FIELD OF FOCUS 4
SELF-REGULATION AND REGULATION
INDIVIDUALS AND ORGANISATIONS

UNIVERSITÄT
HEIDELBERG
ZUKUNFT
SEIT 1386

Journal of Self-Regulation and Regulation

Volume 01 (2015)

Das Internet: ein umfassendes Überwachungssystem

William Binney

Abstract

Die Veröffentlichungen des Whistleblowers Edward Snowden enthüllten die systematische Massenüberwachung zahlloser Menschen durch die National Security Agency (NSA), die seit den Anschlägen vom 11. September 2001 quasi unkontrolliert und ohne Beschränkungen handeln konnte. Dieser Beitrag untersucht dabei die Funktions- und Wirkungsweise dieser Überwachungstätigkeit und stellt ihr eine kritische Betrachtung sowie eine funktionale Alternative entgegen.

Die NSA nutzt für die massenhafte Überwachung von US-Bürgern und Nicht-US-Bürgern nicht nur eigene Fähigkeiten, sondern geht in zahlreichen Fällen Kooperationen mit sowohl staatlichen wie auch nicht-staatlichen Akteuren zur Erreichung ihrer Ziele ein. Der Beitrag zeigt auf, dass diese massenhafte Überwachung nicht nur in vielfacher Weise gegen amerikanisches Gesetz und gegen die Verfassung verstößt, sondern darüber hinaus sogar dazu beiträgt, dass die NSA, aufgrund der nicht zu bewältigenden Datenmenge, an Effizienz und Sicherheitskompetenz einbüßt. Es wird dabei argumentiert, dass es zwar funktionale Alternativen zum vorherrschenden System gäbe – eine wird dabei skizziert – jedoch von Seiten der NSA keine Bestrebungen vorhanden sind, die einmal erhaltenen Befugnisse und Kompetenzen wieder einzuschränken. Im Gegenteil, so weckte der Datenbestand bereits Begehrlichkeiten anderer Einrichtungen, die diesen für ihre Zwecke heimlich missbrauchten.

Keywords

NSA; Massenüberwachung; PRISM; Metadaten; Target Development and Discovery

DOI: 10.11588/josar.2015.0.23485

Das Internet: ein umfassendes Überwachungssystem

William Binney[1]

1 Einleitung

Der vorliegende Beitrag beschreibt die (Aus-)Nutzung des Internets durch die National Security Agency (NSA) zum Zweck der Individual- und Massenüberwachung von US-Bürgern und Nicht-US-Bürgern. Auf vier Punkte wird hierbei besonderes Gewicht gelegt. So soll zunächst (Abschnitt 2) auf die besonderen Möglichkeiten und Zugangspunkte der massenhaften Datenüberwachung und das jeweilige Vorgehen der NSA eingegangen werden. Hierbei wird Einblick in die drei am häufigsten angewandten Methoden gegeben und diese werden anhand der Überwachungspraktiken auf der nationalen und internationalen Ebene exemplifiziert. Danach (Abschnitt 3) werden weitere Methoden der Überwachung aufgezeigt und die Ineffizienz des gesamten Überwachungssystems verdeutlicht. In Abschnitt 4 folgt die Kontrastierung einer ursprünglich von uns – einer früheren Riege von Mitarbeitern der NSA, der ich angehörte – mitentwickelten, zielgerichteten und rechtlich unbedenklichen Überwachung sozialer Netzwerke mit jener der NSA. Diese Analyse wird ergänzt durch eine Einschätzung über die Anpassung des Überwachungsprogramms seit den Enthüllungen durch Edward Snowden. Schließlich werden in Abschnitt 5 die weiteren, problematischen Folgen der Massenüberwachung angesprochen. Es wird gezeigt, wie das NSA-Überwachungssystem bereits über die reine geheimdienstliche Arbeit hinausgreift und bestehendes Recht und Gesetz bricht.

Alle verwendeten Materialien und Dokumente, auf die sich dieser Artikel stützt, stammen aus frei zugänglichen Quellen, aus öffentlich zugänglichen und legalen Seiten im Internet. Der überwiegende Anteil – wenngleich nicht ausschließlich – entstand rund um die Enthüllungen des Whistleblowers Edward Snowden. Sie wurden für den vorliegenden Beitrag erklärend aufgearbeitet und mit eigenen Analysen ergänzt. Das Bild, das sich hieraus abzeichnet, macht deutlich, dass die NSA nicht nur erheblichen Einfluss auf das Internet besitzt, sondern das Internet bereits kontrolliert. Dies gilt zumindest, was den Zugang zu den Daten betrifft.

2 Die Massenüberwachung der NSA

Die NSA überwacht nahezu den gesamten Internetverkehr, immer auf der Suche nach relevanten Informationen. Als relevante Informationen oder zumindest potentiell rele-

1 Der Text beruht auf einem Vortrag. Er wurde von Stefan Artmann erstellt.

vante Informationen werden von der NSA dabei inzwischen nahezu alle Daten angesehen: Entweder weil sie aus sich selbst heraus interessant sind oder durch die intelligente oder automatisierte Kombination mit anderen Datenbeständen zu einem lückenlosen Informationsbild beitragen; oder weil sie für die Abwehr bereits bekannter Gefahren oder noch unbekannter Gefahren eingesetzt werden können. Dieses Informationsinteresse beginnt bereits bei den so genannten Metadaten, also Informationen die über die Inhaltsdaten hinausgehen. Bei einer E-Mail beispielsweise ist der Inhalt der geschriebene Text. Die Metadaten hingegen umfassen Informationen über den Absender, das Absendedatum, den Empfänger, die Größe der E-Mail, aber auch die Betreffzeile der Nachricht. Derartige Informationen sind vielfach sogar von größerem Nutzen für die Geheimdienste, da sie einfachere, schnellere und spezifischere Rückschlüsse über eine Person zulassen, als dies die Inhaltsdaten bei gleichem Aufwand erlauben würden. Diese Metadaten sind daher oftmals auch das begehrtere Gut für die NSA.

Das starke Interesse der NSA für Metadaten ist darauf zurückzuführen, dass ein jeder Mensch, der den Cyberspace nutzt, hierin über den Besitz und die Nutzung von elektronischen Geräten Spuren hinterlässt, mit deren Hilfe sich nahezu lückenlose Bewegungsprofile generieren lassen. Hierbei ist die Nutzung des Cyberspace in einem breiten Sinne zu verstehen. Darunter fallen nicht nur die offensichtlichen Praktiken wie die Nutzung von PCs, Smartphones oder ähnlichen Geräten, sondern auch der Umgang mit vielen weiteren, alltäglichen Geräten. So nutzen EC- und Kreditkartensysteme für die Abrechnung den Cyberspace genauso, wie ein Großteil der heutigen Telefonkommunikation digital verläuft. Dies betrifft dabei nicht nur Smartphone-Gespräche, selbst vermeintlich analoge Festnetzanschlüsse werden, dank Voice-over-IP-Technologie, inzwischen ebenfalls vielfach vollautomatisch in digitale Datenpakete umgewandelt und über den Cyberspace abgewickelt.

Geheimdienste, wie die NSA, haben somit ein hohes Interesse diesen Datenverkehr aufzufangen, abzuhören und auszuwerten. Die bisher von Edward Snowden veröffentlichten Dokumente machen dabei bereits jetzt deutlich, dass die NSA in ihrer Informationsbeschaffung einem Stufenmodell folgt. Diese Stufen sollen im Folgenden vorgestellt werden.

2.1 Die drei Stufen der Überwachung

Die Online-Überwachung der NSA folgt einem Drei-Stufenmodell, das abhängig nach Zugangsmöglichkeit des Ziels und der Kooperationsbereitschaft der jeweiligen Betreiber ausgeführt wird. Die drei Stufen schließen sich in ihrer Anwendung dabei nicht gegenseitig aus. Sie können vielmehr auch parallel Anwendung finden, wobei jedoch die Kosten für die NSA mit jeder Stufe ansteigen.

Auf der ersten und untersten Stufe steht die direkte Zusammenarbeit mit einem Unternehmen, etwa einem Internet Service Provider oder Internetdienstanbieter (ISP). Gerade bei US-Unternehmen oder Unternehmen, die auf US-amerikanischem Territo-

rium technische Einrichtungen besitzen, ist dies vielfach der erste und gängigste Weg. Die Unternehmen werden mit finanziellen Anreizen, zum Teil in Verbindung mit rechtlichem, richterlich durchgesetztem Zwang zur Kooperation verpflichtet. In der Abfolge übernehmen sie dann, im direkten Auftrag der NSA, Sammelaufgaben, leiten die Suchergebnisse entsprechend weiter und richten generell Zugangsmöglichkeiten für die NSA ein. Das NSA-Überwachungsprogramm „Prism" ist hierfür wohl das inzwischen bekannteste Beispiel, und doch steht es nur exemplarisch für eine ganze Reihe einer inzwischen nahezu unüberschaubaren Anzahl derartiger Systeme.

Wenn die interessanten Informationseinrichtungen außerhalb des US-amerikanischen Hoheitsgebietes liegen, so wird die zweite Stufe eingeführt. Hierbei baut die NSA auf die Kooperation mit Partnerstaaten bzw. deren Geheimdiensten. Auf dieser Stufe werden die Geheimdienste dieser Partnerstaaten als Intermediäre gebraucht, die, in Abbildfunktion der Methoden der NSA in den USA, die Kooperation mit den Unternehmen in ihren jeweiligen Ländern koordinieren und die Ergebnisse an die NSA weiterreichen. Die NSA besitzt, durch ihre zentrale Stellung als Informationsbeschaffer für Geheimdienste in vielen Drittstaaten, unterschiedliche Anreize und Möglichkeiten der Gegenleistung wie auch der Druckausübung, mit denen sie sich die Gefolgschaft der Partnerländer und deren Geheimdienste sichern kann. Dabei wird nicht jedes Land von der NSA gleich behandelt. So ist den Snowden-Dokumenten zu entnehmen, dass die USA 37 „approved SIGINT [Signals Intelligence; Anm. d. Verf.] partners" besitzen, die sie in unterschiedliche Gruppen (sogenannte parties) einteilen. Die erste Party oder Gruppe bezeichnet dabei die USA selbst. Zur zweiten Gruppe (second party) zählen Australien, Kanada, Neuseeland und das Vereinigte Königreich, also alle primär englischsprachigen Staaten. Die erste und zweite Gruppe bilden zusammen die inzwischen berühmt gewordenen *Five Eyes*, einen Verbund jener fünf Staaten, die seit dem Zweiten Weltkrieg besonders eng geheimdienstlich zusammenarbeiten. Deutschland zählt zusammen mit 33 anderen Staaten – zu denen die meisten europäischen Länder gehören – zur „third party", also einer Staatengruppe, mit der reger Geheimdienstaustausch stattfindet, die aber nicht ohne Vorbehalte betrachtet wird.

Die dritte Stufe ist der unilaterale Weg. Er wird von der NSA verwendet, wenn Unternehmen und/oder die entsprechenden Regierungen der Länder nicht gewillt sind, sich den Wünschen der NSA zu beugen und die entsprechenden Informationen und Zugänge bereitzustellen – oder eine Kooperation sehr unwahrscheinlich ist bzw. sich die Spionage gar gegen die betreffenden Länder selbst richtet. In diesem Fall handelt die NSA im Alleingang und ohne Kenntnis der entsprechenden Unternehmen oder Regierungen und besorgt sich die benötigten Informationen mit anderen geheimdienstlichen Methoden. Diese Informationsbeschaffung kann über verschiedene Wege erfolgen, etwa über das direkte Anzapfen der Glasfaserkabel und das „Abhören" der Kommunikation. Eine andere Möglichkeit ist die gezielte Manipulation der Technik, entweder durch Einspeisung von Schadsoftware zur geheimen Kontrollübernahme jener Techniken oder über die physische Einfügung veränderter oder additiver Hardware in

bestehende Systeme. Der Fall der Cisco-Router ist hierbei aufschlussreich. Diese Router wurden von der NSA im Versand heimlich abgefangen und mit entsprechender Hardware „nachgerüstet", bevor sie an ihre eigentlichen Empfänger zugestellt wurden (Greenwald 2014).

Dass sich die drei Stufen nicht gegenseitig ausschließen, sondern je nach Erkenntnisinteresse auch parallel erfolgen können, macht der Fall Google deutlich. So gewährte das Unternehmen Google im Rahmen des PRISM-Übereinkommens[2] der NSA bereits Einblick in ihre Daten. Dies hinderte die NSA jedoch nicht daran, sich zusätzlich zu dem bereits durch Google bereitgestellten Zugang noch einen weiteren und geheimen Zugang zu verschaffen (Gellman et al. 2013), um noch weitreichendere Informationen als die bereits von Google zur Verfügung gestellten zu gewinnen.

Diese Doppelstrategie der NSA, sich nicht nur auf das eine Programm Prism zu verlassen, sondern darüber hinaus auch andere Methoden anzuwenden, macht wohl am deutlichsten, dass Prism zwar das bekannteste Tool darstellt, letztlich aber weder das einzige, noch das wichtigste ist. Viel entscheidender ist womöglich die sogenannte Upstream Collection. Hierbei werden die Kommunikationsleitungen direkt am Backbone und anderen zentralen Leitungen angezapft und die anfallenden Daten und Metadaten direkt mitgeschnitten. Die rechtliche Grundlage für dieses Verfahren, mit dem auch die meiste Kommunikation innerhalb der USA überwacht wird, bietet bereits die *Executive Order 12333* des damaligen Präsidenten Ronald Reagan aus dem Jahr 1981. Ausgeweitet und auf den Stand der heutigen Massenüberwachung gebracht, wurde diese jedoch erst deutlich später. Dies lässt sich nicht nur mit der verbesserten Computertechnologie und dem Wandel vom Nischenphänomen Internet in eine Massentechnologie begründen. Beide mögen Bedingungen sein, die entscheidende Variable, das formative Ereignis, liegt hingegen bei den Anschlägen vom 11. September 2001. Der Schock, der durch die terroristischen Anschläge ausgelöst wurde, ermöglichte die Einführung umfassender Gesetzgebungen, die den verfassungsrechtlich verbrieften Freiheitsrechten entgegenstehen und die Befugnisse der US-Regierung massiv ausweiteten: USA-Patriot Act, FISA Amendement Act und andere Regelungen sind den meisten interessierten Bürgern zumindest vom Namen her bekannt und seit ihrer Einführung mehrfach verlängert, vereinzelt sogar verschärft worden. Durch diese und andere Regelungen genossen und genießen die US-Geheimdienste seit den Anschlägen vom 11. September 2001 nahezu alle Freiheiten bei der massenhaften Überwachung von Bürgern der USA und anderer Staaten. Ob dies indes mit der US-Verfassung vereinbar ist, daran gibt es nicht nur ernsthafte Zweifel: So hat am 7. Mai 2015 im Fall ACLU v. Clapper das Gericht entschieden, dass zumindest die „bulk collection" (massenhafte Sammlung) der Telefondaten von US-Bürgern illegal ist (Aclu v. Clapper 2015). Diese Praxis musste in seiner bestehenden Form ausgesetzt werden.

2 Zu dieser Gruppe gehörten neben Google noch Microsoft, Yahoo, Facebook, PalTalk, AOL, Skype, Youtube und Apple.

Dennoch: Welche Formen und Auswirkungen die Überwachungen bereits angenommen haben, und dies sowohl auf nationaler als auch auf internationaler Ebene, darüber sollen die beiden folgenden Unterabschnitte einen kurzen Einblick geben.

2.2 Nationale Ebene

Für die „Upstream Collection" also das bereits angesprochene direkte Abhören an großen Datenleitungen auf amerikanischem Boden, ist das sogenannte Fairview-Programm eines der umfangreichsten, auf das im Folgenden eingegangen werden soll.

Tabelle 1: Netzknoten vier großer ISPs in den USA

Major Communications Cables

– Points of Convergence – USA

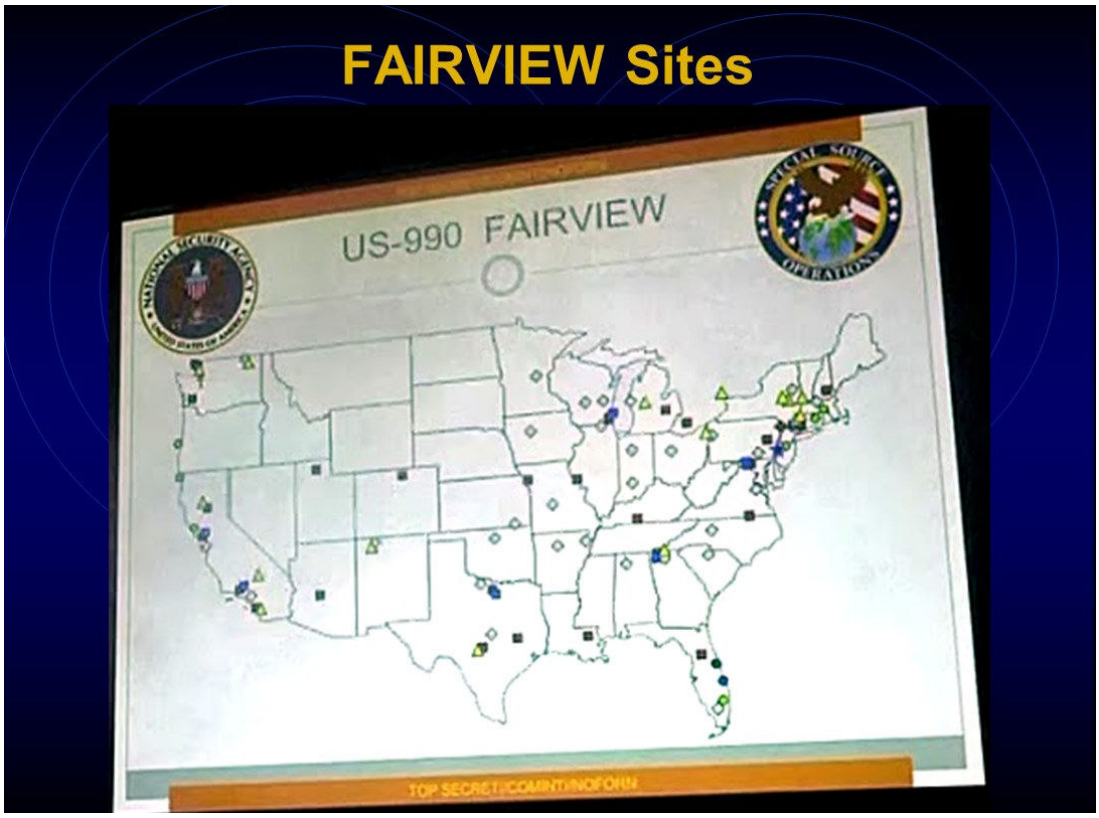
AT&T	**Verizon**	**British Telecom**	**T-Mobile**
New York	New York	New York	New York
Chicago	Chicago	Chicago	Chicago
Los Angeles	Los Angeles	Los Angeles	Los Angeles
Salt Lake City	Salt Lake City	Salt Lake City	
Denver	Denver	Denver	
Phoenix	Phoenix	Phoenix	
Kansas City	Kansas City	Kansas City	
Atlanta	Atlanta	Atlanta	
Miami	Miami	Miami	
Washington DC	Washington DC	Washington DC	
Seattle	Seattle	Seattle	
San Francisco	San Francisco		San Francisco
Dallas	Dallas		Dallas
San Joese	San Joese		
San Diego	San Diego		
St Loius	St Loius		
Orlando	Orlando		
Boston	Boston		
Newark	Newark	Newark	
		Houston	
	Philadelphia		Philadelphia
Nashville	Portland	Sunnyvale	
Cleveland	San Diego	Burbank	
	Las Vegas	Tucson	
	Detroit	Tampa	
	Charlotte NC	Eckington	
	Richmond		

Quelle: eigene Darstellung.

Ideale Standorte für eine effiziente Abhörung des Upstreams sind jene Orte, an denen möglichst viele Datenstränge zahlreicher Internetdienstanbieter sich kreuzen, die sogenannten (Internet-)Knotenpunkte. Die nachfolgende Tabelle 1 führt die Knotenpunk-

te vier großer Internetdienstanbieter (ISP) in den USA auf, jene von AT&T, Verizon, British Telecom und T-Mobile.

Abbildung 1: Map of FAIRVIEW SIGAD



Quelle: NSA 2013a.

Auf einer durch Edward Snowden veröffentlichen Landkarte (Abbildung 1) sind die Vereinigten Staaten übersät mit einer Vielzahl von unterschiedlich gefärbten kleinen Kreisen, Dreiecken und Quadraten, die jeweils verschiedene Aktivitäten sowie Speicher- und Leistungsfähigkeit einzelner Abhöreinrichtungen im Rahmen des Fairview-Programms symbolisieren. Jede dieser Anlagen kostet dabei zwischen 10 und 100 Millionen US-Dollar.[3] Untersucht man die Standorte der schwarzen Quadrate genauer und vergleicht ihre kartographische Verortung mit den Netzknoten von AT&T, so ist auffällig, dass sie nahezu deckungsgleich sind. Dies ist vermutlich kein Zufall, sondern Anzeichen dafür, dass die NSA für jeden der großen AT&T-Netzknoten einen Zugriffspunkt unterhält. Schließt man die übrigen Symbole der Karte noch in ähnliche Überlegungen mit ein, so ergibt sich daraus die begründete Vermutung, dass die NSA die Fähigkeit besitzt, quasi den gesamten relevanten US-Web-Verkehr abzuhören (d.h. Chat, Video, E-Mail etc.). Darüber hinaus kann die NSA – Schätzungen zufolge – auch 80 Prozent

3 Die großen Speicherzentren, wie in Fort Mead oder Utah, die allein im Bau bereits Milliarden US-Dollar kosteten, sind hierbei noch gar nicht mit eingerechnet.

aller Telefongespräche für 20 bis 30 Tage speichern; im Bedarfsfall und für Einzelfälle natürlich noch länger, gar unbegrenzt.

Der Erfassung und Speicherung dieser unfassbar großen Datenmenge stehen dabei nicht nur rechtliche und ethische Bedenken gegenüber, sondern auch ganz pragmatische. So sind 10.000 bis 20.000 Analysten mit der Auswertung der täglichen Massenüberwachung betraut. Diese Zahlen erscheinen zunächst sehr hoch, doch zugleich nehmen sie sich geradezu gering aus, wenn man sie den gut 300 Millionen US-Bürgern entgegenstellt, von denen sie Daten erhalten. Selbst mit den besten Analysetools fällt hierbei noch immer eine nicht zu bewältigende Datenmenge an. Es ist zu vergleichen mit einer beliebigen Google-Anfrage, die man bis zur letzten Seite überprüfen und durcharbeiten müsste. Die Folge dieser Massenanhäufung ist ein „Datenmasseversagen“ (bulk data failure). Die Geheimdienste versagen, nicht weil sie zu wenig Daten haben, sondern weil sie in den Datenmassen versinken.

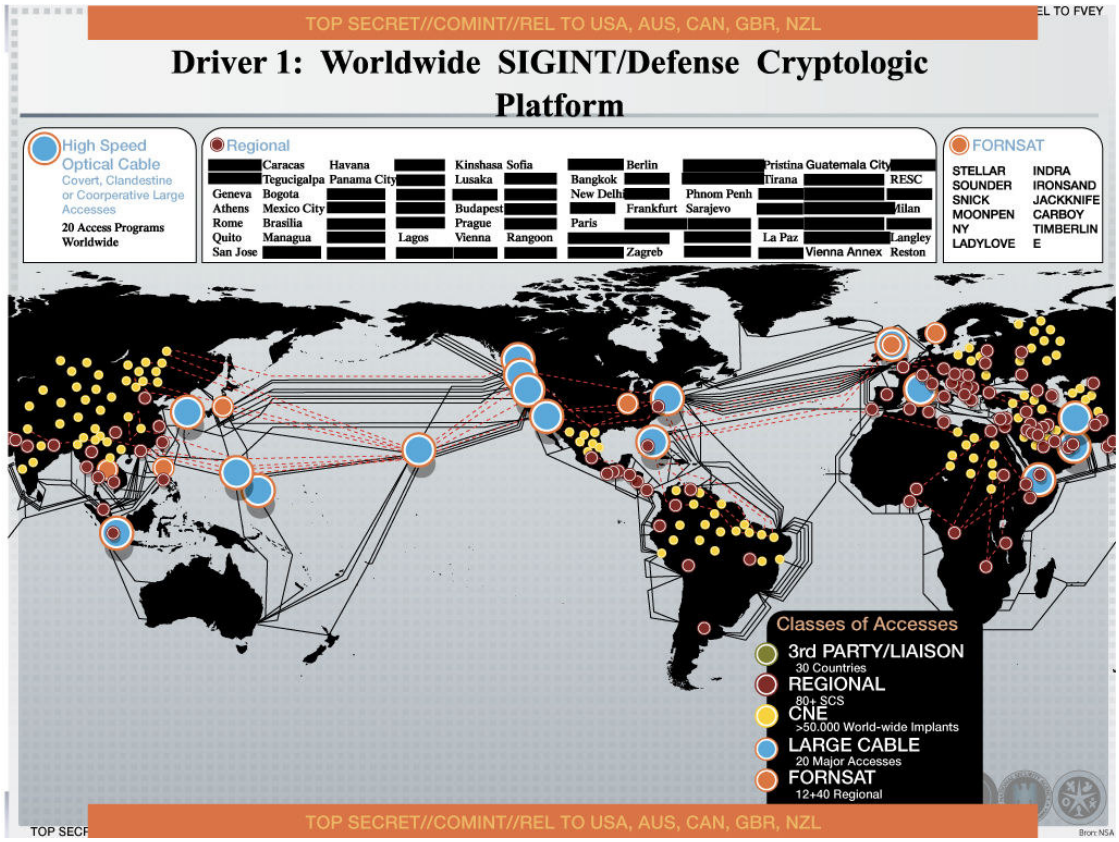
2.3 Internationale Ebene

Betrachten wir nun die Überwachung der internationalen Datenströme, also das Anzapfen an Orten außerhalb der USA, so zeigt sich ein kaum besseres Bild. Zwar wurden die Unterlagen Snowdens in der Worldwide SIGINT/Defense Cryptologic Platform (vgl. Abbildung 2) nur stark zensiert veröffentlicht und enthalten deshalb keine Informationen über die First Party (USA), noch zeigen sie die Zusammenarbeit mit Second (UK, Kanada, Australien, Neuseeland) oder Third Party Mitgliedern (Deutschland etc.); obgleich dies in der Vorschaugrafik angekündigt wird. Dennoch lässt sich Vieles über die internationale Zusammenarbeit der NSA aus der Grafik und den im Kontext veröffentlichten Informationen herauslesen. Von besonderem Interesse sind dabei die Computer Network Exploitations (CNE), d.h. Maßnahmen zur Ausnutzung von Computernetzwerken. Dabei gelingt der NSA das Abfangen und Abgreifen von Informationen am einfachsten über die Implementierung von zusätzlicher Soft- und/oder Hardware von Geräten und Anlagen in Schlüsselpositionen, wie es etwa in dem bereits erwähnten Fall der Cisco-Router erfolgte. Durch die Einbringung derartiger Soft/Hardware (so genannte Implants), schafft sich die NSA Hintertüren (Backdoors), die es ihr ermöglichen direkten Zugang zu den entsprechenden Computernetzwerken zu erhalten und sie zu deren eigentlichen Herren zu erheben. Die Hintertür befähigt die Agency alle für sie interessanten Informationen live einzusehen, mitzuschneiden und eine Kopie für spätere Untersuchungen abzuspeichern.

Wie viele derartige Implants die NSA tatsächlich installiert hat und wie viele der Geräte auch tatsächlich noch im Betrieb sind, ist weiterhin Teil wilder Spekulationen in der Netzgemeinde und der weiteren Öffentlichkeit. Erste Schätzungen und Berichte gingen von 50.000 derartigen Implants aus. Andere reichen aber bis zu einer Million und mehr. Am wahrscheinlichsten ist meiner Ansicht nach eher der niedrigere Wert, so dass es vermutlich „nur“ zwischen 50.000 und 100.000 Implants sind, die auch tatsäch-

lich zur Anwendung kommen. Dies ist jedoch kein Grund zur Erleichterung. Diese Anzahl – an den richtigen Schlüsselpositionen platziert – ist mehr als ausreichend, um eine nahezu lückenlose Überwachung zu gewährleisten und die elektronische Kommunikation jeder beliebigen Zielperson, gleich wo sie sich auf der Erde befindet, egal zu welcher Zeit und an welchem Ort, verfolgen zu können.

Abbildung 2: Worldwide SIGINT



Quelle: NSA 2013b.

Ein anderes NSA-Programm, das diese Massenüberwachung nutzbar machen soll, nennt sich Treasuremap. Es verspricht eine Kartierung des gesamten Internets, zumindest nach den veröffentlichten NSA-Dokumenten von Snowden: „Map the entire Internet – Any device, anywhere, all the time“ (Horchert 2014).

Den ungefähren Standort eines Gerätes zu bestimmen, ist dabei nicht sonderlich schwierig. Für das herkömmliche Telefonnetz lässt sich zumindest die Landesherkunft leicht erkennen, da das gesamte System durch das Global Public Service Telephone Network Switching System (PSTN) unterteilt ist. Nordamerika hat etwa die Eins, Westeuropa die Drei und Osteuropa die Vier.[4] Das System gliedert sich dann auf und lässt einige Rückschlüsse über die Herkunft des Anrufers zu. Ähnlich in der Art, aber in technischer Hinsicht deutlich zu unterscheiden, ist die Strukturierung des World Wide Web.

4 Den meisten Telefonnutzern dürfte diese Einteilung durch die gleichlautende Vorwahl für internationale Gespräche vertraut sein.

Im WWW besitzt jedes Gerät einen Machine Access Code (MAC) und eine Internetprotokoll-Adresse (IP). Jedes Gerät muss eine eigene, einzigartige Nummer besitzen, wenn es sich mit dem Internet verbinden möchte. Dies erfolgt über IPv4- oder IPv6-Nummern. Diese Nummern werden den Endgeräten von den ISPs zugeteilt, sind also nicht frei wählbar. Und auch den ISPs werden die IP-Adressen nur zugewiesen. Oberste Vergabestelle der IP-Adressen ist die Internet Corporation for Assigned Names and Numbers (ICANN) mit ihrer Internet Assigned Numbers Authority (IANA), die die IP-Adressen in Paketen an verschiedene Anbieter herausgibt.[5] Allein an der IP-Adresse und ihrer Zugehörigkeit zu einem bestimmten Paket lässt sich somit viel über den Aufenthalt einer Person oder zumindest ihres elektronischen Gerätes aufzeigen. Über die IP-Adresse und die Vergabe der Provider lässt sich somit der ungefähre geografische Standort des Benutzers verorten.[6] Für alles Weitere können dann die MAC-Adresse, GPS-Daten oder sonstige relevante Infos aus den Inhaltsdaten und Metadaten der Kommunikation herangezogen werden, um den exakten Standort der Person ausfindig zu machen.

Hierdurch ist aber nur angedeutet, was machbar ist. Welche Probleme sowohl in rechtlicher Hinsicht als auch in ganz pragmatischer Hinsicht mit dem Umgang dieser Datenmengen entstehen, davon handelt das nächste Kapitel.

3 Ineffizienz und rechtliche Bedenken

Prism, Treasuremap oder Fairview sind nur einige der führenden Programme, mit denen die NSA US-Bürger und Bürger anderer Nationen abhört und überwacht. Und der Wunsch der Agency nach noch mehr Zugriff, noch mehr Einblick und nach noch mehr Kompetenzen ist ungestillt. In den Folgen der Anschläge vom 11. September 2001 erhielten die Geheimdienste nahezu freie Hand und wurden in einer geradezu panischen Reaktion mit hohen Geldsummen und weitreichenden Befugnissen ausgestattet, ohne sich mit tiefergehenden Fragen nach Sinn oder Unsinn der Entwicklung aufzuhalten. Was folgte, war ein aufgeblähter, aus meiner Sicht völlig ineffizienter Geheimdienstapparat, der seine neue Macht nutzen und Kompetenzen rechtfertigen musste, ohne dabei aus den Fehlern zu lernen, die man nach den Anschlägen des 11. September eigentlich hätte ziehen müssen.

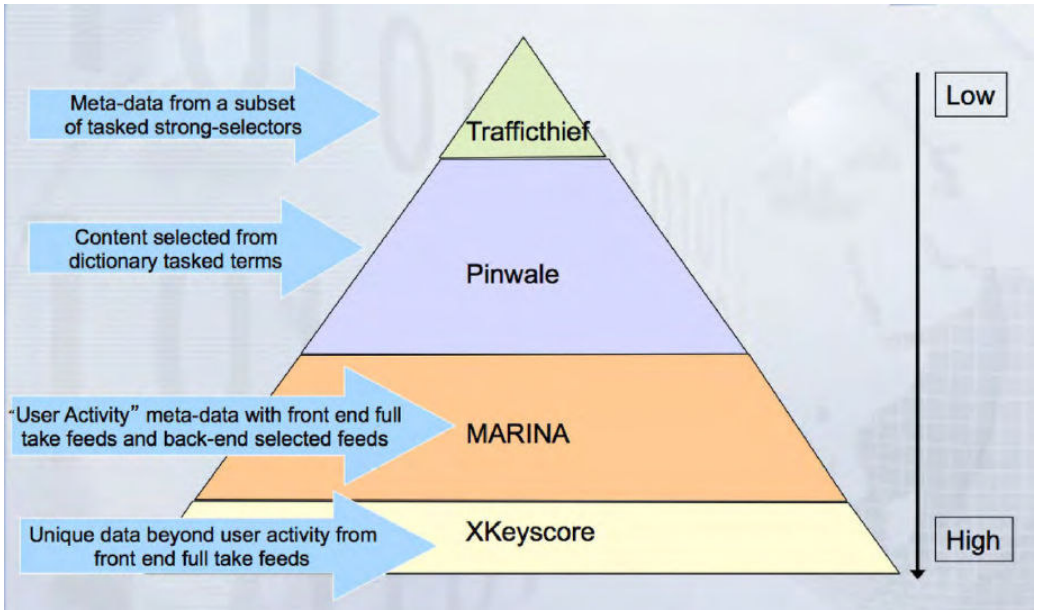
5 ICANN vergibt IP-Adressen an fünf internationale Registraturen (Regional Internet Registries, RIR), die zuständig sind für Afrika (AfriNIC), Nordamerika (ARIN), Lateinamerika und den Karibikraum (LACNIC), Europa, den Nahen Osten und Zentralasien (RIPE NCC) und den asiatisch-pazifischen Raum (APNIC). Diese RIR verteilen dann ihrerseits wieder IP-Adressen an Local Internet Registries (LIR) oder National Internet Registries (NIR), die sie an die Internet Service Provider (ISP) weiterreichen. Diese geben die Adressen schließlich an die Endnutzer aus. Jeder Zwischenhändler erhält die durch ihn zu vergebenden IP-Adressen natürlich nicht einzeln, sondern in größeren Paketen, je nach Ebene von einigen zehntausend für die ISPs bis zu Paketen von mehreren Millionen für die RIRs.

6 Natürlich gibt es auch hier technische Möglichkeiten, eine andere IP vorzutäuschen. Das resultierende technische Katz-und-Maus-Spiel soll hier aber nicht weiter diskutiert werden (vgl. etwa Stein 2010).

Die Anschläge von 9/11 konnten nicht deswegen nicht verhindert werden, weil nicht genügend Geheimdienstinformationen vorlagen. Im Gegenteil: Es lagen nahezu alle Informationen vor, die es ermöglicht hätten, die Terroristen rechtzeitig zu stoppen. Und noch weit mehr. Und genau hierin liegt das Problem: Die Anschläge konnten nicht verhindert werden, weil die Menge an Informationen so groß war und die Kommunikation unter den Diensten so gering, dass die Zusammenhänge nicht rechtzeitig erkannt wurden. Allein der 9/11 Commission Report von 2004 widmet diesem Versagen ein ganzes Kapitel, das unter der Überschrift „the system was blinking red" (Kean et al. 2004: Kapitel 8) steht. Die Anstrengungen sind zu vergleichen mit der Suche nach der Nadel im Heuhaufen.

Nach dem 11. September, nachdem man die Nadel übersehen hatte, wurden die Suchmannschaften verstärkt. Doch statt effizienter das Heu zu durchsuchen, wurde die Arbeitskraft nun darauf abgestellt, noch mehr Heu herbeizuschaffen. Die NSA-Überwachungen sind somit nicht nur ungesetzlich und verstoßen – meiner Ansicht nach – gegen die US-Verfassung, sondern sie erfüllen noch nicht einmal ihren angestrebten Zweck eines erkennbaren Sicherheitszuwachses. Die NSA erstickt förmlich in all den für sie nutzlosen Daten und ist derart angewachsen, dass sie ihre Arme überall hinaus ausstreckt, jedoch an zielgerichteter und gebündelter Schlagkraft für die Gefahrenabwehr eingebüßt hat.

Abbildung 3: DNI Discovery Options



Quelle: Bildausschnitt nach NSA 2014.

Wie fehlgeleitet die Perspektivität ist, entlarvt auch eine Dreiecksgrafik der NSA, bei der verschiedene Programme aufgeführt werden und deren „Erkenntnisgewinn" von Low (die Spitze des Dreiecks) zu High (seine Hypotenuse) bewertet wird (vgl. Abbildung 3). Die beiden obersten Stufen des Dreiecks, also der Bereich mit dem vermeintlich

geringsten Erkenntnisgewinn, genügen im Folgenden bereits, um die Verirrungen der NSA deutlich zu machen und ihre fehlgeleitete Gleichsetzung von Datenmenge mit Informationsgewinn zu verdeutlichen.

3.1 Bulk Data Failure: Weniger ist mehr

Auf einer Grafik der NSA wurden verschiedene Programme zusammengefasst und in Form eines Dreicks hinsichtlich ihres Nutzens gruppiert (vgl. Abbildung 3). An der Spitze und damit an der Stelle des geringsten Erkenntnisgewinns, steht „Trafficthief“, ein Programm das Metadaten nach einer Auswahl spezifischer Selektoren sammelt. Die NSA erwartet hierbei wenig Gewinn, es handelt sich um Daten von einem sehr engen Personenkreis. Sie verkennt, dass es genau dieser enge Personenkreis ist – ein Personenkreis von bereits Verdächtigen und mit tatsächlich bereits gesuchten Personen –, bei dem die Chance ausgesprochen hoch ist, weitere gefährliche Personen aufzufinden. In der bereits verwendeten Analogie gesprochen: Dieser Heuhaufen ist klein, und es wurde darin bereits eine oder mehre Nadeln gefunden.

Wird nun der direkte Vergleich mit der zweiten Stufe, mit „Pinwale“, gezogen, wird das Missverhältnis noch deutlicher. Pinwale operiert mit Inhalten die mit Hilfe von Schlagwörtern, d.h. Wörterbucheinträgen, operiert. Hierbei werden also Suchwörter ausgewählt und wann immer diese Suchwörter irgendwo bei Personen auftauchen, schlägt das Programm Alarm. Es ist im Grunde nichts anderes als eine Google-Suche, die eine scheinbar endlose Zahl an Treffern generiert, die aber dennoch überprüft werden muss, wenn man damit womöglich eine neue, unter Umständen tatsächlich gefährliche Person ausfindig machen möchte.

Wie häufig hierbei ein Fehlalarm ausbrechen muss, wie absurd das Vorgehen der NSA geworden ist, wird allein schon dadurch deutlich, wenn man sich die Suchbegriffe genauer anschaut. Eine solche mehrere hundert Wörter umfassende Selektorenliste musste das DHS bereits 2012 veröffentlichen (US Department of Homeland Security 2011: 20ff.). Zwar galt die damalige Liste nur der Überprüfung sozialer Medienseiten, für das Projekt Pinwale dürfte die Liste aber ähnlich, wenn nicht gar noch umfassender ausgesehen haben. Auf dieser Liste findet sich dabei eine ganze Reihe von Suchwörtern, die die Anzahl von zu überprüfenden Personen in astronomische Höhen treiben dürften, ohne tatsächlich signifikanten Mehrwert zu produzieren. So steht auf dieser Liste unter anderem das Wort „pork“ (Schweinefleisch). Dies heißt, wann immer – zumindest in diesem Fall innerhalb sozialer Medien – jemand das Wort „pork“ verwendet, verzeichnet die Suchmaske einen Treffer, und es muss untersucht werden, ob der Produzent der Äußerung sich im Kontext terroristischer Kreise bewegt.

Wenn wir beim Heuvergleich bleiben, so wird die Nadel nicht länger in einem Heuhaufen gesucht, sondern während der Heuernte, und es besteht keine Möglichkeit auch nur ansatzweise die täglich auflaufenden Mengen an neuem Heu zu überprüfen und abzuarbeiten. Doch auch bei einer spezifischeren Untersuchung, der Überwachung

von sozialen Netzwerken, zeigen sich das überaus bedenkliche Vorgehen der NSA und ihre gleichzeitige Verblendung.

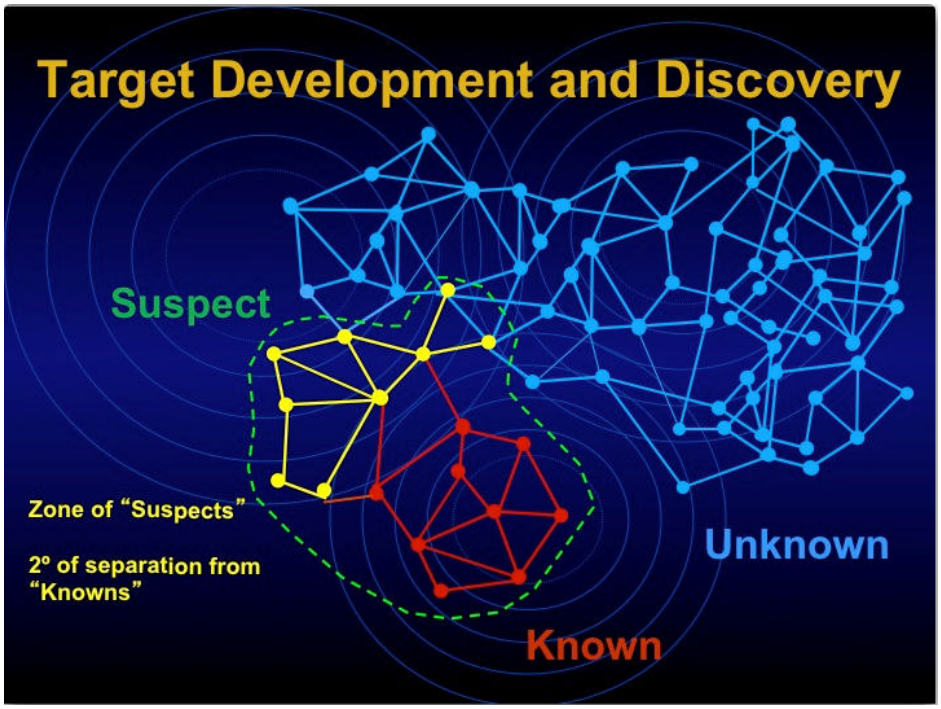
4 Überwachung sozialer Netzwerke

Programme wie jene im vorangegangenen Abschnitt beschriebenen sind ausgerichtet auf die anlasslose Überwachung vieler Menschen sowohl von US-Bürgern als auch Nicht-US-Bürgern. Das Ziel dahinter ist, die Möglichkeit zu besitzen, möglichst viele Menschen gleichzeitig und live zu überwachen. Die derzeitigen Fähigkeiten der NSA, dies effektiv zu tun, dürften sich indes auf einige wenige Millionen Nutzer belaufen. Das gesamte Überwachungssystem ist somit aufgrund der schieren Datenmasse bereits im Vorfeld zum Scheitern verurteilt. Viel nutzbringender wäre es natürlich nur diejenigen zu überwachen, die tatsächlich eine potentielle Gefahr darstellen, bzw. Personen zu identifizieren, bei denen dieses Potential signifikant ist. Die Frage ist klar: Wie kann man herausfinden, ohne alle Nutzer permanent zu überwachen, wer eine Gefahr für die Sicherheit darstellt? Eine Antwort darauf ist die „target development and discovery"-Methode, die in einer eingeschränkten und funktionalen Form von uns bereits in den 1990er Jahren vorgeschlagen wurde und die bei der NSA in einer anderen, einer pervertierten und dysfunktionalen Form Anwendung findet.

4.1 Eine theoretische Alternative

Die Idee hinter der „target development and discovery"-Methode ist es nicht, alle Menschen zu überwachen. Vielmehr geht es darum, ausgehend von bekannten Personen, die eine Gefahr für die Sicherheit darstellen, deren soziale Netzwerke zu überprüfen und dort nach weiteren verdächtigen Personen zu suchen. Dies erfolgt rein über die Metadaten und vollautomatisch, ohne dass ein Beamter Einblick in die Daten erhält. Auch die Inhaltsdaten der Personen werden nicht berührt oder gesammelt, und nur bei einem vermeintlichen Treffer wird diese Person genauer untersucht. In diesem Fall und nur in diesem Fall werden Inhaltsdaten erhoben, ausgewertet und die Person entweder als Bedrohung eingestuft und somit genauer observiert, einschließlich ihrer Kontakte, oder sie wird als falsch-positiver Befund auf eine Sperrliste gesetzt, so dass sie vom System unter den gleichen Verhaltensweisen und Parametern nicht mehr aufgefunden wird. Die gesamte Überprüfung des sozialen Netzwerks sollte dabei einer sog. Zwei-Sprung-Regelung folgen, das heißt, dass nicht nur Personen überprüft werden, die direkten Kontakt mit der bekannten Gefahr haben, sondern auch all jene Personen, die im sozialen Umfeld mit dem sozialen Umfeld der bekannten Gefahr stehen. Hierdurch kann das Problem von Mittelsmännern und indirekten Kontakten umgangen werden und eine größere Aufklärung erreicht werden (vgl. Abbildung 4).

Abbildung 4: Target Development and Discovery



Quelle: eigene Darstellung.

4.2 Die praktische Anwendung

Der NSA ging dieser Vorschlag aber damals nicht weit genug. Sie wählte eine Form, die den klaren Zuschnitt des vorgeschlagenen Programms pervertierte und schließlich auch nutzlos werden ließ. Dies liegt hauptsächlich an zwei Gründen: Zunächst einmal verwendeten die Analysten der Behörde für die Überprüfung des sozialen Umfelds keine Zwei-Sprung-Regelung, sondern eine Drei-Sprung-Regelung. Dies klingt zunächst wie ein geringfügiger Unterschied, der Zuwachs ist jedoch exponentiell. Gehen wir der Einfachheit halber davon aus, dass eine Person im weitesten Sinne 100 Menschen kennt – ein geringer Wert, doch soll er für das Beispiel genügen – so müssen bei einer Zwei-Sprung-Regelung 100^2 Menschen oder 10.000 Personen überprüft werden. Bei einer Drei-Sprung-Regelung sind es 100^3 oder 1.000.000 Menschen. Die Idee einer schlanken, zielgerichteten Methode wird somit zerstört.

Nach Bekanntwerden der Praktiken der NSA durch Edward Snowden kam auch gegen dieses Vorgehen der Überwachung vereinzelt Kritik auf und nach einiger Diskussion und Verhandlungen einigte sich die US-Regierung mit den Behörden Anfang 2014 auf eine Reduzierung der Regelung auf die Zwei-Sprung-Marke. Dies wurde als großer Erfolg gefeiert und als Zugeständnis an die Freiheitsrechte. Der Prozess dorthin erfolgte dabei erstaunlich widerstandsarm. Weder die NSA noch das FBI, CIA, DHS, DOD oder irgendeine andere Einrichtung bezog vehement gegen diese Einschränkung Position. Dieses Eingeständnis der benannten Institutionen sagt jedoch nichts über ihre jeweili-

ge Positionierung zugunsten der Freiheitsrechte aus. Es hat mit einem zweiten Grund zu tun, der die Einschränkung von Drei- zu Zwei-Sprüngen bedeutungslos werden lässt.

Anders als im propagierten Verfahren sind im NSA-Verfahren Personen innerhalb des sozialen Netzwerks nicht nur als Menschen gemeint, sondern auch juristische Personen, also Einrichtungen, Firmen, Unternehmen und dergleichen mehr. Dies hat zur Folge, dass jeder Kontakt eines Pizzalieferanten Teil der Sprungkette ist, genauso wie die eigene Regierung und auch Internetunternehmen. Allein durch Google, mit seinem Kundenkreis von monatlich deutlich über einer Milliarde Nutzern, wird so faktisch im Alleingang die Vollüberwachung nahezu aller Menschen legitimiert.

Vollüberwachung heißt in diesem Fall die Erfassung aller Metadaten und – ohne signifikante Hürden zumindest für nicht US-Bürger – auch aller Inhaltsdaten. Dies ist ein weiterer Unterschied zwischen dem vorgeschlagenen Entwurf und dem in Kraft getretenen Verfahren. Im vorgeschlagenen Verfahren wäre die Erstellung der Analyse der sozialen Netzwerke vollauf automatisiert erfolgt. Die Verbindungen wären maschinenbasiert erfolgt und die Daten und Metadaten verschlüsselt gewesen. Die NSA und ihre Mitarbeiter hätten keine direkte Einsicht in die Informationen, sondern nur dann, wenn das System auf Grundlage des Algorithmus eine möglicherweise verdächtige Person ausmacht.[7] Die NSA hätte dann mittels eines Antrags bei Gericht und Kongress die Entschlüsselungsrechte und somit Einblick in die Metadaten erhalten und bei einem dadurch erhärteten Verdacht auch Einsicht in die Inhaltsdaten bekommen. Dieses Vorgehen hätte sich prinzipiell für alle erfassten Nutzer anwenden lassen, zumindest aber für US-Bürger, deren Privatrechte im amerikanischen Recht deutlich besser geschützt sind als jene von Nicht-US-Bürgern.

Bedauerlicherweise kam dieses Verfahren nie zur Anwendung. Die Versuchung an derart viele Daten und somit vermeintlich auch an alle Informationen zu kommen, war einfach zu groß. Viel zu viel lässt sich damit bewerkstelligen. Die NSA ist dabei nicht die einzige Einrichtung, die Gefallen an einer derartigen Datenfülle gefunden hat. Auch bei anderen Einrichtungen wurden diesbezüglich Interessen geweckt.

5 Die weiteren Folgen der Massenüberwachung

Für das Auffinden neuer potentieller Straftäter sind Treasuremaps, Prism etc. wie auch die meisten anderen Verfahren denkbar ungeeignet, wie in den vorangegangenen Abschnitten gezeigt wurde. Für das Ausspähen bereits identifizierter Ziele sowohl rückwirkend, dank der umfassenden Speicherung, als auch im Rahmen einer Live-Verfolgung ist die Datenfülle und die Dichte des Abhörnetzes umso geeigneter. Die NSA arbeitet daher mit Nachdruck an Verfahren, alle abgefangenen Informationen zusammenzuführen, zu systematisieren und die Daten in eine personalisierte Timeline

7 Als verdächtig hätte noch nicht die Verbindung mit einer bereits identifizierten und als gefährlich eingestuften Person gezählt. Erst wenn ein doppelter Treffer, das heißt der Kontakt zu zwei bereits Bekannten und als Bedrohung registrierten Personen vorgelegen hätte, hätte das System eine Überprüfung veranlasst.

zu überführen. Dies gelingt bereits in vielfacher Form, so dass die NSA Programme nutzt, die Listen generiert, mit denen nicht nur alle Informationen, sowohl Metadaten und – wo vorhanden – auch Inhaltsdaten aus den verschiedenen Quellen, einzelnen Personen zugeordnet werden, sondern darüber hinaus auch die Kontakte zwischen den einzelnen Einträgen aufgezeigt werden können. Es lässt sich also mittlerweile minutiös nachzeichnen, wann eine Person im – elektronischen – Kontakt mit einer anderen stand und für wie lange. Und dies gilt für nahezu alle Menschen, also auch für jeden Kongressabgeordneten, jedes Mitglied eines Parlaments und jeden Regierungschef und jede Regierungschefin der Erde.

Eine derartige Masse an Daten über jeden Menschen, seien es auch „nur" Metadaten von US-Bürgern oder Meta- und Inhaltsdaten von Nicht-US-Bürgern, gebündelt in den Händen einer einzelnen Organisation, der NSA, ist bereits für sich selbst genommen mehr als besorgniserregend. Sie lässt sich aus meiner Sicht durch keine Antiterrorstrategie oder geheimdienstliche Aufklärung rechtfertigen. Doch wird es noch schlimmer: Die Erhebung der Daten durch die NSA soll dem Schutz des Landes vor terroristischen Bedrohungen dienen, doch eine derartige Datenfülle schafft auch Begehrlichkeiten bei weiteren Einrichtungen. So sind die Geheimdienste allein schon durch die reine Datenmenge nicht in der Lage, tatsächliche Vorhersagen zu treffen. Für den Bereich der strafrechtlichen Forensik, also das Auffinden von Straftätern nach begangener Tat, sind sie aber umso interessanter! Und die NSA scheint Anfragen von Ermittlungsbehörden nach Einsicht nur allzu gern nachzukommen. So können Polizei und Ermittlungsbehörden nach einem erfolgten Anschlag die Daten verwenden, um den oder die Täter zu finden. Doch war diese Nutzungsart nie Rechtfertigung noch Aufgabe der geheimdienstlichen Massenüberwachung. Sie wurden gegründet um terroristische Anschläge zu verhindern, nicht um nachträglich bei ihrer Aufklärung zu helfen.

Doch damit nicht genug. Auch hier hat die Begehrlichkeit nach den Datensätzen das Ermittlungsziel zur Aufklärung von Terroranschlägen und vergleichbaren Angriffen auf die nationale Sicherheit überholt und längst weitere Bereiche ergriffen, die nie Teil der Überwachungsaufgaben hätten sein sollen. So berichtete die Nachrichtenagentur Reuters bereits im August 2013 von einem Sondereinsatzkommando (SOD), das privilegierten Zugang zu den Daten der NSA hat und diese zur Aufspürung krimineller Aktivitäten nutzt (Shiffman et al. 2013). Innerhalb dieses Sondereinsatzkommandos finden sich Beamte sowohl der NSA, des FBI (Federal Bureau of Investigation; Bundespolizei/Inlandsgeheimdienst), der CIA (Central Intelligence Agency; der Auslandsgeheimdienst) wie auch des DHS (Department of Homeland Security; Heimatschutzministerium), aber auch der IRS (Internal Revenue Service; Bundessteuerbehörde) und des DEA (Drug Enforcement Agency; Drogenvollzugsbehörde), die alle nach verdächtigen Personen oder auffälligen Mustern suchen. Und dies in allen von ihnen angestrebten Bereichen, also auch im Drogenkampf oder bei der Suche nach Steuersündern. Die Daten sind vorhanden, also will man möglichst viel Nutzen daraus ziehen. Dabei kann eine Person bereits als verdächtig angesehen werden, wenn sie zu einer bestimmten religi-

ösen Gruppe zählt oder es sich etwa um einen Sympathisanten der Occupy-Bewegung oder ein Mitglied einer bestimmten politischen Partei handelt. All dies erfolgt ohne einen zuvor erstellten Haft- oder Untersuchungsbefehl und ohne Kontrolle durch den US-Kongress oder eine richterliche Anordnung. So stehen nach SOD alle Menschen unter Schuldverdacht, bis ihre Unschuld zweifelsfrei bewiesen ist. Und nicht umgekehrt, wie es nach geltendem Recht in den Vereinigten Staaten der Fall sein müsste.

Dies verstößt nicht nur gegen die amerikanische Verfassung. Es ist auch hinsichtlich der Ermittlungstechnik höchstproblematisch, was sowohl die NSA als auch das Sondereinsatzkommando zumindest geahnt zu haben scheinen. So zeigen die Snowden-Dokumente (RT 2013), dass die Ermittlungsbehörden für die Verfolgung von Verdächtigten und eine daran angeschlossene Anklage strengen Regeln unterlagen, die jedoch nicht dem Schutz der angeklagten Personen galten, sondern der Wahrung der Geheimhaltung der Massenüberwachung. Wie durch die Dokumente klar wurde, durften Informationen, die durch den Einsatz des Sondereinsatzkommandos gewonnen wurden, nicht mit anderen geteilt werden, nicht an die Öffentlichkeit gelangen und selbst bei einem angeschlossenen Prozess nicht den zuständigen Richtern, Verteidigern oder Staatsanwälten zugänglich gemacht werden, noch durften diese über die Daten in Kenntnis gesetzt werden; vom Informationsaustausch im Rahmen internationaler Rechtshilfe ganz zu schweigen. Die beteiligten Institutionen wurden vielmehr dazu aufgerufen, Parallelkonstruktionen zu schaffen. So sollten sie, auf Grundlage der bereits erfolgten Vor-Verurteilung durch die Daten der Massenüberwachung, mit konventioneller Ermittlungsarbeit neue und andere Beweise zusammentragen, die dann vor einem Gericht und der Öffentlichkeit Verwendung finden durften. Hierdurch ist weder ein ausgewogenes Sammeln von Beweisen, noch eine vorurteilsfreie Beurteilung dieser möglich, da die Schuld scheinbar bereits bewiesen wurde und nur noch auf anderem Wege vorgetragen werden muss.

Dieses Vorgehen, das laut Aussage des damaligen Direktors des FBI, Robert Mueller, bereits seit 2001 Verwendung fand, soll nun immerhin eingeschränkt werden. Präsident Obama hat diesbezüglich versprochen, dass fortan alle Angeklagten über die Quellen der Anklage informiert werden, so dass sie sich im Rahmen eines ordentlichen Verfahrens gegen die Anschuldigungen wehren können. Wie es eigentlich auch Rechtsvorschrift ist. Allein, es wurde weiterhin keine Aussage über all diejenigen getroffen, die im Rahmen dieses Überwachungssystems, ohne Kenntnis der Praxis und somit ohne Möglichkeit einer fairen Verteidigung, in den Jahren seit 2001 verurteilt wurden. Noch besteht irgendein Ansatz zur Änderung der weltweiten Überwachung. Das Überwachungssystem der NSA besteht also fort.

6 Konklusion

Der vorliegende Beitrag stellte die Überwachungstechniken der NSA im Cyberspace vor, wie sie durch den Whistleblower Edward Snowden bekannt geworden sind und

lieferte eine anschließende Untersuchung und kritische Bewertung der verwendeten Praktiken. Im Fokus der Kritik stand hierbei die rechtlich problematische Überwachung bei gleichzeitigem Vorwurf der Ineffizienz des Programms. Komplementiert wurde die Kritik durch die Skizzierung eines funktionalen Gegenentwurfs, der eine effizientere Geheimdiensttätigkeit unter höchstmöglicher Wahrung individueller Freiheitsrechte ermöglichte.

Innerhalb des Beitrags wurden eine Reihe von Überwachungsmethoden der NSA vorgestellt und ihre Umsetzung wie auch Auswirkung genauer untersucht. Dabei wurden die Praktiken der Überwachung dem Drei-Stufenmodell der NSA zugeordnet, bei dem sich die Überwachungs- und Informationsbeschaffungsmaßnahmen anhand der Einbindung Dritter orientieren. Sie reichen von der Zusammenarbeit mit (US-) Unternehmen (1), über die Kooperation mit befreundeten Regierungen oder deren Geheimdiensten (2) bis hin zum eigenmächtigen Vorgehen der NSA (3). Hierbei wurde sowohl auf die unterschiedlichen rechtlichen Positionen von US-Bürgern gegenüber Nicht-US-Bürgern in der Überwachung eingegangen als auch auf den verschiedenartigen Gehalt von Inhaltsdaten und Metadaten hinwiesen.

In der Bewertung der Überwachungspraktiken zeigte der Beitrag, dass die angewandten Methoden aus vielfacher Hinsicht höchst problematisch sind. So wurde auf die eklatante Schieflage von Sicherheitsrechten zu Ungunsten von Freiheitsrechten eingegangen sowie eine Anzahl (verfassungs-)rechtlicher Bedenken als auch bereits gerichtlich bestätigter Übertretungen angeführt. Diese Vorwürfe wiegen umso schwerer, als sie sich nicht einmal über den scheinbaren Mehrwert an Sicherheitszuwachs rechtfertigen lassen. Es wurde gezeigt, dass die Überwachungsprogramme in höchstem Maße ineffizient arbeiten, da sie sich mit einem Übermaß an unwichtigen Informationen konfrontiert sehen, die den Blick auf die wirklich wichtigen Daten verstellen.

Letztlich verdeutlichte der Beitrag, dass, obgleich die Enthüllungen Edward Snowdens eine Welle der Empörung bezüglich der Praktiken der NSA auslöste, sich in der Tätigkeit der Überwachung durch die NSA kein fundamentaler Wandel abzeichnet. Die Reaktionen sind minimal und vielfach kaum mehr als kosmetischer Natur. Für einen echten Wandel bedarf es vielmehr der stärkeren Kontrolle durch Gerichte und Parlamente sowie einer informierten und kritischen Öffentlichkeit, die sich der Freiheit des Einzelnen verpflichtet fühlt.

Literatur

ACLU v. Clapper (2015): Second Circuit Court of Appeals Ruling in ACLU v. Clapper (Docket No. 14-42-cv), USCourts.gov. 2015-05-07. (25.07.2015).

Gellman, Barton / Soltani Ashkan (2013): NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say, in: The Washington Post, 30.10.2013, https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (12.07.2015).

Greenwald, Glenn (2014): Glenn Greenwald: how the NSA tampers with US-made internet routers, in: The Guardian, 12.05.2014, http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden (07.07.2015).

Horchert, Judith / Grothoff, Christian / Stöcker, Christian (2014): NSA-System Treasuremap: „Jedes Gerät, überall, jederzeit", in: Spiegel Online, 17.09.2014, http://www.spiegel.de/netzwelt/netzpolitik/nsa-wie-der-geheimdienst-mit-dem-system-treasuremap-daten-sammelt-a-991496.html (20.07.2015).

US Department of Homeland Security (2011): Analyst's Desktop Binder, http://de.scribd.com/doc/82701103/Analyst-Desktop-Binder-REDACTED (20.07.2015).

NSA (2013a): Map of FAIRVIEW SIGAD, in: wikipedia.org: https://commons.wikimedia.org/wiki/File%3AUS-990_Fairview_Map_-_crop.jpg (20.07.2015).

NSA (2013b): Worldwide SIGINT/Defense Cryptologic Platform, in edwardsnowden.com, https://edwardsnowden.com/de/2013/11/23/worldwide-sigintdefense-cryptologic-platform/ (20.07.2015).

NSA (2014): DNI Discovery Options, in ACLU.org, https://www.aclu.org/foia-document/dni-discovery-options (20.07.2015).

RT (2013): DEA agents use NSA intercepts to investigate Americans – report, in: RT Question more, 05.08.2013, http://www.rt.com/usa/dea-agents-nsa-evidence-067 (20.07.2015).

Shiffman John / Cooke Kristina (2013): Exclusive: U.S. directs agents to cover up program used to investigate Americans, in Reuters.com, 05.08.2013, http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805 (20.07.2015).

Stein, Thomas (2010): Intrusion Detection System Evasion durch Angriffsverschleierung in Exploiting Frameworks, Diplomica Verlag: Hamburg.

Kean, Thomas H. / Hamilton, Lee (2004): The 9/11 Commission Report. Final report of the National Commission on Terrorist Attacks upon the United States. Official government: Washington, D.C.

Autor

William Binney

Ehemaliger Technischer Direktor der National Security Agency und US-amerikanischer Nachrichtendienst-Mitarbeiter

DOI: 10.11588/josar.2015.0.23485

The **Journal of Self-Regulation and Regulation** is an open-access peer-reviewed journal serving as a potential outlet for edge-cutting interdisciplinary research on regulatory processes in individuals and organizations. It is published by the research council of Field of Focus 4 (FoF4) of Heidelberg University. The research council stimulates and coordinates interdisciplinary activities in research and teaching on self-regulation and regulation as part of the university's institutional strategy "Heidelberg: Realising the Potential of a Comprehensive University", which is funded by the Federal Government as part of the excellence initiative.

The *Journal of Self-Regulation and Regulation* publishes two volumes per year, regular volumes containing selected articles on different topics as well as special issues. In addition, the reader will be informed about the diverse activities of FoF4, uniting scientists of the faculty of behavioural and cultural studies, the faculty of social sciences and economics, as well as the faculty of law.

Imprint

Journal of Self-Regulation and Regulation Volume 01 (2015)

Research Council of Field of Focus 4, Heidelberg University
Forum Self-Regulation and Regulation
Hauptstr. 47–51
69117 Heidelberg, Germany

Fon: +49 (0)6221 / 54 – 7122
E-mail: fof4@psychologie.uni-heidelberg.de
Internet: https://www.uni-heidelberg.de/fof4

Publisher: Research Council of Field of Focus 4, Heidelberg University
Spokesperson: Sabina Pauen, Department of Psychology
Guest Editors: Wolf J. Schünemann, Department of Political Science
Sebastian Harnisch, Department of Political Science
Editorial Team: Melanie Bräunche, Sabine Falke

You can download the volumes of the *Journal of Self-Regulation and Regulation* free of charge at:
http://journals.ub.uni-heidelberg.de/index.php/josar/index