei zu starker Abweichung mit Ausschluss im Rahmen gehalten wird. Dennoch sind auch heute noch verschiedene Formen der disziplinargesellschaftlichen Sozialkontrolle präsent.

Der Untersuchungsgegenstand, die massenhafte Telekommunikationsüberwachung westlicher Überwachungsgeheimdienste, soll daher auf Elemente sozialer Kontrolle sowohl der Disziplinargesellschaft als auch der Sicherheitsgesellschaft überprüft werden. Massenhafte Telekommunikationsüberwachung zielt auf eine möglichst umfassende Überwachung jedweder menschlichen Telekommunikation ab: „Collect it all“.[2] Die westlichen Überwachungsgeheimdienste arbeiten im Bereich der massenhaften

[1] Singelnstein und Stolle 2012: S. 11.
[2] National Security Agency 2014: S. 146.

Telekommunikationsüberwachung eng zusammen, tauschen Daten, Analysemethoden, Soft- und Hardware aus und betreiben zum Teil ganze Überwachungsprogramme und -projekte gemeinsam. Die westlichen Überwachungsgeheimdienste können aufgrund dieser engen Verzahnung als Einheit betrachtet werden.

In der Untersuchung wird die Überwachung und Normierung der Allgemeinheit eine zentrale Rolle spielen. Neben der Allgemeinheit sind für eine demokratische Gesellschaft bestimmte Bevölkerungsgruppen besonders relevant: (investigative) Journalist_innen, Aktivist_innen und Whistleblower_innen. Diese stellen in demokratischen Gesellschaften eine (kritische) Informationsquelle jenseits des Mainstreams dar, sie ermöglichen Meinungspluralität und regen zu gesellschaftlichen Diskussionen und Veränderungen an. Daher spielen sie für den Bestand und die Weiterentwicklung pluralistischer, demokratischer Gesellschaften eine zentrale Rolle. Die Arbeit wird deshalb auch die Wirkungen auf diese besonderen Bevölkerungsgruppen betrachten.

Massenhafte geheimdienstliche Telekommunikationsüberwachung ist eine neuere Erscheinung: die Entwicklung mobiler Kommunikationsgeräte und des Internets - oder allgemein die Computerisierung der Gesellschaft - bietet komplett neue Möglichkeiten der Telekommunikation, die binnen relativ kurzer Zeit alltäglich wurden. Zeitgleich befanden sich die westlichen Geheimdienste mit Ende des Kalten Krieges in einer (Sinn-)Krise, die erst nach den Terroranschlägen des 11. Septembers 2001 überwunden wurde. Eine neue Ära geheimdienstlicher Überwachung begann, die sich im großen Stil gegen Bevölkerungen richtet.

Dies wirft die Frage auf, wie geheimdienstliche Programme und Strategien zur Überwachung ganzer Gesellschaften, Kontroll- und Normierungswirkungen entfalten. Diese Wirkungen sollen mit Hilfe der Theorien zur sozialen Kontrolle im Rahmen der vorliegenden Arbeit herausgearbeitet werden.

In einem Satz: Wie wird soziale Kontrolle über massenhafte geheimdienstliche Telekommunikationsüberwachung vermittelt?

1.2 Methodik, Verortung und Aufbau

Die vorliegende Arbeit wendet die Theorien der sozialen Kontrolle von Michel Foucault, Gilles Deleuze und Singelnstein/Stolle auf die massenhafte Telekommunikationsüberwachung durch Geheimdienste an. Es handelt sich um eine Fallanalyse, deren Gegenstand die Überwachungsprogramme westlicher Geheimdienste sowie deren normative Wirkungen in der Disziplinar- und der Sicherheitsgesellschaft darstellt.

Disziplinar- und Sicherheitsgesellschaft arbeiten mit spezifischen Techniken, die Subjekte dazu anhalten, sich normkonform zu verhalten. Verhalten sich Subjekte nicht normkonform, stellen die jeweiligen Regime sozialer Kontrolle zudem Techniken bereit, mit deren Hilfe die Subjekte sanktioniert oder normiert werden. Die Arbeit prüft, inwiefern massenhafte geheimdienstliche Telekommunikationsüberwachung mit den Theorien und Techniken der sozialen Kontrolle zu fassen sind und die Überwachungsprogramme normierende Wirkungen entfalten.

Analytisch geht die Arbeit heuristisch vor. Obgleich die empirische Situation sich durch die von Edward Snowden geleakten Originaldokumente drastisch verändert hat und eine Innensicht auf die geheimdienstliche Telekommunikationsüberwachung ermöglicht wurde, die vorher so undenkbar war, sind auch diese Einblicke begrenzt. Zum einen ist eine umfassende Betrachtung der geheimdienstlichen Telekommunikationsüberwachung insofern unmöglich, da Geheimdienste naturbedingt keinerlei Einblick in ihre Arbeit gewähren. Zum anderen sind auch bis dato nicht alle Snowden-Dokumente journalistisch bearbeitet und die dazugehörigen Originaldokumente veröffentlicht worden. Diese Dokumente sind wiederum nur eine Auswahl, die von Edward Snowden kopiert, sortiert und an Journalisten übergeben wurden. Das Wissen um geheimdienstliche Telekommunikationsüberwachung bleibt somit begrenzt. Des Weiteren kann die Arbeit ob des begrenzten Umfangs nur den wichtigsten Teil der Programme analysieren. Trotz dieser Einschränkungen ist eine Analyse des Komplexes - nach Kenntnis des Autors - in bisher nie dagewesener Tiefe möglich.

Die Publikmachung der problematisierten massenhaften Telekommunikationsüberwachung durch Geheimdienste war eines der Hauptanliegen Edward Snowdens, da seines Erachtens nach die Überwachung des Alltages eines großen Teils der Menschheit zu weit ginge und zumindest bekannt und gesellschaftlich diskutiert werden solle. Deshalb ist anzunehmen, dass die zum Zeitpunkt der Veröffentlichungen wichtigsten Programme massenhafter geheimdienstlicher Telekommunikationsüberwachung bereits publik gemacht wurden.

Trotz der genannten Einschränkungen ist die Quellenlage für eine Analyse der Überwachungsprogramme sehr umfangreich. Die internen Dokumente erlauben eine unvoreingenommene Innenperspektive auf den Geheimdienstkomplex und seine Programme. Diese Bedingungen lassen heuristische Schlüsse und Aussagen zu.

Die Aussagen und Schlüsse über die soziale Kontrolle durch geheimdienstliche Telekommunikationsüberwachung werden mit Hilfe der Hermeneutik als Metho-

de[3] getroffen. Die Arbeit geht insofern interpretativ vor, als dass sie die theoretischen Grundlagen aus den Texten und Büchern von Foucault, Deleuze und Singelnstein/Stolle zur sozialen Kontrolle der Disziplinar- und Sicherheitsgesellschaft destilliert. Dieses Destillat zur sozialen Kontrolle wendet die Arbeit auf die Überwachungsprogramme der westlichen Geheimdienste (Primär NSA, GCHQ und BND) an. Auch hier bedient sich die Arbeit der hermeneutischen Methode.

Bei den Original-Dokumenten der Geheimdienste handelt es sich häufig um Präsentationen, von denen nur die Folien veröffentlicht wurden, um kurze Wiki-Artikel oder andere Texte, die ihrerseits interpretationsbedürftig sind und häufig technische Zusammenhänge beschreiben, die eigenständig nachvollzogen werden müssen. Die Autoren sind dabei weitgehend unbekannt, insofern bleibt nur eine textimmanente Interpretation, unter Einbezug anderer Texte aus dem Snowden-Fundus, sowie explizierter Ziele der Geheimdienste. Den Dokumenten, die für den internen Gebrauch unter strenger Geheimhaltung erstellt wurden, um die mit den entsprechenden Programmen konfrontierten Geheimdienstmitarbeiter_innen über diese zu unterrichten, können ob der bedienungsanleitenden oder lexikalischen Ader eine entsprechende Objektivität abgewonnen werden. Dennoch sind die Absichten und Ziele durch die Beraubung ihres Zusammenhangs häufig nicht expliziert, insofern befreit dies nur bedingt von einer Auslegung im Rahmen der veröffentlichten geheimdienstlichen Zusammenhänge. Die journalistischen und technischen Auslegungen der Dokumente und Zusammenhänge gilt es mit anderen Analysen zusammenzubringen, anhand der Original-Dokumente zu prüfen und die Ergebnisse im Kontext der sozialen Kontrolle der Disziplinar- und Sicherheitsgesellschaft ergebnisoffen neu zu interpretieren. Letztlich nähert sich die Arbeit hermeneutisch einem heuristischen Problem. Sie versucht dabei so nah wie möglich an der Realität zu operieren.

Diese Näherung ist letztlich nur mit einem Verständnis von politischer und soziologischer Theorie und Arbeitstechnik, sowie einem grundlegenden Verständnis von Software und Sicherheit im Rahmen der Informationstechnologie möglich.[4] Sie erfordert das Hinterfragen fremder beziehungsweise eigener Thesen und Zugänge.

Geheimdienste sind ein integraler Bestandteil von Macht- und Herrschaftssicherung. Ziel der Arbeit ist es, diese Machtwirkungen im Bereich der sozialen Kontrolle zu analysieren. Die Arbeit ist somit im Bereich der Macht- und Herrschaftsanalyse zu verorten. Sie sieht sich als Teil der Surveillance-Studies und ist primär in den

[3] vgl. Zapf 2013: S. 52 ff.
[4] Lyon, Haggerty und K. Ball 2014: S. 6.

Disziplinen Soziologie, Politikwissenschaft und Informatik angesiedelt.

Die Surveillance-Studies sind ein junges, interdisziplinäres Forschungsfeld, deren Kerndisziplinen Soziologie, Politikwissenschaften und Geographie werden ergänzt durch Informatik, Rechtswissenschaften, Philosophie und Anthropologie. Sie stellen einen thematischen Schwerpunkt, einen Aspekt moderner Gesellschaften, in den Mittelpunkt ihres Erkenntnisinteresses.[5] Zurawski definiert Surveillance-Studies als „Forschungsansätze, die sich mit den Veränderungen und historischen Bedingungen von Überwachung, Kontrolle und gesellschaftlicher Steuerung durch Technologien und deren gesellschaftlicher Diskurse widmen."[6]

Unter diesen theoretischen Rahmenbedingungen wird die Arbeit in einem ersten Schritt soziale Kontrolle definieren, den Wandel der Disziplinar- zur Sicherheitsgesellschaft aufzeigen und deren spezifischen Eigenheiten und Techniken herausarbeiten. In einem zweiten Schritt wird der Untersuchungsgegenstand westliche Überwachungsgeheimdienste in Gesellschaften westlichen Typus geklärt. Dabei werden die Überwachungsgeheimdienste verortet und die Programme zur massenhaften Telekommunikationsüberwachung vorgestellt. Auf dieser Grundlage folgt die Analyse der disziplinargesellschaftlichen Elemente der geheimdienstlichen Telekommunikationsüberwachung. Hierauf folgt die Prüfung der Überwachungsprogramme mit Hilfe sicherheitsgesellschaftlicher Konzepte und Techniken. In einem letzten Schritt sollen die Ergebnisse der Untersuchung vorgestellt und bewertet werden.

1.3 Literatur

1.3.1 Forschungsstand und Relevanz

Foucaults Theorie der Disziplinargesellschaft und des panoptischen Prinzips erfreuen sich in den Surveillance-Studies ausgesprochener Beliebtheit.[7] Viele Arbeiten beziehen sich auf das Panoptikum respektive Foucault. Gary T. Marx sieht Foucault sogar als Begründer der gegenwärtigen Surveillance-Studies.[8] Insbesondere im Bereich der Videoüberwachung, aber auch in anderen Bereichen der Surveillance-Studies, wird Foucaults Theorie nicht nur gerne als Analysewerkzeug verwendet, sondern liefert auch Erklärungen rund um die Wirkungszusammenhänge und Funktionen von Über-

[5] Lyon 2002: S. 5; Zurawski 2007: S. 9; Lyon, Haggerty und K. Ball 2014: S. 1.
[6] Zurawski 2007: S. 8.
[7] Zurawski 2015: S. 26; Elmer 2014: S. 21.
[8] Marx 2015.

wachung. Auch in den gesellschaftlichen Überwachungsdiskursen ist das Panoptikum neben George Orwells Werk „1984“ fest verankert. Dennoch gerieten die Konzepte der Disziplin und des panoptischen Prinzips in den letzten Jahren zunehmend in Kritik. Ihnen wird vorgeworfen, dass sie heute an Erklärungs- und Überzeugungskraft verlieren würden. Der ökonomische, kulturelle und soziale Wandel[9] im letzten Jahrhundert und die damit verbundene Ablösung des Fordismus durch den Postfordismus, führe auch zu einer Krise der Disziplin und ihrer Institutionen (siehe Kapitel 2).[10] Das Panoptikum wurde daher als Analysewerkzeug immer wieder angepasst und weiterentwickelt, es entstanden neue Formen wie das Superpanoptikum, das Synoptikum oder das Post-Panoptikum.[11]

Auch Foucault und sein enger Freund Deleuze sahen schon im letzten Jahrhundert die Disziplinargesellschaft und damit das Panoptikum auf dem Rückzug, abgelöst von einer neuen Gesellschaftsform mit neuen Kontrolltechniken. Diese Gesellschaft trägt viele Namen: Deleuze nennt sie *Kontrollgesellschaft*,[12] Foucault beschreibt mit seinen *Sicherheitsdispositiven* in seiner Vorlesung „Sicherheit, Territorium, Bevölkerung“ ein ähnliches Phänomen,[13] Singelnstein/Stolle nennen sie *Sicherheitsgesellschaft*,[14] Beck nutzt als Begriff *Risikogesellschaft*[15]. Daneben gibt es noch die Bezeichnungen Präventions-, Überwachungs- und Sicherheitsstaat.

Obwohl diese Konzepte den gesellschaftlichen Umbruch der letzten Jahrzehnte ähnlich begreifen und theoretisch zu fassen versuchen, differieren die Begrifflichkeiten und damit die zu erfassenden oder erfassbaren gesellschaftlichen (Teil-)Bereiche und (Teil-)Entwicklungen. Deleuzes Begriff der Kontrollgesellschaften ist entgegenzuhalten, dass er sich zu sehr auf Kontrolltechniken fokussiert. Zwar kann Selbstführung unter das Konzept subsumiert werden, die gegenwärtig stattfindende Renaissance des Ausschlusses fällt allerdings nicht mehr unter diesen Begriff und er lässt somit ein wichtiges Element der sozialen Kontrolle im Postfordismus außer Acht.[16]

Becks Konzept der Risikogesellschaft beschreibt zwar die grundsätzlichen gesellschaftlichen Veränderungen hin zu einer Risikoabwägung und -konstruktion. Er kon-

[9] Vielfach wird auch auf die Computerisierung und Technisierung der Überwachung als Ursache der eingebüßten Erklärungskraft verwiesen.
[10] Kammerer 2011: S. 20; Bogard 2014: S. 30.
[11] Marx 2015: S. 733.
[12] vgl. Deleuze 1993.
[13] vgl. Foucault 2006.
[14] vgl. Singelnstein und Stolle 2012.
[15] vgl. Beck 2000.
[16] Singelnstein und Stolle 2012: S. 121.

zentriert sich jedoch auf Vorverlagerungstendenzen und die zunehmende Abwägung des Risikos, doch hierunter lassen sich die immer weiter um sich greifenden Sicherheitsideologien und die Konzepte der Selbstführung und des Ausschlusses nur schwer fassen.

Bezeichnungen wie Präventions-, Überwachungs- und Sicherheitsstaat sind ihr einseitiger Blick auf den Staat vorzuhalten. Sicherheitsproduktion und soziale Kontrolle sind jedoch bei weitem nicht nur staatliche Angelegenheiten. Die Sicherheitsproduktion wird zunehmend privatisiert, soziale Kontrolle findet nicht nur zwischen Staat und Bürger_innen statt, sondern ist ein gesamtgesellschaftliches Phänomen. Hinzu kommt das generalisierte Sicherheitsbedürfnis der Bevölkerung, welches ebenfalls mit einem staatszentrierten Begriff von sozialer Kontrolle nicht oder nur am Rande gefasst werden kann.[17]

Foucault stellt in seiner Vorlesung „Sicherheit, Territorium, Bevölkerung“[18] zwar Konzepte der (neo-)liberalen Sicherheitsproduktion, die er Sicherheitsdispositive nennt, vor und beschreibt damit die gesellschaftlichen Veränderungen detailliert, führt aber keinen Begriff für das auf die Disziplinargesellschaft folgende Regime ein. Es liegt nahe, der Bedeutung der Sicherheit insofern gerecht zu werden, in dem die auf die Disziplinargesellschaft folgende Gesellschaft Sicherheitsgesellschaft genannt wird.

Die Arbeit folgt Singelnstein/Stolle mit ihrem Begriff der Sicherheitsgesellschaft, der auch die von Foucault beschriebenen Veränderungen umfasst. Angesichts der zentralen Bedeutung von Sicherheit, sowohl als staatliches Legitimationsmittel, als auch die gesellschaftlichen Diskurse um Sicherheit, das generalisierte Sicherheitsbedürfnis, sowie die grassierende Verunsicherung der Bevölkerung, legen die Verwendung einer Begriffskombination aus Sicherheit und Gesellschaft nahe. Die Verwaltung des empirisch Normalen, die auf eine umfassende Herstellung sozialer Ordnung gerichtet ist und ihre Techniken der Selbstführung, der Kontrolle und des Ausschlusses lassen sich damit begrifflich gut fassen. Ebenso wird die umfassende Detektion von Risiken, sowie deren Prävention, erfasst - welches ein zentrales Element der Kontrolltechniken und der Sicherheit darstellt. Auch staatliche, kulturelle, ökonomische und soziale Transformationsprozesse lassen sich damit analytisch beschreiben.[19]

In den Surveillance-Studies spielen diese Konzepte in den letzten Jahren eine im-

[17] Singelnstein und Stolle 2012: S. 121.
[18] vgl. Foucault 2006.
[19] Singelnstein und Stolle 2012: S. 121 ff.

mer größere Rolle. Erhofft wird sich ein neues Paradigma und damit die Ablösung des teilweise als veraltet und unzulänglich angesehenen Panoptikums.[20] Doch obwohl die Sicherheitsgesellschaft die Disziplinargesellschaft zunehmend ablöst und sich die Disziplin auf dem Rückzug befindet, ist die Disziplinargesellschaft immer noch aktiv. In der Arbeit werden daher sowohl die disziplinargesellschaftlichen als auch die sicherheitsgesellschaftlichen Formen sozialer Kontrolle analysiert, obgleich der Fokus auf der Sicherheitsgesellschaft liegt. Die Vermutung liegt nahe, dass die westlichen Geheimdienste nach dem Kalten Krieg einen Wandel hin zu sicherheitsgesellschaftlicher Sozialkontrolle unternommen haben. Die Arbeit wird dabei nicht den Wandel, sondern den aktuellen Stand untersuchen. Wie stark sind disziplinargesellschaftliche Elemente sozialer Kontrolle (noch) aktiv, lässt sich die massenhafte geheimdienstliche Telekommunikationsüberwachung in der Sicherheitsgesellschaft verorten und greift sie auf die Verwaltung des empirisch Normalen mit ihren Techniken der Selbstführung, der Kontrolle und des Ausschlusses zurück?

Geheimdienste, obgleich eine zentrale Überwachungsinstitution in westlichen Staaten, sind zwar ein Referenzpunkt in den Surveillance-Studies, es gibt jedoch kaum tiefgehende Analysen zum Thema. Die wissenschaftliche Auseinandersetzung mit Geheimdiensten ist, abgesehen von juristischen Fragestellungen und historischen Aufarbeitungen, recht übersichtlich. Sicherlich hängt dies auch mit der schwierigen Quellenlage zusammen. Es gibt wenig valide Informationen aus dem Geheimdienstapparat, welcher - wie der Name schon sagt - im Geheimen agiert und nur wenige Informationen nach außen dringen lässt. Diese sind oft schwer zu überprüfen, da auf Aussagen aus Geheimdienstkreisen oder von Aussteiger_innen zurückgegriffen werden muss. Weitergegebene interne Dokumente werden von Journalist_innen häufig nicht im Original veröffentlicht. Anders sieht die Situation bei älteren Archiv-Dokumenten aus, die aus Gründen der Regierungstransparenz veröffentlicht werden (beispielsweise „Freedom of Information Act“ (FOIA) in den USA), diese lassen logischerweise eine Analyse der aktuellen Situation nicht zu.[21] Ein weiteres Problem stellt die originär geheimdienstliche Taktik, Desinformationen zu streuen, dar.[22]

Diese Situation ändert sich mit den Snowden-Leaks seit Juni 2013 und setzt sich fort. Nach mehreren Jahren journalistischer,[23] rechtswissenschaftlicher und techni-

[20] Kammerer 2011: S. 19.
[21] Daher gibt es vor allem historisch orientierte Forschung zu Geheimdiensten.
[22] Krieger 2009: S. 9 f., 14 f.; Piper 2015.
[23] vgl. Greenwald 2014a; Rosenbach und Stark 2014; Fuchs und Goetz 2013.

scher Aufarbeitung[24] der Telekommunikationsüberwachung ist es an der Zeit, die geheimdienstliche Telekommunikationsüberwachung auch tiefgehend sozialwissenschaftlich aufzuarbeiten. Die vorliegende Arbeit möchte hierzu ihren Beitrag leisten und analysieren inwiefern geheimdienstliche Telekommunikationsüberwachung sozialkontrollierende Wirkungen entfaltet. Eine weitergehende sozialwissenschaftliche Auseinandersetzung mit Überwachung im Allgemeinen, Überwachungstechnologien (deren Entwicklung rasant fortschreitet), sowie speziell auch der geheimdienstlichen Tätigkeiten ist, ob zunehmendem Ausbau und Relevanz, sowie damit verbundener Sicherheitsdiskurse, unabdingbar. Mit den Snowden-Leaks gibt es erstmals umfangreiche aktuelle Originaldokumente über eine umfassende, weltweite Überwachung durch Geheimdienste. Dieser reichhaltige Fundus sollte für die geisteswissenschaftliche Forschung genutzt werden.

1.3.2 Literatur und Quellenlage

Das theoretische Fundament der Arbeit bilden die Werke von Foucault, allen voran „Überwachen und Strafen“,[25] in welchem er die Disziplinargesellschaft beschreibt, sowie die Aufschriebe zu seiner Vorlesung „Sicherheit, Territorium, Bevölkerung. Geschichte der Gouvernementalität I“[26] in welcher er das Sicherheitsdispositiv als eine Form der Gouvernementalität beschreibt. Ebenfalls von besonderer Bedeutung sind die Arbeiten von Singelnstein/Stolle zur Sicherheitsgesellschaft[27] und Deleuzes' „Postskriptum über die Kontrollgesellschaften“.[28] Hervorheben möchte ich zudem die Arbeiten von Thomas Lemke,[29] die Schriften und Sammelbände von Nils Zurawski,[30] sowie eigene Veröffentlichungen.[31]

Prägend für die Auseinandersetzung mit Geheimdiensten ist die dürftige und schwierige Quellenlage, wenn es um aktuelle Phänomene geht. Vor dem Jahr 2013 gibt es nur wenige Bücher, die sich intensiv mit einzelnen Geheimdiensten auseinandersetzen. Für die amerikanischen Überwachungsgeheimdienste ist hier der Journalist und NSA-Experte James Bamford zu nennen, der mit seinen Büchern[32] und

[24] vgl. Schneier 2015a.
[25] Foucault 1994.
[26] Foucault 2006.
[27] Singelnstein und Stolle 2012; Singelnstein und Stolle 2007b; Singelnstein und Stolle 2007a.
[28] Deleuze 1993.
[29] Lemke 2014; Lemke 2004.
[30] Zurawski 2015.
[31] Tremmel 2010; Tremmel 2012b.
[32] Bamford 2001; Bamford 1986.

Artikeln eine fundierte Beschreibung des bis zu diesem Zeitpunkt kaum bekannten Geheimdienstes NSA (National Security Agency) lieferte. Die Existenz des britischen Überwachungsgeheimdienstes GCHQ (Government Communications Headquarters) wurde erst durch den Enthüllungsjournalisten Duncan Campbell im Jahr 1976 aufgedeckt.[33]

Zu problematisieren sind Veröffentlichungen die am Rande oder schon im Bereich der Verschwörungstheorien anzusiedeln sind, auf die sich eine wissenschaftlich-faktenbasierte Arbeit aus einer inhärenten Logik heraus nicht berufen kann und will.

Die Quellenlage zu geheimdienstlichen Überwachungsprogrammen hat sich mit den Snowden-Leaks verändert. Musste davor auf vage Informationen oder zugespielte Dokumente[34], sowie Annahmen und Vermutungen auf Basis geheimdienstlichen Agierens,[35] Whistleblower_innen (u.a. William Binney, Thomas Drake, J. Kirk Wiebe) und Pensionäre, die über ihre Erfahrungen im Geheimdienst sprechen und publizieren, sowie Untersuchungen, Verfahren und Anhörungen zurückgegriffen werden, können nun Originalquellen analysiert werden. Dieser nicht nur für die Forschung glückliche Umstand ist zum einen Edward Snowden zu verdanken, zum anderen auch einigen Medien,[36] die zu ihren Artikeln auch die Original-Dokumente online stellen. Dies ermöglicht, diese Arbeit auf Original-Dokumente aus dem Geheimdienstbereich zu stützen.

Die Empirie der Arbeit basiert daher auch primär auf Original-Dokumenten westlicher Geheimdienste, sowie auf Büchern und Artikeln die diese aufarbeiten. Zu nennen sind hier Glenn Greenwald, dem gemeinsam mit Laura Poitras und Ewen Ma-

[33] Taureck 2014: S. 9.

[34] Allerdings werden diese zugespielten Dokumente üblicherweise von Journalist_innen nicht veröffentlicht. Dies führt dazu, dass oftmals nur die Interpretation und die Auswahl der Journalist_in zur Verfügung steht und die Aussagen nicht überprüfbar sind. Hinzu kommen die mögliche Missinterpretation (speziell von technischen Sachverhalten und Zusammenhängen), sowie die Nicht-Publikation von als nicht wichtig erachteten Informationen, die beispielsweise für die Forschung oder die Herstellung tiefgehenderer Zusammenhänge eine erhebliche Relevanz haben können.

[35] Beispielsweise wurden geheimdienstliche Stellenangebote (an bestimmten Orten), bestimmte Einrichtungen und Technologien, sowie bekanntgewordene Angriffe, die den entsprechenden Geheimdiensten zugeordnet wurden, analysiert. Aber auch Einkäufe, Ausschreibungen, Tarnfirmen oder Wege gecharterter Jets führten zu Informationen - beispielsweise zu Geheimgefängnissen und Entführungen (Renditions).

[36] Dank gebührt an dieser Stelle theintercept.com, netzpolitik.org und bei einigen Artikeln auch Spiegel Online und The Guardian.

cAskill die Dokumente von Edward Snowden übergeben wurden, Greenwalds Buch[37] über die Enthüllungen, die davor entstandenen Guardian Artikel und das von ihm mitgegründete Journalismus-Projekt The Intercept.[38] Des Weiteren wurde Literatur von den Spiegel-Redakteuren Marcel Rosenbach und Holger Stark verwendet, die sowohl Artikel, als auch ein Buch[39] zum Thema geschrieben haben, sowie das Buch „Geheimer Krieg“[40] der Investigativ-Journalisten Christian Fuchs und John Goetz. Besonders hervorzuheben sind die Artikel und Bücher[41] des IT-Sicherheitsexperten und Kryptologen Bruce Schneier. Hinzu kommen Artikel des Blogs netzpolitik.org[42] und des IT-Newsportals heise.de.

[37] Greenwald 2014a.
[38] theintercept.com
[39] Rosenbach und Stark 2014.
[40] Fuchs und Goetz 2013.
[41] vgl. Schneier 2015a; Schneier 2014a.
[42] Disclaimer: Der Autor bloggt bei netzpolitik.org.

2 Theorie der Sozialen Kontrolle

2.1 Soziale Kontrolle

Unter sozialer Kontrolle[43] fasst man staatliche und private Mechanismen und Techniken zusammen, mit welchen eine Gesellschaft oder eine soziale Gruppe ihre Mitglieder dazu anhält, sich entsprechend der von ihr aufgestellten Normen zu verhalten.[44] Sie kann sowohl reaktiv, nach erfolgter Devianz wieder in den Normalbereich holend (bspw. durch Sanktionen oder Therapien), als auch präventiv erfolgen, die Wahrscheinlichkeit von Abweichung im Vorfeld verringernd.[45] Scheerer definiert soziale Kontrolle als „Ensemble all dessen [..], was unerwünschtes Verhalten verhindern soll und/oder faktisch verhindert.“[46] Soziale Kontrolle ist ein gesellschaftsimmanentes Phänomen, sie ist einem Wandel unterworfen und hängt von den herrschenden gesellschaftlichen Bedingungen ab.

Überwachung hingegen rückt Dinge ins Licht, betrachtet sie, vergleicht die Ist-Werte mit vorgegebenen Soll-Werten. Hierzu wird häufig auf die Hilfe technischer Geräte zurückgegriffen. Wird etwas überwacht, wird kontrolliert was es tut und ob dies mit definierten Werten übereinstimmt. Das kann ein Server im Internet sein, dessen Dienste, Logs und Sensoren (Temperatur, Sektorenfehler der Festplatte, ...) überwacht werden, es kann ein Mensch in einem Krankenbett sein, dessen Herzfrequenz und Atmung überwacht wird, oder es können Personen in einem Bahnhofsgebäude sein, welche vom Wachdienst oder der Polizei auf abweichendes Verhalten hin überprüft werden. Zwischen Überwachten und Überwacher_innen besteht dabei meist ein asymmetrisches Machtverhältnis. Überwachung kann, muss aber nicht notwendigerweise, ein Mittel der sozialen Kontrolle sein.

> Sicherheit ist „ein Zustand, der erreicht wird oder werden soll, gestört oder gefährdet wird und Ziel oder Mittel (von Politik, Technik, Gesellschaft) sein kann. Überwachung und Kontrolle sind Verfahren, die zur Erreichung dieses Zustandes eingesetzt werden. Das Risiko ist in diesem Zusammenhang eine Form der Operationalisierung, mit der der Grad des Zustandes Sicherheit bestimmt bzw. zukünftige Handlungen rationali-

[43] Zur Herkunft und Wandel des Begriffes und Entwicklung des Konzeptes vgl. Peters 2009; Nogala 2000; Scheerer 2000; Kammerer 2011.
[44] Singelnstein und Stolle 2012: S. 11.
[45] Franz 2000: S. 71.
[46] Scheerer 2000: S. 167.

siert werden können. Hier geht es im Wesentlichen um sozial bewertete Wahrscheinlichkeiten. [...] Sicherheitstechnologien beschreiben Technologien, mit denen der Zustand der Sicherheit gewährleistet oder mit denen Gefährdungen dieses Zustandes antizipiert werden sollen."[47]

Sicherheit (und Unsicherheit) ist gesellschaftlich konstruiert und hat einen normativen Charakter, der politischen, wirtschaftlichen oder gesellschaftlichen Interessen unterliegen kann.[48] Diese unterliegen, wie die soziale Kontrolle, einem Wandel und hängen von den gesellschaftlichen Bedingungen ab.

2.1.1 Soziale Kontrolle im Wandel

Soziale Kontrolle und ökonomische, soziokulturelle und politische Bedingungen sind eng miteinander verflochten und stehen in einem Verhältnis der Wechselwirkung und des Wandels.[49] Dieser Wandel soll für den Übergang der Disziplinar- in die Sicherheitsgesellschaft in Anlehnung an Singelnstein/Stolle[50] anhand der Regulationsschule[51] für Gesellschaften westlichen Typus skizzenhaft dargestellt werden. Die gesellschaftlichen Entstehungsbedingungen und Hintergründe sind vielfältig und können daher in diesem Rahmen nur kurz angerissen werden.

Im 18. Jahrhundert wandelten sich die gesellschaftlichen Bedingungen massiv. Das feudal-absolutistische Zeitalter ging zu Ende, ein demographischer Wachstumsschub ließ die zu kontrollierende Bevölkerung massiv ansteigen, die industrielle Revolution und mit ihr ein kapitalistischer Produktionsapparat, dessen Produktivität und Rentabilität permanent gesteigert werden musste, forderte ihren Tribut. Im Zuge dieses Wandels veränderte sich auch die soziale Kontrolle. Die Disziplinargesellschaft entstand.[52]

Ihren Höhepunkt erlebte die Disziplinargesellschaft zu Beginn des 20. Jahrhunderts im Fordismus.[53] Kennzeichnend für diesen war „eine hoch rationalisierte Massenproduktion, staatliche Regulierung und ein korporatives Integrationsmodell".[54]

[47] Zurawski 2015: S. 13, 21.
[48] Ebd.: S. 21.
[49] Lemke 2014: S. 103; Singelnstein und Stolle 2012: S. 17.
[50] vgl. Singelnstein und Stolle 2012: S. 17 ff.
[51] vgl. Hirsch und Roth 1986.
[52] Wolf 2008: S. 281 f; P.-A. Albrecht 2010: S. 66; Marinis 2000: S. 34; Kroener und Neyland 2014: S. 144.
[53] Deleuze 1993: S. 254.
[54] Singelnstein und Stolle 2012: S. 18.

Der Sozial- und Wohlfahrtsstaat legitimierte sich durch ein *Inklusionsversprechen*:[55] Der Staat betrieb (soziale) Sicherungssysteme, überbrückte schwierige Lebensphasen (z.B. vorübergehende Arbeitslosigkeit, Krankheit) und sorgte für anschließende Reintegration. Auch die Strafpolitik orientierte sich an dem Prinzip der Resozialisierung.[56]

Ende des 20. Jahrhunderts geriet der Fordismus in die Krise und wurde vom Postfordismus und der Sicherheitsgesellschaft abgelöst. Wohlfahrtsstaatlich-intervenierende Regulation, tariflich abgesicherter Arbeitsmarkt, Vollbeschäftigung, all dies konnte der Staat in einer immer weitergehenden Flexibilisierung und Deregulierung der Produktionsweise und damit einhergehend des Arbeitsmarktes nicht mehr gewährleisten. Immer breitere Sektoren der Gesellschaft wurden von einer ökonomischen, politischen und sozialen Teilhabe ausgeschlossen. Das wohlfahrtsstaatliche Legitimationsversprechen des Staates konnte nicht mehr aufrecht erhalten werden und musste ersetzt werden.[57] Diese Entwicklungen führen zu einer ansteigenden Verunsicherung, Verängstigung und Prekarisierung großer Teile der Bevölkerung. Dies stellt den idealen Nährboden für Feindkonstruktionen und Abschottungsbedürfnisse dar. Gleichzeitig steigt das Bedürfnis nach materieller Absicherung und Sicherheit.[58]

> „Der Staat greift dies[es Bedürfnis] auf und verstärkt diese Entwicklung, indem er anbietet, die Bürger vor Kriminalität und sonstigen Bedrohungen zu schützen oder ihnen zumindest ein Gefühl von Schutz zu vermitteln. An die Stelle des Versprechens sozialer Inklusion tritt das alleinige *Versprechen individueller Sicherheit*.“[59]

Der immer weitere Rückzug des Staates aus der Sozialpolitik wird durch einen populistischen Umgang mit Straftaten und einer „law-and-order“-Mentalität begleitet. Die Sicherheits- und Kriminalpolitik wandelt sich hin zu einer immer umfassenderen, anlasslosen Kontrolle, sowie einem repressivem Ausschluss. Sicherheit wird zur zentralen Legitimationsfigur staatlichen Handelns und Verunsicherung/Unsicherheit zur einer Grundkonstante der Politik.[60]

[55] Obgleich die Leistungen und Versprechungen nur für einen Teil der Bevölkerung galten.
[56] Foucault 2005: S. 139; Singelnstein und Stolle 2012: S. 19.
[57] Marinis 2000: S. 40.
[58] Singelnstein und Stolle 2012: S. 21 f, 40, 45; Trump 2012: S. 36.
[59] Singelnstein und Stolle 2012: S. 42 f. Hervorhebung durch den Verfasser.
[60] Peters 2009: S. 148 f; Singelnstein und Stolle 2007b: S. 48 f, 123.

Die Überwachung und Kontrolle wird zunehmend technisiert, das überwachende Individuum wird durch Maschinen (z.B. Überwachungskameras) unterstützt oder durch automatisierte, algorithmische Vermessung teilweise oder komplett ersetzt (z.B. Big Data Analysen, Videoüberwachungssysteme, die Objekte und die damit verbundenen Gefahrenpotentiale selbstständig erkennen können). Damit geht eine Herausbildung eines ganzen Dienstleistungssektors im Überwachungsbereich einher sowie einem lukrativen, wachsenden Markt für Überwachungstechnik, die ihrerseits stetig neue Entwicklungen hervorbringt.[61]

2.1.2 Foucaults Machttheorie

Soziale Kontrolle rekurriert auf Macht. Bei Foucault ist Macht nicht, wie beispielsweise bei der klassischen Definition von Weber, „jede Chance, innerhalb einer sozialen Beziehung den eigenen Willen auch gegen Widerstreben durchzusetzen, gleichviel, worauf diese Chance beruht“[62], vielmehr sieht Foucault in der Macht einen (sozialen) Prozess, der auch Produktivität entfalten kann.[63]

> „Diese Macht ist nicht so sehr etwas, was jemand besitzt, sondern vielmehr etwas, was sich entfaltet; nicht so sehr das erworbene oder bewahrte »Privileg« der herrschenden Klasse, sondern vielmehr die Gesamtwirkung ihrer strategischen Positionen - eine Wirkung, welche durch die Position der Beherrschten offenbart und gelegentlich erneuert wird. Ander[er]seits richtet sich diese Macht nicht einfach als Verpflichtung oder Verbot an diejenigen, welche »sie nicht haben«; sie sind ja von der Macht eingesetzt, die Macht verläuft über sie und durch sie hindurch“.[64]

> „Macht ist also nicht Eigentum einer Person, eines Subjekts, vielmehr ist sie ein omnipräsentes Phänomen - eine strategische Position. Sie spannt sich wie ein Netz zwischen Menschen sowie gesellschaftlichen Anforderungen und Einrichtungen. Man muss sich die Macht wie eine immerwährende Schlacht vorstellen – als ein komplexes und heterogenes Geflecht von Machtbeziehungen, die Änderungsprozessen unterworfen sind (Un-

[61] Benkel 2011: S. 105.
[62] Weber 1978: S. 79.
[63] Tremmel 2010: S. 11.
[64] Foucault 1994: S. 38. Hervorhebung im Original.

ruheherde, Kämpfe, (vorübergehende) Umkehrung der Machtverhältnisse).“[65]

2.2 Disziplinargesellschaft

Ende des 18. Jahrhunderts[66] wird nach Foucault die feudal-absolutistische Gesellschaft durch die Disziplinargesellschaft abgelöst. Mit ihr ändern sich auch die Machttechniken und die soziale Kontrolle.

Die traditionelle Macht ist eine Macht, die sich sehen lässt, sich zeigt, sich kundtut - jene, an denen sie sich entfaltet, aber im Dunkeln lässt. Die Disziplinarmacht hingegen agiert in der Unsichtbarkeit, eine Mikrophysik der Macht, die so kleinteilig arbeitet, dass sie fast schon verborgen bleibt, wohingegen sie den von ihr Unterworfenen die Sichtbarkeit aufzwingt, sie ans Licht zerrt, sie vermisst.[67] „Es ist gerade das ununterbrochene Gesehenwerden, das ständige Gesehenwerdenkönnnen,... was das Disziplinarindividuum in seiner Unterwerfung festhält.“[68]

Die Disziplinargesellschaft zielt auf die Dressur der Körper, auf ein Nutzbarmachen im ökonomischen Sinne. Die Dressur und das Nutzbarmachen geschieht mit Hilfe der Disziplinarmacht, welche durch „Überwachung und Normierung der Tätigkeiten zu dauerhaftem, persönlichkeitsprägendem Verhalten führt.“[69] Dies geschieht durch

> „das Erlernen von Gesten und Verhaltensweisen, das Ausbilden von Gewohnheiten und die Modellierung der Zeit- und Raumvorstellungen. Gleichzeitig setzt die Disziplinartechnologie die Produktion eines Wissens von diesen Individuen voraus, das es ermöglicht, sie zu kennen, die Möglichkeiten und Grenzen ihrer Leistungsfähigkeit abzuschätzen, die Bedingungen ihrer Veränderung zu untersuchen, ihre 'Normalität' zu spezifizieren etc.“[70]

[65] Tremmel 2010: S. 11 f.
[66] Bei den angegeben Jahreszahlen handelt es sich um Näherungswerte. Die Ablösung eines Regimes der gesellschaftlichen sozialen Kontrolle ist ein vielschichtiger Prozess, der sich in verschiedenen Staaten und Gesellschaften in unterschiedlichen Geschwindigkeiten und Ausformungen vollzog. Es wird daher ein Zeitraum angegeben in dem das neue Regime in den westlichen Staaten und Gesellschaften über das Alte dominierte.
[67] Foucault 1994: S. 241; Ruoff 2009: S. 103.
[68] Foucault 1994: S. 241.
[69] Bogdal 2008: S. 74.
[70] Lemke 2014: S. 92. Hervorhebung im Original.

> „Die Disziplin fabriziert auf diese Weise unterworfene und geübte Körper, fügsame und gelehrige Körper. Die Disziplin steigert die Kräfte des Körpers (um die ökonomische Nützlichkeit zu erhöhen) und schwächt diese selben Kräfte (um sie politisch fügsam zu machen).“[71]

Die Disziplinargesellschaft zeichnet sich durch ein allgemeingültiges Normengefüge aus. Normen umfassen sowohl Gesetze, als auch nicht kodifizierte gesellschaftliche Reglementierungen, deren kontinuierliche Einhaltung als Anforderung an das Subjekt gestellt wird. Abweichendes Verhalten wird nicht toleriert, sondern durch Überwachung des Subjekts erkannt und anschließend sanktioniert. Ziel von Sanktionen ist nicht die bloße Bestrafung oder Abschreckung vor einem möglichen Regelübertritt, vielmehr soll auch die Sanktionierung eine normierende Wirkung entfalten. Die „normierende Sanktion“ soll das Subjekt wieder zu regelkonformem Verhalten anhalten und in den Normalbereich zurückholen. Letztlich verlangt die Disziplinargesellschaft „die Akzeptanz der bestehenden Normen und der ihnen zu Grunde liegenden herrschenden Ordnung.“[72] Diese Bereitschaft zur Integration muss nötigenfalls erzeugt werden.[73]

Die Normierung des Subjekts erfordert eine kontinuierliche Kontrolle, einen Abgleich des Ist-Zustandes (Verhalten des Subjekts) mit dem Soll-Zustand (Normengefüge). Die Disziplin richtet hierzu den „zwingenden Blick“ ein: „eine Anlage, in der die Techniken des Sehens Machteffekte herbeiführen und in der umgekehrt Zwangsmittel die Gezwungenen deutlich sichtbar machen.“[74] Die Räume werden dabei derart gestaltet, dass sie die Einsehbarkeit und damit die Sichtbarkeit der Individuen gewährleisten. Gleichzeitig werden die Individuen im Raum verteilt, ihnen Positionen zugewiesen. Dies gewährleistet die Kontrolle und Ansprechbarkeit (und damit die Nützlichkeit) der Individuen.

Als Beispiel kann das klassische amerikanische Großraumbüro mit seinen geometrisch angeordneten Arbeitsparzellen, den sogenannten Cubicles, dienen. Schalldämmende, mittelhohe Raumteiler schirmen die sitzend arbeitenden Büroangestellten voneinander ab, ermöglichen aber die Einsehbarkeit und somit die Kontrolle durch stehende oder umhergehende Individuen oder Videoüberwachung.[75] Jeder Mitarbei-

[71] Foucault 1994: S. 177.
[72] Singelnstein und Stolle 2012: S. 61.
[73] Foucault 1994: S. 231; Singelnstein und Stolle 2012: S. 62.
[74] Foucault 1994: S. 221.
[75] Richter 2015.

ter_in wird eine Parzelle zugewiesen, dies sichert die Ansprechbarkeit und Effizienz. Ein Tableaus[76] entsteht, das eine stetige Kontrollierbarkeit durch einen (zwingenden) Blick gewährleistet. „Der perfekte Disziplinarapparat wäre derjenige, der mit nur einem einzigen Blick ermöglichte, dauernd alles zu sehen.“[77]

Das Verhalten, die Taten und die Leistungen der Individuen werden überwacht und protokolliert, im Hinblick auf Normen *verglichen*. Es handelt sich um eine wertende Messung: Die Individuen werden untereinander *differenziert* und *hierarchisiert*, sie werden gezwungen sich anzupassen (*homogenisiert*) und es wird eine Grenze zu anormalem Verhalten bzw. Anormalem gezogen, welche *ausgeschlossen* werden. Die Disziplinarmacht wirkt normendund normierend.[78]

Die Kontrolle findet dabei nicht nur von oben nach unten, sondern auch von unten nach oben und zur Seite statt. Die Menschen kontrollieren und disziplinieren sich gegenseitig. Die Individuen überwachen aber nicht nur andere, sondern auch sich selbst. Das Subjekt soll sich nicht nur in das Normengefüge integrieren, vielmehr soll es die Normen internalisieren, sie als seine eigenen Normen verinnerlichen und wahrnehmen.[79]

> „Diese Vorstellungen gipfeln im Panoptikum, einem Gefängnis, das architektonisch die perfekte Überwachung seiner Insassen gewährleistet. Das [von Jeremy Bentham 1787 entwickelte] Panoptikum ist ein ringförmiges Gebäude in dessen Mitte sich ein Turm befindet. Der Turm sichert die perfekte Einsehbarkeit des Gebäudes, von welchem aus nicht festgestellt werden kann, ob und wann eine Überwachung stattfindet. Es muss daher von einer stetigen Überwachung ausgegangen werden, ohne dass diese tatsächlich stattfindet. Der Insasse internalisiert die Überwachung und normalisiert sich selbst.“[80]

Das Panoptikum automatisiert und entindividualisiert die Macht. Die Macht liegt nicht bei einer Person, sondern in einer Apparatur, die eine Machtasymmetrie generiert. Die überwachende Person ist austauschbar, sie ist nur ein Rädchen in einer Kontrollmaschinerie.[81]

[76] Foucaultsche Machttechnik durch Zuweisung eines Ortes in einem Raum.
[77] Foucault 1994: S. 224.
[78] Ebd.: S. 236.
[79] Ruoff 2009: S. 149 f.
[80] Tremmel 2012b: S. 7.
[81] Foucault 1994: S. 259 f.

> „In seinem durchsichtigen kreisrunden Käfig auf dem hohen Turm von Wissen und Macht mag es Bentham darum gehen, eine vollkommene Disziplinarinstitution zu entwerfen; aber es geht auch um den Aufweis, wie man die Disziplinen »entsperren« und diffus, vielseitig, polyvalent im gesamten Gesellschaftskörper wirken lassen kann.“[82]

Foucault abstrahiert aus der physischen Architektur des Panoptikums dessen Wirkungszusammenhang und entwickelt daraus das *panoptische Prinzip*, welches immer dann zum Einsatz kommen könne, wann immer man es mit einer Vielfalt an Individuen zu tun habe, denen eine Aufgabe oder ein Verhalten aufzuzwingen sei.[83] Benthams Panoptikum wird so zu einem Prototyp einer Machtwirkung, die sich durch (scheinbar) ununterbrochene Beobachtung entfalten kann. „Das Sichtbarkeits- und Disziplinarregime des [Panoptikum] ließ sich in Fabriken, Schulen, der Armee, und dem modernen Wohlfahrtsstaat insgesamt wiederfinden.“[84] Foucault verwendet das Panoptikum als Metapher für die moderne Gesellschaft, die Disziplinargesellschaft.[85]

2.3 Sicherheitsgesellschaft

Die Disziplinargesellschaft gerät in der zweiten Hälfte des 20. Jahrhunderts in die Krise und wird von der Sicherheitsgesellschaft abgelöst. Es handelt sich dabei um einen fließenden Übergang, so sind Elemente der Disziplinargesellschaft auch in der Sicherheitsgesellschaft weiterhin vorhanden.[86] Mit der Sicherheitsgesellschaft halten neue Konzepte Eingang in das Repertoire der sozialen Kontrolle: das wichtigste Konzept ist die Verwaltung des empirisch Normalen.

Im Gegensatz zu der disziplinargesellschaftlichen Norm, einer starren Verhaltensregel der entsprochen werden musste, nimmt die Verwaltung des empirisch Normalen die vorgefundene Realität in den Fokus: Normal ist nun der gesellschaftliche Durchschnitt. Das Individuum muss sich dabei nicht mehr an einem festen Ideal ausrichten - es kann unter einer Vielzahl von Verhaltensoptionen wählen. Allerdings muss es dabei beachten, dass es nicht bestimmte Toleranzgrenzen überschreitet, die es zum

[82] Foucault 1994: S. 268. Hervorhebung im Original.
[83] Ebd.: S. 264.
[84] Zurawski 2015: S. 27.
[85] Kroener und Neyland 2014: S. 144.
[86] Deleuze 1993: S. 254; Kammerer 2011: S. 28.

Risiko werden lassen. Abweichung wird insofern nicht mehr als zu behandelnder „Defekt“ verstanden, sondern als zu verwaltende gesellschaftliche Realität. Es geht um eine „möglichst effektive, ökonomische Erfassung und Bearbeitung der erwartbaren und als normal verstandenen Abweichung“.[87] Hierbei wird mit Wahrscheinlichkeiten und Risikofaktoren gearbeitet. Im Unterschied zu konkreten Gefahren sind Risiken zwar abstrakt, dafür aber statistisch berechenbar - so kann schon weit im Vorfeld einer Gefahr, aufgrund eines Verdachts, einer Wahrscheinlichkeit präventiv interveniert werden. Dabei findet weniger eine Orientierung an Individuen statt, sondern an spezifischen Situationen und Gruppen. In einem Satz: Von Interesse ist die Zugehörigkeit zu einer Risikogruppe, also eine Prognose auf Basis bestimmter Kriterien, die zu einer präventiven Verwaltung führt. Exemplarisch dafür steht die Vorverlagerung polizeilicher Eingriffsbefugnisse, wie dem Einsatz verdeckter Ermittler_innen, verdachtsunabhängige Personenkontrollen und teilweise auch Telekommunikationsüberwachung.[88]

> „Anders gesagt, das Gesetz verbietet, die Disziplin schreibt vor, und die Sicherheit hat - ohne zu untersagen und ohne vorzuschreiben, wobei sie sich eventuell einiger Instrumente in Richtung Verbot und Vorschrift bedient - die wesentliche Funktion, auf eine Realität zu antworten, so daß die Antwort die Realität aufhebt, auf die sie antwortet - sie aufhebt oder einschränkt oder bremst oder regelt.“[89]

Es sollen Probleme und Gefahren ermittelt werden, die die Gesamtheit der Gesellschaft betreffen. Diese sollen ökonomisch und effektiv gehandhabt werden. Es geht um „eine möglichst frühzeitige Erkennung und Abwendung von Grenzüberschreitungen einerseits sowie eine Unschädlichmachung bei nicht mehr hinnehmbaren Fällen oder Wiederholungstätern andererseits“.[90]

Soziale Kontrolle in der Sicherheitsgesellschaft arbeitet mit verschiedenen Techniken. Im Folgenden sollen diese kurz vorgestellt werden.

[87] Singelnstein und Stolle 2012: S. 65.
[88] Lemke 2014: S. 188; Singelnstein und Stolle 2012: S. 63 ff; Foucault 2006: S. 19 f, 78 f.
[89] Foucault 2006: S. 76.
[90] Singelnstein und Stolle 2012: S. 65.

2.3.1 Selbstführungstechniken

An die Stelle der Selbstdisziplinierung (Disziplinargesellschaft) treten in der Sicherheitsgesellschaft die Selbstführungstechniken. Das Verhalten wird von alleine und vermeintlich selbstgewollt an antizipierte Standards angepasst. Konformität wird nicht mehr durch Unterdrückung bestimmter Verhaltensweisen gewährleistet, vielmehr werden inhaltliche Vorgaben mit Freiräumen verbunden. Das Subjekt kann sich auf verschiedene Weise verhalten, muss aber mit den Konsequenzen seines Verhaltens leben. Dabei werden bestimmte Verhaltensweisen gefördert und andere erschwert. Damit funktionieren die Selbstführungstechniken nicht absolut, sondern schaffen (Verhaltens-)Wahrscheinlichkeiten.[91]

Eine wesentliche Grundlage für die Selbstbeschränkung und -führung stellt eine steigende gesellschaftliche Verunsicherung dar. Dabei erfüllen die Sicherheitsdiskurse die Funktion, eine permanente Verunsicherung zu gewährleisten. Die (Sicherheits-)Diskurse beschreiben nicht die Wirklichkeit, sondern konstituieren sie und werden so zur wahrgenommenen „Wahrheit“.[92]

2.3.2 Kontrolltechniken

Die Kontrolltechniken umfassen zunächst klassische Strategien der Überwachung, diese werden in zunehmenden Maße technisiert, automatisiert und computergestützt.[93] Es geht ihnen darum, auf Basis der Überwachung, *Risikopotentiale* zu erkennen um diesen frühzeitig begegnen zu können (Prävention). Die Detektion der Risiken funktioniert dabei zunehmend anlasslos und hat die Bestrebung, allgegenwärtig und umfassend zu sein. Durch die Zunahme der Kontrolle und der damit verbundenen Zunahme der Entdeckung neuer Risikofaktoren, steigt auch die Anzahl der Risikoträger_innen kontinuierlich an.[94]

Um die Risikofaktoren erkennen zu können, nutzen die Kontrolltechniken die moderne Datenverarbeitung, welche algorithmisch Muster, Regelmäßigkeiten und Abweichungen in großen Datenmengen erkennen und wiederfinden kann (Big Data). Dies wird zum einen zur Verhaltenskontrolle eingesetzt, zum anderen aber auch um Individuen zu konformem und unauffälligem Verhalten anzuleiten. Außerdem dient

[91] Ähnlich der „Unternehmer_in ihrer selbst“ im Wirtschaftsleben, die aufgrund prekärer Verhältnisse dazu angehalten ist, sich den ständig wechselnden Anforderungen anzupassen.
[92] Singelnstein und Stolle 2012: S. 34, 75 ff; Lemke 2004.
[93] Singelnstein und Stolle 2007a: S. 216.
[94] Singelnstein und Stolle 2012: S. 81 f, 119.

sie der Risikobeherrschung und -vermeidung.[95]

„Prävention will etwas Ungewolltes verhindern, sie will etwas ausschließen, von dessen Eintreten sie nie sicher wissen kann, weil es erst in der Zukunft liegt.“[96] Um diese Unwissenheit bändigen zu können, werden Informationen benötigt, massenhaft Informationen - zu Ende gedacht bedeutet Prävention absolute Kontrolle. Prävention ist aber nicht nur Überwachung und Kontrolle von oben, sondern dient auch dazu, „(fremdbestimmte) Logiken von den Subjekten als *eigene* Logik“[97] zu verinnerlichen (z.B. Gesundheitsprävention). Sie ist also auch im Bereich der Selbstführungstechniken (siehe oben) aktiv.

2.3.3 Ausschlusstechniken

Der sozialkontrollierende Ausschluss erlebt eine Renaissance. Menschen und Gruppen, denen die Fähigkeit zu Selbstführung abgesprochen wird und die auch mit Kontrolltechniken nicht mehr zu lenken sind, werden aus sozialen Strukturen oder bestimmten Räumen ausgeschlossen und/oder kriminalisiert. Häufig sind diese ökonomisch „überflüssig“, Randgruppen oder werden als für die Gesellschaft gefährlich eingestuft - und damit ihr Ausschluss gerechtfertigt.[98]

Die Freiheitsstrafe, ein klassisches Mittel des gesellschaftlichen Ausschlusses, vollzieht einen Funktionswandel. Sie setzt, vor allem in den USA, aber zunehmend auch in Deutschland, nicht mehr auf Resozialisierung und Besserung, sondern auf das simple Wegsperren der „Gefährlichen“. Weitere Beispiele für Ausschlusstechniken sind die Sicherheitsverwahrung, als dauerhafter Ausschluss aus der Gesellschaft, die Grenzzäune und -abschottungspolitik gegenüber Flüchtlingen, aber auch Betretungs- und Aufenthaltsverbote.[99]

[95] Singelnstein und Stolle 2012: S. 82; Singelnstein und Stolle 2007a: S. 216 f; Deleuze 1993: S. 261.
[96] Ullrich 2012: S. 211.
[97] Ebd.: S. 211. Hervorhebung im Original.
[98] Singelnstein und Stolle 2012: S. 120, 138.
[99] Singelnstein und Stolle 2007a: S. 218 f.

3 Geheimdienste und Telekommunikationsüberwachung

Im Folgenden wird der Untersuchungsgegenstand der Arbeit dargestellt. Zuerst soll Telekommunikation und ihr Wandel beschrieben werden. Anschließend wird geklärt, wie Geheimdienste durch unterschiedliche Tätigkeitsbereiche voneinander abzugrenzen sind und was im Zuge der vorliegenden Arbeit unter Geheimdienst verstanden wird. Danach sollen die Telekommunikationsüberwachungsprogramme der zuvor definierten Geheimdienste vorgestellt werden. Im nächsten Kapitel werden die Theorien der sozialen Kontrolle (Disziplinargesellschaft und Sicherheitsgesellschaft) sowie der Untersuchungsgegenstand der geheimdienstlichen Telekommunikationsüberwachungsprogramme zusammengeführt und analysiert.

3.1 Telekommunikation

Gesellschaften ohne Kommunikation sind undenkbar. In den letzten Jahren hat sich die Kommunikation durch die Computerisierung, das Aufkommen des Internets, mobiler Telefone und Smartphones massiv gewandelt. Ein Leben ohne medial vermittelte Kommunikation ist heutzutage kein leichtes Unterfangen. Im Gegenteil: für die meisten Menschen ist Telekommunikation zum Alltagsphänomen geworden.[100]

Telekommunikation ist die signalvermittelte Übertragung menschlicher Kommunikation über eine Distanz. Hierzu zählen beispielsweise (mobile) Telefonie, Messaging, Internetkommunikation (E-Mail, Voice over IP (VoIP), Social Media etc.), Satellitenkommunikation und Funk aber auch Massenmedien wie Fernsehen oder Rundfunk. Das Telekommunikationsgesetz (TKG) definiert Telekommunikation in den Begriffsbestimmungen als den „technische[n] Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen“.[101] Telekommunikationsanlagen werden als „technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können“ verstanden.[102]

Der technische Fortschritt und die Computerisierung entwickelten immer mehr Geräte und Möglichkeiten zur Telekommunikation. Dies führte zu einer immer wei-

[100] Höflich 2016: S. 1 ff.; Zurawski 2007: S. 10 f.
[101] TKG §3 Abs. 22.
[102] TKG §3 Abs. 23.

teren Zunahme, bis hin zu einer Omnipräsenz von mobilen Telekommunikationsmöglichkeiten (Handys, Smartphones, Tablets, Net- und Notebooks). Dieser Wandel zu immer mehr digitaler Kommunikation führt zu einem immer höheren Datenaufkommen. Im Jahr 2010 produzierten die Menschen mehr Daten an einem Tag, als sie von Beginn der menschlichen Existenz bis 2003 produzierten.[103]

Laut Statistischem Bundesamt nutzen im Jahr 2015 85% der Menschen in Deutschland das Internet, 70% auch mobil.[104] Weltweit nutzen zwei Drittel der Menschen das Internet, in den USA 90%, 88% in Großbritannien. 43% der Menschen besitzen ein Smartphone, 60% in Deutschland, 72% in den USA, 68% in Großbritannien.[105]

Parallel zu dieser Entwicklung avancierten viele Telekommunikationsfirmen Geschäftsmodelle, die nicht mehr auf eine monetäre Vergütung durch Kund_innen setzt, sondern auf Werbemaßnahmen.[106] Diese wurden im Laufe der Zeit immer weiter an die Interessen der Kund_innen angepasst. Um individuelle, kontextbezogene Werbung generieren zu können, benötigten die Anbieter Informationen über Nutzer_innen, die in Form ihrer Kommunikation, der besuchten Webseiten oder anderer Dienstleistungen bereits vorlagen. Mit dem Aufkommen immer größerer Speicherkapazitäten und Rechenleistung ließen sich diese immer besser analysieren und immer mehr Aussagen über Interessen, Gewohnheiten, Bedürfnisse und Wünsche der Nutzer_innen treffen. Im Internet ist Überwachung somit ein omnipräsentes Phänomen geworden.[107]

Hinter Big Data zur Analyse von Nutzer_innenverhalten und Big Data zu Massenüberwachung steckt dasselbe Prinzip: Man benötigt massenhaft Daten von Nutzer_innen und analysiert diese auf (verdächtige) Muster. Die westlichen Geheimdienste adaptierten dieses System um die Jahrtausendwende.[108]

3.2 Geheimdienste

Geheim- oder Nachrichtendienste (engl. Secret Service, Intelligence Service oder Intelligence) sind Organisationen, meist in Form von Behörden, welche Informationen

[103] Schneier 2015a: S. 18.
[104] Statistisches Bundesamt 2015.
[105] Poushter 2016: S. 4 ff.
[106] Zur Entwicklung der Geschäftsmodelle: Schneier 2015a: S. 50 ff.
[107] Lyon 2015: S. 50 ff.; Schneier 2015a: S. 32.
[108] Lyon 2015: S. 69.

aus öffentlichen und nicht öffentlich zugänglichen Quellen für die (politische) Exekutive eines Staates sammeln und auswerten.[109]

Je nach Ausgestaltung können Geheimdienste auch selbständig oder unter Zuhilfenahme des Militärs verdeckte Aktionen (Covert Actions) durchführen. Manche Geheimdienste können im Sinne einer Geheimpolizei direkte Zwangsmaßnahmen vollstrecken. Weitere Aufgabenbereiche können Spionageabwehr, Eigensicherung und Kommunikationssicherheit (z.B. Verschlüsselungsstandards für Regierungskommunikation) sein.[110]

Unterschieden wird zwischen Geheimdiensten die primär nach außen tätig werden (z.B. CIA, BND, NSA, MI6) oder solchen die innerhalb der Grenzen ihres Nationalstaates agieren (z.B. FBI, MI5, Bundesamt für Verfassungsschutz (BfV)).[111] Des weiteren werden Geheimdienste in unterschiedliche Aufgabengebiete unterteilt. Diese Unterteilung kann sowohl auf verschiedene Behörden entfallen (z.B. NSA, CIA) oder in verschiedenen Abteilungen des selben Geheimdienstes (z.B. BND).

Bei der Signal Intelligence (SIGINT) liegt der Fokus auf den Signalen - also elektronischer Kommunikation zwischen Menschen und/oder Maschinen und deren Analyse. Unterteilt wird diese wiederum in Communication Intelligence oder Fernmeldeaufklärung (COMINT), Electronic Intelligence (ELINT) und Foreign Instrumentations Intelligence (FISINT). COMINT umfasst jegliche Art von Telekommunikation. Hierzu zählen u.a. (mobile) Telefonie und Messaging, Internetkommunikation (E-Mail, VoIP, Social Media etc.), Satellitenkommunikation und Funk. Die ELINT konzentriert sich auf die Erfassung elektromagnetischer Signale, die keine (Tele-)Kommunikation enthalten (z.B. Erfassung von Radarsystemen). FISINT sammelt elektromagnetische Emissionen die bei der Entwicklung und Erprobung von Plattformen und Waffensystemen in anderen Staaten anfallen.[112]

Von der SIGINT wird die Human Intelligence (HUMINT) abgegrenzt. Im Unterschied zur SIGINT, die sich auf Signale und Datenübertragung konzentriert, erhebt die HUMINT Informationen von menschlichen Quellen (z.B durch Informant_innen, Beschattung, Verhöre, Folter etc.), die auch mit technischen Hilfsmitteln wie Wanzen, Kameras oder Richtmikrofonen stattfinden kann. Weitere Aufgabenbereiche sind Wirtschaftsspionage, im Geheimdienstjargon Competitive Intelligence (CI),

[109]Narr 2004: S. 80; Krieger 2009; Eichenberger 2013: S. 11 f.; Henze und Knigge 1997: S. 17 f.
[110]Henze und Knigge 1997: S. 17 ff.
[111]Narr 2004: S. 80 f.
[112]Bamford 2001: S. 16; National Security Agency 2009a; Piper 2015.

Operations Security (OPSEC), der Schutz vor anderen Geheimdiensten, oder Open Source Intelligence (OSINT), die das sammeln von öffentlich zugänglichen Informationen umfasst.[113]

Aufgabenverteilung und Anzahl der Geheimdienste unterscheidet sich von Staat zu Staat und hat teils organisatorische, rechtliche und/oder historische Gründe. Viele westliche Geheimdienste oder ihre Vorläufer wurden während der Weltkriege gegründet und konsolidierten sich Mitte des 20. Jahrhunderts mit dem Beginn des Kalten Krieges. In der bipolaren Welt bestand ihre Hauptaufgabe in der Aufklärung des sog. Kommunismus. Mit dem Zusammenbruch des Ostblocks waren die westlichen Geheimdienste ihrer Kernaufgabe oder ihres Hauptfeindes beraubt und gerieten in eine Krise. Diese konnten sie mit den Terroranschlägen des 11. September 2001 und dem damit verbundenen neuen Primärfeind internationaler Terrorismus überwinden. Im Rahmen der auf die Anschläge folgenden Anti-Terror-Gesetzgebung und des „War on Terror“ wurden die Befugnisse der Geheimdienste deutlich ausgeweitet. Bedeutung, Budget und Möglichkeiten des nachrichtendienstlichen Komplexes wuchsen dadurch immens.[114]

Westliche Geheimdienste arbeiten im Bereich der SIGINT eng zusammen. Es werden Überwachungsprogramme und -zentren gemeinsam betrieben, Daten, Analysen und Technologien ausgetauscht, verliehen oder verkauft. Die *Five Eyes*,[115] ein Zusammenschluss der Überwachungsgeheimdienste der Staaten USA, Großbritannien, Australien, Kanada und Neuseeland, betreiben einen (Groß-)Teil ihrer Überwachung gemeinsam. Die USA und Großbritannien (UKUSA) arbeiten mit ihren Diensten NSA und GCHQ noch enger zusammen. Die Staaten der Five Eyes sichern sich zu, sich nicht gegenseitig zu überwachen. Der BND gehört zur zweiten Riege (Tier B) der NSA-Partner, direkt nach den Five Eyes, und ist somit ebenfalls Teil des westlichen Geheimdienstnetzwerkes.[116] Die von der NSA entwickelte Software XKeyscore wird beispielsweise auch von GCHQ, BND und testweise vom Bundesamt für Verfassungsschutz[117] eingesetzt. Die Geheimdienste aus Kanada, Australien und Neuseeland haben ebenfalls zugriff. Auch das Social Media Überwachungsprogramm

[113] Bamford 2001: S. 16; National Security Agency 2009a; Piper 2015.

[114] Pütter 2009: S. 3; Rosenbach und Stark 2014: S. 115, 119; Piper 2015; Eichenberger 2013: S. 12 ff.; Schneier 2015a: S. 63.

[115] Die Five Eyes wurden 1941 von USA und Großbritannien gegründet (formell 1946). In den 1950er Jahren kamen mit dem aufflammenden Kalten Krieg Neuseeland, Kanada und Australien hinzu. Die NSA hat eine Schlüsselrolle im Bündnis inne.

[116] Greenwald 2014a: S. 174 ff.; MacAskill und J. Ball 2013; Snowden 2014b.

[117] Hier allerdings nur intern.

der NSA PRISM wird von GCHQ und BND verwendet. In Bad Aibling hat der BND eine Überwachungsstation der NSA übernommen und betreibt diese mit deren Unterstützung weiter. Dabei werden abgefangene Daten in großem Umfang weitergegeben. Um dies zu erleichtern gibt es ein Verbindungsgremium zwischen BND und NSA „Special U.S. Liaison Activity Germany“ (SUSLAG). BND und NSA führten im In- und Ausland gemeinsame Abhörprogramme, beispielsweise Operation Eikonal (2004 - 2008), durch.[118]

Der GCHQ lobt in einem internen Dokument die Fertigkeiten des BNDs Glasfaserleitungen mit einer max. Geschwindigkeit von 40 bis 100 GBit/s erfassen zu können, die eigenen Fähigkeiten lägen nur bei 10 GBit/s.[119] Die NSA Policy nennt als Ziel das Teilen der gesammelten Daten mit anderen Stellen: „SIGINT information originated by NSA/CSS shall be shared ... with U.S. Government customers and partners ... and with Foreign Partners... to the maximum extent possible“[120]

Offiziell überwachen die Geheimdienste nur die Telekommunikation ausländischer Bürger_innen massenhaft, nicht jedoch die der Menschen innerhalb ihres „eigenen“ Hoheitsgebietes.[121] Für die Telekommunikationsüberwachung im Ausland gelten keine rechtliche Einschränkungen. Dies ist zumindest in Deutschland umstritten. Führende Verfassungsrechtler sahen in einer Befragung vor dem NSA-Untersuchungsausschuss des Bundestages in der Auslandsüberwachung des BND keinen grundrechtsfreien Raum - in dem sich allerdings der BND sieht.[122]

Allerdings gilt die Regel der „rein ausländischen Überwachung“ ohnehin nicht generell: Telekommunikation ist spätestens in Zeiten des Internets international geworden und es ist nicht ohne weiteres bzw. ohne Überwachung feststellbar, zu welchem Nationalstaat die Kommunikationsteilnehmer_innen gehören. Um die abgefangenen Daten von der Telekommunikation der „eigenen“ Bürger_innen zu trennen, entwickelten die Geheimdienste technische Filtersysteme. Diese arbeiten jedoch nicht 100% zuverlässig.[123]

Die NSA sieht grundsätzlich alle Telekommunikation, die zwischen den USA und anderen Staaten geführt wird als ausländische Kommunikation an. Sie unterliegt

[118] Piper 2015; Marquis-Boire, Greenwald und Lee 2015.
[119] Rosenbach und Stark 2014: S. 126 f.
[120] National Security Agency 2007: Folie 3, Auslassungen im Original.
[121] Gezielte Telekommunikationsüberwachung durch Inlandsgeheimdienste unter strengeren Bedingungen ist hingegen üblich.
[122] Greenwald 2013; Meister 2014a.
[123] vgl. zu Funktion und Zuverlässigkeit der G10-Filter des BND Biselli 2015a.

dadurch nach Ansicht der NSA keinerlei rechtlichem Schutz. Der GCHQ geht indes noch weiter und sieht auf Basis einer Gesetzeslücke Metadaten[124] als generell nicht geschützt an, auch von Bürger_innen aus Großbritannien oder der Five Eye Mitgliedsstaaten. Für die Daten, die der GCHQ von der NSA erhält, gelten jedoch die etwas strengeren Regeln der NSA (außer für britische Bürger_innen).[125]

Da Geheimdienste Daten untereinander austauschen, können sie die illegale Überwachung der „eigenen" Bürger_innen von anderen Geheimdiensten erledigen lassen oder an diese weitergeben. Beispielsweise sieht das Abkommen zur Nutzung der NSA-Software XKeyscore beim Verfassungsschutz vor, dass dieser der NSA dafür im Gegenzug Daten weitergibt.[126] Hinzu kommen etliche gesetzliche Ausnahmen und weitreichende Interpretationen, die den Geheimdiensten ermöglichen, die Bevölkerung ihres Landes zu überwachen. Diese unterliegt in den meisten Ländern einer Erlaubnisinstanz (USA: Foreign Intelligence Surveillance Court (FISC), BRD: G-10-Kommission).

Die vorliegende Arbeit wird sich ob der Zielsetzung auf westliche Geheimdienste, die der Signal Intelligence (SIGINT), spezieller der Communication Intelligence (COMINT) zuzuordnen sind, beschränken. Die Five Eyes und der BND sind derart eng verzahnt und arbeiten so eng zusammen, dass die Arbeit sie als einen Untersuchungsgegenstand behandelt und sie im Folgenden als Geheimdienste bezeichnen wird. Dabei möchte die Arbeit nicht die Geheimdienste selbst untersuchen, sondern ihre Programme zur Telekommunikationsüberwachung, deren erklärtes Ziel die Überwachung jeglicher menschlicher Telekommunikation ist.[127] Der Fokus wird dabei auf der NSA, dem GCHQ und dem BND liegen. Dies hängt zum einen damit zusammen, dass die Snowden-Dokumente und der NSA-Untersuchungsausschuss des deutschen Bundestages sich explizit mit diesen befassen und daher die Quellenlage entsprechend aktueller und umfangreicher ist. Zum anderen arbeiten die drei Geheimdienste sehr eng zusammen.

Im folgenden stellt die Arbeit die wichtigsten Überwachungsprogramme und die zentralen Vorgehensweisen vor.

[124] Zudem definiert der GCHQ Metadaten weit. Diese umfassen nach Auffassung des GCHQ auch Zugangsdaten zu E-Mailaccounts.
[125] vgl. Government Communications Headquarters 2007.
[126] Biermann und Musharbash 2015.
[127] National Security Agency 2014: S. 146; Heumann und Scott 2013: S. 167 ff.; MacAskill und J. Ball 2013.

3.3 Überwachungsprogramme

Die Geheimdienste arbeiten bei der massenhaften Telekommunikationsüberwachung mit der sogenannten *Heuhaufen-Theorie*. Die relevanten Daten sind metaphorisch die Nadel in jenem Heuhaufen. Um diese zu finden braucht es den kompletten Heuhaufen - also jegliche Telekommunikation weltweit.[128] Metaphorisch-idealtypisch geht es den Geheimdiensten in einem ersten Schritt darum, den Heuhaufen anzuhäufen - also massenhaft Daten an verschiedenen Stellen zu sammeln. In den nächsten Schritten wird der Heu- oder Datenhaufen gerastert und durchkämmt - teilweise werden für nicht notwendig erachtete oder illegale[129] Daten verworfen. Der Rest wird in verschiedenen Datenbanken abgelegt und für kurze Zeiträume oder bis auf unbestimmte Zeit in Geheimdienstrechenzentren gespeichert.[130]

Im Telekommunikationsbereich wird zwischen verschiedenen Datenarten unterschieden: Inhalts-, Meta- und Bestandsdaten. Bei einem Brief sind die Inhaltsdaten beispielsweise der Brief selbst. Die Meta- oder Kommunikationsdaten sind die Daten auf dem Briefumschlag - also von wem an wen, um welche Uhrzeit, von welchem Postkasten etc. pp. Stamm- oder Bestandsdaten dagegen sind zum Beispiel Name und Adresse der Nutzer_innen, darunter fallen aber auch Nutzungs- beziehungsweise Vertragsbeginn.

Metadaten werden häufig unterschätzt oder die daraus resultierenden Möglichkeiten und ihre Wichtigkeit, die sich auf den ersten Blick nicht erschließen, heruntergespielt. Metadaten sind normalerweise analytisch wertvoller und wichtiger, da sie in einer standardisierten Form vorliegen, mit welcher ein Computer rechnen, sie algorithmisch auswerten kann. Inhalte hingegen müssen aufwändig interpretiert und übersetzt werden.[131]

> „Metadata is extraordinarily intrusive. As an analyst, I would prefer to be looking at metadata than looking at content, because it's quicker and easier, and it doesn't lie."[132]

[128] Rosenbach und Stark 2014: S. 121; Schneier 2015a: S. 138; Lyon 2015: S. 68.

[129] Auch Geheimdienste sind Gesetzen unterworfen - allerdings sind diese oft sehr schwammig formuliert und juristisch unklar definiert. Die Geheimdienste entwickeln oft waghalsige juristische Begründungen für ihre Überwachungen - so dass letztlich kaum „illegale" Daten entstehen. Man könnte sagen, dass die Geheimdienste mittels kaum haltbarer juristischer Argumentationen oder Theorien, sowie Rechtslücken und juristischen Grauzonen ihre eigenen Freibriefe ausstellen.

[130] Tremmel 2013: S. 256, 258 – 259; Fennen 2013.

[131] Mehr zur Auswertung von Metadaten: Tremmel 2010: S. 16 f.

[132] Snowden 2014a: S. 66.

Die Metadaten einer Person spiegeln nahezu alle persönlichen Kontakte wieder. Dabei können Rückschlüsse auf Beziehungsintensitäten anhand des Kommunikationsverhaltens gezogen werden. Wird nur während der Arbeitszeiten kommuniziert oder auch vor und nach der Arbeit, ist der Kontakt vor allem am Wochenende intensiv, hält er auch während Urlauben und Auslandsaufenthalten an? Zusammen mit den Ortsdaten, beispielsweise des Mobiltelefons, lassen sich auch physische Treffen erkennen. Die Analyse des Beziehungsnetzwerks und der -strukturen sind so mächtig, dass zwischen Geschäftspartner_innen, Beziehungspartner_innen und Affären unterschieden werden kann. Es können automatisiert Rückschlüsse auf Beziehungsnetzwerke und -strukturen, Kommunikationswege und oft auch Inhalte gezogen werden:

> „So ließe sich Beispielsweise aus einem E-Mail-Kontakt mit einem auf Familienrecht spezialisierten Anwalt gefolgt von telefonischen Anfragen bei Wohnungsmaklern eine Scheidungsabsicht prognostizieren. Kontakte zu Konflikt- und Schwangerschaftsberatungen, spezialisierten Ärzten, Prostituierten, Telefonsex-Hotlines, spezialisierten Versandhändlern, Kreditvermittlern, Jobcentern, Umzugsservices, Interessenverbänden etc. ergeben aus einer minimalen Datenmenge jeweils umfangreiche Rückschlüsse auf das Privatleben eines Betroffenen.“[133]

Hinzu kommt die Möglichkeit, bestimmte Kommunikations- und Verhaltensmuster in den Daten zu finden und diese mit den genannten Mustern anderen Menschen abzugleichen.

Stewart Baker, ehemaliger Leiter der Rechtsabteilung der NSA, fasst die Bedeutung von Metadaten und Big Data gut zusammen:

> „Metadata absolutely tells you everything about somebody's life,[...] If you have enough metadata you don't really need content.... [It's] sort of embarrassing how predictable we are as human beings.“[134]

Ein zentraler Baustein in der Überwachungsarchitektur der NSA ist das PRISM-Programm. Die NSA hat durch PRISM Zugriff auf die Daten der Kund_innen von neun amerikanischen Internettelekommunikationsunternehmen (Microsoft, Yahoo,

[133]Kurz und Rieger 2009: S. 10.
[134]Baker, Stewart zitiert nach Alan Rusbridger 2013.

Google, Facebook, PalTalk, Youtube, Skype, AOL, Apple). Diese Firmen stellen populäre und viel genutzte Telekommunikationsplattformen bereit und haben abermillionen an Nutzer_innen. Die NSA kann mit PRISM auf die Internetsuchabfragen, E-Mails, Chats, Videos, Fotos, Internet(video)telefonie und weitere Daten, die die Nutzer_innen in ihren Onlinespeichern ablegen oder über die Plattformen teilen, zugreifen. Beispielsweise durchsuchen mehr als 90% der deutschen Internetnutzer_innen das Netz mit Google; Facebook steuert weltweit gerade auf 1,5 Milliarden aktive Nutzer_innen zu und wird von 71% der Erwachsenen in den USA verwendet, Skype nutzen 300 Millionen Menschen auf der Welt.[135] Die Masse und Bedeutung der Daten ist nicht zu unterschätzen: PRISM ist eines der wichtigsten Programme für die tägliche Unterrichtung des Präsidenten der USA („President's Daily Brief").[136]

UPSTREAM sammelt die Daten nicht wie PRISM direkt bei Internettelekommunikationsunternehmen, sondern macht sich den Aufbau des Internets zu nutze. Dieses ist primär ein Netz aus Kabeln und Verteilern (Routern). Es gibt lange Unterseekabel, die ganze Kontinente verbinden, und große und kleine Knotenpunkte, an denen sich die Kabel aus verschiedenen Ländern oder von verschiedenen ISPs (Internet Service Provider) treffen. Diese Kabel und Knotenpunkte sind das Rückgrat des Internets. Durch Zugriff auf die Knotenpunkte oder die Unterseekabel, kann das Internet im großen Stil überwacht werden. Die Telekommunikationsüberwachung direkt an der Kommunikationsinfrastruktur wird UPSTREAM genannt.

Wichtige Unterseekabel, die Europa mit den USA verbinden, landen in Großbritannien an. Durch diese Kabel flossen 2010 ca. 25% des kompletten Internettraffics.[137] Der britische GCHQ nutzt dies mit dem Programm TEMPORA aus: Die Daten, die nach oder durch Großbritannien fließen, werden mit TEMPORA abgefangen und für 3 Tage komplett gespeichert - ein sogenannter „Full Take". Die Metadaten werden für 30 Tage gespeichert. Um den vorhandenen Speicherplatz sinnvoll zu nutzen wird ein Teil des Traffics aussortiert (beispielsweise P2P Downloads oder Videotraffic). 2012 waren mehr als 1'000 Server im Einsatz, die täglich 40 Milliarden Inhalte zur Verfügung stellen. Der Fokus liegt dabei auf dem Nahen Osten, Nord Afrika und Europa.[138] Die Daten werden mit dem Kooperationspartner NSA geteilt. Etwa 250 Analyst_innen aus den USA und 300 aus Großbritannien haben Zugriff

[135] Greenwald und MacAskill 2013; National Security Agency 2013: Folie 5 f.; Rosenbach und Stark 2014: S. 132; Appelbaum et al. 2014.
[136] Greenwald 2014a: S. 164; Rosenbach und Stark 2014: S. 133.
[137] Government Communications Headquarters 2010: Folie 3.
[138] National Security Agency 2012d: S. 2.

auf die Daten von TEMPORA.[139]

Um an die Daten, die über die Telekommunikationsnetze transportiert werden, heranzukommen, arbeiten die Geheimdienste eng mit den ISPs zusammen. Die NSA hat mit den „Special Sources Operation“ (SSO) eine eigene Unterabteilung, die sich um die Kooperationsprogramme kümmert. BLARNEY und FAIRVIEW sind die Namen solcher Kooperationen zwischen der NSA und dem amerikanischen Telekommunikationsanbieter und ISP AT&T, der weltweit aktiv ist. Über AT&T kommt die NSA an Daten aus den Ländern Deutschland, Frankreich, Griechenland, Brasilien, Israel, Italien, Mexiko, Südkorea, Japan, Venezuela, der Europäischen Union und den Vereinten Nationen. Allein FAIRVIEW sammelte im Dezember 2012 200 Millionen Datensätze pro Tag und rangiert damit regelmäßig in den Top 5 der NSA-Überwachungsprogramme. Als STORMBREW bezeichnet die NSA eine Kooperation mit dem FBI und dem amerikanischen ISP Verizon - und damit den Zugang zu Glasfaserleitungen an der Ost- (QUAILCREEK) und Westküste (BRECKENRIDGE) der USA. Unter dem Decknamen OAKSTAR wird mit mehreren nicht bekannten Telekommunikationsunternehmen kooperiert. Für den Zugang bezahlt die NSA jährlich Millionenbeträge an die Unternehmen.[140]

Jenseits der freiwilligen Kooperationen, in denen durchaus ein partnerschaftliches Verhältnis herrschen kann (beispielsweise NSA und AT&T), arbeiten die Geheimdienste auch mit Zwang[141] oder greifen heimlich auf die Telekommunikationsverkehre zu (beispielsweise durch Auftrennung der Glasfaserstrecke (Splicing) an eigenen Zugangspunkten).[142]

Jenseits der Zusammenarbeit mit US-Anbietern und der USA, arbeitet die NSA mit anderen Geheimdiensten, die auch zur zweiten Riege (Tier B) gehören, im Projekt RAMPART-A zusammen. Meist zapfen die Partner einen Knotenpunkt oder eine Glasfaserleitung, auf die sie Zugriff haben, mit technischer Unterstützung der NSA, an. Aus den gesammelten Daten wird sowohl die amerikanische, als auch die Kommunikation des zum kooperierenden Geheimdienst gehörenden Landes, ausge-

[139] Rosenbach und Stark 2014: S. 124 ff.; Fuchs und Goetz 2013: S. 170 ff.; MacAskill und J. Ball 2013; Lyon 2015: S. 70; Government Communications Headquarters 2012f: S. 1 f.; Ermert und Holland 2015: S. 73.

[140] Greenwald 2014a: S. 153 ff.; National Security Agency o. J.

[141] In den USA können Provider mit einem National Security Letter (NSL) zur Kooperation gezwungen werden. Den betroffenen Unternehmen ist es dabei untersagt, an die Öffentlichkeit zu gehen oder mit anderen Menschen über den NSL zu reden.

[142] Meister 2013.

filtert.[143] Zum Teil arbeitet die NSA mit einem Trick: Sie sammelt beispielsweise einmal in Zusammenarbeit mit Dänemark Daten am eine Ende einer Glasfaserleitung und filtert die dänische Kommunikation aus. Gleichzeitig kooperiert sie mit der BRD am anderen Ende der Leitung und filtert dort die deutschen Daten aus. Durch die doppelte Sammlung bekommt sie am Ende alle Daten.[144]

Als Gegenleistung für den Zugriff auf die Glasfaserleitungen gibt die NSA den Partnergeheimdiensten Zugang zu ihrem anspruchsvollen Überwachungsequipment. RAMPART-A umfasst Codenamen für 13 Stationen von denen 2013 9 aktiv waren. Es wurden 3 Terabits pro Sekunde erfasst, das sind 375 Gigabyte pro Sekunde, 22,5 Terabyte pro Minute oder 32'400 Terabyte pro Tag. Die Daten flossen in über 9'000 SIGINT-Berichte der NSA ein.[145]

Unter dem Namen „Operation Eikonal" kooperierten der BND, die NSA und das deutsche Telekommunikationsunternehmen Telekom und leiteten mindestens zwischen 2006 und 2008[146] die Kommunikations-Rohdaten am Frankfurter Knotenpunkt der Telekom aus. Die Daten wurden von der Telekom an den BND und gefilterte Auszüge an die NSA weitergegeben. Neben dem Telekomknoten ist in Frankfurt auch der Internetknotenpunkt DE-CIX ansässig. Hier tauschen 600 Provider (nicht die Telekom) Daten aus. Am DE-CIX greift der BND seit 2009 direkt Daten ab.

In Bad Aibling übernahm der BND eine Überwachungsstation der NSA und sammelt dort Daten (Satellitenüberwachung) - auch für die NSA.[147] Leider ist über die BND-Programme recht wenig bekannt.[148] Geschwärzte Listen im NSA-Untersuchungsausschuss legen allerdings nahe, dass mindestens zwölf weitere derartige Programme existieren oder bis vor kurzem existierten.[149]

Die exemplarisch vorgestellten Programme werden durch viele weitere ergänzt. Hier eine Auswahl: MUSCULAR greift Daten ab, die Google und Yahoo intern zwi-

[143] R. Gallagher 2014a; Meister 2014b.
[144] Meister 2014b.
[145] R. Gallagher 2014a; Meister 2014b.
[146] Die Operation Eikonal wurde bereits 2004 begonnen, allerdings wurden anfangs „nur" Telefonleitungen angezapft. Erst 2005 begannen die Geheimdienste Internetkommunikation auszuleiten. Aufgrund technischer Probleme begann die Sammlung erst 2006. EIKONAL war vermutlich Teil von RAMPART-A unter dem CODENAMEN WHARPDIVE.
[147] Mascolo, Leyendecker und Goetz 2014; Fuchs und Goetz 2013: S. 175 ff.; DE-CIX o. J.
[148] Im NSA-Untersuchungsausschuss werden vor allem die bereits eingestellten Programme (EIKONAL, GLOTAIC) behandelt. Programme die der BND noch immer alleine, mit anderen Staaten als den Five Eyes oder im Ausland betreibt, sind nicht Teil des Untersuchungsgegenstandes. (Meister 2015a)
[149] Ebd.

schen ihren Rechenzentren transportieren.[150] Mit OPTIC NERVE speichern GCHQ und NSA Standbilder aus Yahoo-Videochats (möglicherweise auch von anderen Anbietern), darunter auch sexuelle Handlungen. Innerhalb von 6 Monaten waren 1,8 Millionen Nutzer_innen betroffen. Der GCHQ nutzte die Daten auch um seine Gesichtserkennungssoftware zu testen.[151] Mit DISHFIRE fängt die NSA täglich 194 Millionen SMS auf der ganzen Welt ab (Stand April 2011). Mit PREFER werden die SMS sortiert und vorausgewertet. So werden zum Beispiel Grenzübertritte durch Roaming-Nachrichten[152] erkannt.[153] CO-TRAVELLER wertet die Standorte von hunderten Millionen Handys und den Wechsel zwischen Funkzellen aus.[154] Die NSA kann durch eine Analyse des gemeinsamen Aufenthalts und Wechsels in beziehungsweise zwischen Funkzellen die Zusammengehörigkeit von Personen(-gruppen) feststellen.[155] Ein weiteres Ziel der NSA sind Adressbücher: Allein an einem Tag sammelte sie 2012 33'697 E-Mail-Adressbücher bei GMail, 82'857 bei Facebook, 105'068 bei Hotmail, 444'743 bei Yahoo und 22'881 von anderen nicht genannten Anbietern. Über ein Jahr sammelte sie 250 Millionen Adressbücher aus unterschiedlichen Quellen.[156] Es existieren unzählige weitere veröffentlichte und nicht veröffentlichte Überwachungsprogramme und Techniken. Eine Übersicht der bisherigen Original Präsentationen und Texte findet sich im Snowden Archive[157] der Canadian Journalists for Free Expression (CJFE).

Häufig sammeln die Geheimdienste mit unterschiedlichen Programmen die gleichen Daten. Beispielsweise wird die Google Kommunikation sowohl Upstream von Programmen wie BLARNEY oder TEMPORA, direkt bei Google durch PRISM und zwischen den Rechenzentren von Google mit MUSCULAR erfasst. Das hat mehrere Vorteile: Zum einen arbeiten die Dienste redundant, sollte ein Überwachungsprogramm ausfallen kommt der Geheimdienst immer noch über ein anderes Programm an einen Großteil der Daten. Durch evtl. bestehende technische oder rechtliche Beschränkungen erfassen die Programme zudem jeweils Daten, die die

[150] Greenwald 2014a: S. 142.
[151] Froitzhuber 2014.
[152] Eine Hinweis-SMS, dass man mit einem Anbieter in einem anderen Land verbunden ist, wofür evtl. zusätzliche Gebühren anfallen können.
[153] National Security Agency 2011.
[154] Der Bereich um einen Handymast (zu diesem verbindet sich das Handy per Funk), in dem das Signal empfangen werden kann.
[155] Toh, Patel und Goitein 2016: S. 6 f.
[156] Gellman und Soltani 2013.
[157] https://snowdenarchive.cjfe.org

anderen Programme nicht erfassen konnten.

Die (Meta-)Daten, die die NSA und ihre befreundeten Geheimdienste tagtäglich abfangen und speichern, werden mit dem Programm BOUNDLESS INFORMANT live gezählt[158] und auf einer Weltkarte grafisch dargestellt. [159] Sie lassen sich nach Land und Art der Daten sortieren, sowie als Diagramm oder Tabelle ausgeben. Ziel ist es, die geheimdienstlichen Aktivitäten in verschiedenen Länder zu dokumentieren. Innerhalb von 30 Tagen wurden 2013 97 Milliarden E-Mails und 124 Milliarden Telefonate weltweit gezählt. Aus Deutschland wurden 500 Millionen Datensätze gesammelt.[160]

Zusammengefasst ergibt sich aus dieser skizzierten Auswahl geheimdienstlicher Überwachungsprogramme eine Vorstellung der umfassenden Überwachungskapazitäten und der geheimdienstlichen Zusammenarbeit um das „Internet zu beherrschen“[161], wie es der GCHQ formuliert. Es geht also um eine Herrschaft, eine Kontrolle der menschlichen Telekommunikation - und damit um die Kontrolle der Menschen selbst. Diese Kontrolle wird allerdings nicht allein durch das reine Sammeln, sondern durch die Auswertung der Daten vorgenommen. Jene Auswertungsprogramme werden im Rahmen der Analyse der geheimdienstlichen Telekommunikationsüberwachung mit den Theorien der sozialen Kontrolle in der Disziplinar- und Sicherheitsgesellschaft vorgestellt.

3.4 Soziale Kontrolle durch Telekommunikationsüberwachung

Die Geheimdienste sammeln mit den vorgestellten Überwachungsprogrammen umfassend Daten eines Großteils der menschlichen (Tele-)Kommunikation, mit dem Ziel, diese Überwachung immer weiter auszubauen. Die Ideologie dahinter lässt sich vereinfacht als 'viel hilft viel' (Heuhaufen-Theorie) beschreiben. In dieser stellt jeder Mensch eine potentielle Terrorist_in, Feind_in oder zumindest ein Risiko dar. Letztlich wird hiermit die ganze Menschheit unter Verdacht gestellt und deren Über-

[158] BOUNDLESS INFORMANT erfasst nicht alle SIGINT-Daten (vgl. National Security Agency 2012a: S. 2). Beispielsweise werden besonders sensitive Daten, die als ECI (Exceptionally Controlled Information) eingestuft werden, nicht erfasst. ECI steht über TOP SECRET und beinhaltet Daten die grundsätzlich nicht aufgeschrieben werden. Dazu gehören Namen von Firmen deren Kryptografie absichtlich geschwächt wurde oder Agent_innen die ausländische IT-Firmen infiltriert haben. (Schneier 2014b)

[159] Der damalige NSA-Direktor Keith Alexander hatte den US-Kongress bei einer Anhörung belogen, als er behauptete, die NSA führe keine zahlenmäßige Erfassung der abgegriffenen Daten durch.

[160] National Security Agency 2012a: S. 1; Greenwald 2014a: S. 140.

[161] MacAskill, Borger et al. 2013.

wachung gerechtfertigt. Die Geheimdienste betreiben mit ihren Programmen ein groß angelegtes, kontinuierliches Monitoring des alltäglichen und nicht alltäglichen Lebens der Bevölkerung. Durch die immer weiter- und tiefergehende Überwachung sollen letztlich die Gedanken, das Innerste der Menschen, kontrolliert werden, um eine Abweichung festzustellen und diese entsprechend behandeln zu können.[162] Dies kann mit (un-)mittelbaren, präventiven und reaktiven Mitteln oder Sanktionen erfolgen. Dabei kann auf die Weitergabe von Daten und Einschätzungen (siehe 4.1.) gesetzt werden, aber auch eigene Aktionen (siehe 5.3.2) ausgelöst werden, welche die Menschen zur Einhaltung von Normen bewegen sollen. Geheimdienste stellen hierdurch eine Instanz der sozialen Kontrolle dar.

Im Folgenden analysiert die Arbeit die Überwachungstätigkeit der Geheimdienste als eine Instanz der sozialen Kontrolle, mit den Regimen der Disziplinar- und Sicherheitsgesellschaft und ihren spezifischen Techniken.

[162]National Security Agency 2014: S. 146; Zurawski 2007: S. 16; Benkel 2011: S. 109; Lyon 2015: S. 71.

4 Geheimdienstliche Sozialkontrolle in der Disziplinargesellschaft

Das Ziel der Disziplinargesellschaft ist die Dressur der Körper. Dies geschieht mit Hilfe der Disziplinarmacht, welche die Individuen überwacht und normiert, was zu dauerhaftem, persönlichkeitsprägendem Verhalten führt. Es geht darum, Normen festzuschreiben, ihre Einhaltung zu überwachen und etwaige Nicht-Einhaltung zu sanktionieren. Ziel ist es, die vollständige Einhaltung der Normen durchzusetzen und Devianz auszuschließen, beziehungsweise durch normierende Sanktionen zu reintegrieren. Dabei wirkt die Disziplinarmacht horizontal, durch eine wechselseitige Kontrolle und Selbstdisziplin, dezentral und weitgehend depersonalisiert.[163]

Für Foucault stellt das Panoptikum eine Verallgemeinerung der Disziplinen dar. Es handelt sich um einen „einfachen und leicht zu übertragenden Mechanismus [der] das elementare Funktionieren einer von Disziplinarmechanismen vollständig durchsetzten Gesellschaft“[164] beschreibt.

Obgleich die Disziplinargesellschaft - und mit ihr das Panoptikum - sukzessive von der Sicherheitsgesellschaft abgelöst wird, bleiben auch weiterhin disziplinargesellschaftliche Elemente und Techniken bestehen. Diese entfalten soziale Kontrollwirkungen und werden im Rahmen der Arbeit auf ebendiese untersucht. Auf den folgenden Seiten werden die wichtigsten Techniken und Funktionsweisen der Disziplinargesellschaft abgeleitet und auf die geheimdienstliche Telekommunikationsüberwachung angewandt.

4.1 Normen und Sanktionen

Die Disziplinargesellschaft zeichnet sich durch einen allgemeingültigen, öffentlich bekannten Normenkatalog aus. Dieser besteht sowohl aus Gesetzen, als auch aus nicht kodifizierten gesellschaftlichen Reglementierungen, deren kontinuierliche Einhaltung als Anforderung an das Subjekt gestellt wird. Diese teilen binär in Gebote und Verbote ein. Es wird zwischen normal und anormal unterschieden.[165]

Die NSA arbeitet unter anderem nach geheimen Aufgabenkatalogen, welche Definitionen, Verfahrensweisen und Prioritäten regeln. Ein Beispiel dafür ist das vom

[163] Bogdal 2008: S. 74.
[164] Foucault 1994: S. 268.
[165] Singelnstein und Stolle 2012: S. 61 f.

Weißen Haus und amerikanischen Geheimdiensten periodisch erstellte „National Intelligence Priorities Framework“ (NIPF).[166] Dieses definiert und priorisiert die Bereiche und Länder, in welchen ein „potential to greatly harm the U.S. or its interests“[167] gesehen wird. Daneben existiert die „Watchlisting Guidance“; Sie ist ein 166 seitiger Kriterienkatalog, der von amerikanischen Geheimdiensten, Militär und Strafverfolgungsbehörden erstellt wurde. Er gibt den Beamt_innen eine Orientierungshilfe, um Terrorist_innen zu erkennen und regelt das weitere Verfahren um (potentielle) Terrorist_innen beispielsweise auf eine Watchlist (siehe 5.4) zu setzen. Diese Listen dienen dazu, (potentielle) Terrorist_innen bei Kontrollen wiederzuerkennen und entsprechend der Liste zu behandeln (z.B. kein Flugzeug betreten zu lassen).[168] In der Watchlisting Guidance wird u.a. „Terrorismus und/oder terroristische Aktivitäten“ definiert:

> „(a) involve violent acts or acts dangerous to human life, property, or infrastructure that maybe a violation of U.S. law, or maybe have been, if those acts were committed in the United States; and (b) appear intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coerce a conduct of government by mass destruction, assassination, kidnapping, or hostage-taking. This includes activities that facilate or support TERRORISM and/or TERRORIST ACTIVITIES, such as providing a safe house, transportation, communications, funds, transfer of funds or other material benefit, false documentation or identification, weapons [...] explosives or trainingfot the commission of act of terrorism and/or TERRORIST ACTIVITY.“[169]

Ein „Suspected Terrorist“ (in Abgrenzung zu „Known Terrorist“) wiederum ist eine Person, bei der ein „hinreichender Verdacht“ („reasonable suspicion“) besteht, dass sie in terroristische Aktivitäten oder deren Unterstützung verstrickt ist. Es reicht allerdings auch aus, wenn eine Person verdächtigt wird, mit einer „verdächtigen Terrorist_in“ in Verbindung zu stehen.[170]

Die Definitionen sind äußerst schwammig: Um als „Suspected Terrorist“ eingestuft zu werden, braucht es keine Beweise, sondern es reichen Annahmen oder eine Kon-

[166] National Security Agency et al. o. J.
[167] National Security Agency / Central Security Service 2007: S. 2.
[168] National Counterterrorism Center 2013; Scahill und Devereaux 2014a.
[169] National Counterterrorism Center 2013: Appendix 1. Hervorhebung im Original.
[170] National Counterterrorism Center 2013: Appendix 1; Scahill und Devereaux 2014a.

taktschuld. Für eine Verhaltensnorm ist dies sehr vage und undurchsichtig. Zudem waren weder das NIPF noch die Watchlisting Guidance, bevor sie geleakt wurden, öffentlich bekannt. Die Disziplinargesellschaft erfordert aber ebendiese Bekanntheit der klaren Normen und die Kontrolle deren Einhaltung.

Das Gesetz stellt einen solchen klaren und öffentlich bekannten Normenkatalog dar. In der Terrorismusdefinition (s.o.) wird sich beispielsweise auch auf das Gesetz berufen, allerdings mit der Einschränkung „möglicherweise“. Die Geheimdienste arbeiten mit ihren Einschätzungen oft weit im Vorfeld strafbarer Handlungen und zudem international. Die Regelungen der westlichen Staaten oder im Falle der Watchlisting Guidance der USA, erreichen so weltweite Gültigkeit.[171]

Auch wenn Geheimdienste primär im Vorfeld strafbarer Handlungen und international agieren, arbeiten sie auch mit Strafverfolgungsbehörden zusammen. In Deutschland[172] wurden hierfür in den letzten Jahren „hybride Organisationen“ geschaffen, in denen Geheimdienste und Polizei zu bestimmten Themen zusammenarbeiten: Gemeinsames Terrorismusabwehrzentrum[173] (GTAZ), Gemeinsames Internetzentrum[174] (GIZ), Gemeinsames Extremismus- und Terrorismusabwehrzentrum[175] (GETZ), Gemeinsames Analyse- und Strategiezentrum illegale Migration[176] (GASIM).[177] Mit den Fusion Centers existieren in den USA und Großbritannien vergleichbare Institutionen.[178]

[171] Wird man auf die No-Fly-List gesetzt, bedeutet das beispielsweise, dass man kein Flugzeug betreten darf, dass die USA überfliegt. Ist man auf einer Kill-List kommt dies einem internationalen Todesurteil, ohne Gericht oder anderen rechtsstaatlichen Mitteln, gleich. (siehe Kapitel 5.4)

[172] In Deutschland gibt es ein Trennungsgebot zwischen Geheimdiensten und Strafverfolgungsbehörden. Dieses wird sukzessive abgebaut. Trafen sich seit 1982 Geheimdienste und Polizeibehörden vierteljährlich, werden seit den 1990er Jahren zunehmend engere Organisationsformen geschaffen.

[173] Gegründet 2004, arbeiten hier 40 Behörden zusammen, dazu gehören unter anderem der BND, BKA, LKA, Verfassungsschutz.

[174] 2007 gegründet, um den islamischen Terrorismus im Internet zu bekämpfen. Teil des GIZ sind u.a. BND, BKA und der Generalbundesanwalt beim Bundesgerichtshof.

[175] Wurde in Folge der Aufdeckung des NSU 2011 mit dem Namen und Aufgabenbereich Gemeinsames Abwehrzentrum gegen Rechtsextremismus (GAR) gegründet. 2012 wurde es umbenannt und um neue Aufgabenbereiche ergänzt: Terrorismus und sog. Extremismus im Bereich Ausländer und Linke sowie Spionage/Proliferation. Es arbeiten u.a. BND, Bundespolizei (BP), Generalbundesanwalt und Zollkriminalamt zusammen.

[176] Wurde 2006 mit dem Namen Gemeinsame Analyse- und Strategiezentrum Schleusungskriminalität (GASS) gegründet. Ziel ist es, der unerlaubten Einwanderung mit operativen und strategischen Maßnahmen entgegenzutreten. Die Organisation besteht u.a. aus Vertreter_innen von BND, BfV, BKA und BP.

[177] Wörlein 2008; Bundesministerium des Innern o. J.

[178] Kayyali 2014.

Zudem wurden Datenbanken zum Informationsaustausch zwischen Geheimdiensten und Strafverfolgungsbehörden geschaffen. In Deutschland existiert seit 2007 eine Antiterrordatei[179] (ATD).[180] In den USA gibt es mit ICREACH[181] eine Suchmaschine auf NSA-Datenbanken, die über 850 Milliarden Metadaten[182] umfasst. Auf diese haben über 1'000 Analyst_innen aus 23 Geheimdiensten und Strafverfolgungsbehörden Zugriff (Stand 2010). Dazu gehören unter anderem das FBI und die Drug Enforcement Administration (DEA). Diese können Selektoren (z.B. Telefonnummer oder E-Mailadresse) in eine google-artige Suchmaske eingeben und bekommen als Ergebnis die Kommunikationsbeziehungen, und damit das soziale Netzwerk, einer Person.[183]

Der britische GCHQ arbeitet ebenfalls Strafverfolgungsbehörden, aber auch der Bank of England, dem Familienministerium und weiteren, zu. Die Abteilung Joint Threat Research Intelligence Group (JTRIG) geht noch deutlich weiter als nur Informationen weiterzugeben. Sie nimmt Online Einfluss auf das Verhalten von Menschen. Sie versucht potentielle Kriminelle oder anderweitig als Risiko wahrgenommene Menschen und Gruppen, von bestimmten Handlungen abzubringen, abzuschrecken oder sie zu erniedrigen (siehe 5.3.2). JTRIG unterstützt die Strafverfolgungsbehörden auch technisch, beispielsweise hilft sie der Polizei bei der Umgehung von Verschlüsselungssoftware.[184]

Geheimdienste geben Strafverfolgungsbehörden immer wieder Daten aus ihren Überwachungsprogrammen weiter, sowohl in Form der oben genannten Fusion Center und Datenbanken, aber auch als direkte Hinweise oder Beweise auf (möglicherweise) geplante oder begangene Straftaten. So gab der BND kurz vor Silvester 2015 Hinweise auf einen möglicherweise bevorstehenden Anschlag[185] auf den Münchner

[179] Eine Verbunddatei, die den Austausch zwischen Geheimdiensten und Strafverfolgungsbehörden erleichtern soll. Der BND liefert knapp 50% der Daten. (Töpfer 2014)

[180] Ebd.

[181] ICREACH wurde 2007 gestartet, allerdings in einer Testphase. Wann diese abgeschlossen wurde, geht aus den Snowden-Leaks nicht hervor. ICREACH ergänzt die Datentauschprogramme CRISSCROSS und PROTON, die schon seit den frühen 1990ern respektive 1999 aktiv sind. ICREACH soll den Metadatenaustausch mindestens um das Zwölffache steigern.

[182] Die Daten stammen zum Teil auch von anderen Five-Eye-Geheimdiensten. Die Daten von US-Amerikaner_innen werden maskiert.

[183] R. Gallagher 2014c; National Security Agency 2007: Folie 10, 28.

[184] Greenwald und Fishman 2015.

[185] Die Informationen stellten sich im Nachgang als falsch heraus. Diese wurden nicht nur vom BND sondern auch von Geheimdiensten anderer Staaten weitergegeben. Recherchen ergaben, dass mehrere dieser Benachrichtigungen auf der selben Quelle basierten: Einem ehemaligen irakischen Geheimdienstoffizier.

Hauptbahnhof und den Pasinger Fernbahnhof in der Neujahrsnacht an die Münchner Polizei weiter. Die Informationen stammten von einem BND-Informanten. Die Polizei in München beschloss daraufhin, die Bahnhöfe zu evakuieren.[186]

Die Datenweitergabe findet auch unter der Hand statt. Die so weitergegebenen Daten sind nicht gerichtsfest, da sie nicht mit den rechtlich für die Strafverfolgung vorgesehenen Mitteln erlangt wurden. Sie können also eigentlich nicht zu Strafverfolgungszwecken verwendet werden. Um dies zu umgehen, besorgen sich die Strafverfolgungsbehörden die Beweise erneut auf legalem Wege und verschweigen den hinweisgebenden Geheimdienst oder sie erfinden einen alternativen Ermittlungsweg, den sie als Ursprung der Beweise nennen.[187] Dieses System wird *parallel construction* genannt und ist durchaus gängige Praxis.[188]

Abweichendes Verhalten wird in der Disziplinargesellschaft nicht toleriert, sondern durch Überwachung des Subjekts erkannt und anschließend sanktioniert. Ziel der Sanktionen ist nicht die bloße Bestrafung oder Abschreckung vor einem möglichen Regelübertritt, vielmehr soll auch die Sanktionierung eine normierende Wirkung entfalten.[189] Durch die massenhafte Überwachung nahezu aller Telekommunikation bestünde für die Geheimdienste die Möglichkeit, einen großen Teil der durch Telekommunikation dokumentierten oder begangenen Abweichung festzustellen. Die Geheimdienste selbst konzentrieren sich aber nicht auf jedwede Abweichung, sondern auf als besonders gefährlich wahrgenommene Taten, Individuen, Gruppen und Orte. Mit dem „National Intelligence Priorities Framework“[190] werden die Prioritäten der geheimdienstlichen Überwachung festgelegt. Diese umfassen Risiken, die den USA beziehungsweise ihren Interessen massiven Schaden zufügen können.[191] Ziel der Geheimdienste ist es nicht, jede Normverletzung nachzuvollziehen oder zu verfolgen.

Geheimdienste dürfen die „eigene“ Bevölkerung meist nur unter bestimmten Bedingungen überwachen, auch wenn dies mehr die Regel als die Ausnahme zu sein scheint. Sie haben kein Interesse daran, dass die „eigene“ Bevölkerung weiß, dass diese von ihnen überwacht wird - vielmehr birgt das Bekanntwerden nationaler (Massen-

[186] Baumgärtner et al. 2016.

[187] Beispielweise bekommt eine Polizeistreife die Aufforderung, an einem Rastplatz ein bestimmtes Auto zu einer genannten Uhrzeit zu kontrollieren. Die Polizei denkt sich dann einen anderen Auslöser für die Kontrolle des Autos mit einem Drogenspürhund aus bzw. nennt als Beginn ihrer Ermittlungen das Anhalten des Autos. (Shiffman und Cooke 2013)

[188] Schneier 2015a: S. 105; R. Gallagher 2014c; Shiffman und Cooke 2013.

[189] Foucault 1994: S. 231; Singelnstein und Stolle 2012: S. 62.

[190] National Security Agency et al. o. J.

[191] National Security Agency / Central Security Service 2007: S. 2.

)Überwachungsmaßnahmen das Potential für politische Skandale. Auslandsüberwachung hingegen erzeugt in der Bevölkerung meist weniger Aufmerksamkeit und Missgunst. Zudem liegt es im geheimdienstlichen Interesse, ihre Überwachungsprogramme, ihre Möglichkeiten und Fähigkeiten nicht zu offenbaren. Insofern besteht auch kein Interesse an einer direkten Verwendung für gerichtliche Sanktionen, da im Prozess die Herkunft der Beweise und damit ihre Beweiskraft sichergestellt werden muss. Die Möglichkeiten und Fähigkeiten der Geheimdienste könnten offenbart werden. Dennoch lösen geheimdienstliche Überwachungsprogramme Sanktionen auf vielerlei Ebenen aus, allerdings häufig ohne direkte Nennung der geheimdienstlichen Überwachung als Ausgangspunkt der Sanktion (zum Beispiel parallel construction).

Insofern sind Geheimdienste an der staatlichen Sanktionierung beteiligt, obgleich verdeckt. Durch Watchlisting (siehe Kapitel 5.4) oder „verdeckten Aktionen", beispielsweise von JTRIG (siehe Kapitel 5.3.2), sind weitere Sanktionsformen gegeben, welche jedoch auf der Ebene der Prävention oder des Ausschlusses stattfinden und daher den Techniken der Sicherheitsgesellschaft zuzuordnen sind. Auch ist ein Wandel des staatlichen Strafsystems, insbesondere in den USA, hin zum Ausschluss und zur Prävention feststellbar (siehe 5.4).[192] Eine normierende Wirkung der Sanktionierung ist somit rückläufig. Um diese Wirkung zu entfalten, muss den Sanktionierten bewusst sein, warum sie sanktioniert werden und wie sie sich „richtig" zu verhalten haben. Die Sanktionierung findet allerdings häufig im Vorfeld devianten Verhaltens, weitgehend verdeckt und mit präventiven oder ausschließenden Mitteln statt, welche zwar Sanktionen darstellen, aber nicht auf die Reintegration eines devianten Individuums (normierende Sanktion) ausgerichtet sind.

Geheimdienste vermitteln ihre Ziele sowie etwaige Normen nicht öffentlich, zudem agieren sie oft im Vorfeld strafbarer Handlungen, international und präventiv. Häufig arbeiten sie politischen Entscheidungsträger_innen und dem Militär zu. Insofern gibt es keinen öffentlich zugänglichen geheimdienstlichen Normenkatalog, an welchem die Individuen ihr Verhalten ausrichten könnten. Allerdings teilen Geheimdienste ihre Daten und Erkenntnisse zu einem gewissen Teil auch mit Strafverfolgungsbehörden, welchen mit dem Gesetz ein öffentlich zugänglicher Normenkatalog zu eigen ist. In diesem Teilbereich - der geheimdienstlichen Unterstützung von Strafverfolgungsbehörden - ist die Bedingung des klaren, zugänglichen Normenkataloges erfüllt. In anderen Bereichen bleiben die Verhaltensanforderungen vage oder un-

[192]Zum Wandel vgl. Garland 2008; Singelnstein und Stolle 2012.

klar.[193]

In einem Satz: Es gibt interne Regelungen und Normen, welche aber weder präzise Verhaltensanforderungen stellen, noch öffentlich bekannt waren/sind. Gesetze spielen eine untergeordnete Rolle, da die Geheimdienste meist international, im Vorfeld und nicht in der Strafverfolgung tätig sind. Die gestellten Verhaltensanforderungen bleiben unklar oder zumindest undurchsichtig und sind damit weit entfernt von den binären Normen der Disziplinargesellschaft. Allerdings unterstützen die Geheimdienste sekundär auch die Strafverfolgungsbehörden, die mit einem öffentlich bekannten und klaren Normenkatalog - dem Gesetz - arbeiten.

4.2 Panoptikum

Die Architektur des Panoptikums ermöglicht eine dauerhafte, asymmetrische Kontrolle der im Raum verteilten Individuen, die zu einer Internalisierung der Überwachung führt. Das Prinzip hinter Benthams Panoptikum steht für Foucault exemplarisch für die Disziplinargesellschaft. „Durch die Bündelung und Verallgemeinerung der Disziplinen im Panoptikum stellt dieses eine politische Technologie dar und ist von seiner spezifischen Verwendung ablösbar.“[194] Es ist das Ideal einer von Disziplinarmechanismen vollständig durchsetzten Gesellschaft.[195]

Mittels des panoptischen Prinzips und seiner inhärenten disziplinargesellschaftlichen Techniken lassen sich Überwachungskomplexe zerlegen und ihre Wirkungsweisen analysieren. Für die Arbeit werden die wichtigsten Elemente des panoptischen Prinzips abstrahiert[196] und auf die geheimdienstliche Telekommunikationsüberwachung angewandt.

4.2.1 Trennung von sehen und gesehen werden

Der wichtigste Aspekt der panoptischen Architektur ist das Paar sehen und gesehen werden. Dabei muss die Überwachte (in der Zelle) jederzeit in den Blick genommen und auf normkonformes Verhalten hin überprüft werden können - diese konkrete Überwachung darf von den Betroffenen allerdings nicht wahrnehmbar sein. In einem

[193] Beispielsweise sind die Terrorismusdefinitionen sehr schwammig und werden recht breit angewandt. Die auf dieser Basis erlassenen Sanktionen erfüllen daher häufig nicht die Anforderungen an eine normierende Sanktion.
[194] Tremmel 2010: S. 11.
[195] Foucault 1994: S. 268.
[196] vgl. Tremmel 2010: S. 12 ff.

Satz: Die Überwachte muss jederzeit sichtbar sein oder gemacht werden können, während der Überwachungsvorgang im Dunkeln bleibt.

4.2.1.1 Kontrollierender Blick

In den letzten Jahrzehnten haben sich die Kommunikationsmedien und -Möglichkeiten massiv verändert und erweitert. Mit dem Aufkommen mobiler Telekommunikationsgeräte und der Computerisierung der Gesellschaft wandelten sich auch die Kommunikationsgewohnheiten massiv. Telekommunikation ist ein omnipräsentes Phänomen geworden, dem man sich kaum noch entziehen kann (siehe Kapitel 3.1).[197] Ein beachtlicher Teil der Menschheit besitzt mindestens ein mobiles Telekommunikationsgerät und ist damit nahezu jederzeit ortbar - auch wenn das Gerät nicht verwendet wird oder ausgeschaltet ist. Die über diese Geräte vermittelte Telekommunikation erzeugt Daten. Dabei sind sowohl die Inhalte, als auch die Metadaten von Relevanz (siehe Kapitel 3.3).

Diese Daten werden in einem riesigen Umfang Upstream, also an der physischen Telekommunikationsinfrastruktur (bspw. mit TEMPORA Glasfaserkabel die u.a. Kontinente verbinden),[198] bei den Telekommunikationsanbietern (bspw. mit PRISM bei Microsoft, Yahoo, Google, Facebook, PalTalk, Youtube, Skype, AOL, Apple)[199] und aus anderen Quellen (bspw. durch das verteilen von Schadsoftware und Hacking),[200] gesammelt (siehe Kapitel 3.3).

Mit der immer umfassenderen Speicherung der Orts-, Inhalts- und Metadaten (teilweise auch Bestandsdaten) über oft sehr lange Zeiträume, hat sich der kontrollierende Blick des Geheimdienstkomplexes immer weiter ausgeweitet und immer mehr an Tiefe und Schärfe gewonnen. Noch vor wenigen Jahren war es sehr aufwändig bis unmöglich, über einzelne Personen, Gruppen oder Orte so umfassende und tiefgehende Informationen zu sammeln. In Zeiten mobiler Telekommunikation und des Internets ist dies mit vergleichsweise geringem Aufwand und bei einem Großteil der Menschheit möglich geworden. Einzelne Personen oder Gruppen können detailliert von Software oder Analyst_innen eingesehen werden. So können beispielsweise ihre aktuelle Kommunikation, ihre Beziehungsnetzwerke, ihr Aufenthaltsort, ihr Lebensrhythmus sowie etwaige Tätigkeiten (sowohl beruflich, privat, als auch aktivistisch)

[197] Höflich 2016: S. 1 ff.; Zurawski 2007: S. 10 f.
[198] Rosenbach und Stark 2014: S. 124 ff.; MacAskill und J. Ball 2013.
[199] Greenwald und MacAskill 2013; National Security Agency 2013: Folie 5 f.
[200] R. Gallagher und Greenwald 2014; Greenwald 2015b.

nachvollzogen werden. Der Datenumfang und die Überwachungstiefe sind enorm: Selbst Affären lassen sich durch die Analyse der Metadaten von Beziehungspartner_innen unterscheiden. Dies gilt insbesondere für ganz normale Menschen, die die Telekommunikationstechnologien alltäglich verwenden.[201]

Das 2007 eingeführte Analyseprogramm XKeyscore stellt die Schnittstelle zwischen den Datenmassen und den Analyst_innen dar. Das von der NSA entwickelte Programm wird auch von diversen Partnerdiensten verwendet (u.a. Verfassungsschutz, BND und Geheimdienste der Five-Eye-Staaten). Das britische Programm TEMPORA (siehe Kapitel 3.3) ist ebenfalls Teil von XKeyscore. Es wird in einem internen NSA-Dokument als „das größte XKEYSCORE der Welt“[202] bezeichnet.[203]

In einem Webfrontend können die Analyst_innen Suchabfragen erstellen und Inhalte betrachten. Diese werden an 150 auf der ganzen Welt verteilten Standorten[204] mit insgesamt 700 Servern (TEMPORA zusätzlich 1’000 Server (2012)) zwischengespeichert (Stand 2008). Innerhalb von 30 Tage standen in XKeyscore im Jahr 2012 41 Milliarden SSO-Datensätze[205] zur Verfügung. Es erfasst, laut einem internen Ausbildungsdokument der NSA, fast alles, was eine typische User_in im Internet so treibt.[206]

Diese Daten können mit harten (strong) und weichen (soft) Selektoren durchsucht werden. Harte Selektoren sind E-Mailadressen, IP-Adressen, Webseiten, Telefonnummern etc. Mit weichen Selektoren können die Telekommunikationsinhalte auf Schlüsselwörter durchsucht werden. Analyst_innen können auch die aktuelle Korrespondenz der Überwachten mitlesen, sie können sie sogar live verfolgen („real-time target activity“).[207] Es lassen sich aber auch die Aktivitäten der letzten Tage nachvollziehen und auswerten.[208] Analyst_innen können bestimmte Selektoren oder Ziele auch kontinuierlich überwachen bzw. Abfragen in bestimmten Zeiträumen (automatisch) wiederholen lassen. Die Daten werden anschließend für die Analyst_in vorgehalten.[209]

[201] Tremmel 2010: S. 16 f.
[202] National Security Agency 2012d: S. 1. Hervorhebung im Original.
[203] Monroy 2014.
[204] Die Server stehen meist in der Nähe der Sammelstellen, beispielsweise Internetknotenpunkten.
[205] Die „Special Sources Operation“ (SSO) sammelt die Daten Upstream bei den ISPs oder von den Servern der Telekommunikationsanbieter via PRISM (siehe Kapitel 3.3).
[206] Holland 2015a: S. 134 f.; Greenwald 2014a: S. 221 ff.; Greenwald 2013.
[207] National Security Agency 2008: Folie 2.
[208] Ebd.: Folie 2.
[209] Greenwald 2013; Booz Allen Hamilton 2010: S. 18.

Metadaten werden ungefähr einen Monat, Inhaltsdaten drei bis fünf Tage vorrätig gehalten.[210] So kann das Internet ein paar Tage angehalten und vergangene Telekommunikation wieder hergestellt werden. Informationen und Ziele, die den Analyst_innen wichtig erscheinen, können in andere Datenbanken überführt und dort für längere Zeiträume gespeichert werden.[211]

XKeyscore sortiert die gesammelten Daten vor. E-Mails werden aus dem Traffic gefiltert und mit Tags (appIDs oder Fingerabdrücken) versehen: Kommt die Mail von Yahoo oder GMail? Enthält sie eine Reiseroute? Ist sie mit GnuPG/PGP verschlüsselt? In welcher Sprache wurde sie verfasst? usw. usf. Mit diesen können wiederum Suchanfragen oder Suchskripte geschrieben werden. GMail hat beispielsweise die appID „mail/webmail/gmail“, der Browser des iPhones „browser/cellphone/iphone“. Arabischsprachige E-Mails können mit dem Fingerabdruck „mail/arabic“ gesucht werden. Insgesamt gab es 2010 fast 10'000 appIDs und Fingerabdrücke.[212]

Die unterschiedlichen Selektoren lassen sich kombinieren und Anfragen wie „germansinpakistan“ stellen, welche die erfasste deutschsprachige Kommunikation aus Pakistan ausgibt. Es lassen sich beispielsweise alle verschlüsselten Word-Dateien aus dem Iran anzeigen, oder alle Dokumente die die IAEO oder Osama Bin Laden erwähnen. Es sind aber auch komplexere Abfragen mit Skripten möglich. Es lassen sich ebenfalls alle Besucher_innen einer Webseite oder eines Forums in einem bestimmten Zeitraum ausgeben.[213]

Eine weitere Möglichkeit besteht darin, die Trackingcookies[214] von Werbenetzwerken und Telekommunikationsanbietern mitzunutzen (siehe Kapitel 5.3.1). Dies ermöglicht Ziele mit wechselnden Orten oder Anonymisierungsdiensten wie VPN (Virtual Private Network)[215] zu tracken.[216]

[210] Die Begrenzungen sind vor allem technischer Natur. Die Speicherkapazitäten gaben 2008 nicht mehr her. Es ist davon auszugehen, dass sie seitdem massiv erhöht wurden.

[211] Holland 2015a: S. 134 f.; Greenwald 2014a: S. 221 ff.

[212] National Security Agency 2009b; Lee, Greenwald und Marquis-Boire 2015.

[213] National Security Agency 2008: Folie 16 ff; Booz Allen Hamilton 2010: S. 13.

[214] Kleine Textdateien, die meist eine ID enthalten und auf dem Computer einer Webseitenbesucher_in ablegt werden. Wird eine Webseite aufgerufen, in welche der Trackingdienst integriert ist, schickt der Browser der Benutzer_in automatisch die ID an die Trackingfirma, welche dadurch das Verhalten der Internetbenutzer_innen beobachten kann. Solche Trackingdienste sind in einem Großteil der Webseiten eingebunden und überwachen die Nutzer_innen sehr detailliert, um ihnen beispielsweise individuelle, situationsspezifische Werbung anzeigen zu können.

[215] VPNs bauen verschlüsselte Verbindungen in interne Netze (z.B. Firmen- oder Universitätsnetz) oder zu einem Server, über den die Nutzer_innen im Internet surfen und sich die gleiche IP-Adresse teilen, um anonymer zu surfen, auf.

[216] Marquis-Boire, Greenwald und Lee 2015.

Es können auch Benutzernamen und Passwörter ermittelt werden. Zudem scannt XKeyscore Computer bzw. Software auf ausnutzbare Sicherheitslücken, welche die Analyst_innen direkt aus XKeyscore heraus angreifen können. So lassen sich mit wenigen Klicks Geräte hacken. Zudem ist es möglich, sich alle hackbaren Devices in Land X ausgeben zu lassen.[217]

Snowden beschrieb die Nutzung von XKeyscore in einem Interview folgendermaßen:

> „You could read anyone's email in the world. Anybody you've got email address for, any website you can watch traffic to and from it, any computer that an individual sits at you can watch it, any laptop that you're tracking you can follow it as it moves from place to place throughout the world. It's a one stop shop for access to the NSA's information. And what's more you can tag individuals using 'XKeyscore'. Let's say I saw you once and I thought what you were doing was interesting or you just have access that's interesting to me, let's say you work at a major German corporation and I want access to that network, I can track your username on a website on a form somewhere, I can track your real name, I can track associations with your friends and I can build what's called a fingerprint which is network activity unique to you which means anywhere you go in the world anywhere you try to sort of hide your online presence hide your identity, the NSA can find you and anyone who's allowed to use this or who the NSA shares their software with can do the same thing. Germany is one of the countries that have access to 'XKeyscore'."[218]

4.2.1.2 Privacy Tools und Geheimdienst Hacking

Doch auch die geheimdienstliche Massenüberwachung ist mitnichten allmächtig. Auch wenn ihr erklärtes Ziel ist, jegliche menschliche Telekommunikation abzufangen, so zeigen interne Präsentationen auch, dass sie mit bestimmten Technologien Probleme hat.

In einer Präsentation auf der SIGDEV-Konferenz 2012 konstatiert die NSA, dass ihr die Verwendung bestimmter Anonymisierungs- und Verschlüsselungstechnologien

[217] Marquis-Boire, Greenwald und Lee 2015; National Security Agency 2008: Folie 24; S. Gallagher 2013.

[218] Snowden 2014b.

massive Probleme bereitet. Als Beispiele werden in den Folien der Anonymisierungsdienst Tor, das auf Tor setzende Live-Betriebssystem TAILS (The Amnesic Incognito Live System), die Chatverschlüsselungssoftware OTR, mit ZRTP verschlüsselte Voice-over-IP-Telefonie (VoIP) unter Linux, die VoIP-App Redphone,[219] sowie die Verschlüsselungssoftware TrueCrypt genannt.[220]

Eine Kombination solcher Technologien führe selbst bei „Highest Priority"-Zielen zu einem „Near-total loss/lack of insight to target communication, presence".[221] Weitere Folien zeigen, dass die E-Mailverschlüsselungssoftware GnuPG/PGP nicht von der NSA geknackt werden kann.[222]

Eine interne Präsentation der NSA zum Anonymisierungsdienst Tor betitelte die NSA lapidar mit „Tor Stinks". Das Tor-Netzwerk besteht aus mehreren tausend Servern (7'000 im Januar 2015), die von Freiwilligen betrieben werden. Installiert man Tor oder den Tor Browser auf seinem Computer oder Smartphone stellt die Software eine verschlüsselte Verbindung zu dem Netzwerk her. Sie wählt drei Tor-Server aus, über die sie mit dem Internet kommuniziert. Die Daten werden dabei derart verschlüsselt, dass keiner der Tor-Server weiß, wer mit wem kommuniziert.[223] In verschiedenen Präsentationen besprechen Geheimdienstmitarbeiter_innen unterschiedliche Konzepte, wie die Tor-Nutzer_innen deanonymisiert werden können. Diese zeigten bis zu den Snowden Leaks kaum bis mäßigen Erfolg, bedeuteten aber erheblichen Aufwand. Bisher könne man zwar eine „sehr kleine Fraktion" der Tor Nutzer_innen deanonymisieren, dies sei aber nicht gezielt auf Anfrage möglich.[224]

Dennoch sammeln die Geheimdienste Daten über Tor-Nutzer_innen und greifen diese an. Die NSA speichert alle Verbindungen[225] zum Tor-Netzwerk, sowie Web-

[219] Redphone wurde mit Textsecure zum Messenger Signal vereint. Dieses verwendet sowohl ZRTP für seine Telefoniefunktion, als auch eine abgewandelte Version von OTR welche „Signal Protocol" genannt wird. Letzteres ermöglicht einen hochgradig verschlüsselten und im Gegenzug zu OTR, asymmetrischen Nachrichtenaustausch.

[220] Die Entwicklung der Software TrueCrypt wurde eingestellt. Sie sollte nicht mehr verwendet werden.

[221] National Security Agency / Central Security Service 2012: Folie 20.

[222] National Security Agency / Central Security Service 2012: Folie 20 ff; Tremmel 2015a.

[223] Zur Funktion von Tor: Tremmel 2015b.

[224] National Security Agency 2012e: Folie 1 ff; Government Communications Headquarters o. J.: Folie 1 ff.

[225] Obwohl (möglichst) alle Nutzer_innen, die sich mit dem Tor-Netzwerk verbinden gespeichert werden, erhalten die Geheimdienste durch die Nutzung von Tor deutlich weniger Informationen. Sie wissen, wer sich mit dem Tor-Netzwerk verbindet und was über Tor im Internet gemacht wird, sie wissen aber im Gegensatz zu herkömmlichen Internetverbindungen nicht, wer was und von welchem Ort aus im Internet macht.

seitenbesuche und Websuchen zum Thema Tor und stuft die Nutzer_innen und Menschen, die sich für Tor, TAILS oder andere Dienste zur anonymen und sicheren Kommunikation interessieren, als Extremist_innen ein. Hierfür stehen in XKeyscore Skripte bereit.[226]

Mit Tailored Access Operations (TAO) verfügt die NSA über eine Einheit aus Staatshackern, die verschiedene Angriffsmethoden und -module vorbereitet und ausführt. Die QUANTUM-Angriffsmethoden der TAO werden auch gegen Tor-Nutzer_innen verwendet. Mit QUANTUMCOOKIE wird dem Tor Browser[227] bei einer bestimmten Webseitenanfrage eine falsche Antwort (bspw. Yahoo oder Hotmail) mittels des QUANTUM-Systems zugeschickt. Der Tor Browser reagiert auf die falsche Antwort und schickt, sofern in der Session vorhanden, die entsprechenden Cookies der Seiten (bspw. Yahoo oder Hotmail) zurück. Diese Cookies können die Identität der Tor-Browser-Nutzer_in verraten. Der Angriff ist nicht trivial und funktioniert nur unter bestimmten Bedingungen.[228]

Mit FOXACID steht ein weiterer Angriff aus dem QUANTUM-System zur Verfügung, der gegen den Tor Browser verwendet werden kann. Hat die NSA eine Tor-Browser-Nutzer_in identifiziert, kann sie dieser auf eine Webseitenanfrage mit einer gefälschten Webseiten Antworten (ähnlich QUANTUMCOOKIE). Diese Webseite enthält einen Exploit[229] der eine (unbekannte) Sicherheitslücke im Firefox, welcher im Tor Browser enthalten ist, ausnutzt. Anschließend kann der Geheimdienst dem Opfer Schadsoftware auf den Computer installieren und so die Kontrolle über diesen übernehmen. Für QUANTUMCOOKIE und FOXACID wird ein geheimes Servernetzwerk (QUANTUM) verwendet. Die Server stehen bei den ISPs verteilt an wichtigen Punkten des Internets. Hierdurch stehen sie nahe beim Opfer einer QUANTUM-Attacke. Dies ermöglicht der NSA, die gefakten Antwortseiten schneller als die regulären Webseiten an das Opfer auszuliefern. Es handelt sich um eine Art Wettrennen, dass die NSA nach eigenen Angaben oft verliert.[230]

Die Massenüberwachungssysteme lassen sich mit bestimmten frei verfügbaren Verschlüsselungs- und Anonymisierungstools oder Services vergleichsweise einfach umgehen.[231] Datenschutz- und sicherheitsorientierte Programme haben in den letz-

[226] Rötzer 2014; Schneier 2014c.
[227] Der Angriff funktioniert auch ohne Tor und mit anderen Browsern.
[228] National Security Agency 2012e: Folie 15.
[229] Aktives Ausnutzen eines Software-Sicherheitsproblems.
[230] Schneier 2013a.
[231] Eine Sicherheit hat man dabei nicht, da die Weiterentwicklung der Angriffe nach den Snowden-

ten Jahren einen steigenden Zulauf, ihr Marktanteil bleibt aber dennoch gering.[232] Möchte man Telekommunikation verschlüsseln und/oder anonymisieren, muss diese Technologie auch von den Kommunikationspartner_innen genutzt werden. Vielen fehlt dazu das Bewusstsein, die technische Kompetenz (obgleich die Verschlüsselungsprogramme immer einfacher werden (z.B. Signal oder Tor Browser)) und die Zeit. Häufig werden Dienste benutzt, die die Nutzer_innen von Haus aus überwachen und die Daten mit Geheimdiensten teilen. So ist es gerade die Masse, die von Überwachung betroffen ist.

4.2.1.3 Unsichtbarkeit der Überwachung

Wichtig für das Panoptikum ist nicht nur die Sichtbarkeit des Individuums, sondern auch die Nicht-Sichtbarkeit des Überwachungsvorgangs. Geheimdienste agieren, wie der Begriff nahe legt, im Geheimen. Ihre Operationen, Fähigkeiten und ihre Infrastruktur versuchen sie möglichst gut zu tarnen. Früher wurde die NSA daher auch scherzhaft „No Such Agency“ oder „Never Say Anything“ genannt. Das Abgreifen der Daten findet primär nicht wahrnehmbar an Internetknotenpunkten, -kabeln, Servern oder heimlich gehackten Geräten statt.

Durch die Snowden-Leaks wurde die NSA und andere westliche Geheimdienste einer breiten Masse bekannt. Ihr neuer Spitzname lautet nun „Not Secret Anymore“. Die Fähigkeiten, Infrastruktur und Operationen westlicher Geheimdienste wurden ins Licht gezerrt und eine gesellschaftliche Diskussion zu Überwachungsfähigkeiten und Sicherheit geführt. Beides dauert an.

Doch auch wenn die westlichen Überwachungsgeheimdienste, allen voran die NSA und ihre Überwachungsprogramme, eine gewisse Berühmtheit erlangt haben, wissen die Menschen nur, dass ein Großteil der Telekommunikation erfasst wird. Doch das Auswerten der Daten, der kontrollierende Blick, findet in Geheimdienstbüros statt - ohne jegliche Öffentlichkeit. Ob man als Individuum oder Teil einer Gruppe Ziel geheimdienstlicher Überwachung ist oder jemals war, ob ein Selektor, ein Raster oder ein Skript auf ein Individuum passt, ob jede Zeile die es tippt mitgelesen wird,

Enthüllungen auf bspw. das Tor-Netzwerk nicht bekannt sind. Expert_innen gehen allerdings davon aus, dass die Geheimdienste in diesem Bereich keine erheblichen Fortschritte gemacht haben. Ein weiterer Unsicherheitsfaktor sind die Hacking-Fähigkeiten der Geheimdienste, oft sind die Sicherheits- und Privacy-Tools an sich sicher, werden aber auf unsicheren Geräten betrieben, die gehackt werden können. Hinzu kommen fehlerhafte Implementierungen und Programmierfehler, welche ebenfalls Angriffe ermöglichen.

[232] Bitkom 2013.

bleibt vollkommen im Dunkeln. Man kann jederzeit eingesehen werden, ob dies real stattfindet, ist wie beim panoptischen Turm nicht nachvollziehbar.

4.2.2 Die bewusste Überwachung

Im Panoptikum symbolisiert der Turm die stetige Überwachbarkeit des Insassen. Die stetige Erinnerung durch die physische Manifestierung der Überwachung „hilft" dem potentiell überwachten Individuum dabei, die Überwachung nicht zu vergessen. Das Individuum beginnt sie mitzudenken, sich selbst zu überwachen und seine Entscheidungen danach auszurichten. Es internalisiert die Überwachung. Daher ist es wichtig, von der Überwachung zu wissen, sie stetig vor Augen zu haben, um normierende Effekte hervorzurufen.

Die geheimdienstliche Überwachung findet im Geheimen statt. Die Programme und Technologien sind weitgehend unbekannt. Mit den Snowden-Leaks änderte sich dies zwar grundlegend, dies war aber von den Geheimdiensten alles andere als intendiert. In der Reaktion auf die Leaks, versuchen die Geheimdienste im Bereich der massenhaften Telekommunikationsüberwachung zu beschwichtigen und die Programme herunterzuspielen. Beispielsweise betonen sie, dass sie nur wenige Menschen überwachen[233] und die Programme von Medien und Öffentlichkeit falsch verstanden würden. Geheimdienste und Regierungsvertreter_innen wurden dabei mehrfach der (beschwichtigenden) Falschaussage überführt.[234]

Gleichzeitig betonen sie die Bedeutung der Überwachungsprogramme im Rahmen der Bekämpfung des internationalen Terrorismus und fordern eine Ausweitung der Überwachung und des internationalen und innerbehördlichen Datenaustausches, sowie zum Teil die Schwächung von Kryptographie. Sie bekräftigen, dass sie sich an Recht und Gesetz halten würden und die jeweilige Bevölkerung des Landes aus dem die Geheimdienste stammen, nicht durch sie überwacht würde (siehe Kapitel 3.2). Ziel der Geheimdienste ist offensichtlich Schadensbegrenzung und Beschwichtigung der Bevölkerung. Ihr Interesse besteht in der Heimlichkeit, nicht im Licht zu agieren. Der Leiter eines britischen Geheimdienstes formulierte dies gegenüber einem Pressevertreter folgendermaßen: „We're a secret organization. There's nothing in it

[233] Im öffentlichen Sprachgebrauch stellt Überwachung (und teilweise auch das Sammeln von Daten) für die Geheimdienste erst das Konkrete auswerten der Daten durch Personen dar, nicht aber das Sammeln [sic!] oder elektronische auswerten. (Schneier 2015a: S. 129)

[234] Schneier 2013b.

for us in being more open about what we do. We see no need to change.“[235]

Die Leaks zerrten die Geheimdienste ungewollt in die Öffentlichkeit und brachten die grundlegende Funktionsweise der Überwachungssysteme der Mehrheitsbevölkerung näher. Es entstand eine Art panoptischer Turm. Bei den Menschen bleibt durch die kontinuierliche Medienberichterstattung ein diffuses Gefühl des überwacht werdens.[236]

Laut einer Studie des deutschen Telekommunikations-Branchenverbandes Bitkom hielten 2011 41% der Menschen in Deutschland ihre persönlichen Daten im Internet für sicher, ein Jahr nach Snowden im Mai 2014 waren es nur 13% (86% hielten sie für unsicher). Auch das Vertrauen im Umgang mit persönlichen Daten bei Staat (2011: 62% - 2014: 25%) und Wirtschaft (2011: 40% - 2014: 28%) sank immens. „[G]ut jeder zweite Internetnutzer (53 Prozent) [fühlt sich] von der Ausspähung seiner persönlichen Daten durch staatliche Stellen bedroht.“[237] Der Bitkom führt diese Entwicklung auf die NSA-Affäre zurück.[238]

Ipsos befragte in einer internationalen Studie im Auftrag des Centre for International Governance 23’376 Internetnutzer_innen in 24 Staaten zu Internetsicherheit und Vertrauen. Laut der 2014 durchgeführten Studie haben 60% der Internetnutzer_innen von Edward Snowden gehört - in Deutschland waren es 94%, in den USA 76% und in Großbritannien 72%. 62% der Menschen, die das Internet verwenden machen sich Sorgen, dass Geheimdienste anderer Staaten ihre Onlineaktivitäten überwachen (Deutschland: 67%, USA: 60%, Großbritannien: 58%). 61% machen sich sorgen, dass Polizei und Geheimdienste des Landes in dem sie leben, heimlich ihre Internetnutzung überwachen (Deutschland: 57%, USA: 64%, Großbritannien: 57%). Nach einem Jahr Snowden-Veröffentlichungen machen sich 64% der User_innen Sorgen um ihre Privatsphäre im Internet (Deutschland: 56%, USA: 63%, Großbritannien: 53%).[239]

Die Zahlen zeigen, dass ein Großteil der Internetnutzer_innen von der geheimdienstlichen Telekommunikationsüberwachung erfahren haben. Zudem macht sich rund zwei Drittel Sorgen um ihre Privatsphäre im Internet sowie einer geheimdienstlichen Überwachung ihrer Internetnutzung. Die Leaks und ihre mediale Aufarbeitung halten seit 2013 das Wissen um die Überwachbarkeit der Telekommunikation in den

[235] Rusbridger 2013.
[236] Shelton, Rainie und Madden 2015: S. 1 ff.; Amnesty International 2015.
[237] Bitkom 2014: S. 1.
[238] Ebd.: S. 1.
[239] Centre for International Governance Innovation und Ipsos 2014: S. 2 ff.

Köpfen. Mit den Skandalen rund um den BND im NSA-Untersuchungsausschuss 2015 dürfte dieses Gefühl in Deutschland weiter manifestiert oder sogar ausgebaut worden sein.

Zentral ist allerdings, dass die Geheimdienste mit ihren Telekommunikationsüberwachungsprogrammen nie die Intention hatten, soziale Kontrolle mit Hilfe eines Wissens um die Überwachung und Überwachbarkeit zu realisieren. Dennoch wurde durch die Snowden-Leaks, die mediale Aufarbeitung und die damit verknüpfte gesellschaftliche Debatte, ein Wissen um die Überwachung und damit eine Art panoptischer Turm geschaffen. Geheimdienstliche Überwachung und ihre Institutionen sind nur schwer wahrnehmbar, ihre Aktivitäten, Weiterentwicklungen und Kapazitäten werden nicht veröffentlicht. Insofern bleibt die Wahrnehmung ebenjener abhängig von (Experten-)Einschätzungen, Untersuchungsausschüssen, Skandalen, Leaks - und der jeweiligen medialen Vermittlung. Das Wissen um die geheimdienstliche Telekommunikationsüberwachung bleibt begrenzt und manifestiert sich nicht immer wieder vor den Augen der Überwachten. Obgleich die Studien nahelegen, dass im Rahmen der Berichterstattung über die Snowden Veröffentlichungen einem Großteil der Bevölkerung die geheimdienstliche Telekommunikationsüberwachung präsent war, fehlt die kontinuierliche Manifestierung, welche den Überwachten die Überwachung vor Augen hält. Diese dürfte mittlerweile deutlich abgenommen haben und je nach medialer Berichterstattung und gesellschaftlicher Diskussion abebben oder erneut aufkommen. In einem Satz: Ein panoptischer Turm ist für einen erheblichen Teil der Bevölkerung auf Zeit mit Abstrichen bei der kontinuierlichen Erneuerung gegeben.

4.2.3 Verhaltensanpassung und Internalisierung der Überwachung

Die Trennung von sehen und gesehen werden, sowie das stetige Wissen um die Möglichkeit der intensiven Überwachung sind - letzteres mit Abstrichen - gegeben. Darauf aufbauend lässt sich mittels des panoptischen Prinzips eine Internalisierung der Überwachung sowie eine daran anschließende Verhaltensanpassung prognostizieren. Das Individuum weiß um die stetige Möglichkeit eines kontrollierenden Blickes, nimmt hierdurch eine stetige Kontrolle an, ohne das diese tatsächlich stattfinden muss. Es beginnt seine Handlungen zu überwachen und an antizipierte Verhaltensnormen anzupassen.

Zu beobachten ist, dass die Überwachung wahrgenommen wird und Versuche unternommen werden, diese zu umgehen. Unternehmen überdenken ihr Verhalten in

Bezug auf sensible Geschäftsdaten. Cloud[240] war in den Jahren vor den Snowden-Enthüllungen ein wichtiges Buzzword in der Wirtschaft. Es war geradezu in, die Datenverarbeitung in Rechenzentren auszulagern, diese und die zugehörige Software von externen Anbietern betreuen zu lassen, um damit Zeit und Geld zu sparen. Seit den Snowden-Enthüllungen werden Befürchtungen um Datenschutz und Sicherheit mit dem Begriff Cloud verbunden. Insbesondere Cloudanbieter aus den USA haben aufgrund der (Wirtschafts-)Spionage der NSA einen schlechten Ruf. 2014 ergab eine Umfrage, dass 25% der britischen und kanadischen Firmen ihre Daten aus den USA abziehen wollen, auch wenn dies eine schlechtere Performance bedeute. US-Anbieter verloren unter anderem im Cloud-Bereich internationale Kunden. Verschiedene Studien schätzen einen Verlust zwischen 2013 und 2016 von 22 - 35 Milliarden US-Dollar[241] bis zu 180 Milliarden US-Dollar im gleichen Zeitraum.

Standorte spielen seitdem eine erhebliche Rolle. Viele europäische Firmen werben damit. Microsoft lässt parallel zu einem Rechtsstreit mit der US-Regierung[242] zwei Cloud-Rechenzentren von der Telekom betreiben, damit sie nicht gezwungen werden können, Daten an US-Geheimdienste herausgeben zu müssen.[243]

Eine ähnliche Reaktion gab es seitens der europäischen Judikative. Am 6. Oktober 2015 kassierte der Europäische Gerichtshof (EuGH) das Safe-Harbor-Abkommen zwischen EU und USA. Dieses sollte[244] die Verarbeitung der personenbezogener Daten europäischer Nutzer_innen in den USA, mit der Argumentation gewährleisten, dass dort ein gleichwertiges Schutzniveau gegeben sei. Dem widersprach der EuGH. Durch die Zugriffsmöglichkeiten amerikanischer Sicherheitsbehörden auf die übermittelten Daten sei dieser Standard nicht gegeben und der Wesensgehalt des Grundrechts auf Achtung des Privatlebens verletzt. Zudem gebe es keinen Rechts-

[240] Cloud ist ein nebulöser Begriff für die Auslagerung von IT-Infrastruktur mitsamt aller Daten.

[241] Die Information Technology and Innovation Foundation (ITIF), Think Tank und Autorin der verlustabschätzenden Studie, korrigierte ihre Schätzung 2015. Die Zahlen müssten erheblich höher angesetzt werden, da nicht nur wie ursprünglich angenommen die Cloud-Branche, sondern die komplette US-Amerikanische IT-Branche unter dem NSA-Skandal leide.

[242] Streitpunkt: Muss Microsoft oder andere US-Amerikanische Unternehmen auch Daten an die US-Sicherheitsbehörden weitergeben, wenn diese in anderen Jurisdiktion in einem anderen Teil der Welt gespeichert sind? Steht das Recht in der anderen Jurisdiktion der Datenweitergabe entgegen, muss das Unternehmen entweder US-Recht oder das Recht des anderen Staates brechen.

[243] Knop 2013; Schneier 2015a: S. 121 f.; Castro und McQuinn 2015: S. 1 ff.; Beuth 2015.

[244] Neben Safe Harbor existieren weitere Möglichkeiten, den Datentransfer juristisch abzusichern, allerdings lässt sich die Argumentation des EuGH auch auf diese anwenden. Das Nachfolgeabkommen Privacy Shield wird derzeit noch verhandelt, dürfte aber keine grundlegende Änderung im Bereich der (geheimdienstlichen) Telekommunikationsüberwachung mit sich bringen.

behelf für europäische Bürger_innen.[245]

Nach einer internationalen Studie zu Internetsicherheit und Vertrauen (s.o.) haben 60% der Internetnutzer_innen von Edward Snowden gehört (Deutschland: 94%, USA: 76%, Großbritannien: 72%). Von diesen 60% wiederum haben 39% Schritte unternommen, um ihre Privatsphäre und Sicherheit im Internet zu steigern. In Deutschland waren es ebenfalls 39%, in den USA 36% und in Großbritannien 31%.[246] Bruce Schneier hat die tatsächliche Zahl der Internetnutzer_innen berechnet: Demnach haben 706 Millionen Menschen Schritte unternommen, um ihre Privatsphäre und Sicherheit im Internet nach den Snowden-Enthüllungen zu erhöhen. Für die Studie wurden Internetnutzer_innen in 24 Ländern befragt, die gemeinsam für 4,7 Milliarden der 7 Milliarden Menschen auf der Welt stehen. Nach einer konservativen Schätzung Schneiers nutzen 20% der restlichen Menschen das Internet, nimmt man an, dass 40% von diesen von Snowden gehört haben und 25% von diesen Schritte unternommen haben, kommt man auf weitere 46 Millionen Menschen. Weltweit dürften also um die 750 Millionen Menschen auf den NSA-Skandal reagiert haben.[247]

> „It's probably true that most of those people took steps that didn't make any appreciable difference against an NSA level of surveillance, and probably not even against the even more pervasive corporate variety of surveillance. It's probably even true that some of those people didn't take steps at all, and just wish they did or wish they knew what to do. But it is absolutely extraordinary that 750 million people are disturbed enough about their online privacy that they will represent to a survey taker that they did something about it."[248]

Festzuhalten bleibt, dass ein relevanter Bevölkerungsteil versucht, sich vor der Überwachung durch westliche Geheimdienste zu schützen. Im Gegensatz zum panoptischen Gefängnis können sich in der realen Welt Menschen vor den Blicken der Überwachungsmaschinerie zumindest teilweise schützen,[249] müssen aber auch hierzu die Überwachung internalisieren und ihr Verhalten anpassen - allerdings können sie sich durch diese Anpassung der normierenden Wirkung entziehen. Die disziplinarische Kontrolle bis ins kleinste Detail versagt. Von der normgebenden Instanz

[245] Biselli 2015b; Holland 2015b.
[246] Centre for International Governance Innovation und Ipsos 2014: S. 10 f.
[247] Schneier 2014d.
[248] Ebd.
[249] Zu den Einschränkungen s.o.

als deviant angesehenes Verhalten kann nicht mehr erkannt beziehungsweise vom Individuum gelebt werden. Normierende Sanktionen bzw. eine Wiedereingliederung können mangels Erkennung der Abweichung nicht vollzogen werden. Dieser Fall tritt allerdings keineswegs gehäuft auf. Es ist zwar möglich sich gegen Massenüberwachung mit relativ einfachen Mitteln zu schützen, dennoch bedarf es dazu ein gewisses technisches Know-How und es bereitet einen gewissen Aufwand sowie eine ähnliche Bereitschaft auf Seiten der Kommunikationspartner_innen.

Hinzu kommt, dass es keine Sicherheit gibt, das nicht doch Fehler gemacht wurden oder die Überwachungsprogramme mächtiger als angenommen sind. Dazu kommt die Möglichkeit des Hackings und der gezielter Überwachung, welchen man sehr viel schwieriger entgehen kann. Dennoch ist diese Umgehungsmöglichkeit im panoptischen Prinzip so nicht vorgesehen.

Trotz dieser Einschränkungen, welche zwar von einem relevanten Teil der Bevölkerung versucht, aber nur bei einem sehr kleinen Teil in einer Form praktiziert wird, die reale Wirkung zeigt, gibt es Verhaltensanpassungen bei den Menschen. Die Vorratsdatenspeicherung[250] in Deutschland, die eine sechsmonatige Speicherung der Metadaten jeglicher Telefon, Mobiltelefon und E-Mail-Telekommunikation, sowie IP-Adressen von Internetanschlüssen vorsah, wurde im März 2010 vom Bundesverfassungsgericht für nichtig erklärt.[251] Das Bundesverfassungsgericht schrieb in der Presseerklärung zu seinem Urteil zur Vorratsdatenspeicherung:

> „Allerdings handelt es sich bei einer solchen Speicherung um einen besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt. Auch wenn sich die Speicherung nicht auf die Kommunikationsinhalte erstreckt, lassen sich aus diesen Daten bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen. Adressaten, Daten, Uhrzeit und Ort von Telefongesprächen erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen. Je nach Nutzung der Telekommunikation kann eine solche Speicherung die Er-

[250] Zur VDS in DE und EU vgl. Tremmel 2010: S. 4 ff.

[251] Allerdings wurde nur die konkrete Umsetzung, nicht eine Vorratsdatenspeicherung im Allgemeinen für nichtig erklärt. Das Bundesverfassungsgericht berücksichtigte nur die besondere Ausgestaltung einer EU-Richtlinie (die mittlerweile vom EuGH kassiert wurde) in Deutschland. Diese Ausgestaltung sei nicht verhältnismäßig und wurde damit als verfassungswidrig eingestuft.

> stellung aussagekräftiger Persönlichkeits und Bewegungsprofile praktisch jeden Bürgers ermöglichen. Auch steigt das Risiko von Bürgern, weiteren Ermittlungen ausgesetzt zu werden, ohne selbst hierzu Anlass gegeben zu haben. Darüber hinaus verschärfen die Missbrauchsmöglichkeiten, die mit einer solchen Datensammlung verbunden sind, deren belastende Wirkung. Zumal die Speicherung und Datenverwendung nicht bemerkt werden, ist die anlasslose Speicherung von Telekommunikationsverkehrsdaten geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann.“[252]

Dies gilt in besonderem Maße auch für geheimdienstliche Telekommunikationsüberwachung, deren Programme der Vorratsdatenspeicherung ähnlich sind. Auch hier werden Metadaten bei den Telekommunikationsanbietern gesammelt. Allerdings in einem deutlich größeren Umfang, da nahezu jegliche Telekommunikationsform weltweit betroffen ist. Zudem werden häufig auch die Inhalte erfasst, die gemeinsam mit den Metadaten in Geheimdienst-Datenbanken gespeichert und von Analyst_innen algorithmisch ausgewertet werden können(siehe Kapitel 5.1 und 5.2). Insofern übertrifft die geheimdienstliche Telekommunikationsüberwachung die Vorratsdatenspeicherung von 2008 bis 2010 in Deutschland deutlich. Auch hier entsteht ein „diffus bedrohliches Gefühl des Beobachtetseins“, welches eine „unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann“.[253] Diese abschreckende Effekte werden *Chilling Effects* genannt. Diese definiert Assion wie folgt:

> „Chilling Effects entstehen, wenn staatliches Handeln – meist mit Breitenwirkung - die Bürger davon abhält, von ihren Grundrechten Gebrauch zu machen.“[254]

Das staatliche Handeln umfasst keinen unmittelbaren Zwang oder eine Sanktionierung, vielmehr schafft es die Rahmensituation,[255] unter welcher die Bürger_in selbst „freiwillig“ auf die Wahrnehmung ihrer Rechte verzichtet, sich selbst einschränkt.[256]

[252] Bundesverfassungsgericht 2010.
[253] Ebd.
[254] Assion 2014: S. 37.
[255] Diese muss nicht ausschließlich von staatlichem Handeln geschaffen werden.
[256] Assion 2014: S. 34 ff.

Im Rahmen der geheimdienstlichen Telekommunikationsüberwachung handelt es sich um ein Gefühl des Überwachtwerdens oder überwachtwerdenkönnens. Es findet eine Internalisierung einer möglichen Kontrolle und eine damit verbundene Verhaltensanpassung statt, in dessen Folge Grundrechte nicht mehr wahrgenommen werden. Diese abschreckende Wirkung staatlicher Überwachung wird sowohl vom Bundesverfassungsgericht, Europäischem Gerichtshof (EuGH) als auch Europäischem Gerichtshof für Menschenrechte (EGMR) als Auslöser von Chilling Effects angesehen.

In der Empirie sind Verhaltensänderungen in Bezug auf das Wissen ob der Überwachung feststellbar. Die bereits zitierte internationale Studie zu Internetsicherheit und Vertrauen (s.o.) befragte Menschen zu Verhaltensänderungen in Bezug auf den NSA-Skandal. 43% der Internetnutzer_innen vermieden den Besuch bestimmter Webseiten und Web-Applikationen (Deutschland: 39%, USA: 40%, Großbritannien: 40%). 18% änderten ihren Adressatenkreis (Deutschland: 17%, USA: 19%, Großbritannien: 15%) und 28% begannen sich online selbst zu zensieren (Deutschland: 16%, USA: 26%, Großbritannien: 24%).[257] Zudem fand eine PEW-Studie heraus, dass sich Menschen im Anschluss an die NSA-Veröffentlichungen ungern über die NSA im Internet äußerten.[258] Wie im Panoptikum beginnen sich die Überwachten konform zu verhalten.

Marthews/Tucker untersuchten das Suchverhalten vor und nach den Snowden-Veröffentlichungen im Internet in 11 Staaten.[259] Sie konnten mit Hilfe von Google Trends, einem Dienst der die Häufigkeiten von Suchbegriffen in Relation zu den gesamten Googlesuchen zur Verfügung stellt, eine signifikante Abnahme der Verwendung als gefährlich empfundener Suchbegriffe[260] feststellen. Eine deutliche Abnahme war bei den Begriffen feststellbar, die als „high government trouble“ eingeschätzt wurden. International, aber nicht in den USA, war zudem eine Verhaltensänderung in Bezug auf Suchbegriffe feststellbar, die Probleme mit Freunden verursachen könnten.[261]

[257] Centre for International Governance Innovation und Ipsos 2014: S. 12 ff.
[258] Schneier 2015a: S. 96.
[259] Die USA und ihre Top 10 Handelspartner, darunter Deutschland und Großbritannien.
[260] Sie analysierten 282 Suchbegriffe, die zum Teil aus einer veröffentlichten Schlüsselbegriff-Liste (vgl. die vollständige Liste und ihr Einsatz Tremmel 2012a) des Department of Homeland Security (DHS) sowie Googles Top 50 Suchbegriffen für 2013 und einer Umfrage zu Suchbegriffen stammen. Diese wurden anschließend in einem Crowd-Sourcing-Verfahren auf ihre Gefährlichkeit hin bewertet.
[261] Marthews und Tucker 2015: S. 3 ff.

Für Demokratien ist ein gesellschaftlicher Kommunikationsprozess, in welchem verschiedene Standpunkte sowie Minderheitsmeinungen vertreten werden und in Konkurrenz zueinander stehen, von enormer Bedeutung. Minderheitsmeinungen stellen den Motor gesellschaftlicher Erneuerung dar. Sie artikulieren Alternativen, die von der Gesellschaft aufgegriffen und zu einer Mehrheitsmeinung werden können. Funktioniert ein demokratischer Diskurs wandelt sich die Gesellschaft so zum Besseren.[262] Man denke an die ursprünglichen Minderheitsmeinungen, die sich zu Bewegungen formierten und schließlich im Mainstream ankamen: Umweltschutz (Umweltbewegung), Frauenrechte (Frauenbewegung), Homosexualität (LGBT-Bewegung (Lesbian, Gay, Bisexual und Transgender)). Diese erneuerten und wandelten die Gesellschaft immens.[263]

Neben Minderheitsmeinungen spielen Journalist_innen, Whistleblower_innen, Aktivist_innen und Meinungsführer_innen eine besondere Rolle im Prozess demokratischer Meinungsbildung und Erneuerung. Gerade auf diese wirkt die geheimdienstliche Überwachung besonders: „Sie macht Einzelpersonen, die aus der Masse heraustreten, für die Hoheitsmacht erkennbar und schüchtert sie so ein.“[264]

Laut einer Studie von PEN America, einer Sektion der internationalen Schriftstellervereinigung PEN, nahmen viele Journalist_innen an, dass die Regierung ihr Onlineverhalten überwacht. Gleichzeitig stellt die Studie fest, dass geheimdienstliche Massenüberwachung zu Selbstzensur unter Journalist_innen führt. 24% mieden bestimmte Themen in Konversationen am Telefon oder via E-Mail - 9% zogen dies in Betracht. 16% der Journalist_innen vermieden es über bestimmte Themen zu schreiben oder zu sprechen - 11% überlegten sich, dies zu tun. Ebenfalls 16% änderten ihr Onlineverhalten (Internetsuchen und Webseitenbesuche) in Bezug auf Themen, die als kontrovers oder verdächtig angesehen wurden.[265]

> „Writers reported self-censoring on subjects including military affairs, the Middle East North Africa region, mass incarceration, drug policies, pornography, the Occupy movement, the study of certain languages, and criticism of the U.S. government.“[266]

Die Veröffentlichung der massenhaften Telekommunikationsüberwachung hatte si-

[262] Assion 2014: S. 63 ff.
[263] Ebd.: S. 67 ff.
[264] Ebd.: S. 81.
[265] PEN American Center 2013: S. 5 f.
[266] Ebd.: S. 6.

gnifikante Auswirkungen auf das Verhalten zahlreicher Internetnutzer_innen. Sie begannen insbesondere als unerwünscht wahrgenommenes Verhalten zu unterlassen oder zu verstecken. Diese Chilling Effects prognostiziert das Panoptikum, durch eine umfassende Überwachung, bei welcher der Überwachungsvorgang selbst nicht wahrnehmbar, die Überwachungsmöglichkeit an sich aber präsent ist - dies geschah durch die Snowden-Veröffentlichungen. Im Speziellen sind diese Verhaltensänderungen und damit die Internalisierung der Überwachung bei Journalist_innen zu beobachten. Anzunehmen sind ähnliche Wirkungen bei Randgruppen, Aktivist_innen, Whistleblower_innen, Meinungsführer_innen, sowie Vertreter_innen von Minderheitsmeinungen. Durch die Einschüchterung dieser Menschen und Gruppen verliert die Gesellschaft ein Großteil ihres ihr Innovations- und Selbsterneuerungspotentials.

4.3 Zwischenfazit

Die geheimdienstliche Telekommunikationsüberwachung weist zwar Züge einer disziplinargesellschaftlichen sozialen Kontrolle auf, sie lässt sich aber nur mit Einschränkungen erklären. Ein allgemeingültiger, öffentlicher, geheimdienstlicher Normenkatalog existiert nicht. Das Gesetz stellt einen solchen dar, allerdings arbeiten Geheimdienste häufig im Vorfeld von gesetzlichen Normverstößen und international. Durch die Zusammenarbeit mit Strafverfolgungsbehörden sind Geheimdienste jedoch auch in ihrer jeweiligen Jurisdiktion aktiv. Es werden Normverstöße detektiert und (normierend) sanktioniert. Insofern ist eine disziplinargesellschaftliche Sozialkontrolle durch Geheimdienste, nur über Strafverfolgungsbehörden vermittelt, feststellbar. Diese Vermittlung wird zudem mittels parallel construction häufig maskiert.

Mit Hilfe des panoptischen Prinzips lassen sich grundsätzliche, disziplinargesellschaftliche Wirkungen jenseits der (normierenden) Sanktion und des festen Normenkataloges feststellen. Das Paar *sehen und gesehen werden* wird wie bei der Architektur des Panoptikums voneinander getrennt: Die geheimdienstliche Telekommunikationsüberwachung gewährleistet einen tiefgehenden, kontrollierenden Blick auf das Individuum. XKeyscore lässt mit einem Blick auf die aktuelle Telekommunikation eine Prüfung auf Normkonformität zu. Hinzu kommt eine rückwirkende Kontrolle sowie ein schweifender Blick, vermittelt über Suchbegriffe, Fingerabdrücke, appIDs.

Weiter lassen sich bestimmte Personen, Gruppen oder Orte dauerhaft in den Blick nehmen. Die Sichtbarkeit kann durch die Verwendung von Verschlüsselung und Anonymisierungsdiensten deutlich herabgesetzt werden. Die Geheimdienste versuchen

diese Möglichkeiten aber möglichst gering zu halten. Ob ein Individuum überwacht wird oder nicht, ist für dieses nicht feststellbar.

Eine weitere Voraussetzung für eine Internalisierung der Überwachung stellt das Wissen um die Überwachungsmöglichkeiten dar. Dieses Wissen bestand bis zu den Snowden-Leaks und deren Aufarbeitung nicht, und war keineswegs durch die Geheimdienste intendiert. Insofern wurde der panoptische Turm ironischerweise von den Kritiker_innen der geheimdienstlichen Massenüberwachung errichtet. Eine Bekanntheit bei einem großen Teil der (Welt-)Bevölkerung kann empirisch nachgewiesen werden. Das Wissen um die Überwachung weist allerdings eine gewisse Fragilität auf, da die kontinuierliche Erneuerung des Wissens von der weiteren Aufarbeitung und medialen Vermittlung des NSA-Skandals abhängt.

Durch eine panoptische Trennung des Paares *sehen und gesehen werden*, obgleich mit kleineren Einschränkungen, in der ein Wissen um die Überwachung gezeigt werden kann, lässt sich eine Internalisierung der Überwachung annehmen. Empirisch ist eine Internalisierung der Überwachung und damit ein Anpassen des Verhaltens, nachweisbar. Eine dieser Wirkungen ist allerdings die Umgehung jener Überwachung. Es sind auch *Chilling Effects* zu beobachten. Die Menschen schränken die als problematisch angesehenen Verhaltensweisen ein. So ist beispielsweise eine Zensur unter Journalist_innen, sowie im Allgemeinen eine Selbstzensur festzustellen.

Die geheimdienstliche Telekommunikationsüberwachung weist panoptische Züge auf.

5 Geheimdienstliche Sozialkontrolle in der Sicherheitsgesellschaft

Es lassen sich zwar disziplinargesellschaftliche beziehungsweise panoptische Effekte der geheimdienstlichen Telekommunikationsüberwachung feststellen, doch eine hinreichende Erklärung für die soziale Kontrolle liefern sie nicht. Mit dem Wandel der Disziplinar- hin zur Sicherheitsgesellschaft liegt es nahe, dass auch die Geheimdienste mit ihrem Wandel nach dem Kalten Krieg und dem massiven Ausbau der Telekommunikationsüberwachung nach den Terroranschlägen des 11. September 2001 primär in der Sicherheitsgesellschaft zu verorten sind.[267] Dabei stellt das wichtigste Konzept die Verwaltung des empirisch Normalen mit ihren Techniken der Selbstführung, der Kontrolle und des Ausschlusses dar.

5.1 Verwaltung des empirisch Normalen

War in der Disziplinargesellschaft ein Normenkatalog der Ausgangspunkt, an welchen sich die Individuen zu halten hatten, dessen Einhaltung kontrolliert und etwaige Abweichung sanktioniert wurde, stellt in der Sicherheitsgesellschaft die empirische Realität den Bezugsrahmen dar. Nicht ein fester Normenkatalog, sondern der gesellschaftliche Durchschnitt ist normgebend. Der Wertekanon ist dabei heterogener geworden und lässt Abweichung bis zu einem bestimmten Punkt, *flexiblen Toleranzgrenzen*, zu. Der Illusion, allen Individuen einen festen Normenkatalog aufzwingen zu können, wird sich nicht mehr hingegeben.[268]

> „In dieser Perspektive sind Abweichung und Kriminalität normale Verhaltensweisen die mit einer gewissen statistischen Häufigkeit in einer Gesellschaft auftreten und mit denen ein pragmatischer Umgang gefunden werden muss, um sie in hinnehmbaren Grenzen zu halten.“[269]

Es sollen Probleme und Gefahren ermittelt werden, die die Gesamtheit der Gesellschaft betreffen, sie sollen ökonomisch und effektiv gehandhabt werden. Es geht um „eine möglichst frühzeitige Erkennung und Abwendung von Grenzüberschreitungen

[267] MacAskill und J. Ball 2013; Rosenbach und Stark 2014: S. 117.
[268] Singelnstein und Stolle 2012: S. 119, 121.
[269] Ebd.: S. 64.

einerseits sowie eine Unschädlichmachung bei nicht mehr hinnehmbaren Fällen oder Wiederholungstäter_innen andererseits“.[270]

In diesem Feld bewegen sich auch die Geheimdienste. Der Zweck der Überwachungsprogramme ist es, möglichst viele Daten anzuhäufen und die Gesellschaft als Ganzes sowie gezielt Gruppierungen, Situationen und Räume in den Blick zu nehmen.[271] Dabei wird (automatisiert) nach Anomalien also Verhaltensauffälligkeiten gesucht.

> „Die *traditional surveillance*, die Kontrolle einzelner Personen und kleiner Gruppen, hat sich zur *new surveillance* der Überprüfung von Kategorien, Mustern und Gruppen gewandelt“.[272]

Mit SKYNET verfügt die NSA über eine cloudbasierte Verhaltenserkennungssoftware. Diese analysiert die gesammelten Meta- und Standortdaten ganzer Länder, um Kommunikations-, Bewegungs- und Reiseprofile von Menschen zu erstellen, um sie auch untereinander in Kontext zu setzen, um Netzwerke zu erkennen: Wer hält sich mit wem auf? Wer kommuniziert mit wem? Zudem errechnet SKYNET typische Tagesroutinen von Millionen von Menschen - und damit das typische Verhalten eines jeden Einzelnen sowie der Gesellschaft.[273]

Zur Auswertung der Daten verwendet SKYNET einen lernenden Algorithmus. Dieser soll die Verhaltensweisen der Individuen selbstständig einordnen und verdächtiges, abweichendes Verhalten von Normalem trennen. Er wird anhand von Referenzdatensätzen trainiert. Die Datensätze enthalten normales Verhalten, sowie das gesuchte deviante Verhalten. In einer internen NSA-Präsentation wird hierzu auf Profile von Kurier_innen, die Botschaften zwischen Terrorist_innen oder terroristischen Gruppen übermitteln,[274] zurückgegriffen. Mit Hilfe dieser Referenz- oder Trainingsdatensätze errechnet der Algorithmus einen Klassifizierungsalgorithmus, der Kurier_innen, Terrorist_innen oder anderes deviantes Verhalten selbstständig erkennen soll. Der Algorithmus verfeinert den Klassifizierungsalgorithmus während

[270] Singelnstein und Stolle 2012: S. 65.
[271] Ebd.: S. 120.
[272] Zurawski 2007: S. 8. Hervorhebung im Original.
[273] Ermert und Grothoff 2016: S. 82; National Security Agency 2012c: Folie 3; National Security Agency 2012b: Folie 9, 15 ff.
[274] Diese greifen aus Angst vor Telekommunikationsüberwachung auf Kuriere zurück, die Nachrichten „offline“ übertragen. Auf diese Weise sollen weder Inhalte, noch Metadaten und damit Organisationsstrukturen, als auch die Standorte der Terrorist_innen, verraten werden.

seiner Arbeit immer weiter, er lernt mit.[275]

Der Algorithmus arbeitet mit Wenn-Dann-Beziehungen: „Telefoniert jemand sehr selten, dann aber nachts und wechselt danach stets den Standort weicht dieses Verhalten signifikant von dem“[276] anderer Personen beziehungsweise von dem des Durchschnittes ab. Aus hunderten solcher Erkenntnisse berechnet SKYNET einen Wert, dessen Höhe davon abhängt, für wie wahrscheinlich der Algorithmus eine Person beispielsweise für eine Kurier_in hält. Anhand eines Schwellenwertes wird die Toleranz definiert. In einer internen Präsentation legt die NSA einen Schwellenwert fest, der eine Erfolgsquote von 50% definiert, das bedeutet, dass das System jede zweite Kurier_in findet, die anderen 50% bleiben als False-Negatives unerkannt. Allerdings stehen diesen False-Positives[277] gegenüber, Menschen die in diesem Beispiel als Kurier_innen eingeordnet werden, obwohl sie keine sind.[278]

Das System vermisst algorithmisch die Bevölkerung und sucht nach abweichendem Verhalten. Sie lässt dabei vom empirischen Mittel abweichendes Verhalten bis zu einer bestimmten Toleranzgrenze zu. Erreicht die Abweichung einen festgelegten Schwellenwert, wird das Verhalten als jenseits der Toleranzgrenze wahrgenommen und entsprechend verwaltet.

Ein Problem stellen allerdings False-Positives dar. Algorithmen sind nicht allmächtig, sie übersehen Gesuchtes (False-Negatives) und finden Nicht-Gesuchtes (False-Positives). So können nicht alle Risikoträger_innen algorithmisch gefunden werden und viele nicht Riskante werden verwaltet. Dies kann durchaus auch Journalist_innen[279] treffen, die beispielsweise ein ähnliches Telekommunikations-, Bewegungs- und Reisverhalten wie Kurier_innen terroristischer Organisationen aufweisen können.

[275] Ermert und Grothoff 2016: S. 82; National Security Agency 2012c: Folie 2; National Security Agency 2012b: Folie 5.

[276] Ermert und Grothoff 2016: S. 82 f.

[277] Die NSA nennt in Testläufen Fehlerraten zwischen 0,008 und 0,18 Prozent. Diese immens niedrige Fehlerrate stellt die sonst von Big Data bekannten Erfolgsquoten in den Schatten und ist vermutlich auf einen Designfehler in einem Testlauf innerhalb Amerikas mit zufällig gewählten Personen, aber einem bekannten Netzwerk aus Terrorist_innen zurückzuführen. Da die Terrorist_innen-Stichprobe nicht auf die selbe Weise wie die Bürger_innen gezogen wurde, ist davon auszugehen, dass sie für den Algorithmus deutlich leichter zu erkennen sind. (vgl. ebd.) Die Zahlen dürften daher utopisch sein.

[278] National Security Agency 2012c; Ermert und Grothoff 2016: S. 82 f.

[279] In einer Präsentation zu SKYNET erreichte der Al Jazeera Journalist Ahmad Muaffaq Zaidan den höchsten Wahrscheinlichkeitswert. Sein Reiseverhalten glich dem einer Kurier_in. Zaidan interviewte - wie andere Journalist_innen auch - mehrfach Terrorist_innen, darunter Bin Laden. (vgl. Currier, Greenwald und Fishman 2015)

Die US-amerikanischen Intelligence Advanced Research Projects Activity (IARPA) führt Forschungsprojekte im Geheimdienstbereich durch. Sie arbeitet Geheimdiensten, darunter auch die NSA, sowie dem Militär zu. Mit MERCURY möchte sie bestehende Probleme bei Programmen zu Vorhersage und Erkennung von Verhalten (wie z.B. SKYNET) beseitigen oder zumindest verbessern:

> „[I]n many cases, relevant data have significant lag times, lack accuracy or are classified. There has been little research to examine whether classified data from foreign Signals Intelligence (SIGINT) can be used to forecast events with high accuracy and lead-time. The Mercury program aims to fill this gap by developing methods for continuous, automated analysis of foreign SIGINT data to anticipate and/or detect significant events, including military and terrorist activities, political crises and disease outbreaks in Arabic-speaking countries in the Middle East and North Africa."[280]

Die Vorhersagen sollen mit der Entwicklung von empirisch-soziologischen Modellen von bevölkerungsweiten Verhaltensänderungen rund um solche Ereignisse detektiert werden. Trainiert werden soll es mit Ereignissen, von denen die USA bzw. die westlichen Geheimdienste überrascht wurden. Das System soll, sofern es Erfolg hat, nahe an den Überwachungspunkten der jeweiligen Länder installiert werden. Dort soll es die Daten nahezu in Echtzeit erhalten, damit die probabilistischen Algorithmen schnell und zeitnah Aussagen treffen können.[281]

Das Forschungsprojekt CAUSE ging 2015 analog dazu vor. Es erforschte die frühzeitige Erkennung oder Prognose von Cyberattacken.[282] In den letzten Jahren gab es ähnliche Forschungsprojekte, die sich auf die Vorhersagen von gesellschaftlichen Ereignissen wie Unruhen oder die Ausbreitung von Krankheiten konzentrierten. Diese verwendeten im Gegensatz zu MERCURY öffentlich zugängliche Daten (OSINT).[283]

Geheimdienste sind zunehmend im Bereich der algorithmischen Verhaltenserkennung und Ereignisvorhersage aktiv. Dabei handelt es sich mitnichten nur um die Erkennung von Terroranschlägen, sondern auch um die frühzeitige Erkennung von Aufständen und Unruhen. Dies ermöglicht eine gezielte, präventive Verwaltung der

[280] Intelligence Advanced Research Projects Activity o. J.
[281] Möchel 2016; Intelligence Advanced Research Projects Activity o. J.
[282] Möchel 2016.
[283] Intelligence Advanced Research Projects Activity o. J.

kommenden Aufstände - bevor oder während sie im Entstehen begriffen sind. So können besonders wichtige Aktivist_innen erkannt und mit staatlichen Einzelmaßnahmen beschäftigt, gegängelt, diffamiert oder ausgeschlossen werden (siehe Kapitel 5.3.2). Das Verfahren lässt sich auch auf (kritische) Journalist_innen und ihre Quellen, sowie Meinungsführer_innen und Minderheiten anwenden.

Neben SKYNET und MERCURY gibt es weitere Programme die vom gesellschaftlichen Durchschnitt abweichendes Verhalten detektieren sollen. Das seit Ende der 1990er Jahre verwendete Programm PROTON nutzt ebenfalls Telekommunikationsdaten zur Verhaltenserkennung. Es soll mittels der Analyse von Telekommunikationsnetzwerken Gruppenzugehörigkeiten sowie deviantes Verhalten erkennen. Als Referenzdaten wird auf das Telekommunikationsverhalten bereits bekannter, devianter Personen zurückgegriffen.[284] Auch mit dem im Geheimdienstbereich verbreiteten Programm XKeyscore soll abweichendes Verhalten detektiert werden: Mit einer internen Folie werden die Analyst_innen geschult, um Verhaltensauffälligkeiten und Anomalien[285] zu suchen.[286] Analyst_innen können, sofern sie die Fähigkeit dazu besitzen, XKeyscore um kleine Programme (Skripte) erweitern und so selbst Verhaltensanalysen durchführen. Der GCHQ setzt SQUEAKY DOLPHIN zur Aufstandserkennung ein (siehe Kapitel 5.3.1). Neben selbst entwickelten Programmen greifen die Geheimdienste auch auf kommerzielle Big Data Anwendungen von Firmen wie Palantir, SAP, IBM und vielen weiteren zurück.[287]

All diese Programme sind Big Data Anwendungen, deren Ziel es ist, eine ungeheure Menge von zumeist unstrukturierten Daten auszuwerten. Um die massenhaft gesammelten Daten nutzbar zu machen, greifen die Geheimdienste auf solche Software zurück. Diese strukturieren die Daten, analysieren sie algorithmisch, um Erkenntnisse aus ihnen zu ziehen. Sie durchsuchen die komplexen Daten nach Mustern, Rastern und erstellen Profile. Das Ganze möglichst „live“ und in Echtzeit. Der Analysevorgang wird Data Mining genannt.[288]

Nichts anderes machen Google, Facebook und weitere Firmen mit dem Verkauf individueller Werbung: Sie analysieren das Onlineverhalten und errechnen daraus bestimmte Prognosen und Abhängigkeiten. Wenn sie erkennen, dass Menschen, die

[284] R. Gallagher 2014c.
[285] Als Beispiele werden Personen genannt, die eine Sprache sprechen, die für die Region unüblich ist, Menschen die Verschlüsselung benutzen oder nach verdächtigen Dingen im Internet suchen.
[286] National Security Agency 2008: Folie 15.
[287] Für einen groben Überblick vgl. Jakobs 2014.
[288] Ciesielski 2014.

A, B und C mögen, auch D gut finden, können sie dieses Wissen auch auf Menschen anwenden, von denen sie nur Wissen, dass diese A, B und C mögen. Diese mögen mit einer bestimmbaren Wahrscheinlichkeit auch D. Bei den Analysen kommen allerdings deutlich mehr als 4 Variablen zum Einsatz und die Berechnungen sind weitaus komplexer.[289] Durch algorithmische Auswertung lassen sich bestimmte wahrscheinlichkeitsbasierte Aussagen errechnen: Bei Frauen ist die Wahrscheinlichkeit am höchsten sich montags hässlich zu fühlen, daher ist dies ein guter Zeitpunkt um Kosmetikartikel zu bewerben.[290] Schwangere Frauen ändern ihr Einkaufsverhalten auf eine bestimmte Weise, daraus lässt sich sowohl eine Schwangerschaft, als auch der aktuelle Schwangerschaftsmonat prognostizieren.[291]

Wieso das so ist, wird mit den Berechnungen nicht herausgefunden, aber das es so ist. Allerdings nicht als sicherer Kausalzusammenhang, sondern als (signifikante) Wahrscheinlichkeit. Menschen tendieren jedoch dazu die Aussagen der Maschinen als Wahrheit anzusehen, auch wenn es sich nur um Wahrscheinlichkeitsaussagen handelt. Dies kann im Falle des Data Mining durch Privatunternehmen drastische Auswirkungen auf das Leben haben: Teilweise werden Arbeitsplätze nach algorithmischen Erfolgsprognosen vergeben, Kredite werden von Scoringwerten (nichts anderes als ein Wahrscheinlichkeitswert eines Algorithmus) abhängig gemacht. Beispiele für die Verwendung von Algorithmen im (Wirtschafts-)Alltag gibt es zuhauf.

Im Vergleich zu den Auswirkungen die geheimdienstliche Analysen haben, wirkt dies jedoch wie eine Banalität: Ein Vertriebsmanager eines kanadischen Telekommunikationsunternehmens benutzte 2012 in einer SMS den Begriff „wegsprengen“ (original franz. „exploser“), er wollte damit seine Kolleg_innen motivieren, eine möglichst mitreißende Präsentation zu halten. Ein Algorithmus hatte allerdings das Schlüsselwort „exploser“ in seiner SMS mit seiner marokkanischen Herkunft in Verbindung gebracht und daraus eine Terrorwarnung generiert.[292] Die Folgen: Ermittler_innen verhafteten ihn vor seiner siebenjährigen Tochter, durchsuchten seine Wohnung und erklärten seiner Frau, dass sie mit einem Terroristen verheiratet sei, Arbeitskolleg_innen wurden auf einer Geschäftsreise abgefangen und über ihn befragt.[293] Ähnliche Fälle gibt es zuhauf.

Für die Terrorismusbekämpfung eignen sich Big-Data-Systeme mehr schlecht als

[289] Ciesielski 2014.
[290] Lobo 2015: S. 115.
[291] Biermann 2014.
[292] Die NSA-Programme dazu heißen DISHFIRE (SMS-Sammlung) und PREFER (Auswertung).
[293] Bleich 2013.

recht. Terroranschläge sind jenseits von Kriegsgebieten selten und bieten daher kaum Referenzdatensätze, die zudem sehr unterschiedlich sind:

> „Terrorists don't fit a profile and cannot be plucked out of crowds by computers. They're European, Asian, African, Hispanic, and Middle Eastern, male and female, young and old."[294]

Es ist schwierig bis unmöglich ein Muster zu identifizieren. Aber ohne eine genaues Muster oder Profil ist das System statistisch nicht effektiver als zufälliges Kontrollieren.[295] Dies mag auch der Grund dafür sein, dass es keine Zahlen zu algorithmisch verhinderten Terroranschlägen gibt beziehungsweise diese einer Überprüfung nicht standhalten. Ursprünglich behauptete die NSA, dass die Sammlung amerikanischer (Mobil-)Telefonmetadaten 54 Terroranschläge verhindert hätte. Diese Zahl musste sie schrittweise revidieren. Es wurde kein einziger Terroranschlag auf Basis dieser Daten verhindert, allerdings führten sie zur Verurteilung eines Mannes, der 8'500 US-Dollar an al Shabaab[296] in Somalia überwiesen hatte. Eine Untersuchung des Weißen Hauses stellte fest, dass das Programm für die Verhinderung von Terroranschlägen nicht notwendig ist.[297] Zu einem ähnlichen Ergebnis kommt eine Studie der New America Foundation. Diese untersuchte 225 Kriminalfälle mit Terrorismusbezug: Die Massenüberwachung der Telefonverbindungen spielte dabei in maximal 1,8% der Fälle eine Rolle.[298]

Diese Aussage kann allerdings nicht verallgemeinert werden, sie gilt für das seltene Phänomen der Terroranschläge: „Algorithms are better for exerting social control or monitoring political views than they are for predicting large-scale violence."[299] Zur Bevölkerungskontrolle eignet sich die algorithmische Überwachung bestens. Menschen, die im Begriff sind Toleranzgrenzen zu überschreiten oder diese bereits überschritten haben, werden immer besser erkennbar (Risikodetektion) - und können verwaltet (Prävention oder Ausschluss) werden. Nachfolgend soll die geheimdienstliche Telekommunikationsüberwachung mit den sicherheitsgesellschaftlichen Techniken der Selbstführung, der Kontrolle (Risikodetektion und Prävention) und des Ausschlusses untersucht werden. In der Empirie arbeiten die Techniken Hand in

[294] Schneier 2014a: S. 80.
[295] Schneier 2014a: S. 80; McLaughlin 2016.
[296] Al Shabaab stellt nach Einschätzung von US-Behörden keine Bedrohung für Amerika dar.
[297] McLaughlin 2015; Snowden 2014c.
[298] Bergen et al. 2014: S. 4.
[299] McLaughlin 2016.

Hand. Eine klare Zuordnung der Programme ist zum Teil nicht möglich, da sie mit mehreren Techniken zugleich arbeiten. Um eine bessere Lesbarkeit zu gewährleisten werden die Techniken nacheinander vorgestellt und die Programme unter die jeweilige Technik subsumiert.

5.2 Selbstführungstechniken

An die Stelle der Selbstdisziplinierung (Disziplinargesellschaft) treten in der Sicherheitsgesellschaft die Selbstführungstechniken. Das Verhalten wird von alleine und vermeintlich selbstgewollt an antizipierte Standards angepasst. Konformität wird nicht mehr durch Unterdrückung bestimmter Verhaltensweisen gewährleistet, vielmehr werden bestimmte inhaltliche Vorgaben mit Freiräumen verbunden. Das Subjekt kann sich auf verschiedene Weise verhalten, muss aber mit den Konsequenzen seines Verhaltens leben. Dabei werden bestimmte Verhaltensweisen gefördert und andere erschwert. Damit funktionieren die Selbstführungstechniken nicht absolut, sondern schaffen (Verhaltens-)Wahrscheinlichkeiten.

Eine wesentliche Grundlage für die Selbstbeschränkung und -führung stellt eine steigende gesellschaftliche Verunsicherung dar. Dabei erfüllen Sicherheitsdiskurse die Funktion eine permanente Verunsicherung zu gewährleisten. Diese beschreiben nicht die Wirklichkeit, sondern konstituieren sie und werden so zur wahrgenommenen „Wahrheit“.[300]

Mit den Terroranschlägen des 11. September 2001 wurde Terrorismus ein elementarer Bestandteil der Sicherheitsdiskurse. Mit ihnen steigerte sich die Wahrnehmung sowie die mediale Berichterstattung zum Thema internationaler Terrorismus immens. Terrorismus ist seitdem ein zentraler Angstfaktor in westlichen Gesellschaften, dabei wird ausgeblendet, dass es international agierende, bewaffnete Gruppen schon seit den 1970er Jahren gibt und Terroranschläge damals viel stärker zum „Alltag“ in Westeuropa gehört haben, als heutzutage.[301]

Geheimdienste, Polizeien, Sicherheitspolitiker_innen und zum Teil auch Kommentator_innen prägen die Sicherheitsdiskurse seit den Terroranschlägen des 11. September 2001 und betonen stetig die neue Quantität und Qualität der Bedrohung durch Terrorismus.[302] Mit dieser begründen und fordern sie den immer weiteren

[300] Singelnstein und Stolle 2012: S. 34, 75 – 77.
[301] Ebd.: S. 38.
[302] Greenwald 2015a.

Ausbau von (Telekommunikations-)Überwachungsmaßnahmen.[303] Diese Argumentation geht einher mit der Vorstellung, dass Terroranschläge einfach und jederzeit durchführbar seien[304] - und nur ein weiterer Ausbau der Sicherheitsorgane und -technologien, der aber immer weiter fortschreiten müsse, der „neuen" Bedrohungen Einhalt gebieten könne. Neben Terrorismus spielt auch die (Gewalt-)Kriminalität sowie ein Versicherheitlichung anderer Themen (beispielsweise Migration) eine Rolle in den Sicherheitsdiskursen. Vermittelt über die sehr prägnanten Sicherheitsdiskurse führen diese zu Rückkopplungseffekten, die auf das Sicherheitsgefühl wirken und jene permanente Verunsicherung erzeugen, die den Nährboden für die Selbstführungstechniken bildet.

Die Angst vor Terroranschlägen ist seit den Anschlägen des 11. September 2001 konstant hoch. So war laut eine Untersuchung von McArdle/Rosoff/John die Angst auch fünf Jahre nach den Anschlägen ähnlich hoch, wie kurz danach.[305] Nach einer Umfrage der Chapman University hatten 2015 44.4% der US-Amerikaner Angst vor einem Terroranschlag.[306] 58% der Briten sorgten sich 2015 um Terrorismus.[307]

Auch die Angst vor Kriminalität ist gesellschaftlich präsent: 59% der US-Amerikaner_innen beschreiben Kriminalität als extremes oder sehr ernsthaftes Problem. Obwohl die Kriminalität in den USA in den letzten Jahren zurückging,[308] geht die Wahrnehmung in der Bevölkerung von einem massiven Anstieg der Kriminalität aus. So sahen 2015 70% der US-Amerikaner$_i$*nneneinewachsendeKriminalittalsgegebenan.*[309]*Vergleichbaresgiltfr Grobritannien.*[3

In Deutschland führt die Versicherungswirtschaft seit 1991 eine Umfrage zu den „Ängsten der Deutschen" durch. Dabei liegt der Index der Personen mit „großer Angst" seit 1992 bei knapp unter 40% bis knapp über 50%. 2015 hatte mit 52%[311] jede Zweite Angst vor Terrorismus.[312] In den Jahren vor dem 11. September 2001 (1996 - 2001) lag die durchschnittliche Angst vor terroristischen Anschlägen bei

[303] Schneier 2015a: S. 138; Rosenbach und Stark 2014: S. 118.
[304] Schneier 2014a: S. 77.
[305] McArdle, Rosoff und John 2012: S. 749 ff.
[306] Ledbetter 2015.
[307] Mann 2015.
[308] Die Viktimisierungsrate sank von 87 Anfang der 1990er Jahre auf 20 2014 (pro 100'000 Einwohner_innen).
[309] McCarthy 2015.
[310] Fogg 2013.
[311] Die Zahlen dürften nach den Anschlägen in Paris im November 2015 und Brüssel im März 2016 weiter angestiegen sein.
[312] R+V Versicherungen 2015.

24,7% und nahm in der Tendenz ab. In den Jahren danach stieg die Angst rapide an und hielt sich seitdem auf einem hohen Niveau mit durchschnittlich 46%.[313]

Nach einer Umfrage des Magazins der Spiegel fühlten sich im Sommer 2015 23% durch den Terrorismus stärker bedroht als zwei Jahre zuvor, während 72% keine große Veränderung in der Bedrohungslage erkannten und nur 4% sich weniger bedroht fühlten.[314]

Die Furcht vor Kriminalität sowie die Angst Opfer eben jener zu werden, ist seit Mitte der 1990 Jahren hingegen rückläufig. Sie liegt 2010 bei 21,5%. Real erlebt haben Kriminalität[315] in einem Zeitraum von 5 Jahren (2005 - 2010) jedoch nur 9,5% - dies ist europaweit einer der niedrigsten Werte.[316] Dennoch wird von einer deutlichen Zunahme von Kriminalität ausgegangen. So nahmen 2003 91% der Menschen in Deutschland einen Kriminalitätsanstieg an.[317]

War das disziplinargesellschaftliche Versprechen die wohlfahrtsstaatliche Absicherung und Inklusion, tritt an diese Stelle das Versprechen der staatlich organisierten Sicherheit. Daher bilden die in einem beträchtlichen Teil der Gesellschaft manifestierte Ängste einen zentralen Bezugspunkt für die Sicherheitsgesellschaft. Angst vor Terrorismus und Kriminalitätsfurcht scheint „die Funktion eines Katalysators für soziale Zukunfts- und Existenzängste zuzukommen.“[318] Der mit der Krise des Wohlfahrtsstaates einhergehende Abbau staatlicher Sozialleistungen und unsicherer werdender Wirtschaftsverhältnisse, ließ die Zukunfts- und Existenzängste massiv ansteigen.[319]

Aus diesen Ängsten entsteht ein verstärktes Bedürfnis nach Sicherheit, dass sich auf der Ebene der Zukunfts- und Existenzängste nur schwerlich begreifen und bearbeiten lässt.[320] Die daraus entstehende diffuse Verunsicherung führt zu einer erhöhten Wahrnehmung und Angst vor (Gewalt-)Kriminalität und Terrorismus, welches durch die Sicherheitsdiskurse stetig befeuert wird.

Obgleich die Sicherheitsgesellschaft zu einer gesellschaftlichen und politischen Toleranz gegenüber unkonventionellen Verhaltensweisen und damit einhergehend einer

[313] R+V Versicherungen o. J.
[314] Spiegel 2015b: S. 22.
[315] Einbruch oder Überfall bezogen auf eine Person oder ein Haushaltsmitglied.
[316] Statistisches Bundesamt 2013: S. 301 f.
[317] vgl. Bundesministerium des Innern und Bundesministerium der Justiz 2006: S. 491 ff.
[318] Singelnstein und Stolle 2012: S. 40.
[319] Zahlen zu wirtschaftl. Verunsicherung vgl. R+V Versicherungen 2015; R+V Versicherungen o. J.
[320] Von staatlicher Seite wird der Sozialabbau mit wirtschaftlichen Sachzwängen und einer notwendigen Standortpolitik begründet. (vgl. Hirsch 1998: S. 31 ff.)

Pluralisierung von Lebensstilen geführt hat, finden sich weiterhin Ausgrenzungstendenzen gegenüber bestimmten, meist migrantischen Randgruppen. Diese werden im Zusammenhang mit Gewalt und Kriminalität thematisiert[321] aber auch als kulturelle Bedrohung wahrgenommen.[322]

In der anhaltend hohen Angst vor dem internationalen Terrorismus verbinden sich die gesellschaftliche Furcht vor (Gewalt-)Kriminalität und Randgruppen, insbesondere Migrant_innen, sowie die auf diese projizierten sozialen Abstiegs-, Zukunfts- und Existenzängste. Diese konstruierten und übersteigerten Ängste finden in Sicherheitsdiskursen ihren Ausdruck, welche von präventiven und punitiven Bekämpfungsmethoden geprägt sind. Das Bedürfnis nach Sicherheit wird vom Staat mit dem Versprechen die Bürger_innen vor Kriminalität, Terrorismus und sonstigen Gefahren zu beschützen bzw. ein Gefühl von Schutz zu vermitteln, aufgegriffen und reproduziert. So ist eine immer weitergehende Verschärfung des Strafrechts sowie eine zunehmende gefahrenabwehrorientierte Ausrichtung der Strafverfolgungsbehörden zu beobachten.[323] Diese werden um geheimdienstliche Praktiken ergänzt, die die Bevölkerung als Ganzes ins Auge fassen und weit im Vorfeld strafbarer Handlungen agieren.

Aus diesem Sicherheitsversprechen leitet sich in der Sicherheitsgesellschaft die Legitimation des Staates ab. Beispielsweise konnte in Folge des 11. September 2001 eine gestiegene Zufriedenheit sowie Vertrauen in die Regierung in den USA beobachtet werden.[324]

Viele der staatlichen Sicherheitsmaßnahmen erzeugen keinen ernstzunehmenden Sicherheitsgewinn. Bruce Schneier hat für diese den Begriff des *Sicherheitstheaters* geprägt. Ein Beispiel sind die Bewachung von Flughäfen durch Polizist_innen mit Maschinenpistolen, die zum Teil nicht oder mit Platzpatronen geladen sind.[325] Auch jenseits der Platzpatronen erzeugen die Polizist_innen keine reale Steigerung der Sicherheit. Dennoch erzeugen sie bei den Menschen zweierlei Gefühle. Zum einen wird ein Gefühl von Unsicherheit erzeugt: Wenn hier schwerbewaffnete Polizist_innen stehen bzw. notwendig sind, muss hier eine Gefahr vorliegen, es sich um einen ge-

[321] Die Verbindung von Gewalt bzw. Kriminalität mit Migrant_innen oder Flüchtlingen entbehrt jeglicher empirischen Grundlage. Nach einer Lageübersicht des BKA sind Flüchtlinge nicht mehr oder weniger kriminell als die restliche Bevölkerung. Allerdings ist ein immenser Anstieg von Straftaten gegen Flüchtlingsheime zu beobachten. (Kampf 2015)

[322] Goenemeyer 2010: S. 15 f.; Lindenberg und Schmidt-Semisch 1995: S. 3.

[323] Singelnstein und Stolle 2012: S. 41 f.; Hirsch 1998: S. 82.

[324] McArdle, Rosoff und John 2012: S. 745.

[325] Schneier 2014a: S. 74.

fährlichen Ort handeln. Zum anderen wird ein Gefühl der Sicherheit vermittelt: Die schwer bewaffneten Polizist_innen werden mich vor Gefahren schützen.

Beide Gefühle sind für die sicherheitsgesellschaftliche Legitimation des Staates wichtig. Dieser „erfüllt“ das Versprechen einer Sorge um die körperliche Unversehrtheit, den Schutz vor Gewalt, Kriminalität und Terror, durch ein Sicherheitsgefühl. Gleichzeitig dient die gefühlte Unsicherheit dazu, dass ihm seine eigene Legitimationsgrundlage, die Schaffung von Sicherheit, nicht abhanden kommt. So reproduziert er stetig seine eigene Legitimation und deren Grundlage.

Das Ideal einer umfassenden Sicherheit führt zu einer Ausweitung der staatlichen Sozialkontrolle. Die Individuen werden mit Hilfe einer permanenten Krise regiert oder geführt.[326] Die Terroranschläge des 11. September 2001 sind dabei nicht der Grund, sondern der Anlass einer Verschärfung bereits länger bestehender Entwicklungen.[327]

Der permanenten Angst vor dem internationalen Terrorismus und anderen Bedrohungen kommt eine weitere Funktion zu: Die als existentiell empfundene Bedrohung rückt andere Sorgen in den Hintergrund und führt zu einem Streben nach individueller Sicherheit.[328] Der einzelne Mensch sieht die Notwendigkeit der Beschneidung seiner Handlungsfreiheit ein, fordert sie sogar selbst.[329] Mit den sicherheitspolitischen Maßnahmen gehen auch Verhaltensanweisungen bzw. -vorschriften einher. Diese entwerfen ein moralisches Programm, welches dem Individuum ein „vernünftigen“ Umgang mit den Risiken nahelegt und unterstellt, dass eine Betroffenheit auch von eigenen Handlungen abhinge.[330] Zudem erfordert die Logik des Risikos (permanente Gefahr, die jederzeit eintreten kann) und der Prävention (es kann nie genug getan werden, um das Risiko zu minimieren) trotz des staatlichen Sicherheitsversprechens auch individuelle Verhaltensänderungen. Die hierdurch erzeugte Selbstverantwortung und -optimierung wird dem Individuum auch in vielen anderen Lebensbereichen abverlangt (Lohnarbeit, Selbstbildung (lebenslanges Lernen), Risikovorsorge (Versicherung), Gesundheit (Sport, Ernährung)).[331]

Diese Entwicklungen führen zu vielfältigen Anpassungsprozessen und der Übernahme von Werten. Diese werden als vermeintlich selbst gewollt wahrgenommen.

[326] Unsichtbares Komitee 2015: S. 85.
[327] P.-A. Albrecht 2010: S. 175.
[328] Lindenberg und Schmidt-Semisch 2000: S. 309.
[329] P.-A. Albrecht 2010: S. 151 f.
[330] Dollinger 2016: S. 62 f.
[331] Singelnstein und Stolle 2012: S. 77 f.

Das Individuum führt sich selbst.

Dieser Prozess wird von Geheimdiensten und anderen Sicherheitsbehörden durch immer neue Warnungen vor Terroranschlägen und anderen Bedrohungen, sowie Forderungen nach dem immer weiteren Ausbau der Sicherheitsarchitektur aufrechterhalten. Die Maßnahmen und Warnungen erzeugen bei den Menschen einerseits ein Sicherheitsgefühl, gleichzeitig aber auch ein Gefühl von Unsicherheit. Die Geheimdienste sind hierdurch an der Schaffung der Rahmenbedingungen zur Selbstführung beteiligt.

5.3 Kontrolltechniken

Den Kontrolltechniken geht es darum *Risikopotentiale* zu erkennen um diesen frühzeitig begegnen zu können (Prävention). Die Detektion der Risiken funktioniert dabei zunehmend anlasslos und hat die Bestrebung, allgegenwärtig und umfassend zu sein. Durch die Zunahme der Kontrolle und der damit verbundenen Zunahme der Entdeckung neuer Risikofaktoren steigt auch die Anzahl der Risikoträger_innen kontinuierlich an.[332]

„Prävention will etwas Ungewolltes verhindern, sie will etwas ausschließen, von dessen Eintreten sie nie sicher wissen kann, weil es erst in der Zukunft liegt.“[333] Um diese Unwissenheit bändigen zu können werden Informationen benötigt, massenhaft Informationen - zu Ende gedacht bedeutet Prävention absolute Kontrolle. Prävention ist aber nicht nur Überwachung und Kontrolle von Oben, sondern dient auch dazu „(fremdbestimmte) Logiken von den Subjekten als *eigene* Logik“[334] zu verinnerlichen (z.B. Gesundheitsprävention). Sie ist also auch im Bereich der Selbstführungstechniken (siehe oben) aktiv.

5.3.1 Kontrolle und Risikodetektion

Der Anstieg und die Omnipräsenz der Telekommunikation führt zu einer Abbildung gesellschaftlicher Realitäten in digitaler Form. Dieser Umstand ermöglicht den Geheimdiensten durch die weltweite Telekommunikationsüberwachung einen Zugriff auf die Realität. Hieraus ergeben sich umfassende Kontrollmöglichkeiten, wie sie niemals zuvor möglich waren. Jeder Mensch kann weltweit in den Blick genommen und

[332] Singelnstein und Stolle 2012: S. 81 – 82, 119.
[333] Ullrich 2012: S. 211.
[334] Ebd.: S. 211. Hervorhebung im Original.

kontrolliert werden. Der Fokus der geheimdienstlichen Telekommunikationsüberwachung liegt auf der Trennung des tolerierbaren Verhaltens von Verhalten jenseits der Toleranzgrenzen. Hierbei wird jedoch nicht im Sinne der klassischen Strafverfolgung auf begangene Taten reagiert, sondern weit im Vorfeld dieser eine Risikodetektion vorgenommen. Es geht darum, welche Menschen, Gruppen und Orte in Zukunft eine Gefahr darstellen könnten. Diese werden zum Teil vorher politisch definiert[335] oder auf Basis der Geheimdienstarbeit und Data Mining erkannt.

Begründet wird die massenhafte Überwachung mit der Suche nach Terrorist_innen,[336] dabei stellen diese nur eines von vielen Zielen bzw. potentiellen Risikoträger_innen dar. Die NSA verwendet nur 35% ihrer Ressourcen zur Bekämpfung des Terrorismus.[337] Neben der Ausspähung anderer Staaten, internationaler Organisationen (UN, WTO, OSZE, Internationaler Strafgerichtshof und weitere), Kriminalität (Waffenhandel, Drogenhandel etc. pp.) und Wirtschaftsspionage (durch die Geheimdienste),[338] richtet sich die Überwachung auch gezielt gegen Journalist_innen, Whistleblower_innen und Aktivist_innen. Aber auch jede normale Bürger_in kann in das Raster der Geheimdienste fallen. An einem Tag im Jahr 2013 hatte die NSA 117'675 aktive Überwachungsziele.[339]

Um Risiken oder Risikoträger_innen erkennen zu können, greifen die Geheimdienste auf Big Data Anwendungen zurück. Mit diesen analysieren die Geheimdienste die Telekommunikationsdaten auf Muster, Raster und Profile - kurz auf Anomalien und Abweichungen die bereits oder in Zukunft als nicht mehr tolerierbar wahrgenommen werden.

Mit dem 2009 gestarteten Überwachungsprogramm KARMA POLICE wertet der GCHQ die in großem Umfang an Glasfaserleitungen und anderen Orten gesammelten Daten automatisiert aus. Hierzu greift KARMA POLICE auf BLACK HOLE zurück, in welchem die gesammelten Metadaten, zum Teil aber auch Inhalte, für einen Zeitraum von 6 Monaten abgelegt werden. Der Umfang des Datenspeichers betrug zwischen August 2007 und März 2009 über 1,1 Trillionen „Events".[340] 2010 kamen 30 Milliarden Einträge pro Tag hinzu, 2012 50 Milliarden. Nach Angaben eines Dokumentes des GCHQ werden Dienste wie Webmail, E-Mail-Übertragung,

[335] vgl. National Security Agency et al. o. J.
[336] Schneier 2015a: S. 138.
[337] MacAskill und J. Ball 2013.
[338] Rosenbach und Stark 2014: S. 147 – 149.
[339] Schneier 2015a: S. 37.
[340] Government Communications Headquarters 2009b: Folie 3.

Webseitenlogins, FTP, Chats, Webforen, Webcams, Computerspiele und Social Media aber auch schlicht das Surfen im Internet erfasst. Die Liste der Dienste wächst kontinuierlich.[341]

BLACK HOLE wird primär mit Programmen wie KARMA POLICE für die Analyst_innen aufbereitet. KARMA POLICE extrahiert den Browsing-Verlauf der Internetnutzer_innen aus BLACK HOLE. Ziel ist es für jeden im Internet sichtbaren Menschen einen Verlauf der besuchten Internetseiten vorrätig zu haben, sowie für jede sichtbare Webseite einen Nutzer_innen-Verlauf. Allerdings wird hier auf der Ebene von IP-Adressen und nicht mit Namen gearbeitet.[342]

Um die Personen hinter den IP-Adressen zu erkennen, scannt der GCHQ mit dem Programm MUTANT BROTH die verwendeten Cookies. Webseiten erkennen mit Hilfe von Cookies[343] ihre Besucher_innen wieder. Diese Eigenschaft macht sich MUTANT BROTH zu nutze, um Menschen im Internet identifizieren zu können. Intern nennt der GCHQ diese darum auch „target detection identifiers“. Der Geheimdienst hatte zwischen Dezember 2007 und Juni 2008 18 Milliarden eben jener Cookies oder „target detection identifiers“ gespeichert. Verwendet werden hierzu unter anderem Cookies von Yahoo, Google, Hotmail, YouTube, Facebook, Reddit, WordPress, Amazon, YouPorn, Reuters, CNN und BBC.[344]

MUTANT BROTH kann sowohl Nutzer_innen hinter IP-Adressen erkennen, als auch Selektoren (z.B. einer E-Mailadresse) die verwendete IP-Adressen zuordnen. Diese lässt sich dann an KARMA POLICE übergeben, welches den zur IP-Adresse gehörenden Browser-Verlauf einer Nutzer_in offenlegt. Neben der Auswertung durch Analyst_innen kann ein Algorithmus auch automatisiert bestimmte (Verhaltens-)Muster extrahieren. So ist es möglich Lebensrhythmen und Profile zu erstellen. Unter anderem können die typischen Tageszeiten und Orte, an denen eine Person online ist herausgefunden werden.[345]

Die zum Teil automatisierten Auswertungen nutzt der GCHQ nicht nur um abweichendes Verhalten und Risikogruppen zu detektieren, sondern auch um Menschen mit wichtigen Funktionen in bestimmten Gruppen oder Netzwerken zu identifizie-

[341] Government Communications Headquarters 2011c: S. 1; R. Gallagher 2015; Government Communications Headquarters 2009a: S. 2 ff.
[342] The Intercept 2015.
[343] Cookies sind kleine Textdateien die von besuchten Webseiten sowie integrierten Drittseiten auf dem Computer der Nutzer_in abgelegt und wieder ausgelesen werden.
[344] R. Gallagher 2015.
[345] Ebd.

ren. Dies wurde unter anderem zur Vorbereitung von Angriffen auf die Netzwerke europäischer Firmen verwendet. So konnte der GCHQ mittels MUTANT BROTH die Mitarbeiter_innen des niederländischen SIM-Kartenherstellers Gemalto aus den Daten filtern, um sich über jene Zugang zum internen Firmennetz zu verschaffen.

Anschließend stahl der GCHQ gemeinsam mit der NSA die in den SIM-Karten[346] hinterlegten Kryptoschlüssel.[347]

Analog dazu ging der GCHQ beim Hack des belgischen Providers Belgacom vor. Zuerst wurden Systemadministrator_innen und Ingenieur_innen des Providers sowie ihre Computer gesucht, welche anschließend mit Schadsoftware angegriffen wurden. So verschaffte sich der GCHQ Zugang zum internen Netz des Providers und hatte Zugriff auf die Telekommunikation der Kund_innen.[348]

Die Überwachungsprogramme MUTANT BROTH und KARMA POLICE werden von vielen weiteren Programmen ergänzt. Ziel der vielfältigen Programme ist eine vereinfachte Auswertung der Daten durch eine „Question Focused Database“, die die Beantwortung von W-Fragen ermöglichen soll: Wo ist mein Ziel? Wann war mein Ziel zuletzt online? Welche Webseiten hat es sich angeschaut, bevor es auf diese Webseite gekommen ist? Wer hat diese Webseite betrachtet? Wer interagiert mit meinem Ziel? Welche Dateien hat mein Ziel hoch- oder heruntergeladen? Welche alternativen IDs kann ich benutzen, um meinem Ziel zu suchen? Was macht mein Ziel im Moment?[349]

Mit SOCIAL ANTHROPOID lässt sich die Telefon- und Internetkommunikation eines Individuums oder einer Gruppe nachvollziehen. Das Programm bereitet diese zudem visuell auf, um den Analyst_innen eine einfachere Auswertung der Kommunikationsnetzwerke zu ermöglichen. Es stellt neben KARMA POLICE und MUTANT BROTH das Herzstück der Programme dar.[350]

MEMORY HOLE konzentriert sich auf Internetsuchmaschinen wie Google. Die Suchbegriffe werden nach verdächtigen Suchanfragen durchsucht. MARBLED GECKO wertet die Ortssuchen auf Google Earth und Google Maps aus: Auf welche Teile der Erde wurde von wo und wann (und wem) geschaut? Die Besucher_innen

[346] In den SIM-Karten werden Schlüssel hinterlegt, mit welchen eine Verschlüsselung zwischen Mobiltelefon und Sendemast gewährleistet wird. Die Verschlüsselung kann zwar auch ohne die zugehörigen Schlüssel geknackt werden (vgl. Nohl 2014), gelangt der Schlüssel jedoch in die Hände von Geheimdiensten oder andere Dritten, ist jedoch keinerlei Sicherheit mehr gegeben.
[347] Scahill und Begley 2015.
[348] R. Gallagher 2014b.
[349] Government Communications Headquarters 2012e: Folie 3 f.
[350] Government Communications Headquarters 2011d: Folie 2 ff.

von Foren werden mit INFINITE MONKEYS erfasst. SAMUEL PEPYS erfasst neben Metadaten auch Inhalte. Es gibt nahezu in Echtzeit aus, was ein Individuum im Moment online macht.[351] SOCIAL ANIMAL analysiert die zwischenmenschliche Interaktion im Internet (mit Chats, Datenaustausch, Freundeslisten). Mit AUTO-ASSOC lassen sich andere Suchidentifikatoren für ein Ziel finden.[352]

Die Programme arbeiten dabei meist wie KARMA POLICE auf Basis von IP-Adressen und können mit MUTANT BROTH Personen zugeordnet werden. Hat man die entsprechende Person herausgefunden, kann man diese über MUTANT BROTH wiederum in den anderen Programmen suchen und damit auch andere W-Fragen als die ursprüngliche beantworten.[353]

Die meisten dieser Systeme wurden um das Jahr 2010 herum entwickelt und sollen mithilfe automatischer Verknüpfungen und einer Vorauswertung sowie der Visualisierung von Daten den Analyst_innen das Auffinden von Abweichung und Zielen/Individuen in großen Datenmengen vereinfachen. Zudem wird das typische Online-Verhalten von Individuen berechnet (ähnlich dem Verfahren von SKYNET). Dies soll die Wiedererkennung und die Detektion von Verhaltensänderungen vereinfachen. Zudem ist ein Abgleich mit Individuen möglich, die als abweichend gelten. Ähnlich wie Amazons „Kunden, die diesen Artikel gekauft haben, kauften auch". Mit solchen Algorithmen arbeitete der GCHQ 2011: „Terrorists who like website X also like website Y"[354], beschrieb aber die bisher verwendeten Fähigkeiten als „sehr einfache Techniken".[355] Ziel des GCHQ ist es, die Systeme zur Verhaltenserkennung, der Analyse von Lebensrhythmen und Systeme zur Vorhersage von Verhalten weiterzuentwickeln und auszubauen.[356]

Diesem Ziel kam der GCHQ mit dem Programm SQUEAKY DOLPHIN bereits sehr viel näher. Das Programm soll gesellschaftliche Entwicklungen, wie etwa Proteste oder Revolutionen weltweit prognostizieren. Um diese Vorhersagen treffen zu können, werden Social Media Dienste wie Youtube, Facebook und Blogs bei Blogspot/Blogger in Echtzeit überwacht und mit der kommerziellen Software Splunk nach Städten und Regionen ausgewertet. Hierdurch lassen sich automatisiert bestimmte Trends feststellen und Ableitungen treffen, was in diesen Städten und Re-

[351] Ähnliches ist auch mit XKeyscore möglich.
[352] Government Communications Headquarters 2011b: S. 2 ff.
[353] Ebd.: S. 2 ff.
[354] Government Communications Headquarters 2011a: Folie 14.
[355] vgl. für Fähigkeiten, Einschätzung und Entwicklung ebd.
[356] Government Communications Headquarters 2012b: Folie 15.

gionen in naheliegender Zukunft passieren wird.[357]

Entwickelt wurde SQUEAKY DOLPHIN nachdem die Geheimdienste vom Arabischen Frühling komplett überrascht wurden. Die ursprüngliche Intention lag daher auch in der Vorhersage ähnlicher Proteste, so konnten die Proteste gegen die Regierung in Bahrain am 14. Februar 2012 schon ein Tag zuvor vorhergesagt werden. Interne Folien, die die Funktionen des Programms vorstellen sollen, zeigen aber, dass das Programm auch Informationen und Prognosen rund um Ereignisse wie Cricket Spiele in London erstellen kann.[358]

Das Programm dient der Vorhersage von Verhalten in ganzen Städten und Regionen - Ziel ist es, entstehende Risiken zu detektieren. Es ermöglicht auf diese frühzeitig oder präventiv zu reagieren. Obgleich der GCHQ betont, dass man nur an Trends interessiert sei und nicht an einzelnen Individuen, lassen sich mit anderen Überwachungsprogrammen sehr einfach die Personen herausfinden, die für den Protest oder dessen Entstehung besonders wichtig sind oder waren. Diese können präventiv „beschäftigt“ werden, um sie so von ihrem politischen Handeln abzuhalten. Überall auf der Welt.[359]

Der Bundesnachrichtendienst arbeitet bei der „strategischen Fernmeldeaufklärung“ mit Schlagwortlisten, welche sowohl inhaltliche als auch formale (z.B. E-Mailadressen oder Telefonnummern) Selektoren enthalten können. Das Parlamentarische Kontrollgremium veröffentlicht jährlich einen Bericht, in welchem der Umfang dieser Überwachung beschrieben wird. Der BND unterscheidet drei Schlagwortlisten: „Internationaler Terrorismus“ diese enthielt 2014 1’922 Begriffe, „Proliferation und konventionelle Rüstung“ mit 13’757 Schlagworten und „Illegale Schleusung“ mit 28 Begriffen.

Anhand dieser Listen filtert der BND die überwachte Telekommunikation aus dem Internet und dem Telefonnetz (Heuhaufen), um aus diesen im Jahr 2014 25’209 Treffer (die Nadeln) in E-Mails, SMS, Fax und Sprachnachrichten zu finden. Von diesen wurden 65 als nachrichtendienstlich relevant eingeschätzt, das entspricht 0,26%. Die restlichen 25’145 sind Falsch-Positive bzw. irrelevante Daten (Nadeln die doch keine Nadeln waren). 2013 hatten die Filter 15’401 verdächtige Verkehre identifiziert, davon waren 0,8% nachrichtendienstlich relevant.[360] Die Schlagwortlisten sind wohl

[357]Government Communications Headquarters 2012d: Folie 27 ff.
[358]Ebd.: Folie 29 ff.
[359]Holland 2014.
[360]Parlamentarisches Kontrollgremium 2016: S. 7 f.; Rudl 2016.

sehr allgemein gehalten: 2010 hatte der BND einen Höchststand mit 37 Millionen abgefangenen Nachrichten, den massiven Anstieg führte er auf ein Spam-Problem zurück.[361]

Der BND sieht sich technologisch im Hintertreffen, die Budgets der Partnergeheimdienste seien in den letzten Jahren deutlich erhöht worden, so habe die USA das Budget der NSA seit 2004 schrittweise um mehr als 50% erhöht. Auch bei den europäischen Partnerdiensten seien die Budgets erhöht worden, zudem hätten diese technische Modernisierungsprogramme erhalten.[362]

> „Sollte der BND nicht nachziehen und seine Fähigkeiten auf den Stand der Technik bringen, droht er hinter Länder wie Italien oder Spanien zurückzufallen, mit negativen Folgen für den Erkenntnisaustausch in der Gemeinschaft und der Gefahr einer Isolation.“[363]

Mit der 300 Millionen Euro teuren „Strategischen Initiative Technik“ will der BND bis 2020 wieder aufschließen. Hiermit möchte der BND die SIGINT-Aufklärung modernisieren und von einer auf Inhalte fokussierten Überwachung zu einer Metadatenerfassung übergehen. Diese sollen mit dem 70 Millionen Euro teuren „Ausbau der integrierten Datenanalyse (AIDA)“ ausgewertet werden. AIDA soll die Daten in Echtzeit aggregieren, miteinander korrelieren und analysieren. Dabei liegt der Fokus auf aktuellen Aktivitäten im Web, sowie speziell Social Media, um Entwicklungen zu erkennen und vorhersagen zu können. Der BND möchte also ebenfalls Programme wie SQUEAKY DOLPHIN und KARMA POLICE entwickeln und diese einsetzen - mit dem Ziel die „enormen Datenmengen“ besser algorithmisch auswerten und Vorhersagen treffen zu können. Dazu soll auf die kommerzielle Software HANA von SAP zurückgegriffen werden oder eine Open-Source-Lösung gefunden werden.[364] Bisher nutzt der BND zur Auswertung u.a. das von der NSA entwickelte Programm XKeyscore.

Das gemeinsame Ziel des Einsatzes von Überwachungsprogrammen wie SKYNET, MERCURY, KARMA POLICE et al, SQUEAKY DOLPHIN, XKeyscore und der strategischen Fernmeldeaufklärung des BND ist das Aufspüren von riskanter Abweichung. Hierzu kommen zunehmend automatisierte, computergestützte Verhaltens-

[361] Krempl 2016.
[362] Bundesnachrichtendienst o. J.
[363] Ebd.
[364] Meister 2015b; Bundesnachrichtendienst o. J.

analysen und die Analyse der Lebensumstände zum Tragen, aus welchen zukünftiges Verhalten prognostiziert werden soll. Sowohl die NSA, als auch der GCHQ und der BND arbeiten mit bzw. entwickeln Programme zur Verhaltenserkennung und -vorhersage. Aus den von Snowden geleakten Dokumenten geht hervor, dass in diesem Bereich immense Anstrengungen unternommen und massiv Gelder investiert wurden. Die geleakten Dokumente datieren sich hauptsächlich auf den Zeitraum zwischen 2009 und 2012. Es ist davon auszugehen, dass die automatisierte, algorithmische Auswertung der Daten zur Verhaltensanalyse und -vorhersage seitdem massiv weiterentwickelt und ausgebaut wurde. Eine umfassende Kontrolle (sowie Risikodetektion und Prävention) kann nur gelingen, wenn umfassend Daten vorliegen, die analysiert werden können. Dies ist im Falle der massenhaften Telekommunikationsüberwachung gegeben. Neben den algorithmischen Auswertung dieser Daten findet auch weiterhin die klassische Analyse mittels Analyst_innen und Selektoren statt. Beide dienen der Risikodetektion jenseits der Toleranzgrenzen. Sie sollen ein zu viel an Abweichung schon frühzeitig erkennen und anschließend verwalten. Die Verwaltung der Abweichung findet mit präventiven Mitteln und (präventivem) Ausschluss statt und wird in den Folgenden Kapiteln behandelt.

5.3.2 Prävention

Risiko und Prävention sind eng verwobene Konzepte. Das Risiko beschreibt die Möglichkeit eines Schadenseintrittes häufig mit einer Wahrscheinlichkeit. Die Prävention setzt hier an, um im Vorfeld eines möglicherweise eintretenden Schadens dessen Wahrscheinlichkeit weiter herabzusetzen oder auf null zu reduzieren. „Richtiges“ Handeln in der Gegenwart soll eine „bessere“ Zukunft verheißen.[365]

Sowohl eine Risikodetektion als auch der präventive Umgang mit eben jener benötigen umfangreiche Informationen, um im Falle des Risikos potentielle Risiken überhaupt erkennen und bewerten zu können und im Falle der Prävention auf Basis der Risikowahrscheinlichkeit, eine möglichst ökonomische und zielführende Reduktion des Risikos zu erreichen.[366] Beides findet nie einen Abschluss: Durch die immer tiefergehende Kontrolle werden immer neue Risiken und Risikoträger_innen entdeckt. Die Prävention versucht ein prognostiziertes Risiko in der Zukunft möglichst auszuschließen oder zumindest zu minimieren. Da der Schadenseintritt in der

[365] Dollinger 2016: S. 60 ff.
[366] Ullrich 2012: S. 211.

Zukunft liegt, kann prinzipiell nie genug Prävention betrieben werden, um einen Schaden auszuschließen (von dem zudem unklar ist, ob er auch ohne Prävention je eingetreten wäre).

Die Logik des Risikos und der Prävention breitet sich immer weiter aus und prägt die Gesellschaft maßgeblich. Sie geht einher mit einer Verunsicherung nicht alle Risiken ausgeschlossen und nicht genug Prävention betrieben zu haben. Diese Logik wirkt sich auf die Individuen aus und „hilft“ ihnen bei der Selbstführung die richtigen Entscheidungen zu treffen bzw. die Logik und mit ihr Werte zu übernehmen und als eigene anzusehen.

Geheimdienste legitimieren ihre Arbeit öffentlich durch die Bekämpfung des Terrorismus, dabei wird der Begriff nicht nur weit ausgelegt, sondern teilweise immens überdehnt. Die britische Regierung setzt die Berichterstattung über staatliche Überwachung, speziell im Zusammenhang mit den Snowden Leaks, mit Terrorismus gleich. Sie begründet dies damit, dass die Veröffentlichungen geeignet seien, Einfluss auf die Regierung auszuüben und damit der Werbung für eine politische oder ideologische Sache dienen würden. Damit falle sie unter die Definition des Terrorismus.[367]

Unter diese extrem weite Definition, die in einer ähnlichen Form auch von amerikanischen Sicherheitsbehörden verwendet wird,[368] fallen aber auch Aktivist_innen, Whistleblower_innen, Lobbyist_innen, kritische Journalist_innen und viele weitere. Letztlich könnte man damit sogar Wähler_innen, sofern sie zu irgendeinem Zeitpunkt die Regierung beeinflussen bzw. eine politische oder ideologische Sache verfolgen, als Terrorist_innen bezeichnen. Abgesehen davon, dass diese Definition zutiefst antidemokratisch ist, da sich eine Demokratie gerade durch die Artikulation von Interessen und deren Diskussion auszeichnet, ermöglicht sie, die als Terrorist_innen deklarierten Menschen einzuschüchtern und mit der ganzen Härte Anti-Terroristischer-Mittel der Exekutive zu verfolgen.

Ein potentielles Risiko für Staaten stellen Whistleblower_innen dar, die (geheime) Informationen aus dem Staatsapparat an die Presse weitergeben. Geheimdienstliche Telekommunikationsüberwachung wird dazu verwendet, auffällige Kontakte zwischen Behördenmitarbeiter_innen und Journalist_innen zu erkennen. Ein Quellenschutz ist nur noch mit erheblichem Aufwand zu gewährleisten. Schon kleinste Fehler können zur Enttarnung der Quelle führen.[369]

[367] Greenwald 2014a: S. 264 f.
[368] National Counterterrorism Center 2013: Appendix 1.
[369] Holland 2013.

Gleichzeitig wird Journalist_innen, die mit Dokumenten von Whistleblower_innen arbeiten, der journalistische Status abgesprochen oder sie werden zu Terrorist_innen umdeklariert. Dieses Klima führt sowohl bei potentiellen und langjährigen Quellen, als auch bei Journalist_innen zu einer erhöhten Vorsicht und zum unterlassen von Leaks. Laut einer Studie von PEN America, einer Sektion der internationalen Schriftstellervereinigung PEN, führt die geheimdienstliche Massenüberwachung zu Selbstzensur unter Journalist_innen (siehe Kapitel 4.2.3).[370]

Mit der Joint Threat Research Intelligence Group (JTRIG) verfügt der GCHQ über eine Abteilung, die verdeckte Operationen durchführt, die im Internet oder in der realen Welt Wirkung entfalten sollen.[371] JTRIG verfolgt mit seinen „Covert Actions“ dreierlei Ziele:

- Mit der Verbreitung gefälschter Informationen im Internet das Ansehen von Risikoträger_innen zu zerstören
- Online auf Diskurse, Aktivismus und Individuen einzuwirken um diese in ihrem Sinne zu beeinflussen
- Den Zugang zu Telekommunikation durch technische Maßnahmen zu unterbinden

Um diese Ziele[372] zu erreichen verwendet JTRIG vielfältige Methoden zur „Verleugnung, Zersetzung, Herabwürdigung und Täuschung“[373]: Um Menschen telekommunikativ auszuschließen „bombardieren“ sie deren Telefone mit SMS oder Anrufen, Löschen ihre Onlinepräsenz (was sie als für die Opfer besonders lästig („annoying“) beschreiben) oder sie blockieren Faxgeräte.

JTRIG sucht im Onlineverhalten der Betroffenen nach Widersprüchen, die gegen diese verwendet werden können. Als Beispiel wird eine islamische Autorität genannt, die sich im Internet pornografisches Material ansieht. Damit könnte man ihre Glaubwürdigkeit gezielt untergraben. Zum Teil helfen sie aber auch gezielt nach, um die Betroffenen in derlei Situationen zu bringen. Beispielsweise verwenden sie sog. „Honey Traps“: Sie versuchen ihr Opfer zum Besuch einer kompromittierenden Webseite zu verleiten oder eine Online-Bekanntschaft, die sich rufschädigend auf die Zielperson auswirken kann (z.B. Flirt oder Affäre), zu lancieren. Um die Paranoia bei ihrem Ziel zu erhöhen, können sie deren Fotos in Sozialen Netzwerken austauschen.

[370] PEN American Center 2013: S. 6; Greenwald 2014a: S. 254, 300 – 301.
[371] Government Communications Headquarters 2012a: S. 5.
[372] Greenwald 2014b; Government Communications Headquarters 2012a: S. 5.
[373] Government Communications Headquarters 2012a: S. 5.

JTRIG arbeitet auch mit False-Flag-Operations: Die Veröffentlichung von (belastenden) Informationen im Internet unter falschem Namen (falscher Flagge). Sie können (belastende) Informationen in Foren, Soziale Netzwerke oder andere Plattformen stellen. JTRIG kann ein Blog im Namen des Betroffenen erstellen oder belastende E-Mails (die nicht der Wahrheit entsprechen müssen) an die Freund_innen, Nachbar_innen und Verwandten des Opfers schreiben, um es zu denunzieren. Eine weitere Methode besteht darin ein Blog im Namen eines gefälschten Opfers des Betroffenen zu betreiben.[374]

Um einer Firma zu schaden, können JTRIG-Mitarbeiter_innen Informationen an andere Firmen oder die Presse „leaken“, sie können Geschäftsbeziehungen oder Verträge enden lassen oder schlechte Bewertungen und Beschreibungen in Foren oder auf Bewertungsplattformen stellen. Sie arbeiten auch mit aktiven Angriffstechniken wie der Zusendung von Viren/Ransomware[375] oder DDoS[376]-Attacken. Fast schon klassische Methoden stellen die Infiltration von Gruppen, sowie die Anstachelung zu Straftaten[377] und verdeckte Ermittlungen dar.[378]

Um bei der Beeinflussung und Zersetzung der Menschen, Gruppen und Diskurse möglichst erfolgreich zu sein, wird den JTRIG Agenten_innen in internen Schulungen die Grundlagen der Verhaltenspsychologie vermittelt. 2013 sollten 150 JTRIG-Mitarbeiter_innen für das Zersetzungsprogramm voll ausgebildet und einsatzfähig gewesen sein. Diese werden unter anderem gegen politische Gruppen, Drogenhandel, islamistische Aktivitäten, Online- und Finanzbetrug eingesetzt.[379]

JTRIG benutzt diese Methoden um erkannte Risikogruppen und -personen zu verwalten. Sie wirken präventiv auf Individuen, Gruppen und Diskurse ein, um deren Verhalten und Meinung weiter innerhalb der Toleranzgrenzen zu halten, von diesen fern zu halten - oder, wenn die Toleranzgrenzen bereits überschritten wurden, wieder

[374] Government Communications Headquarters 2012a: S. 7 ff.; Greenwald 2014b.

[375] Ransomware verwehrt den Zugang oder die Nutzung von bestimmten Teilen oder dem kompletten Computersystem. Dies geschieht durch die Verschlüsselung bestimmter Dateien oder des ganzen Computers. Häufig wird für die Entschlüsselung Geld verlangt.

[376] Bei einem DDoS-Angriff (Distributed Denial of Service) wird ein Computer oder Server mit extrem vielen Anfragen überhäuft. Dies geschieht von einer größeren Anzahl von Computern aus, die meist Teil eines Botnetzes (Ein Netz aus Computern, die beispielsweise mit Malware übernommen wurden und unter der Kontrolle eines Botnetz-Operator stehen) sind oder zum Teil auch durch Freiwillige, die die Technik als Protestform nutzen (z.B. Anonymous). Ziel ist die Überlastung des attackierten Systems, das zusammenbricht bzw. seinen Dienst verweigert und damit nicht mehr zu erreichen ist.

[377] Welche anschließend strafverfolgt oder zu Denunziationszwecken verwendet werden.

[378] Government Communications Headquarters 2012a: S. 10 ff.; Greenwald 2014a: S. 272, 275.

[379] Greenwald 2014a: S. 275.

zurück in den Normalbereich zu holen.

Neben präventiven Mitteln arbeitet JTRIG auch mit exkludierenden Methoden, die durchaus existenzielle Wirkungen haben können. Der Ausschluss kann dabei nur vorübergehend sein, in dem sie ein Ziel beispielsweise von Telekommunikationsdiensten abschneidet. Kann ein Individuum oder eine Gruppe jedoch nicht innerhalb der Toleranzgrenzen gehalten werden oder weicht es zu sehr ab, können sie es mittels Denunziation aus dem öffentlichen Diskurs ausschließen. Sie können das Leben von Individuen soweit ruinieren, dass diese mit sich selbst beschäftigt sind und dadurch fügsam gehalten werden.

Ein ähnliches Vorgehen schlug Cass Sunstein, Jura-Professor in Harvard, enger Berater von Obama und ehemaliges Mitglied des NSA-Kontroll-Ausschusses des Weißen Hauses 2008 für die USA vor. Undercover-Agent_innen und „unabhängige“ Expert_innen sollten Aktivist_innen-Gruppen on- und offline, Social Media, Chaträume und Webseiten „kognitiv“ infiltrieren.[380]

Eine von der JTRIG als Risiko eingestufte Gruppe umfasst Hacktivist_innen. Der Begriff setzt sich aus den Worten Hack[381] und Aktivismus zusammen und beschreibt Protestformen des zivilen Ungehorsams in Verbindung mit dem Internet. Anonymous ist der bekannteste lose Zusammenschluss von Hacktivist_innen, den mehr eine Idee, als eine Organisation, verbindet.[382]

JTRIG fuhr gegen Anonymous False-Flag-Operations, verwendete „Honey Traps“ und Täuschungsmanöver, griff sie mit Schadsoftware an und sammelte Informationen um sie zur Rufschädigung einsetzen zu können.[383] JTRIG führte im Sommer 2011 unter anderem DDoS-Angriffe auf zentrale Telekommunikationsinfrastrukturen von Anonymous durch.[384]

Um die Auswirkungen ihrer Aktionen abschätzen zu können und mit Anonymous-Mitglieder in Kontakt zu kommen, die sie zum Teil deanonymisierten und an

[380] Greenwald 2014a: S. 276.

[381] Der Begriff des Hackens oder der Hacker_in wird in der Alltagssprache häufig mit Kriminalität in Verbindung gebracht, obgleich er ursprünglich schlicht den kreativen Umgang mit Technik bedeutete. Der Begriff ist nach wie vor vieldeutig und wird beispielsweise für Programmierer_innen und programmieren, Auffinden von Sicherheitslücken sowie deren Reparatur oder Meldung, das (aktive) Ausnutzen von Sicherheitslücken oder jemanden, der Teil der Hackerkultur ist verwendet. Es wurde immer wieder versucht neue Begriffe, die eine klarere Abgrenzung der unterschiedlichen Hackertypen bieten, zu etablieren. Diese konnten sich aber nicht durchsetzen (z.B. white hat, black hat, grey hat).

[382] Greenwald 2014b.

[383] Greenwald 2014a: S. 271.

[384] Government Communications Headquarters 2012c: S. 12 f.

die Strafverfolgungsbehörden übergaben, hielten sich die JTRIG-Agent_innen auf Kommunikationsplattformen[385] von Anonymous auf.[386]

Muslime werden von der NSA generell als Risiko angesehen und geraten daher besonderes in den Fokus der Überwachung. Die NSA sammelt unter anderem Daten, mit denen sie die Glaubwürdigkeit der Menschen untergraben kann. Dazu gehören betrachtete Pornoseiten im Internet oder uneheliche Sex-Chats. Die Radikalisierer seien in ihrer Autorität besonders angreifbar, wenn ihr öffentliches Auftreten und ihr privates Verhalten nicht miteinander übereinstimmen würden. Die NSA interessiert sich zudem für die Krankengeschichte, politische Einstellung, intime Beziehungen und die Aktivitäten im Internet.[387]

5.4 Ausschlusstechniken

Der sozialkontrollierende Ausschluss erlebt eine Renaissance. Menschen und Gruppen, denen die Fähigkeit zu Selbstführung abgesprochen wird und die auch mit Kontrolltechniken nicht mehr zu lenken sind, werden aus sozialen Strukturen oder bestimmten Räumen ausgeschlossen und/oder kriminalisiert. Häufig sind dies ökonomisch „überflüssige“ Randgruppen. Alternativ werden die Personen oder Gruppen als für die Gesellschaft gefährlich eingestuft - und damit ihr Ausschluss gerechtfertigt.[388]

Bewertet ein Geheimdienst auf Basis seiner Telekommunikationsüberwachung ein Individuum, eine Gruppe oder einen Raum als Risiko, stehen ihm vielfältige Ausschlussmöglichkeiten zur Verfügung. Ein häufig verwendetes Mittel ist das räumliche Fernhalten von den „Gefährlichen“, die neben Terrorverdächtigen auch Flüchtlinge, Aktivist_innen oder Journalist_innen sein können. Dies geschieht u.a. mit verschiedenen Listen, die auf Basis geheimdienstlicher und polizeilicher Risikodetektion gefüllt werden.[389] In den USA umfasste die auch als „Terrorist Watch List“ bekannte „Terrorist Screening Database“ (TSDB)[390] im September 2011 420’000 Personen

[385] Meist im IRC (Internet Relay Chat).
[386] Government Communications Headquarters 2012c: S. 4 f.
[387] Greenwald 2014a: S. 266 f.
[388] P.-A. Albrecht 2010: S. 176; Singelnstein und Stolle 2012: S. 120, 138.
[389] National Counterterrorism Center 2013: S. 11.
[390] Die Terrorist Watch List wird vom Terrorist Screening Center (TSC), das dem FBI angegliedert ist, verwaltet. Sie basiert primär auf dem Terrorist Identities Datamart Environment (TIDE), welches zusätzlich umfangreiche, als geheim eingestufte Informationen von Geheimdiensten und Militär zu den Terrorverdächtigen enthält. Diese wird vom National Counterterrorism Center verwaltet.

(2013 waren es ca. 680'000[391]).

Teil der Terrorist Watch List ist die „No Fly List", die im September 2011 ungefähr 16'000 Einträge hatte(2013 waren es 47'000[392]). Personen die auf der No Fly List stehen dürfen weder in die USA, noch den amerikanischen Luftraum überfliegen. Sie werden aktiv räumlich ausgeschlossen.[393]

Ist ein Individuum als Terrorist_in gelistet (oder wird verwechselt, was bei ähnlichen Namen durchaus passieren kann), wirkt sich dies im Falle von Behördenkontakten direkt aus. Die Liste wird unter anderem im Falle einer Immigration, einem VISA-Antrag oder bei Grenzkontrollen, sowie bei Kontakt mit FBI, Polizei (auch lokaler), ausländischen Partnern und bei anderen Behördenkontakten eingesehen.[394] Die Behörden sind dazu angehalten verschiedenste Daten über die potentielle Terrorist_in zu sammeln:[395] Krankenversicherungsinformationen, Medikamentierungen, alle Karten, die über einen elektromagnetischen Streifen verfügen, Handys, E-Mailadressen, Gehaltsbescheinigungen, Social-Media-Accounts, Kopien von Laptops und anderen Speichermedien, Kameras, Buchtitel und wie benutzt die Bücher aussehen, Informationen über Mitreisende und viele mehr.[396] Die Betroffenen werden nicht darüber informiert, dass sie auf einer Watchlist stehen.[397]

Die „Watchlisting Guidance" legt die regulativen Rahmenbedingungen für ein Watchlisting von bekannten oder vermuteten Terrorist_innen fest. Sie wurde von amerikanischen Geheimdiensten, Militär und Strafverfolgungsbehörden erstellt. Die Definition von Terrorismus[398] ist dabei sehr allgemein gehalten und ermöglicht die Exklusion oder vertiefende, präventive Kontrolle verschiedener Risikoträger_innen. Ein Grund hierfür stellt das Konzept des „hinreichenden Verdachts" („reasonable suspicion") dar, welches die Einordnung auf erfahrungsbasierten Annahmen ermöglicht, welche weit entfernt von einer beweis- und evidenzbasierten Klassifikation sind. Zwar sollen Individuen nicht auf Basis unzuverlässiger Informationen gewatchlistet werden, „single source information", wie Beiträge in Social Media, sollen aber nach

[391] Scahill und Devereaux 2014b.
[392] Ebd.
[393] Federal Bureau of Investigation 2011; Scahill und Devereaux 2014a.
[394] National Counterterrorism Center 2013: S. 15.
[395] Diese sollen in das Terrorist Identities Datamart Environment (TIDE) hochgeladen werden.
[396] Scahill und Devereaux 2014a.
[397] Seit 2015 müssen nach einem Gerichtsurteil die Menschen auf der No Fly List über diese informiert werden.
[398] National Counterterrorism Center 2013: Appendix 1.

einer Evaluation, auch wenn sie unbestätigt sind, als Grund dienen können.[399] Da auch einzelne Aussagen, selbst Slang-Ausdrücke, einbezogen werden können, hat das Procedere direkte Auswirkungen auf das gesellschaftlich Sagbare.

Zudem reicht auch ein vermuteter Kontakt zu vermuteten Terrorist_innen aus, um auf eine Watchlist gesetzt zu werden (z.B. wenn die Telefonnummer einer Person bei einer verdächtigten Terrorist_in gefunden wird).[400] Dies ermöglicht das Watchlisting von Risikogruppen. Insbesondere gelten Muslime als potentielles Risiko, denen eine besondere Gefährlichkeit, sowie eine weniger ausgeprägte Fähigkeit oder Willen unterstellt wird, sich mit Mitteln der Selbstführung innerhalb der Toleranzgrenzen zu bewegen.

Die Definitionen der Watchlisting Guidance enthalten zudem auch Verhalten, das nur rudimentär bis gar nichts mit Terrorismus gemein hat. Terroristisches Verhalten besteht demnach auch in „influence the policy of a government by intimidation".[401] Darunter kann man durchaus auch Aktivismus oder Journalismus fassen.

Diese drei Merkmale - sehr weite Terrorismusdefinition, verdachts- und kontaktbasierte Terrorismuseinstufungen sowie die weitläufige Terrorifizierung (devianten) Verhaltens - ermöglichen das Watchlisting unterschiedlicher Risikoträger_innen, die mithin nichts mit hinlänglich unter Terrorismus verstanden Handlungsformen zu tun haben. Bei über 40% der gewatchlisteten Personen kann nach Regierungsangaben keine Verbindung zu terroristischen Gruppierung erkannt werden.[402]

Zu den originären Kontroll- und Ausschlusseffekten durch die Listen kommen Formen des gesellschaftlichen Ausschlusses. Wird das Watchlisting eines Individuums bekannt, kann dies eine gesellschaftliche Wahrnehmung als potentielle Terrorist_in nach sich ziehen, welche zu einer Veränderung der Behandlung einer Betroffenen führt (beispielsweise Arbeitsplatzverlust oder Nichtanstellung, Schwierigkeiten beim Reisen oder zu reisen).[403]

Die Definition von Terrorismus und die hinreichenden Verdachtsmomente sind dabei so vage,[404] dass auch Journalist_innen wie Laura Poitras oder Ahmad Muaffaq Zaidan teil des Watchlistsystems wurden. Der Al Jazeera Jounalist Zaidan berichtet und interviewt seit Jahren über Al-Qaida(-Mitglieder). Die NSA hält ihn aufgrund

[399] National Counterterrorism Center 2013: S. 34.
[400] Scahill und Devereaux 2014a.
[401] National Counterterrorism Center 2013: Appendix 1.
[402] Scahill und Devereaux 2014b.
[403] Scahill und Devereaux 2014a.
[404] National Counterterrorism Center 2013: S. 8–9.

seines Reiseverhaltens (durch Metadatenanalyse) für einen Al-Qaida-Kurier - mit dem Wissen, dass er für Al Jazeera arbeitet.[405]

Durch die Weitergabe von Informationen an Strafverfolgungsbehörden sind die Geheimdienste auch Teil des punitiven Ausschlusssystems Gefängnis. Geheimdienste können hierdurch eine Strafverfolgung initiieren oder die nötigen Beweise liefern. Mit *parallel construction* steht eine gängige[406] Methode zur Verfügung um die Informationsquelle Geheimdienst zu maskieren. Die Strafverfolgung beginnt offiziell erst zu einem späteren Zeitpunkt oder die von Geheimdiensten besorgten Beweise werden auf legalem Wege (mit einem Gerichtsbeschluss) erneut beschafft. Diese Methode wird auch bei Alltagskriminalität verwendet und dürfte eine nicht unerhebliche Rolle bei der Verbrechenssanktion und dem zum Teil damit verbundenen Ausschluss spielen.[407]

In den USA wird zudem die Speicherung in der Terrorist Screening Database (TSDB) im Vorstrafenauszug genannt, der im Falle eines Prozesses dem Gericht vorliegt. Dies kann punitive Auswirkungen haben.[408] Insgesamt ist eine zunehmende Zusammenarbeit von Geheimdiensten und Strafverfolgungsbehörden festzustellen, welche sich auf Strafverfahren und auf die damit einhergehende Möglichkeit des Ausschlusses auswirkt. Zahlen hierzu existieren der Natur der Sache nach nicht.

Insbesondere in den USA vervielfachten sich die Strafgefangenen in den letzten Jahrzehnten. Es ist ein Trend zum Ausschluss durch Einsperren zu beobachten.[409] 2015 waren über 2,2 Millionen Menschen in amerikanischen Gefängnissen untergebracht. Dies sind 698 Strafgefangene pro 100'000 Einwohner_innen.[410] In Großbritannien ist ebenfalls ein Anstieg zu beobachten, der allerdings nicht mit den Entwicklungen in den USA zu vergleichen ist. 2014 waren 149 pro 100'000 Einwohner_innen im Gefängnis.[411] In Deutschland blieben die Gefangenenzahlen trotz Schwankungen relativ stabil.[412] Seit 2004 ist eine Abnahme der Gefangenenzahlen zu beobachten. 2014 waren in Deutschland 76 Menschen pro 100'000 Einwohner_innen

[405] Currier, Greenwald und Fishman 2015.

[406] Offizielle Zahlen existieren hierzu nicht, allerdings legen interne Dokumente, sowie Aussagen von Strafverfolgungsbehördenmitarbeiter_innen nahe, dass die Praxis zum Alltag gehört: „Parallel construction is a law enforcement technique we use every day [...] It's decades old, a bedrock concept." (Shiffman und Cooke 2013)

[407] Schneier 2015a: S. 105; R. Gallagher 2014c; Shiffman und Cooke 2013.

[408] Kane 2016.

[409] H.-J. Albrecht 2011: S. 112 ff.

[410] International Centre for Prison Studies o. J.(a).

[411] International Centre for Prison Studies o. J.(b).

[412] Dollinger 2011: S. 52.

im Gefängnis.[413]

Dies untermauert den Wandel der Disziplinargesellschaft, in welcher auf eine Inklusion bzw. Resozialisierung Devianter gesetzt wurde, hin zu einem sicherheitsgesellschaftlichen Umgang mit nicht verwaltbarer Devianz, welcher mit dem Mittel des Ausschlusses begegnet wird. Dieser Wandel ist in Deutschland aber weit weniger fortgeschritten. Dies wird zum Teil auf einen weniger weit fortgeschrittenen Neoliberalismus zurückgeführt.[414] Dennoch sind auch in Deutschland punitive Tendenzen bspw. die Verschärfung von Strafgesetzen, feststellbar.[415]

Die finale Form des Ausschlusses stellt die Auslöschung des Lebens dar. Neben den Watchlists existiert eine weitere Liste, die den finalen Ausschluss realisiert: die sogenannte Kill-List. Personen die auf diese Liste gesetzt wurden, werden „gezielt getötet“, häufig mittels Drohnen.[416]

Auf der Joint Prioritized Effects List (JPEL) der NATO (North Atlantic Treaty Organization) standen zwischenzeitlich 750 Menschen, darunter auch Drogenhändler, da sie die Aufständischen unterstützen würden. Die Listen sind naturgemäß fluktuativ, da die „Ziele“ nach und nach ausgelöscht werden. Dabei werden zivile, unbeteiligte Opfer in Kauf genommen, wenn das Ziel diese „rechtfertigt“. Die Rechtfertigung findet in einer Aufrechnung der zivilen Opfer, die durch den Drohnenschlag sterben, mit den potentiellen Opfern der potentiellen Terrorist_in statt.[417]

Die „gezielte Tötung“ durch Drohnenschläge fordere nach Militärangaben kaum zivile Opfer und sei sehr effektiv. Das liegt mitunter daran, dass alle Männer im kampffähigen Alter als feindliche Kämpfer eingestuft und damit nicht den zivilen Opfern zugerechnet werden. Nur wenn zweifelsfrei nachgewiesen werden kann, dass es sich bei den Männern im kampffähigen Alter um Zivilisten handelt, werden diese neben Frauen, Kindern und Alten, als solche anerkannt.[418]

Ein Studie untersuchte die „gezielten Tötungen“ von 41 Personen, die auf einer amerikanischen „Kill List“ standen. Insgesamt kamen 1’147 Menschen bei den Drohnenschlägen gegen die 41 Ziele ums Leben, 28 im Zweifel Unbeteiligte auf jede „gezielte Tötung“.[419] Zwischen Januar 2009 und Januar 2015 wurden nach Anga-

[413]International Centre for Prison Studies o. J.(c).
[414]Klimke 2008: S. 20.
[415]Dollinger 2011: S. 55.
[416]Spiegel 2015a: S. 82 f.; Fuchs und Goetz 2013: S. 238.
[417]Spiegel 2015a: S. 80 ff.
[418]Spiegel 2015a: S. 82; Biermann und Wiegold 2015: S. 147.
[419]Biermann und Wiegold 2015: S. 131 f.

ben des Bureau of Investigative Journalism mindestens 2'464 Menschen[420] durch Drohnenschläge getötet.[421]

Die Drohnenschläge hängen immens von der Erkennung und Lokalisierung der Ziele durch Geheimdienste und SIGINT-Daten ab. GCHQ, BND und NSA erkennen mit ihren Überwachungsprogrammen potentielle Risikoträger_innen[422] in Krisengebieten.[423] Sie helfen mit ihren SIGINT-Daten aber nicht nur beim Erkennen von Risikoträger_innen, sondern spielen auch bei deren Eliminierung eine zentrale Rolle.[424]

GCHQ und NSA ermitteln die Handys der Ziele anhand ihrer Telekommunikationsüberwachung und beginnen dann das Mobiltelefon zu orten. Handys stellen im Drohnenkrieg Peilsender[425] dar. Ist das Ziel geortet, wird auf den Ort das Handys eine Rakete abgefeuert.[426]

Der geheimdienstlich-militärische Ausschluss aus dem Leben findet auch auf Basis einer Kontaktschuld statt, die sowohl bei der Listenbefüllung, als auch beim „gezielten Töten" zur Anwendung kommt. Wer sich mit Mitgliedern einer derart „abgeschotteten und paranoiden Organisation" wie Al-Qaida aufhalte, müsse schuldig sein bzw. stelle ein Risiko dar („guilt by association").[427] Eine ähnliche Vorgehensweise ist auch bei anderen Überwachungsprogrammen zu beobachten.

Die *preemptive strikes* werden gegen Ziele, die eine „Bedrohung für US-Interessen oder Personal darstellen"[428], geflogen. Die Idee hinter diesen ist es, einem vermuteten Angriff der Gegner_in zuvorzukommen. Sie stellen daher eine Form des präventiven

[420] Die reale Zahl dürfte weitaus höher sein. Da es keine (veröffentlichten) offiziellen Datenerhebungen gibt, müssen die Journalist_innen auf (lokale) Zeitungsberichte und Satellitenbilder zurückgreifen. Hierdurch dürften viele der Drohnenschläge und damit der Toten nicht erfasst worden sein. (vgl. Biermann und Wiegold 2015: S. 132 f.) Andere Quellen gehen von knapp 5'000 getöteten Menschen bis 2013 aus. (Fuchs und Goetz 2013: S. 239)

[421] Serle 2015.

[422] Die bei weitem nicht nur Terrorist_innen sondern beispielsweise auch Drogenhändler_innen umfassen.

[423] Am Hindukusch arbeiten die westlichen Geheimdienste im Bündnis der 14 Eyes zusammen und betreiben mit CENTER ICE eine gemeinsame Überwachungs- und Datenaustauschplattform.

[424] Das Motto der NSA lautet dabei: „We Track 'Em, You Whack 'Em".

[425] Der NSA stehen für die Ortung verschiedene Systeme zur Verfügung: Sie kann die Mobiltelefone durch Geolokationsdaten bei den Telefonprovidern oder bei Handymasten orten, ihr stehen Wifi-Landkarten verschiedener Städte zur Verfügung, auf Basis derer sie den Ort eines dort eingeloggten Gerätes feststellen kann. Des Weiteren kann sie mit Hilfe von Überwachungsdrohnen, die sich als Handymasten ausgeben, in das sich die Mobiltelefone in der Umgebung automatisch einloggen, auch in schwer zugänglichen Gebieten den Ort eines Mobiltelefons erfassen.

[426] Scahill und Greenwald 2014; Scahill 2015.

[427] Biermann und Wiegold 2015: S. 147 f.

[428] Intelligence Surveillance Reconnaissance Task Force 2013: Folie 6.

Komplettausschlusses und damit eine Ausschaltung jeglichen Risikos dar. Nicht berücksichtigt werden dabei die hasserzeugenden Effekte des Drohnenkrieges, welche unter der bekriegten Bevölkerung entstehen. Diese spielen letztlich dem internationalen Terrorismus direkt in die Hände. John Brennan, Leiter der CIA, fasste dies prägnant zusammen:

> „I think the president has tried to make sure that we're able to push the envelope when we can to protect this country. But we have to recognize that sometimes our engagement and direct involvement will stimulate and spur additional threats to our national security interests.“[429]

Um potentielle Terrorist_innen zu erkennen kommen aber auch automatisierte Mustererkennungsprogramme wie SKYNET zum Einsatz. Werden Menschen auf Basis der Verhaltenserkennungsprogramme getötet wird dies im Militärjargon *signature strikes* genannt. Die Ziele werden hierbei nur mit Hilfe von Verhaltensauffälligkeiten in SIGINT-Daten ausgewählt. Dies können Bilder aus der Satellitenüberwachung sein, auf denen Menschen bei potentiell devianten Tätigkeiten erspäht werden: Beispielsweise wenn sie Waffen, Sprengstoff oder Dünger (der als Sprengstoff aber eben auch zum Düngen verwendet werden kann) auf einen Laster laden oder das Fahrzeug einer bekannten Terrorist_in verwenden.

Signature Strikes basieren aber auch auf Mustern, die mit Hilfe von Data Mining in den abgefangenen Telekommunikationsdaten der Bevölkerung aus Krisengebieten errechnet werden. Das können Terrorist_innen-Treffen, Anschlagsvorbereitungen oder Kuriere sein, aber auch False-Positives, die ein ähnliches oder gleiches Muster aufweisen, wie schlichte Menschenansammlungen oder Hochzeitsgesellschaften, die wie ein Konvoi aus Terrorist_innen-Fahrzeugen erscheinen. Taliban und Al-Qaida haben bereits auf die Drohnenschläge reagiert und empfehlen ihren Kämpfer_innen möglichst keine Mobiltelefone zu verwenden und diese häufig zu wechseln.[430]

Dazu passt die Aussage des ehemaligen NSA- und CIA-Direktors Michael Hayden: „We kill people based on metadata!“[431]

In einem Satz: Wer bestimmte verdächtige Telekommunikationsmuster aufweist oder verdächtige Handlungen begeht und sich in einem Kriegs- oder Krisengebiet

[429] Brennan, John zitiert nach Jon Schwarz 2015.
[430] Biermann und Wiegold 2015: S. 135, 156 f.
[431] Schneier 2015b.

[432] (Afghanistan, Pakistan, Somalia, Jemen[433]) befindet oder dorthin reist, kann präventiv getötet werden - was den ultimativen Ausschluss bedeutet.

5.5 Zwischenfazit

Die geheimdienstliche Telekommunikationsüberwachung ist in der Sicherheitsgesellschaft zu verorten. Soziale Kontrolle wird über die sicherheitsgesellschaftliche Verwaltung des empirisch Normalen mit den Techniken der Selbstführung, der Kontrolle und des Ausschlusses vermittelt.

Im Bereich der Selbstführungstechniken sind die Geheimdienste an der Betonung eines kontinuierlichen Bedrohungsszenarios durch den internationalen Terrorismus beteiligt und tragen so zu einer stetigen Verunsicherung der Subjekte bei, die den Nährboden für Selbstführungstechniken bildet. Diese Verunsicherung greift der Staat mit einem Versprechen individueller Sicherheit auf. Dieses wird in Form staatlicher Sicherheitsmaßnahmen eingelöst, welche sowohl ein Gefühl der Sicherheit, als auch der Unsicherheit erzeugen.

Das Subjekt sieht die hierdurch entstehende Beschränkung seiner Handlungsfreiheit nicht nur ein, sondern fordert diese sogar. Dies führt gemeinsam mit dem Ideal der Sicherheit, der stetigen Bedrohung, einer erhöhten Wahrnehmung des Risikos, Opfer eben jener zu werden und einem Präventionsgedanken, zu einer Verhaltensanpassung. Das Subjekt internalisiert Verhaltensanforderungen und nimmt diese als die eigenen wahr. Die Geheimdienste sind mit anderen Sicherheitsbehörden an der Schaffung des Rahmens dieser Form von sozialer Kontrolle beteiligt.

Die geheimdienstliche Telekommunikationsüberwachung bildet die empirische Realität ab, welche Abweichung bis zu einem gewissen Grad toleriert. Dies machen sich die Geheimdienste zu Nutze, um einen Großteil der Menschen sozial kontrollieren zu können. Flexible Toleranzgrenzen werden mittels einer Risikodetektion gezogen. Diese findet mit vielfältigen Überwachungsprogrammen statt, bei welchen unter

[432] Die USA argumentieren völkerrechtlich (vereinfacht), dass sie sich in einem asymmetrischen Krieg mit Gegner_innen (die maximal eine gemeinsame Basisideologie teilen, aber keinerlei Organisation!) befinde, die sie bekämpfen dürfe/müsse. Diese würden über viele Staaten verteilt agieren. In anderen Staaten, sofern kein Krieg vorherrsche, dürfe sie dies mit Erlaubnis. Sollte der andere Staat nichts gegen die terroristische Bedrohung innerhalb seiner Landesgrenzen unternehmen auch ohne. Mit dieser Argumentation berufen sich die USA auf das Kriegsrecht und können im Prinzip jeden Menschen auf der Welt (geheim) als Risiko definieren und (geheim) töten. Da dieser Argumentation nicht zu Folgen ist handelt es sich um eine extralegale Tötung.

[433] Vermutlich auch Irak und Syrien.

anderem Analyst_innen mit Hilfe von Selektoren nach zu sehr abweichenden Individuen, Gruppen oder Orten suchen. Dies findet computergestützt statt und lässt sich teilweise automatisieren (u.a. XKeyscore, MUTANT BROTH). Andere Überwachungsprogramme (u.a. SKYNET, PROTON, SQUEAKY DOLPHIN) erkennen mit Data Mining Risikoträger_innen automatisiert auf Basis von (Verhaltens-)Mustern, Rastern, Profilen und Lebensrhythmen zum Teil ganzer Gesellschaften. Algorithmen ermitteln Verhalten, das jenseits der Toleranzgrenzen liegt. Die Dokumente legen nahe, dass die algorithmische Vermessung zunehmend ausgebaut wird.

Risikoträger_innen werden mit präventiven Methoden dazu angehalten, sich wieder in den Normalbereich zu begeben. Ist diese Form der sozialen Kontrolle nicht zielführend, das Risiko zu groß, oder handelt es sich um eine Wiederholungstäter_in wird mit repressivem Ausschluss reagiert.

Hierbei nutzen die Geheimdienste eine sehr vage Terrorismusdefinition, welche zur Rechtfertigung von Prävention und Ausschluss herangezogen wird. Mit JTRIG existiert eine Abteilung des GCHQ, welche präventive Soziale Kontrolle durch gezielte Einflussnahme auf Risikoträger_innen, Gruppen und Diskurse oder die Bevölkerung ausübt und diese in ihrem Sinne beeinflusst. So sollen die Betroffenen im Rahmen des empirisch Normalen gehalten werden.

Der repressive Ausschluss erlebt auch bei den Geheimdiensten eine Renaissance und wird über Strafverfolgungsbehörden, Terrorist Watchlist, No Fly List, bis hin zum finalen Ausschluss durch die „gezielte Tötung“ ausgeführt.

6 Ergebnis der Untersuchung

In den letzten Jahrzehnten haben sich die Kommunikationsmöglichkeiten massiv gewandelt. Mit der Computerisierung der Gesellschaft und den damit einhergehenden (mobilen) Telekommunikationsmöglichkeiten erzeugt die Menschheit Daten in einem nie dagewesenen Ausmaß. Telekommunikation ist ein omnipräsentes Alltagsphänomen geworden, welchem man sich nur mit erheblichem Aufwand und diversen Einschränkungen entziehen kann.

Nach dem Kalten Krieg wurden die westlichen Geheimdienste ihres Primärfeindes beraubt und gerieten in eine Krise, die sie in Folge der Terroranschläge des 11. September 2001 überwanden. Die Anschläge dienen als Begründungszusammenhang für die Überwachung der gesamten Bevölkerung weltweit. Ziel ist es, sich den ungeheuren Datenreichtum der Telekommunikation zu Nutze zu machen und so jeden Mensch, jede Gruppe und jeden Ort auf der Welt kontrollieren zu können.

Dies wirft die Frage auf, inwiefern diese Kontrolle auf die Gesellschaft zurück wirkt. Die Arbeit verfolgt das Ziel, diese Wirkungen anhand der disziplinargesellschaftlichen und sicherheitsgesellschaftlichen sozialen Kontrolle zu analysieren. In einem Satz: Wie wird soziale Kontrolle über massenhafte geheimdienstliche Telekommunikationsüberwachung vermittelt?

6.1 Disziplinargesellschaft

6.1.1 Normen und Sanktionen

Die Grundlage der disziplinargesellschaftlichen Sozialkontrolle stellt eine kleinteilige Überwachung des Verhaltens dar, welche Abweichung auf Basis eines festen Normenkataloges detektiert und anschließend normierend sanktioniert. Das Wissen um diese Überwachung sowie die Unsichtbarkeit der Überwachung selbst, führt zu einer Internalisierung der Überwachung, welche das normkonforme Verhalten der Individuen sichert.

Zentral für die disziplinargesellschaftliche Sozialkontrolle ist ein allgemeingültiges Normengefüge, welches binär in Ge- und Verbote einteilt. An diesem müssen sich die Individuen ausrichten und anhand diesem werden sie kontrolliert und etwaige Abweichung detektiert. Gesetze stellen ein solches Normengefüge dar.

Geheimdienste arbeiten mit geheimen Kriterienkatalogen und Zielsetzungen (beispielsweise Intelligence Priorities Framework (NIPF) und Watchlisting Guidance),

welche der frühzeitigen Erkennung von Gefahren auf Basis von Einschätzungen dienen. Diese Einschätzungen finden häufig weit im Vorfeld etwaiger (gesetzlicher) Normverletzungen statt. Zudem agieren Geheimdienste nicht primär in ihrer Jurisdiktion, sondern international. Insofern erfüllen sie die Bedingungen eines öffentlichen, klaren Normenkataloges nicht. Allerdings arbeiten sie auch Strafverfolgungsbehörden zu, obgleich dies nicht ihre originäre Aufgabe darstellt. Diese Zusammenarbeit geschieht in hybriden Organisationen (Fusion Center, Gemeinsames Terrorismusabwehrzentrum (GTAZ) uvm.), durch die Weitergabe von geheimdienstlichen Erkenntnissen und Daten via Datenbanken (Antiterrordatei (ATD), ICREACH, PROTON) oder auf direktem Wege sowie durch technische Unterstützung.

Die Disziplinen wollen jede kleinteilige Abweichung erkennen und normierend sanktionieren. Die massenhafte Telekommunikationsüberwachung ermöglicht den Geheimdiensten zwar eine weitgehende Erkennung von (kleinteiligen) Normabweichungen, diese werden aber nicht verfolgt. Die Geheimdienste konzentrieren sich auf definierte Ziele (NIPF) und Risiken - als nicht riskant eingestuftes deviantes Verhalten lassen sie gewähren. Durch die Weitergabe von Erkenntnissen und Daten an Strafverfolgungsbehörden triggern sie allerdings auch Sanktionen auf Basis von Normverstößen. Die Herkunft der Informationen kann durch *parallel construction* maskiert werden, daher ist das Ausmaß dieser nicht bekannt. Diese Sanktionen müssen zudem keine normierende Wirkung haben, sondern können auch dem Ausschluss dienen.

Festzuhalten ist, dass die Geheimdienste nur insofern Teil des Normenkataloges sind, als das sie mit Strafverfolgungsbehörden zusammenarbeiten. Gleiches gilt für (normierende) Sanktionen. Vermittelt über Strafverfolgungsbehörden ist hingegen eine Detektion abweichenden Verhaltens sowie dessen Sanktionierung nachweisbar. Sanktionen halten Individuen dazu an, sich gesetzeskonform zu verhalten und ahnden Abweichungen. Die Sanktionen haben zum Teil eine normierende Wirkung. Auch Soziale Kontrolle kann insofern nur vermittelt über Strafverfolgungsbehörden und damit nur zum Teil mit der Disziplinargesellschaft erklärt werden. Es deutet sich bereits an, dass die geheimdienstliche Sozialkontrolle im Bereich der Normen und Sanktionen mit sicherheitsgesellschaftlichen Techniken erklärt werden kann.

6.1.2 Panoptikum

Das panoptische Prinzip ermöglicht eine Analyse der Überwachungswirkung. Das Panoptikum trennt hierzu verschiedene Sphären der Sichtbarkeit voneinander ab, um eine kontinuierliche Wirkung der Überwachung zu gewährleisten. Die selbige kann dabei sporadisch oder sogar ganz unterlassen werden.

Im Panoptikum können mit einem kontrollierenden Blick viele Individuen auf Normkonformität geprüft werden. Die geheimdienstliche Telekommunikationsüberwachung folgt dem Prinzip, jedwede Telekommunikation zu erfassen („Collect it all“). Mit den vielfältigen Überwachungsprogrammen ist es den Geheimdiensten möglich, einen Großteil der menschlichen Telekommunikation zu erfassen und diese anschließend auszuwerten. Diese Form der Bevölkerungskontrolle war bis vor wenigen Jahren sehr aufwändig bis unmöglich. Durch die weite Verbreitung von Telekommunikation und immer neueren Diensten und Geräten, die allesamt digitale Daten produzieren, welche geheimdienstlich erfasst und ausgewertet werden können, ist dies jedoch vergleichsweise einfach und kostengünstig geworden.

XKeyscore, das von NSA, GCHQ, BND und weiteren Geheimdiensten eingesetzt wird, erfasst nach Angaben der NSA fast alle Bewegungen und Eingaben einer typischen User_in im Internet. Mit der Software kann mit einem Blick auf die Telekommunikation eines Individuums festgestellt werden, wo sich dieses befindet, was dieses macht, was es gerade beschäftigt, was es plant. Die Telekommunikation von Individuen, Gruppen oder an bestimmten Orten lässt sich live nachvollziehen und auf Normkonformität prüfen (ähnliches ist mit der GCHQ-Software SAMUEL PEPYS möglich). XKeyscore bzw. TEMPORA hält die Telekommunikation für mehrere Tage, die Metadaten sogar für einen Monat komplett vor (Inhalte und Metadaten können für eine längere Speicherung in andere Datenbanken überführt werden). Die Überprüfung kann deshalb auch rückwirkend vorgenommen werden. Zudem kann der kontrollierende Blick, wie im Panoptikum, umherschweifen und Individuen, Gruppen und Orte in den Fokus nehmen. Die Analyst_innen können die Daten nach Inhalten oder nach Personen, beispielsweise via E-Mailadresse, durchsuchen. Es lassen sich aber auch die Besucher_innen von bestimmten Webseiten (Orten) oder Auffälligkeiten in bestimmten Ländern oder Regionen ausgeben. Vergleichbares ist mit den GCHQ Programmen KARMA POLICE, MUTANT BROTH, SOCIAL ANTHROPOID und weiteren möglich.

Dieser tiefgehende Blick kann allerdings durch Verschlüsselung und Anonymisie-

rungsdienste getrübt werden. Die Geheimdienste thematisieren in verschiedenen, nicht für die Öffentlichkeit bestimmten, Dokumenten ihre Probleme mit starker Verschlüsselung oder dem Tor-Netzwerk. Um die Auswirkungen möglichst gering zu halten, forschen sie aktiv an Umgehungsmöglichkeiten und Angriffen auf die Verschlüsselung. Ziel ist es die Inhalte weiterhin überwachen oder die Nutzer_innen deanonymisieren zu können. Die Arbeiten sind zum Teil mit erheblichem Aufwand verbunden, der Erfolg jedoch mäßig.

Die Mehrheit der Internetnutzer_innen verwendet jedoch Dienste, die sie von Haus aus überwachen (beispielsweise Google-Dienste, Facebook) und auf welche vielfältige Zugriffsmöglichkeiten seitens der Geheimdienste bestehen.

Insgesamt ist die Sichtbarkeit mit wenigen Ausnahmen gewährleistet. Wichtig ist zudem die Unsichtbarkeit des Überwachungsvorgangs: Das Individuum darf nicht wissen, ob es gerade überwacht wird. Die geheimdienstliche Telekommunikationsüberwachung findet im Geheimen, im Unsichtbaren statt. Ob ein Individuum gerade überwacht wird oder nicht, kann es also nicht wissen.

Um eine kontinuierliche Wirkung der Überwachung und damit eine Internalisierung zu gewährleisten, muss dem Subjekt die Überwachung bewusst sein. Im Panoptikum wird dies durch die stetige Sichtbarkeit des Turmes gewährleistet. Diese Sichtbarkeit ist bei geheimdienstlichen Überwachungsprogrammen, die nicht bekannt sind und nicht bekannt gemacht werden sollen, nicht gegeben. Dies änderte sich im Juni 2013 mit dem Beginn der Berichterstattung und der Veröffentlichung interner, nicht für die Öffentlichkeit bestimmter Geheimdienstdokumente, die von Edward Snowden an die Presse weitergegeben wurden. Die Medienberichterstattung wurde weithin wahrgenommen und führte zu einem Bewusstwerden der stetigen Überwachbarkeit. Dies kann mit Umfragen empirisch belegt werden. Ironischerweise wurde der panoptische Turm von den Kritiker_innen der geheimdienstlichen Massenüberwachung errichtet. Durch die mediale Aufarbeitung und gesellschaftliche Diskussion manifestierte sich der Turm immer wieder, fraglich ist, wie lange dieser Prozess anhält. Verblasst der Turm, verblasst auch die Wirkung der Überwachung.

Ist dem Subjekt bewusst, dass es jederzeit überwacht werden kann, beginnt es sich so zu verhalten, als würde es kontinuierlich überwacht. Es internalisiert die Überwachung, es überwacht sich selbst. Hierdurch bleibt die Überwachungswirkung bestehen, auch wenn das Subjekt nicht oder nur sporadisch überwacht wird. Dies führt zu Verhaltensanpassung an antizipierte Normen.

Empirisch sind zwei Arten der Verhaltensanpassungen festzustellen, die durchaus auch in Kombination auftreten können: Zum einen versuchen Individuen, aber auch Firmen, die Telekommunikationsüberwachung zu umgehen. Die Effektivität vieler Maßnahmen dazu darf bei den ausgereiften Überwachungsprogrammen der Geheimdienste bezweifelt werden, obgleich eine Umgehung der Massenüberwachung technisch möglich ist. Dennoch ist hier eine Verhaltensänderung bei einem beträchtlichen Teil der Bevölkerung festzustellen. Zum anderen sind Chilling Effects zu beobachten. Es findet eine Anpassung an antizipierte Verhaltensanforderungen bzw. Normen statt, da kein klarer Normenkatalog seitens der Geheimdienste existiert. Die Anpassungen sind daher vor allem im Bereich der Selbstzensur bei der Nutzung von Telekommunikation zu finden. Thematisch umfasst die Selbstzensur, dies legen Studien nahe, vor allem Geheimdienste und deren Telekommunikationsüberwachung.

Die Studie von Marthews/Tucker[434] zeigt zudem die Vermeidung von Themen, die als möglicherweise problemgenerierend in Bezug auf die Exekutive angesehen werden. Außerhalb der USA vermieden die Menschen auch Themen, von denen sie annahmen, dass sie Probleme in Freundschaften verursachen könnten.

Die Arbeit stützt diese Erkenntnisse, insofern kein geheimdienstlicher Normenkatalog gegeben ist und dieser von den Überwachten antizipiert werden muss. Es liegt daher nahe, dass die Überwachten das Thema geheimdienstliche Telekommunikationsüberwachung und die mit ihnen verbundene Exekutive als anpassungsbedürftig ansehen, da hier die Überwachung und deren Intention vermutet wird. Außerhalb der USA, scheinen auch private Daten, die zu Problemen in Freundschaften führen könnten, als ein Ziel der geheimdienstlichen Überwachungsprogramme wahrgenommen zu werden.

Dies könnte mit einer Privatsphärediskussion rund um den NSA-Skandal sowie die besondere Wahrnehmung der NSA, welche betont vor allem beziehungsweise nur außerhalb der USA tätig zu werden, zusammenhängen. Dies wurde allerdings empirisch bisher nicht untersucht, es besteht weiter Forschungsbedarf. Vermutet wird, dass durch ein „diffus bedrohliches Gefühl des Beobachtetseins“[435] auch Chilling Effects bei anderen Grundrechten auftreten, hierzu liegen aber bisher keine Studien vor. Auch hier besteht Forschungsbedarf.

Journalist_innen, Whistleblower_innen, Aktivist_innen und Meinungsführer_innen, sowie Vertreter_innen von Minderheitsmeinungen sind essentiell für ei-

[434]Diese untersuchten die Verwendung als gefährlich eingestufte Suchbegriffe mit Google Trends.
[435]Das BVerfG zur weniger invasiven Vorratsdatenspeicherung: Bundesverfassungsgericht 2010.

nen demokratischen Prozess und eine gesellschaftliche Erneuerung. Chilling Effects wirken sich bei ihnen in besonderem Maße aus und haben eine gesellschaftskonservierende Funktion, die durchaus intendiert sein kann. Bei Journalist_innen sind Chilling Effects empirisch nachweisbar. Diese internalisieren die Überwachung und beginnen bestimmte Themen zu meiden oder weniger kritisch zu berichten. Die mediale Berichterstattung wird in demokratischen Gesellschaften häufig als die *vierte Gewalt* beschrieben, da ihr eine außerstaatliche Kontrollfunktion zukommt und sie die Plattform für gesellschaftliche Diskurse darstellt. Chilling Effects sind bei Journalist_innen besonders problematisch im Bezug auf Meinungspluralität im demokratischen Prozess sowie einer Weiterentwicklung der Gesellschaft allgemein. Ähnliches gilt für Whistleblower_innen, Aktivist_innen und Meinungsführer_innen sowie Vertreter_innen von Minderheitsmeinungen, bei diesen sind Chilling Effects durch die geheimdienstliche Telekommunikationsüberwachung anzunehmen, empirische Studien bzw. Nachweise fehlen bisher.

6.1.3 Zusammenschau

Eine Selbstdisziplinierung der Überwachten ist nachweisbar. Diese wird durch panoptische Wirkungen der massenhaften Telekommunikationsüberwachung seitens der Geheimdienste, in Kombination mit einer Berichterstattung und gesellschaftlichen Diskussion über die geleakten Originaldokumente, erzeugt. Panoptische Effekte bei heimlicher Telekommunikationsüberwachung, die der Bevölkerung weitgehend unbekannt ist, können hingegen nicht nachgewiesen werden. Insofern handelt es sich zwar um eine Selbstdisziplinierung, die allerdings erst durch die Snowden-Leaks entstand und deren Ursache nicht in der originären Geheimdienstarbeit zu finden ist.

Die soziale Kontrolle, vermittelt über eine Selbstdisziplinierung, führt zu einer Anpassung an beziehungsweise Einhaltung von antizipierten Normen. Die Disziplinargesellschaft erfordert allerdings ein allgemeingültiges Normengefüge, das den Überwachten bekannt ist. Ein solches ist im Bereich der geheimdienstlichen Telekommunikationsüberwachung nur gegeben, wenn die Daten an die Strafverfolgungsbehörden weitergegeben werden. Hier gibt es mit dem Gesetz einen bekannten Normenkatalog. Entsprechend findet hier in einem nicht bekannten Umfang eine Sanktionierung devianten Verhaltens auf Basis geheimdienstlicher Telekommunikationsüberwachung statt. Allerdings findet hier zunehmend ein Wandel von der normierenden Sanktion mit dem Ziel der Reintegration hin zu Ausschluss und Prävention statt.

Außerhalb der Zusammenarbeit mit den Strafverfolgungsbehörden sowie jenseits der nicht-intendierten panoptischen Sozialkontrolle kann eine disziplinarsch-normierende Wirkung nicht nachgewiesen werden.

Die Untersuchung kann disziplinargesellschaftliche beziehungsweise panoptische Sozialkontrolle durch die geheimdienstliche Telekommunikationsüberwachung nachweisen, allerdings kann die soziale Kontrolle hierdurch nicht hinreichend erklärt werden.

6.2 Sicherheitsgesellschaft

Die Analyse der disziplinargesellschaftlichen Sozialkontrolle deutet bereits an, dass sich die Zugriffe auf die Individuen verändert haben: Beispielsweise fehlt absolute Kontrolle und Sanktion jeglicher Abweichung sowie der dazu notwendige Normenkatalog, der den Subjekten als Verhaltensanforderung bekannt ist. Diese Veränderungen werden mit dem Wandel hin zu einer postfordistischen Sicherheitsgesellschaft erfasst, die neue Techniken der sozialen Kontrolle entwickelt, die die disziplinargesellschaftlichen zunehmend ablösen.

6.2.1 Verwaltung des empirisch Normalen

Im Gegensatz zum festen Normenkatalog der Disziplinargesellschaft, welcher eingehalten und akzeptiert werden musste, orientiert sich die Sicherheitsgesellschaft an der empirischen Realität. Der empirische Durchschnitt wird zur normgebenden Instanz, welcher Abweichungen bis zu flexiblen Toleranzgrenzen gewähren lässt.

Die Telekommunikation bildet gesellschaftliche Realitäten ab. Mit einer massenhaften Überwachung der Telekommunikation und den damit einhergehenden Datenbergen wird eine Gesellschaft berechenbar. Diesen Umstand machen sich die Geheimdienste zu Nutze, indem sie die massenhaft überwachte Telekommunikation mit Hilfe von Big-Data-Anwendungen analysieren. Die Daten werden gerastert, nach Mustern durchsucht und Profile erstellt. Auf dieser Basis wird computergestützt ein Großteil der Weltbevölkerung kontrolliert und zwischen dem empirisch Normalen sowie tolerierbaren Abweichungen von diesem und Abweichungen die jenseits von Toleranzgrenzen liegen, getrennt. Dies geschieht anlasslos, massenhaft, möglichst live und in Echtzeit.

Geheimdienste nutzen Big-Data-Analysen mit vielfältigen Programmen (zum Beispiel PROTON, SQUEAKY DOLPHIN, MUTANT BROTH und XKeyscore). Die

Auswertung geschieht sowohl algorithmisch-automatisiert, als auch mit Hilfe von Selektoren und Analyst_innen. SKYNET ist eine cloudbasierte Verhaltenserkennungssoftware, welche unter Zuhilfenahme eines lernenden Algorithmus Verhalten ermittelt, das jenseits der Toleranzgrenzen vermutet wird. Die Einordnung des Verhaltens als Risiko hängt dabei von einem Wahrscheinlichkeitswert ab, überschreitet dieser einen bestimmten Schwellenwert (Toleranzgrenze), wird das Individuum als Risikoträger_in klassifiziert.

Das Forschungsprojekt MERCURY soll Verhaltensänderungen um große Ereignisse wie Aufstände, Revolutionen oder Epidemien analysieren und auf dieser Basis eine Ereignisvorhersage treffen.

Big Data Analysen eignen sich allerdings weniger zur proklamierten frühzeitigen Erkennung von Terroranschlägen, da sie mit der Erkennung von Mustern und Rastern arbeiten. Diese fehlen bei den seltenen und zumeist einzigartigen Terroranschlägen in Nicht-Kriegsgebieten. Allerdings eignet sich die algorithmische Auswertung von Big Data sehr gut, um Abweichungen jenseits von seltenen Ereignissen wie Terroranschlägen, zu detektieren. Insofern qualifiziert sich Data Mining zur sozialen Kontrolle mit Hilfe einer Risikodetektion und anschließendem präventivem oder ausschließendem Eingreifen.

Ein weiteres Problem stellen False-Positives und False-Negatives dar. So bleibt ein Teil der Risikoträger_innen unerkannt, während gleichzeitig, mitunter eine große Zahl, Menschen, die sich innerhalb der Toleranzgrenzen befinden, als Risiko eingestuft werden.

Risikoträger_innen und -situationen werden häufig im Vorfeld etwaiger Normverletzungen erkannt und frühzeitig präventiv verwaltet oder ausgeschlossen, um eine Auswirkung der Abweichung erst gar nicht entstehen zu lassen. Insofern sagen die Algorithmen die Zukunft wahrscheinlichkeitsbasiert voraus.

6.2.2 Selbstführungstechniken

Die Selbstführungstechniken lösen die Selbstdisziplinierung der Disziplinargesellschaft ab. Dem Individuum wird kein Normenkatalog mehr aufgezwungen, vielmehr wird ihm eine Entscheidungsfreiheit gelassen. Es muss jedoch mit den Konsequenzen seines Verhaltens leben. Konformität wird über antizipierte Normen, die vom Individuum vermeintlich selbst gewollt werden, erreicht. Eine zentrale Grundlage der Selbstführung beziehungsweise -beschränkung stellt eine gesellschaftliche Ver-

unsicherung dar.

Seit dem 11. September 2001 stellt der internationale Terrorismus einen zentralen Angstfaktor in westlichen Gesellschaften dar. Dieser findet in Sicherheitsdiskursen ihren Ausdruck, welche für eine permanente Verunsicherung der Gesellschaft sorgen.

Die Krise des Wohlfahrtsstaates führt zu einem Sozialabbau und der Aufgabe des staatlichen Inklusionsversprechens. Dies führt in Zeiten wirtschaftlicher Umbrüche zu einer Verunsicherung weiter Teile der Gesellschaft. Diese diffuse Verunsicherung führt zu einer erhöhten Wahrnehmung von (Gewalt-)Kriminalität und einer Abgrenzung von Randgruppen, insbesondere Migrant_innen, auf welche die sozialen Abstiegsängste projiziert werden. In der Angst vor dem internationalen Terrorismus verbinden sich diese und werden in Sicherheitsdiskursen ausgetragen.

Der Staat greift diese Ängste mit einem Versprechen individueller Sicherheit auf und reproduziert sie durch die Einführung immer neuer Sicherheitsmaßnahmen, welche zugleich ein Sicherheits- und ein Unsicherheitsgefühl erzeugen. Der Staat erschafft so seine eigene Legitimitätsgrundlage immer wieder neu.

Das verstärkte Streben nach Sicherheit führt dazu, dass das Subjekt die Notwendigkeit der Beschneidung der Handlungsfreiheit einsieht, sogar fordert. Das Ideal der umfassenden Sicherheit führt zur erhöhten Wahrnehmung von Risiken und individueller Prävention, welche der Annahme folgt, durch „vernünftiges“ Verhalten könne man Bedrohungen abwenden. Mit staatlichen Sicherheitsmaßnahmen einhergehende Verhaltensanforderungen und Beschneidungen der Handlungsfreiheit werden so vom Subjekt übernommen und vermeintlich selbst gewollt.

Die Geheimdienste befördern gemeinsam mit anderen Sicherheitsbehörden durch die stetige Betonung der neuen Quantität und Qualität der terroristischen Bedrohung sowie Warnungen vor Terroranschlägen den Nährboden der sozialen Kontrolle, in welcher sich das Individuum durch die Führung seiner selbst an der eigenen Konformität beteiligt.

6.2.3 Kontrolltechniken

Die Verwaltung des empirisch Normalen lässt Abweichung rund um das empirische Mittel bis zu flexiblen Toleranzgrenzen zu. Letztere stellen ein Risiko dar, dass es zu verwalten gilt. Um die Risikoträger_innen zu erkennen, setzen die Geheimdienste auf Telekommunikationsüberwachung, welche die Realität abbildet. Mit Data Mining kann diese Realität statistisch und wahrscheinlichkeitsbasiert erfasst und aus-

gewertet werden. Dies ermöglicht eine automatisierte, algorithmische Risikodetektion. Hinzu kommt die Auswertung mit Hilfe von Selektoren durch Analyst_innen, welche ebenfalls der Risikodetektion dient, aber nur teilautomatisiert erfolgt. Die Überschreitung der Toleranzgrenzen soll möglichst frühzeitig erkannt werden, um die Risikoträger_innen möglichst ökonomisch verwalten zu können. Dies geschieht auf Basis probabilistischer Aussagen, die darlegen wer in Zukunft eine Gefahr darstellen könnte.

Ziel der Geheimdienste ist dabei mitnichten nur der postulierte Terrorismus, sondern jedwede Abweichung, die als Gefährdung angesehen wird. Darunter fallen auch Journalist_innen, Whistleblower_innen, Aktivist_innen - letztlich kann jeder Mensch, Gruppe oder Ort im Raster hängen bleiben, sofern sie als (vermeintliches) Risiko deklariert oder erkannt wird.

Mit KARMA POLICE verfügt der britische GCHQ über ein Programm, das Browsing-Verläufe von Internetnutzer_innen offenlegen kann, aber auch die Besucher_innen bestimmter Webseiten oder Foren (INFINITE MONKEYS) anzeigen kann. Auf deren Basis lassen sich im Amazon Stil Abfragen á la „Terrorists who like website X also like website Y“[436] stellen. Eine Vielzahl weiterer Programme erlauben die Beantwortung weiterer Fragen („Question Focused Database“). Beispielsweise können Kommunikationsnetzwerke analysiert und damit Gruppen erkannt werden (SOCIAL ANTHROPOID). Durch die Erkennung von Gruppen sowie Personen mit zentralen Funktionen in diesen, können Menschen gezielt „beschäftigt“ oder mit Schadsoftware angegriffen werden.

Zudem lassen sich automatisiert Verhaltensmuster von Internetnutzer_innen erfassen, auf deren Basis der Geheimdienst Lebensrhythmen und Profile erstellen kann. Hierdurch lässt sich abweichendes Verhalten von normalen Rhythmen oder vom gesellschaftlichen Durchschnitt feststellen.

Mit SQUEAKY DOLPHIN existiert ein Programm, das ursprünglich zur Vorhersage von Protesten, Aufständen und Revolutionen entwickelt wurde, es soll aber auch andere gesellschaftliche Entwicklungen prognostizieren. Es wertet Social Media Dienste aus und soll Verhaltensvorhersagen für Städte und Regionen realisieren. Es ermöglicht so, frühzeitig oder präventiv zu reagieren. Der BND möchte mit „Ausbau der integrierten Datenanalyse (AIDA)“ ebenfalls ein System zur automatisierten algorithmischen Auswertung entwickeln beziehungsweise kaufen.

[436] Government Communications Headquarters 2011a: Folie 14.

Die von Snowden geleakten Dokumente stammen hauptsächlich aus den Jahren 2009 - 2012. Sie legen nahe, dass die Entwicklung seitdem massiv vorangetrieben wurde und die algorithmische Überwachung zunehmend zum Standard der Geheimdienste wird. Gemeinsam haben die Programme, dass sie die riesigen Datenmengen der geheimdienstlichen Telekommunikationsüberwachung algorithmisch nach Mustern, Rastern, Verhaltenskontrolle und Profilierung erfassen und dort anhand von flexibel festlegbaren Toleranzgrenzen Risiken erkennen können. Diese sind meist probabilistischer Natur und lassen so eine Reaktion im Vorfeld eines eintretenden Schadens verwalten.

Hier setzt die Prävention an: Sie versucht, die Wahrscheinlichkeit des Schadenseintrittes weiter zu reduzieren. Berichten Journalist_innen zu bestimmten Themen zu kritisch oder veröffentlichen unbequemes Material, wird ihnen zum Teil der journalistische Status abgesprochen oder sie zu Terrorist_innen deklariert (USA und GB). Bei Journalist_innen ist eine Selbstzensur in bestimmten Themenbereichen empirisch nachweisbar. Insgesamt ist die Terrorismusdefinition soweit gehalten, dass mit ihr flexibel gearbeitet werden kann. Terrorismusvorwürfe können zu Verhaltensanpassungen bei den Individuen und Gruppen, aber auch zu gesellschaftlichem Ausschluss führen.

Die Abteilung Joint Threat Research Intelligence Group (JTRIG) des GCHQ führt verdeckte Aktionen durch, um präventiv auf Individuen, Gruppen und Diskurse einwirken zu können. Diese sollen mit verschiedenen Techniken im Normalbereich gehalten oder dorthin zurückgeholt werden. Sie verwenden hierzu vielfältige Methoden, welche mit „Verleugnung, Zersetzung, Herabwürdigung und Täuschung“[437] operieren. JTRIG arbeitet nicht nur mit präventiven, sondern auch mit exkludierenden Methoden, sie können Individuen oder Gruppen von der Telekommunikation abschneiden, aus Diskursen ausschließen oder Leben ruinieren. Mit JTRIG vergleichbares wurde in den USA gefordert.

Eines der Ziele von JTRIG waren Aktivist_innen (Anonymous oder allgemein Hacktivist_innen), welche mit vielfältigen Methoden drangsaliert wurden. Ziel war es, Anonymous durch verschiedene Angriffe zu zersetzen, öffentlich zu diskreditieren, sowie Aktivist_innen von Anonymous zu inhaftieren.

JTRIG kann als eine Institution staatlicher Sozialkontrolle angesehen werden. Sie versucht, durch gezielte Beeinflussung die Einzelnen, Gruppen oder die Bevölkerung

[437] Government Communications Headquarters 2012a: S. 5.

dazu zu bewegen, sich im Normalbereich zu bewegen. Dies kann schon weit im Vorfeld einer Abweichung, als auch nach Überschreiten einer Toleranzgrenze geschehen.

Die NSA stuft Muslime als Risiko ein und versucht diese präventiv zu verwalten. Eine Form dieser Verwaltung besteht darin, die Glaubwürdigkeit von Risikoträger_innen zu unterminieren und sie so aus Diskursen auszuschließen. Der präventive Ausschluss von Meinungsführer_innen, die die Geheimdienste als Gefahr wahrnehmen, führt gleichzeitig zu einer Prävention und Konservation der Gesellschaft. Schließen Geheimdienste Minderheitsmeinungen aus Diskursen aus, sind diese für einen großen Teil der Bevölkerung nicht mehr wahrnehmbar und können aus Geheimdienstperspektive keinen Schaden anrichten. Die gezielte Beschneidung der Meinungspluralität ist eine gesellschaftskonservierende Methode der sozialen Kontrolle.

6.2.4 Ausschlusstechniken

Ist ein Individuum weder mit Selbstführungstechniken, noch mit Kontrolltechniken im Rahmen zu halten (nicht hinnehmbare Fälle oder Wiederholungstäter_innen), wird mit sozialkontrollierendem Ausschluss reagiert.

Geheimdienste können Individuen oder Gruppen auf unterschiedliche Arten ausschließen. Eine Möglichkeit besteht in Form von sogenannten Watchlists, welche auf Basis geheimdienstlicher und polizeilicher Risikodetektion gefüllt werden. Die Terrorist Watchlist umfasste 2013 680'000 Menschen. Die No Fly List 47'000. Letztere dürfen kein Flugzeug betreten, das den amerikanischen Luftraum überquert.

Auch hier wird mit äußerst vagen Definitionen von Terrorismus gearbeitet, welche auch den Ausschluss von Menschen gewährleistet, die eigentlich keine Terrorist_innen sind. Für eine Einstufung als Terrorist_in reicht dabei zum Teil schon eine falsche Äußerung in sozialen Netzwerken oder ein Kontakt zu anderen als Terrorist_in eingestuften Personen. So lassen sich ganze Risiko- oder Randgruppen watchlisten. Zudem hat das Watchlisting, beziehungsweise die spezielle Behandlung auf Basis von Aussagen, Auswirkungen auf das gesellschaftlich Sagbare. So sind beispielsweise auch kritische Journalist_innen gewatchlistet.

Wird eine Person als Terrorist_in gelabelt, führt dies zu vielfältigen repressiven Handlungen seitens des Staates, die zum Teil ausschließende, aber auch präventive Wirkungen haben. Mit dem Labeling kann auch ein gesellschaftlicher Ausschluss verbunden sein, wenn bekannt wird, dass eine Person eine Terrorist_in „ist“.

Mit der Kill List existiert eine Liste, die von der NATO verwaltet wird, welche die gezielte Tötung und damit den finalen Ausschluss aus dem Leben festschreibt. Die Liste wird auf Basis geheimdienstlicher Informationen u.a. von NSA, GCHQ und BND befüllt. Die Geheimdienste orten zudem die Handys der Personen, die eine Art Peilsender für die Raketen der Drohnen darstellen.

Signature Strikes werden gegen unbekannte Personen geflogen, deren Verhalten als zu riskant eingeschätzt wird. Dies geschieht auf Basis von Satellitenüberwachung, sowie mittels Data Mining gefundenen Verhaltensauffälligkeiten in der geheimdienstlich überwachten Telekommunikation (z.B. SKYNET).

Eine weitere Möglichkeit des Ausschlusses besteht vermittelt über Strafverfolgungsbehörden, welchen Informationen weitergegeben werden, die zu (Gefängnis-)Strafen führen können. Etwaige Watchlisteinträge werden in einem Prozess auch an das Gericht weitergegeben und können so strafverschärfend wirken. Insbesondere in den USA und Großbritannien ist ein Trend zum Ausschluss durch Einsperren zu beobachten, in Deutschland ist dieser weit weniger ausgeprägt.

6.2.5 Zusammenschau

Mit der Betonung der kontinuierlichen Bedrohung durch den internationalen Terrorismus sowie angeblich verhinderten Terroranschlägen, unterstützen die Geheimdienste eine permanente Verunsicherung, die die Grundlage für die Selbstführungstechniken bilden. Insofern üben die Geheimdienste, vermittelt über ein Angstszenario, eine soziale Kontrolle auf die Subjekte aus, die auf deren Basis Verhaltensanforderungen als die vermeintlich eigenen wahrnehmen und die „richtigen“ Handlungsoptionen wählen.

Dieser Prozess ist nicht unfehlbar und nicht alleinig auf die Geheimdienste zurückzuführen, dennoch stützen sie ihn. Die Fehlbarkeit wird durch eine Risikodetektion an den Rändern des empirisch Normalen ausgeglichen. Diese Risikodetektion, die teils vollautomatisch durch Big-Data-Analysen vorgenommen werden, führen zur flexiblen Ziehung von Toleranzgrenzen, an welchen die Individuen, die sich nicht selbst führen, mit präventiven Maßnahmen in den Normalbereich zurückgeholt werden sollen.

Die Geheimdienste nehmen hierbei Einfluss auf Risikoträger_innen, Gruppen und Diskurse, um diese zur Konformität zu bewegen. Diese präventive soziale Kontrolle wird durch den Ausschluss von Minderheitsmeinungen, Aktivist_innen und Mei-

nungsführer_innen auf die gesamte Gesellschaft ausgeübt. Die Gesellschaft wird konserviert. Die Prävention trifft auch (kritische) Journalist_innen und ihre Quellen (z.B. Whistleblower_innen), die von - aus geheimdienstlicher Perspektive - gefährlichem Verhalten abgehalten werden sollen. Bei Journalist_innen sind Chilling Effects empirisch nachweisbar.

Führt auch die Prävention nicht zum Erfolg oder wird das Risiko als zu ausgeprägt wahrgenommen, triggern die Geheimdienste Maßnahmen des repressiven Ausschlusses. Hierzu gehört das Einsperren vermittelt über Strafverfolgungsbehörden und Watchlists, die sowohl präventive als auch ausschließende Einzelmaßnahmen beinhalten können und zudem zu einem gesellschaftlichen Ausschluss, der als Terrorist_in gelabelten führen kann. Eine besondere Form des nachhaltigen Ausschlusses, der auf Basis geheimdienstlicher Risikodetektion durchgeführt wird, stellt die gezielte Tötung dar. Sie ist der ultimative Ausschluss.

Die Techniken des Ausschlusses und der Prävention sind analytisch schwer zu trennen, da sie meist Hand in Hand gehen. Oft arbeiten die Abteilungen (z.B. JTRIG) mit beiden oder die Programme und Maßnahmen (z.B. Watchlists) enthalten beide Techniken. So hat der Ausschluss einer Meinungsführer_in beispielsweise auch präventive Effekte auf die Gesellschaft und/oder ihr Umfeld.

6.3 Soziale Kontrolle durch geheimdienstliche Telekommunikationsüberwachung

Ein Wandel von disziplinargesellschaftlichen hin zu sicherheitsgesellschaftlichen Techniken der sozialen Kontrolle ist im Bereich der geheimdienstlichen Telekommunikationsüberwachung zu konstatieren. Zwar können disziplinargesellschaftliche Kontrollelemente im Bereich der Strafverfolgung, welche von Geheimdiensten teilweise unterstützt wird, erkannt werden, doch sind diese rückläufig. Zudem stellen sie nur einen Nebenaspekt geheimdienstlicher Telekommunikationsüberwachung dar. Interessant ist die Feststellung einer Selbstdisziplinierung, die seitens der Geheimdienste nicht intendiert war, über die Veröffentlichung der geheimdienstlichen Überwachungspraxis und der darüber geführten gesellschaftlichen Diskussion. Diese Formen der sozialen Kontrolle erscheinen allerdings rückläufig und stellen nicht mehr den Fokus der sozialen Kontrolle dar.

Mit den Terroranschlägen des 11. September 2001 wurde Terrorismus eine zentrale Angst in westlichen Gesellschaften. Mit dieser Angst konnten die Geheimdiens-

te ihre Krise überwinden und fanden im internationalen Terrorismus einen neuen Primärfeind. Seitdem betonen sie die kontinuierliche Gefährdung durch eben jenen und schüren so die Angst in der Bevölkerung. Diese permanente Angst bildet die Grundlage für die geheimdienstliche Telekommunikationsüberwachung und die Selbstführungstechniken. Hier ist eine parallele Entwicklung zwischen gesellschaftlicher Angst vor dem Terrorismus und geheimdienstlicher Erneuerung durch eben jene festzustellen. Insofern scheint die Modernisierung der Geheimdienste sicherheitsgesellschaftlich geprägt zu sein.

Terrorismus stellt dabei den Begründungszusammenhang für den stetigen Ausbau der Überwachungsprogramme der Geheimdienste dar. Terrorismus wird dabei allerdings so weit verstanden, dass er sich für die soziale Kontrolle vieler Risiken eignet. Zudem stellt Terrorismus nicht den einzigen Aufgabenbereich der Geheimdienste dar.[438]

Die Arbeit zeigt, dass in Überwachungsprogrammen im Bereich der automatisiert-algorithmischen Verhaltenserkennung und Prognose die Zukunft gesehen wird. Diese eignet sich aber schlechterdings nicht zur Erkennung und Verhinderung von Terroranschlägen. Insofern legt die Untersuchung nahe, dass eine zentrale, wenn nicht sogar die primäre, Aufgabe der Geheimdienste in der Verwaltung des empirisch Normalen liegt. Terrorismus ist hier eine Abweichung unter vielen, die es zu verwalten gilt.

Im Rahmen der Untersuchung konnte festgestellt werden, dass die Geheimdienste sich am empirisch Normalen orientieren und Abweichung bis zu einem gewissen Grad tolerieren (z.B. Gesetzesverstöße). Die Überwachungsprogramme arbeiten mit den sicherheitsgesellschaftlichen Kontrolltechniken. Sie detektieren Risiken, die flexible Toleranzgrenzen überschreiten oder zu überschreiten drohen und verwalten diese.

Die Geheimdienste arbeiten hierzu mit Prävention und Ausschluss, welche jedoch häufig eng miteinander verwoben sind. Eine klare Sphärentrennung ist in der Realität nicht gegeben. Die Geheimdienste üben hier aktiv soziale Kontrolle aus. Diese reicht von der Beeinflussung von Risikoträger_innen, Gruppen und Diskursen, die gesellschaftlich konservierende sowie im Normalbereich haltende oder holende Effekte hat, über die Zersetzung von Gruppen und die Zerstörung von Existenzen, bis hin zum ultimativen Ausschluss durch gezielte Tötung.

In einem Satz: Die Geheimdienste üben soziale Kontrolle aus. Hierbei greifen sie auf die sicherheitsgesellschaftliche Verwaltung des empirisch Normalen mit ih-

[438] vgl. National Security Agency et al. o. J.

ren Techniken der Kontrolle und des Ausschlusses zurück. Zudem agieren sie in Sicherheitsdiskursen und unterstützen hierin eine permanente Verunsicherung, die die Grundlage für die sicherheitsgesellschaftliche Selbstführung schafft. Insofern sind sie hier zumindest an der sozialen Kontrolle beteiligt. Die Erklärungskraft der disziplinargesellschaftlichen Sozialkontrolle und ihren Techniken lässt zu wünschen übrig. Sie sind zwar vorhanden, befinden sich aber auf dem Rückzug.

6.4 Bewertung der Methode und Theorie

In den Surveillance Studies wird seit längerem die Erklärungs- und Überzeugungskraft des panoptischen Prinzips, und mit ihm die disziplinargesellschaftlichen Theorien, diskutiert. Diesen kann insofern gefolgt werden, als dass die disziplinargesellschaftlichen und panoptischen Theorien der sozialen Kontrolle weithin nicht die gewünschte Erklärungskraft für die geheimdienstliche Telekommunikationsüberwachung bieten. Mit der sicherheitsgesellschaftlichen sozialen Kontrolle kann die geheimdienstliche Telekommunikationsüberwachung und ihre sozialen Kontrollwirkungen jedoch gut und weitreichend erklärt werden.

Mit der heuristisch-hermeneutischen Vorgehensweise konnte sich die Untersuchung trotz des Mangels an umfassenden Informationen der Realität nähern und Aussagen zu dieser treffen. Unterstützend wirkte hierbei die Interpretation der Originaldokumente und der journalistischen, wissenschaftlichen und technischen Aufarbeitung der Thematik. Die Reinterpretation der Dokumente und der älteren Arbeiten zum Thema, im Kontext neuer Veröffentlichungen, war dabei unabdingbar. Hilfreich war außerdem das umfangreiche Vorwissen und technische Verständnis des Autors.

Weitere Forschungsarbeiten im Anschluss an die vorliegende Untersuchung (beispielsweise die Analyse nicht untersuchter Programme oder neuer Veröffentlichungen mit anderen Zielsetzungen oder Theorien), sowie jenseits dieser, scheinen dem Autor unabdingbar. Geheimdienste und ihre Überwachung erscheinen sozialwissenschaftlich unterforscht insbesondere was die aktuellen Entwicklungen rund um die Dokumente von Edward Snowden angeht. Dies erscheint umso unverständlicher, ob der Reichweite und Tiefe der Überwachungsprogramme und ihrer gesellschaftlichen Auswirkungen. Unklar bleibt, warum die Forschung hier nur langsam voranschreitet. Möglicherweise handelt es sich hierbei auch um Chilling Effects.

Literatur

Albrecht, Hans-Jörg (2011): Bestrafung der Armen? Zu Zusammenhängen zwischen Armut, Kriminalität und Strafrechtsstaat. In: Gerechte Ausgrenzung? Wohlfahrtsproduktion und die neue Lust am Strafen. Hrsg. von Bernd Dollinger und Henning Schmidt-Semisch. Wiesbaden: VS Verlag, S. 111–129.

Albrecht, Peter-Alexis (2010): Der Weg in die Sicherheitsgesellschaft. Auf der Suche nach staatskritischen Absolutheitsregeln. Berlin: BWV - Berliner Wissenschafts-Verlag.

Amnesty International (2015): Global opposition to USA big brother mass surveillance. URL: https://www.amnesty.org/en/latest/news/2015/03/global-opposition-to-usa-big-brother-mass-surveillance/.

Appelbaum, Jacob et al. (2014): Snowden-Dokumente: Was die NSA knacken kann - und was nicht. URL: http://www.spiegel.de/netzwelt/netzpolitik/snowden-dokument-so-unterminiert-die-nsa-die-sicherheit-des-internets-a-1010588.html.

Assion, Simon (2014): Überwachung und Chilling Effects. In: Überwachung und Recht. Tagungsband zur Telemedicus Sommerkonferenz 2014. Hrsg. von Telemedicus e.V. Berlin: epubli, S. 31–82. URL: https://www.telemedicus.info/uploads/Dokumente/Ueberwachung-und-Recht-Tagungsband-Soko14.pdf.

Baker, Stewart zitiert nach Alan Rusbridger (2013): The Snowden Leaks and the Public. URL: http://www.nybooks.com/articles/2013/11/21/snowden-leaks-and-public/.

Bamford, James (1986): NSA, Amerikas geheimster Nachrichtendienst. Zürich: Orell Füssli.

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

Baumgärtner, Maik et al. (2016): Silvester in München: Terrorwarnung basierte maßgeblich auf einer Quelle. URL: http://www.spiegel.de/politik/deutschland/muenchen-silvester-terrorwarnung-basierte-auf-nur-einer-quelle-a-1071140.html.

Beck, Ulrich (2000): Risikogesellschaft: auf dem Weg in eine andere Moderne. Erstausgabe, 15. Nachdruck. Frankfurt am Main: Suhrkamp.

Benkel, Thorsten (2011): AUGEN OHNE GESICHT. Videoüberwachung zwischen Kontrolltechnik und Ordnungsutopie. In: Überwachungspraxen - Praktiken der Überwachung. Analysen zum Verhältnis von Alltag, Technik und Kontrolle. Hrsg. von Nils Zurawski. Opladen & Farmington Hills MI: Budrich UniPress, S. 103–117.

Bergen, Peter et al. (2014): Do NSA's Bulk Surveillance Programs Stop Terrorists? Hrsg. von New America Foundation. URL: https://www.newamerica.org/downloads/IS_NSA_surveillance.pdf.

Beuth, Patrick (2015): Microsoft nutzt künftig Telekom-Rechenzentren. URL: http://www.zeit.de/digital/datenschutz/2015-11/cloud-microsoft-rechenzentren-deutschland.

Biermann, Kai (2014): Algorithmen Allmächtig? Freiheit in den Zeiten der Statistik. URL: https://netzpolitik.org/2014/algorithmen-allmaechtig-freiheit-in-den-zeiten-der-statistik/.

Biermann, Kai und Yassin Musharbash (2015): Suche NSA-Spionagesoftware, biete deutsche Daten. URL: http://www.zeit.de/digital/datenschutz/2015-08/xkeyscore-nsa-verfassungsschutz.

Biermann, Kai und Thomas Wiegold (2015): Drohnen. Chancen und Gefahren einer neuen Technik. Lizenzausgabe für die BpB. Berlin: Christoph Links Verlag.

Biselli, Anna (2015a): Live-Blog aus dem Geheimdienst-Untersuchungsausschuss: BND löscht trotz Moratorium Mails mit Selektoren. URL: https://netzpolitik.org/2015/live-blog-aus-dem-geheimdienst-untersuchungsausschuss-2/.

– (2015b): Safe-Harbor-Urteil schränkt nicht nur Datentransfer in die USA ein, es ruft auch EU-Staaten zur Verantwortung. URL: https://netzpolitik.org/2015/safe-harbor-urteil-schraenkt-nicht-nur-datentransfer-in-die-usa-ein-es-ruft-auch-eu-staaten-zur-verantwortung/.

Bitkom (2013): NSA-Affäre bringt Verschlüsselung in Mode. URL: https://www.bitkom.org/Presse/Presseinformation/NSA-Affaere-bringt-Verschluesselung-in-Mode.html.

– (2014): Internetnutzer halten ihre Daten im Web für unsicher. URL: https://web.archive.org/web/20140607132440/http://www.bitkom.org/files/documents/BITKOM_Presseinfo_Ein_Jahren_Sowden_-_Vertrauen_im_Internet_04_06_2014.pdf.

Bleich, Holger (2013): Globaler Abhörwahn. Wie digitale Kommunikation belauscht wird. URL: http://www.heise.de/ct/ausgabe/2013-16-Wie-digitale-Kommunikation-belauscht-wird-2317919.html.

Bogard, William (2014): Simulation and post-panopticism. In: Routledge Handbook of Surveillance Studies. Hrsg. von Kristie Ball, Kevin D. Haggerty und David Lyon. Paperback. New York u.a.: Routledge, S. 30–37.

Bogdal, Klaus-Michael (2008): Überwachen und Strafen. In: Foucault Handbuch. Leben - Werk - Wirkung. Hrsg. von Clemens Kammler, Rolf Parr und Ulrich Johannes Schneider. Stuttgart: J.B. Metzler, S. 68–80.

Booz Allen Hamilton (2010): The Unofficial XKEYSCORE User Guide. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH012e/6318a2b1.dir/doc.pdf.

Brennan, John zitiert nach Jon Schwarz (2015): CIA Director John Brennan Admits U.S. Foreign Policy Could Spur Terrorism. URL: https://theintercept.com/2015/06/06/cia-director-john-brennan-admits-killing-people-countries-might-make-want-kill-us/.

Bundesministerium des Innern (o. J.): Zusammenarbeit der Sicherheitsbehörden. Den Netzwerken der Terroristen wird ein Netzwerk der Sicherheitsbehörden entgegengestellt.

URL: https://www.bmi.bund.de/DE/Themen/Sicherheit/Terrorismusbekaempfung/Sicherheitsbehoerden/sicherheitsbehoerden_node.html.

Bundesministerium des Innern und Bundesministerium der Justiz (2006): Zweiter Periodischer Sicherheitsbericht. URL: https://www.bmi.bund.de/SharedDocs/Downloads/DE/Veroeffentlichungen/2_periodischer_sicherheitsbericht_langfassung_de.pdf.

Bundesnachrichtendienst (o. J.): Strategische Initiative Technik (SIT). Schutz deutscher Interessen. URL: https://netzpolitik.org/2015/strategische-initiative-technik-wir-enthuellen-wie-der-bnd-fuer-300-millionen-euro-seine-technik-aufruesten-will/.

Bundesverfassungsgericht (2010): Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäß. URL: https://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.html.

Castro, Daniel und Alan McQuinn (2015): Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness. URL: http://www2.itif.org/2015-beyond-usa-freedom-act.pdf.

Centre for International Governance Innovation und Ipsos (2014): 83% of Global Internet Users Believe Affordable Access to the Internet Should be a Basic Human Right. URL: https://www.cigionline.org/sites/default/files/survey/factum.pdf.

Ciesielski, Rebecca (2014): Müssen wir mit allem rechnen? Ein Lagebericht aus der Welt des Dataismus 1. URL: https://netzpolitik.org/2014/muessen-wir-mit-allem-rechnen-ein-lagebericht-aus-der-welt-des-dataismus-1/.

DE-CIX (o. J.): Quick Facts. URL: https://www.de-cix.net/about/quick-facts/.

Currier, Cora, Glenn Greenwald und Andrew Fishman (2015): U.S. Government Designated Prominent Al Jazeera Journalist as „Member of Al Qaeda“. URL: https://firstlook.org/theintercept/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaeda-member-put-watch-list/.

Deleuze, Gilles (1993): Unterhandlungen. Frankfurt am Main: Suhrkamp Verlag.

Dollinger, Bernd (2011): Punitivität in der Diskussion. Konzeptionelle, theoretische und empirische Referenzen. In: Gerechte Ausgrenzung? Wohlfahrtsproduktion und die neue Lust am Strafen. Hrsg. von Bernd Dollinger und Henning Schmidt-Semisch. Wiesbaden: VS Verlag, S. 25–73.

– (2016): Sicherheit als politische Narration: Risiko-Kommunikation und die Herstellung von Un-/Sicherheit. In: Sicherer Alltag? Politiken und Mechanismen der Sicherheitskonstruktion im Alltag. Hrsg. von Bernd Dollinger und Henning Schmidt-Semisch. Wiesbaden: VS Verlag, S. 58–80.

Eichenberger, Heinrich (2013): Geheimdienste im Wandel. Grundsätzliches aus einer verschlossenen Welt. 2. überarbeitete Auflage. Berlin: Hubert W. Holzinger Verlag.

Elmer, Greg (2014): Panopticon - discipline - control. In: Routledge Handbook of Surveillance Studies. Hrsg. von Kristie Ball, Kevin D. Haggerty und David Lyon. Paperback. New York u.a.: Routledge, S. 21–29.

Ermert, Monika und Christian Grothoff (2016): Data Mining für den Drohnenkrieg. Lexikon des NSA-Skandals: XKeyscore. In: *c't Magazin für Computertechnik* 2016 Heft 3, S. 82–84.

Ermert, Monika und Martin Holland (2015): Spion im Kabel. Lexikon des NSA-Skandals: Tempora. In: *c't Magazin für Computertechnik* 2015 Heft 18, S. 72–73.

Federal Bureau of Investigation (2011): Ten Years After: The FBI Since 9/11 - Terrorist Screening Center. URL: https://www.fbi.gov/about-us/ten-years-after-the-fbi-since-9-11/just-the-facts-1/terrorist-screening-center-1.

Fennen, Nicolas (2013): PRISM: neue Folien gewähren tieferen Einblick ins Spionageprogramm. URL: https://netzpolitik.org/2013/prism-neue-folien-gewahren-tieferen-einblick-ins-spionageprogramm/.

Fogg, Ally (2013): Crime is falling. Now let's reduce fear of crime. URL: http://www.theguardian.com/commentisfree/2013/apr/24/crime-falling-reduce-fear-crime.

Foucault, Michel (1994): Überwachen und Strafen. Die Geburt des Gefängnisses. Frankfurt am Main: Suhrkamp Verlag.

– (2005): Analytik der Macht. Frankfurt am Main: Suhrkamp Verlag.

– (2006): Sicherheit, Territorium, Bevölkerung. Geschichte der Gouvernementalität I. Frankfurt am Main: Suhrkamp Verlag.

Franz, Peter (2000): Wie weit trägt das Konzept „soziale Kontrolle“ bei der Analyse aktueller gesellschaftlicher Entwicklungstrends? Eine Diskussion anhand der These der gefährdeten Integrationsfunktion der Stadt. In: Soziale Kontrolle. Zum Problem der Normkonformität in der Gesellschaft. Hrsg. von Helge Peters. Opladen: Leske + Budrich, S. 67–74.

Froitzhuber, Kilian (2014): GCHQ hat 1,8 Millionen Yahoo-Nutzer durch ihre Webcams angeschaut. URL: https://netzpolitik.org/2014/gchq-hat-18-millionen-yahoo-nutzer-durch-ihre-webcams-angeschaut/.

Fuchs, Christian und John Goetz (2013): Geheimer Krieg. Wie von Deutschland aus der Kampf gegen den Terror gesteuert wird. Reinbek bei Hamburg: Rowohlt.

Gallagher, Ryan (2014a): How Secret Partners Expand NSA's Surveillance Dragnet. URL: https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/.

– (2014b): Operation Socialist. The Inside Story of How British Spies Hacked Belgium's Largest Telco. URL: https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/.

– (2014c): The Surveillance Engine. How the NSA Built Its Own Secret Google. URL: https://theintercept.com/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/.
– (2015): Profiled. From Radio to Porn, British Spies Track Web Users' Online Identities. URL: https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/.

Gallagher, Ryan und Glenn Greenwald (2014): How the NSA Plans to Infect 'Millions' of Computers with Malware. URL: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/.

Gallagher, Sean (2013): NSA's Internet taps can find systems to hack, track VPNs and Word docs. X-Keyscore gives NSA the ability to find and exploit vulnerable systems. URL: http://arstechnica.com/tech-policy/2013/08/nsas-internet-taps-can-find-systems-to-hack-track-vpns-and-word-docs/.

Garland, David (2008): Kultur der Kontrolle: Verbrechensbekämpfung und soziale Ordnung in der Gegenwart. Frankfurt am Main: Campus Verlag.

Gellman, Barton und Ashkan Soltani (2013): NSA collects millions of e-mail address books globally. URL: https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

Goenemeyer, Axel (2010): Wege der Sicherheitsgesellschaft. Transformationen der Konstruktion und Regulierung innerer Unsicherheiten. In: Wege der Sicherheitsgesellschaft. Gesellschaftliche Transformationen der Konstruktion und Regulierung innerer Unsicherheiten. Hrsg. von Axel Goenemeyer. Wiesbaden: VS Verlag, S. 7–19.

Government Communications Headquarters (2007): Legalities - GCHQ Databases eg Pilbeam, Salamanca, UDAQ etc. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH013a/c8b311c2.dir/doc.pdf.
– (2009a): Next Generation Events NGE - Black Hole ConOp. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01d4/ef815e69.dir/doc.pdf.
– (2009b): QFDs and BLACHOLE Technology behind GCHQ/INOC. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH015d/f4899a33.dir/doc.pdf.
– (2010): Supporting Internet Operations. Special Source Access. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH017d/08954fff.dir/doc.pdf.
– (2011a): „ITCR Cloud Efforts". developing „canonical" SIGINT analytics, finding hard targets and exploratory data analysis at scale. In: *Snowden Archive*. Hrsg. von Edward

Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH016c/7768c9ff.dir/doc.pdf.

– (2011b): Blazing Saddles. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASHd779.dir/doc.pdf.
– (2011c): Data stored in BLACK HOLE. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH017c/04e1431d.dir/doc.pdf.
– (2011d): SOCIAL ANTHROPOID. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01e3/50d2705c.dir/doc.pdf.
– (2012a): Cyber Integration. „The Art of the Possible“. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0128/9e0b815f.dir/doc.pdf.
– (2012b): GCHQ Analytic Cloud Challenges. Innovation Lead for Data, Analytics Visualisation Engineering. URL: https://theintercept.com/document/2015/09/25/gchq-analytic-cloud-challenges/.
– (2012c): Hacktivism: Online Covert Action. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01b7/cc3c2766.dir/doc.pdf.

Government Communications Headquarters (2012d): Psychology. A New Kind of SIGDEV. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH4aab/c6231e74.dir/doc.pdf.

– (2012e): ROCKRIDGE. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0823.dir/doc.pdf.
– (2012f): TEMPORA. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0105/09f49f0f.dir/doc.pdf.
– (o. J.): A potential technique to deanonymise users of the TOR network. URL: http://www.spiegel.de/media/media-35538.pdf.

Greenwald, Glenn (2013): XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. URL: http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

– (2014a): Die globale Überwachung. Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen. München: Droemer.

– (2014b): How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations. URL: https://theintercept.com/2014/02/24/jtrig-manipulation/.
– (2015a): For Terrorist Fearmongers, It's Always the Scariest Time Ever. URL: https://theintercept.com/2015/06/02/fear-mongers-always-scariest-time-ever/.
– (2015b): Western Spy Agencies Secretly Rely on Hackers for Intel and Expertise. URL: https://theintercept.com/2015/02/04/demonize-prosecute-hackers-nsa-gchq-rely-intel-expertise/.

Greenwald, Glenn und Andrew Fishman (2015): Controversial GCHQ Unit Engaged in Domestic Law Enforcement, Online Propaganda, Psychology Research. URL: https://theintercept.com/2015/06/22/controversial-gchq-unit-domestic-law-enforcement-propaganda/.

Greenwald, Glenn und Ewen MacAskill (2013): NSA Prism program taps in to user data of Apple, Google and others. URL: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Henze, Saskia und Johann Knigge (1997): Stets zu Diensten. Der BND zwischen faschistischen Wurzeln und neuer Weltordnung. Münster: Unrast.

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

Hirsch, Joachim (1998): Vom Sicherheitsstaat zum nationalen Wettbewersstaat. Berlin: ID Verlag.

Hirsch, Joachim und Roland Roth (1986): Das neue Gesicht des Kapitalismus: vom Fordismus zum Post-Fordismus. Hamburg: VSA-Verlag.

Höflich, Joachim R. (2016): Der Mensch und seine Medien. Mediatisierte interpersonale Kommunikation. Eine Einführung. Wiesbaden: VS Verlag.

Holland, Martin (2013): Obamas „War on Leaks“: Informanten gefährdet, Informationen unter Verschluss. URL: http://www.heise.de/newsticker/meldung/Obamas-War-on-Leaks-Informanten-gefaehrdet-Informationen-unter-Verschluss-1973478.html.
– (2014): NSA-Skandal: Geheimdienste überwachen Facebook, um Proteste vorherzusagen. URL: http://www.heise.de/newsticker/meldung/NSA-Skandal-Geheimdienste-ueberwachen-Facebook-um-Proteste-vorherzusagen-2098916.html.
– (2015a): Alles ist durchleuchtet. Lexikon des NSA-Skandals: XKeyscore. In: *c't Magazin für Computertechnik* 2015 Heft 17, S. 134–135.

– (2015b): Datenschutz bei Facebook Co.: EuGH erklärt Safe Harbor für ungültig. URL: http://www.heise.de/newsticker/meldung/Datenschutz-bei-Facebook-Co-EuGH-erklaert-Safe-Harbor-fuer-ungueltig-2838025.html.

Intelligence Advanced Research Projects Activity (o. J.): Mercury. URL: http://www.iarpa.gov/index.php/research-programs/mercury.

Intelligence Surveillance Reconnaissance Task Force (2013): ISR Support to Small Footprint Operations - Somalia / Yemen. Executive Summary. URL: https://www.documentcloud.org/documents/1232171-91-3.html.

International Centre for Prison Studies (o. J.[a]): World Prison Brief. United States of America. URL: http://prisonstudies.org/country/united-states-america.

– (o. J.[b]): World Prison Brief. United Kingdom: England Wales. URL: http://prisonstudies.org/country/united-kingdom-england-wales.

– (o. J.[c]): World Prison Brief. Germany. URL: http://prisonstudies.org/country/germany.

Jakobs, Joachim (2014): Von der Kraft der Metadaten: Wie ein Geheimdienst-Chef Opfer seiner Überwachungsdoktrin wurde. URL: https://netzpolitik.org/2014/von-der-kraft-der-metadaten-wie-ein-geheimdienst-chef-opfer-seiner-ueberwachungsdoktrin-wurde-2/.

Kammerer, Dietmar (2011): Das Werden der „Kontrolle“: Herkunft und Umfang eines Deleuze'schen Begriffs. In: Überwachungspraxen - Praktiken der Überwachung. Analysen zum Verhältnis von Alltag, Technik und Kontrolle. Hrsg. von Nils Zurawski. Opladen & Farmington Hills MI: Budrich UniPress, S. 19–34.

Kampf, Lena (2015): Kaum ansteigende Kriminalität durch Flüchtlinge. URL: https://www.tagesschau.de/inland/fluechtlinge-kriminalitaet-101.html.

Kane, Alex (2016): Terrorist Watchlist Errors Spread to Criminal Rap Sheets. URL: https://theintercept.com/2016/03/15/terrorist-watchlist-errors-spread-to-criminal-rap-sheets/.

Kayyali, Dia (2014): Why Fusion Centers Matter: FAQ. URL: https://www.eff.org/deeplinks/2014/04/why-fusion-centers-matter-faq.

Klimke, Daniela (2008): Wach- & Schließgesellschaft Deutschland. Sicherheitsmentalitäten in der Spätmoderne. Wiesbaden: VS Verlag.

Knop, Carsten (2013): Edward Snowden und die Cloud. URL: http://www.faz.net/aktuell/wirtschaft/unternehmen/datenschutz-von-unternehmen-edward-snowden-und-die-cloud-12270178.html.

Krempl, Stefan (2016): BND: 2014 nahm Überwachung von Internet und Telefonnetz zu. URL: http://www.heise.de/newsticker/meldung/BND-2014-nahm-Ueberwachung-von-Internet-und-Telefonnetz-zu-3092088.html.

Krieger, Wolfgang (2009): Geschichte der Geheimdienste. Von den Pharaonen bis zur CIA. München: C.H. Beck.

Kroener, Inga und Daniel Neyland (2014): New technologies, security and surveillance. In: Routledge Handbook of Surveillance Studies. Hrsg. von Kristie Ball, Kevin D. Haggerty und David Lyon. Paperback. New York u.a.: Routledge, S. 141–148.

Kurz, Constanze und Frank Rieger (2009): Stellungnahme des Chaos Computer Clubs zur Vorratsdatenspeicherung. URL: https://ccc.de/de/vds/VDSfinal18.pdf.

Ledbetter, Sheri (2015): America's Top Fears 2015. URL: https://blogs.chapman.edu/wilkinson/2015/10/13/americas-top-fears-2015/.

Lee, Micah, Glenn Greenwald und Morgan Marquis-Boire (2015): Behind the Curtain. A Look at the Inner Workings of NSA's XKEYSCORE. URL: https://theintercept.com/2015/07/02/look-under-hood-xkeyscore/.

Lemke, Thomas (2004): „Eine Kultur der Gefahr" - Dispositive der Unsicherheit im Neoliberalismus. URL: http://www.thomaslemkeweb.de/publikationen/EineKulturderGefahr.pdf.

– (2014): Eine Kritik der politischen Vernunft. Foucaults Analyse der modernen Gouvernementalität. 6. Auflage. Hamburg: Argument Verlag.

Lindenberg, Michael und Henning Schmidt-Semisch (1995): Sanktionsverzicht statt Herrschaftsverlust: Vom Übergang in die Kontrollgesellschaft. In: *Kriminologisches Journal* 27 (1995), S. 2–17.

– (2000): Komplementäre Konkurrenz in der Sicherheitsgesellschaft : Überlegungen zum Zusammenwirken staatlicher und kommerzieller Sozialer Kontrolle. In: *Monatsschrift für Kriminologie und Strafrechtsreform. - Köln* 83 (2000), S. 306–319.

Lobo, Sascha (2015): Daten, die das Leben kosten. In: Technologischer Totalitarismus. Eine Debatte. Hrsg. von Frank Schirrmacher. Berlin: Suhrkamp, S. 107–117.

Lyon, David (2002): Editorial. Surveillance Studies: Understanding visibility, mobility and the phenetic fix. In: *Surveillance & Society* Volume 1: Issue 1, S. 1–7.

– (2015): Surveillance after Snowden. Cambridge und Malden: Polity Press.

Lyon, David, Kevin D. Haggerty und Kristie Ball (2014): Introducing surveillance studies. In: Routledge Handbook of Surveillance Studies. Hrsg. von Kristie Ball, Kevin D. Haggerty und David Lyon. Paperback. New York u.a.: Routledge, S. 1–11.

MacAskill, Ewen und James Ball (2013): Portrait of the NSA: no detail too small in quest for total surveillance. URL: http://www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance.

MacAskill, Ewen, Julian Borger et al. (2013): Mastering the internet: how GCHQ set out to spy on the world wide web. URL: http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet.

Mann, Jim (2015): Britain Uncovered survey results: the attitudes and beliefs of Britons in 2015. URL: http://www.theguardian.com/society/2015/apr/19/britain-uncovered-survey-attitudes-beliefs-britons-2015.

Marinis, Pablo de (2000): Überwachen und Ausschließen. Machtinterventionen in urbanen Räumen der Kontrollgesellschaft. Pfaffenweiler: CENTAURUS-Verlagsgesellschaft.

Marquis-Boire, Morgan, Glenn Greenwald und Micah Lee (2015): Featured News. XKEYSCORE: NSA's Google for the World's Private Communications. URL: https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/.

Marthews, Alex und Catherine Tucker (2015): Government Surveillance and Internet Search Behavior. URL: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2600645_code512675.pdf?abstractid=2412564&mirid=1.

Marx, Gary T. (2015): Surveillance Studies. URL: http://web.mit.edu/gtmarx/www/surv_studies.html.

Mascolo, Georg, Hans Leyendecker und John Goetz (2014): Codewort Eikonal - der Albtraum der Bundesregierung. URL: http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432.

McArdle, Shelly C., Heather Rosoff und Richard John (2012): The Dynamics of Evolving Beliefs, Concerns Emotions, and Behavioral Avoidance Following 9/11: A Longitudinal Analysis of Representative Archival Samples. URL: http://create.usc.edu/sites/default/files/publications/thedynamicsofevolvingbeliefsconcernsemotionsandbehavior.pdf.

McCarthy, Justin (2015): More Americans Say Crime Is Rising in U.S. URL: http://www.gallup.com/poll/186308/americans-say-crime-rising.aspx.

McLaughlin, Jenna (2015): U.S. Mass Surveillance Has No Record of Thwarting Large Terror Attacks, Regardless of Snowden Leaks. URL: https://theintercept.com/2015/11/17/u-s-mass-surveillance-has-no-record-of-thwarting-large-terror-attacks-regardless-of-snowden-leaks/.

– (2016): Twitter Says There's No „Magical Algorithm" to Find Terrorists. URL: https://theintercept.com/2016/02/05/twitter-says-theres-no-magical-algorithm-to-find-terrorists/.

Meister, Andre (2013): Glasfaserkabel und Spionage-U-Boote: Wie die NSA die Nervenzentren der Internet-Kommunikation anzapft. URL: https://netzpolitik.org/2013/glasfaserkabel-und-spionage-u-boote-wie-die-nsa-die-nervenzentren-der-internet-kommunikation-anzapft/.

– (2014a): Live-Blog aus dem Geheimdienst-Untersuchungsausschuss: „Die gesamte deutsche Auslandsaufklärung ist rechtswidrig." URL: https://netzpolitik.org/2014/live-blog-erste-oeffentliche-sitzung-des-nsa-untersuchungsausschusses/.

– (2014b): RAMPART-A: Die NSA schnorchelt mehr als 3 Terabit pro Sekunde von Glasfasern ab – und der BND macht mit (Updates). URL: https://netzpolitik.org/2014/rampart-a-die-nsa-schnorchelt-mehr-als-3-terabit-pro-sekunde-von-glasfasern-ab-und-der-bnd-macht-mit/.
– (2015a): Angezapfte Glasfasern: BND und Kanzleramt verschweigen zehn weitere Operationen zur Internet-Überwachung. URL: https://netzpolitik.org/2015/angezapfte-glasfasern-bnd-und-kanzleramt-verschweigen-zehn-weitere-internet-abschnorchel-aktionen/.

Meister, Andre (2015b): Strategische Initiative Technik: Wir enthüllen, wie der BND für 300 Millionen Euro seine Technik aufrüsten will. URL: https://netzpolitik.org/2015/strategische-initiative-technik-wir-enthuellen-wie-der-bnd-fuer-300-millionen-euro-seine-technik-aufruesten-will/.

Möchel, Erich (2016): Daten von der Königswarte für NSA-Projekt. URL: http://fm4.orf.at/stories/1766028.

Monroy, Matthias (2014): XKeyscore beim deutschen In- und Auslandsgeheimdienst. URL: https://netzpolitik.org/2014/xkeyscore-beim-deutschen-in-und-auslandsgeheimdienst/.

Narr, Wolf-Dieter (2004): Die herrschaftssichernden Funktionen von Polizei und Geheimdiensten. In: Herrschaftstheorien und Herrschaftsphänomene. Hrsg. von Hartmut Aden. Wiesbaden: VS Verlag, S. 73–88.

National Counterterrorism Center (2013): Watchlisting Guidance. URL: https://s3.amazonaws.com/s3.documentcloud.org/documents/1227228/2013-watchlist-guidance.pdf.

National Security Agency (2007): Sharing Communications Metadata Across the U.S. Intelligence Community - ICREACH. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH1aaa.dir/doc.pdf.
– (2008): XKEYSCORE. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0138/e130028c.dir/doc.pdf.
– (2009a): Frequently Asked Questions Terms and Acronyms. URL: https://www.nsa.gov/about/faqs/terms_acronyms.shtml.
– (2009b): Introduction to XKS Application IDs and Fingerprints. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH4ca8.dir/doc.pdf.
– (2011): Content Extraction Enhancements for Target Analytics. SMS Text Messages: A Goldmine to Exploit. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https:

//snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01d3/87e0fcd5.dir/doc.pdf.

– (2012a): BOUNDLESSINFORMANT - Frequently Asked Questions. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH71a8.dir/doc.pdf.

– (2012b): SKYNET: Applying Advanced Cloud-based Behavior Analytics. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01f2/b6bec2ec.dir/doc.pdf.

National Security Agency (2012c): SKYNET: Courier Detection via Machine Learning. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH019f/aef5cc0b.dir/doc.pdf.

– (2012d): TEMPORA – „The World's Largest XKEYSCORE" – Is Now Available to Qualified NSA Users. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASHc5f6.dir/doc.pdf.

– (2012e): Tor Stinks. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0111/093a3538.dir/doc.pdf.

– (2013): PRISM/US-984XN Overview. The SIGAD Used Most in NSA Reporting. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0286/0f30a474.dir/doc.pdf.

– (2014): Interne Folien aus dem Snowden Fundus. In: Die globale Überwachung. Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen. Hrsg. von Glenn Greenwald. München: Droemer.

– (o. J.): Special Sources Operation (SSO) - Various Documents. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH2047.dir/doc.pdf.

National Security Agency / Central Security Service (2007): SIGINT Mission Strategic Plan. FY2008-2013. In: *Snowden Archive*. Hrsg. von Edward Snowden. URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH9ef8.dir/doc.pdf.

– (2012): Making Things Measureable: Technology Trending Challenges an Approaches. URL: http://www.spiegel.de/media/media-35535.pdf.

National Security Agency et al. (o. J.): National Intelligence Priorities Framework. In: Hrsg. von Cryptome. URL: https://cryptome.org/2013/11/nsa-nipf-v3.htm.

Nogala, Detlef (2000): Erscheinungs- und Begriffwandel von Sozialkontrolle eingangs des 21. Jahrhunderts. In: Soziale Kontrolle. Zum Problem der Normkonformität in der Gesellschaft. Hrsg. von Helge Peters. Opladen: Leske + Budrich, S. 111–131.

Nohl, Karsten (2014): Mobile self-defense. URL: https://media.ccc.de/v/31c3_-_6122_-_en_-_saal_1_-_201412271830_-_mobile_self-defense_-_karsten_nohl.

Parlamentarisches Kontrollgremium (2016): Bericht gemäß § 14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8 G 10. URL: http://dip21.bundestag.de/dip21/btd/18/074/1807423.pdf.

PEN American Center (2013): Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor. URL: http://www.pen.org/sites/default/files/2014-08-01_Full%5C%20Report_Chilling%5C%20Effects%5C%20w%5C%20Color%5C%20cover-UPDATED.pdf.

Peters, Helge (2009): Devianz und soziale Kontrolle. Eine Einführung in die Soziologie abweichenden Verhaltens. 3., vollständig überarbeitete Aufl. Weinheim und München: Juventa Verlag.

Piper, Gerhard (2015): Abhörstaat Deutschland. Die SIGINT-Landschaft seit 1945 in Ost und West. Heise, Online-Ressource.

Poushter, Jacob (2016): Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies. But advanced economies still have higher rates of technology use. Hrsg. von Pew Research Center. URL: http://www.pewglobal.org/files/2016/02/pew_research_center_global_technology_report_final_february_22__2016.pdf.

Pütter, Norbert (2009): Die Dienste der Bundesrepublik. Vom kalten Krieg zur „neuen Sicherheitsarchitektur“. In: *Bürgerrechte & Polizei/CILIP 2/2009*, S. 3–20.

R+V Versicherungen (2015): Grafiken zur Studie „Die Ängste der Deutschen 2015“. URL: https://www.ruv.de/presse/aengste-der-deutschen/grafiken-die-aengste-der-deutschen-2015.

– (o. J.): Die Ängste der Deutschen im Langzeitvergleich. URL: https://www.ruv.de/presse/aengste-der-deutschen/aengste-der-deutschen-langzeitvergleich.

Richter, Peter (2015): Eingekastelt im Billig-Büro-Würfel. URL: http://www.sueddeutsche.de/karriere/grossraumbuero-eingekastelt-im-billig-buero-wuerfel-1.2288809.

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

Rötzer, Florian (2014): Wer seine Privatsphäre schützt, ist für die NSA ein Extremist. URL: http://www.heise.de/tp/artikel/42/42165/1.html.

Rudl, Tomas (2016): Strategische Überwachung: gerade mal 0,26 Prozent „nachrichtendienstrechtlich relevant“. URL: https://netzpolitik.org/2016/strategische-ueberwachung-gerade-mal-026-prozent-nachrichtendienstrechtlich-relevant/.

Ruoff, Michael (2009): Foucault-Lexikon. Entwicklung - Kernbegriffe - Zusammenhänge. 2., durchgesehene Auflage. Paderborn: Wilhelm Fink GmbH und Co. Verlags-KG.

Rusbridger, Alan (2013): The Only Way to Restore Trust in the NSA. URL: http://www.theatlantic.com/politics/archive/2013/09/the-only-way-to-restore-trust-in-the-nsa/279314/.

Scahill, Jeremy (2015): The Assassination Complex. Secret military documents expose the inner workings of Obama's drone wars. URL: https://theintercept.com/drone-papers/the-assassination-complex/.

Scahill, Jeremy und Josh Begley (2015): The Great SIM Heist. How Spies Stole the Keys to the Encryption Castle. URL: https://theintercept.com/2015/02/19/great-sim-heist/.

Scahill, Jeremy und Ryan Devereaux (2014a): The Secret Government Rulebook For Labeling You a Terrorist. URL: https://theintercept.com/2014/07/23/blacklisted/.

– (2014b): Watch Commander. Barack Obama's Secret Terrorist-Tracking System, by the Numbers. URL: https://theintercept.com/2014/08/05/watch-commander/.

Scahill, Jeremy und Glenn Greenwald (2014): The NSA's Secret Role in the U.S. Assassination Program. URL: https://theintercept.com/2014/02/10/the-nsas-secret-role/.

Scheerer, Sebastian (2000): „Soziale Kontrolle“ - schöner Begriff für böse Dinge. In: Soziale Kontrolle. Zum Problem der Normkonformität in der Gesellschaft. Hrsg. von Helge Peters. Opladen: Leske + Budrich, S. 153–169.

Schneier, Bruce (2013a): Attacking Tor: how the NSA targets users' online anonymity. URL: http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity.

– (2013b): The Snowden Leaks and the Public. URL: http://www.nybooks.com/articles/2013/11/21/snowden-leaks-and-public/.

– (2014a): Carry On. Sound Advice from Schneier on Security. Indianapolis, Indiana: John Wiley & Sons, Inc.

– (2014b): NSA Classification ECI = Exceptionally Controlled Information. URL: https://www.schneier.com/blog/archives/2014/10/nsa_classificat.html.

Schneier, Bruce (2014c): NSA Targets the Privacy-Conscious for Surveillance. URL: https://www.schneier.com/blog/archives/2014/07/nsa_targets_pri.html.

– (2014d): Over 700 Million People Taking Steps to Avoid NSA Surveillance. URL: https://www.schneier.com/blog/archives/2014/12/over_700_millio.html.

– (2015a): Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World. New York: W. W. Norton & Company, Inc.

– (2015b): NSA Doesn't Need to Spy on Your Calls to Learn Your Secrets. URL: https://www.wired.com/2015/03/data-and-goliath-nsa-metadata-spying-your-secrets/.

Serle, Jack (2015): Almost 2,500 now killed by covert US drone strikes since Obama inauguration six years ago: The Bureau's report for January 2015. URL: https://www.thebureauinvestigates.com/2015/02/02/almost-2500-killed-covert-us-drone-strikes-obama-inauguration/.

Shelton, Martin, Lee Rainie und Mary Madden (2015): Americans' Privacy Strategies Post-Snowden. Hrsg. von Pew Research Center. URL: http://www.pewinternet.org/files/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf.

Shiffman, John und Kristina Cooke (2013): Exclusive: U.S. directs agents to cover up program used to investigate Americans. URL: http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805.

Singelnstein, Tobias und Peer Stolle (2007a): Mechanismen und Techniken einer neuen Sozialkontrolle. In: Sicherheitsdiskurse. Angst, Kontrolle und Sicherheit in einer „gefährlichen" Welt. Hrsg. von Nils Zurawski. Frankfurt am Main: Peter Lang GmbH, S. 213–224.

– (2007b): Von der sozialen Integration zur Sicherheit durch Kontrolle und Ausschluss. Zum Wandel sozialer Kontrolle und seinen gesellschaftlichen Grundlagen. In: Surveillance Studies. Perspektiven eines Forschungsfeldes. Hrsg. von Nils Zurawski. Opladen & Farmington Hills: Verlag Barbara Budrich, S. 47–66.

– (2012): Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert. 3., vollständig überarbeitete Auflage. Wiesbaden: VS Verlag.

Snowden, Edward (2014a): Edward Snowden's Speech on Moment of Truth. URL: https://www.youtube.com/watch?v=PWAZ8fr4MUE.

– (2014b): Snowden-Interview: Transcript. URL: https://www.ndr.de/nachrichten/netzwelt/snowden277_page-3.html.

– (2014c): Snowden-Interview: Transcript. URL: https://www.ndr.de/nachrichten/netzwelt/snowden277_page-1.html.

Spiegel (2015a): Obamas Listen. In: *Der Spiegel 1/2015*, S. 80–83.

– (2015b): Spiegel-Umfrage Terrorismus. In: *Der Spiegel 24/2015*, S. 22.

Statistisches Bundesamt (2013): Datenreport 2013. Ein Sozialbericht für die Bundesrepublik Deutschland. URL: https://www.destatis.de/DE/Publikationen/Datenreport/Downloads/Datenreport2013.pdf.

– (2015): Fast jede zweite Person ab 65 Jahre nutzt das Internet. URL: https://www.destatis.de/DE/PresseService/Presse/Pressemitteilungen/2015/12/PD15_466_63931.html.

Taureck, Bernhard H. F. (2014): Überwachungsdemokratie. Die NSA als Religion. Paderborn: Wilhelm Fink.

The Intercept (2015): GCHQ Profiling: An Appendix. URL: https://theintercept.com/gchq-appendix/.

Toh, Amos, Faiza Patel und Elizabeth Goitein (2016): Overseas surveillance in an intercOnnected WOrld. URL: https://www.brennancenter.org/sites/default/files/publications/Overseas_Surveillance_in_an_Interconnected_World.pdf.

Töpfer, Eric (2014): Was die Novellierung des Antiterrordateigesetzes mit den Snowden-Enthüllungen zu tun hat. URL: https://netzpolitik.org/2014/was-die-novellierung-des-antiterrordateigesetzes-mit-den-snowden-enthuellungen-zu-tun-hat/.

Tremmel, Moritz (2010): Die Vorratsdatenspeicherung und der Panoptismus. Anwendbarkeit und Erkenntnisse aus der Analyse der Vorratsdatenspeicherung mit Foucaults Machttheorie. URL: http://nbn-resolving.de/urn:nbn:de:bsz:21-opus-56063.

– (2012a): 377 Schlüsselbegriffe des US Heimatschutzministeriums veröffentlicht. URL: https://netzpolitik.org/2012/377-schlusselbegriffe-des-us-heimatschutzministeriums-veroffentlicht/.

– (2012b): Post or Privacy? Schöne neue Kontrollgesellschaft? Eine Analyse des Post-Privacy Ansatzes mit Foucault & Deleuze. URL: https://moritztremmel.de/files/2012/12/Moritz_Tremmel_-_Post_or_Privacy_-_2012-CC_BY_NC_SA.pdf.

– (2013): Neue Geheimdienstrechenzentren in den USA. In: Überwachtes Netz. Edward Snowden und der größte Überwachungsskandal der Geschichte. Hrsg. von Markus Beckedahl und Andre Meister. Berlin: newthinking communications in Kooperation mit epubli, S. 256–259.

Tremmel, Moritz (2015a): 31c3: Überwachung, NSA, Crypto, Spionage, Todeslisten und Du? URL: https://netzpolitik.org/2015/31c3-ueberwachung-nsa-crypto-spionage-todeslisten-und-du/.

– (2015b): Privacy Tools: Anonym surfen mit Tor. URL: https://netzpolitik.org/2015/privacy-tools-anonym-surfen-mit-tor/.

Trump, Carl Philipp (2012): Überwachung der Bürger aus neogramscianischer Perspektive: Die EU zwischen Hegemonie und Vorherrschaft. URL: https://epub.ub.uni-muenchen.de/14048/1/Trump27.pdf.

Ullrich, Peter (2012): Überwachen und Vorbeugen. Prävention und das Ende der Kritik. In: *Ausgabe 1 - Zeitschrift für Weltverdoppelungsstrategien - zweite und dritte Ausgabe*, S. 211–219.

Unsichtbares Komitee (2015): An unsere Freunde. Hamburg: Verlag Lutz Schulenberg.

Weber, Max (1978): Soziologische Grundbegriffe. 4., durchges. Aufl. Tübingen: Mohr.

Wolf, Burkhardt (2008): Panoptismus. In: Foucault Handbuch. Leben - Werk - Wirkung. Hrsg. von Clemens Kammler, Rolf Parr und Ulrich Johannes Schneider. Stuttgart: J.B. Metzler, S. 279–284.

Wörlein, Jan (2008): Das Trennungsgebot zur Zusammenarbeit. Institutionalisierte Kooperation von Polizei und Diensten. URL: https://www.akweb.de/ak_s/ak532/08.htm.

Zapf, Holger (2013): Methoden der Politischen Theorie. Eine Einführung. Opladen, Berlin Toronto: Verlag Barbara Budrich.

Zurawski, Nils (2007): Einleitung: Surveillance Studies. Perspektiven eines Forschungsfeldes. In: Surveillance Studies. Perspektiven eines Forschungsfeldes. Hrsg. von Nils Zurawski. Opladen & Farmington Hills: Verlag Barbara Budrich, S. 7–24.

– (2015): Technische Innovationen und deren gesellschaftliche Auswirkungen im Kontext von Überwachung. URL: http://www.sicherheit-forschung.de/publikationen/schriftenreihe/sr_v_v/sr_16.pdf.