F A C H H O C H S C H U L E W E D E L

S E M I N A R A R B E I T

in der Fachrichtung
Wirtschaftsingenieurwesen
Sommersemester 2018

Seminar: Informatik

Thema:

Die Aktivitäten der NSA und deren Aufdeckung durch Snowden, Greenwald und Poitras

Eingereicht von: Danyel Ural (Matrikelnummer 100929)

E-Mail: da.ural@web.de

Erarbeitet im: 9. Semester

Abgegeben am: 02.05.2018

Betreuer: Prof. Dr. Michael Anders
Fachhochschule Wedel
Feldstraße 143
22880 Wedel
Tel. (04103) 8048-24

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Vorstellung des Themas

Die einen nennen ihn Held, die anderen einen Verräter. Er gab der Welt einen Einblick in die Machenschaften der Geheimdienste und löste damit global eine Welle der Empörung aus. Getrieben zur Flucht veröffentlichte er die Praktiken und Vorgehensweisen der NSA, GCHQ und ihrer Verbündeten, in der Hoffnung die Welt ein Stück besser und freier zu machen. Des Weiteren wollte er den Menschen helfen ein Bewusstsein dafür zu entwickeln, was um sie herum im digitalen Zeitalter mit ihren persönlichen Daten passiert und wie diese gezielt genutzt werden, ob mit oder ohne ihre Kenntnis. Es handelt sich bei der diskutierten Person um den US-amerikanischen Whistleblower und ehemaligen NSA-Angestellten Edward Snowden.

1.2 Zielsetzung

Durch die belegte Existenz der umfangreichen Überwachungsprogramme und dessen gezieltes Nutzen durch die Geheimdienste, ist es das Ziel dieser Ausarbeitung, dem Leser einen Einblick, in die Person Edward Snowden, seinen Motiven und den Möglichkeiten und den Spähprogrammen zur Überwachung der Bevölkerung, zu gewähren.

1.3 Vorgehensweise

In der vorliegenden Arbeit werden zunächst die Personen Edward Snowden, Laura Poitras und Glenn Greenwald vorgestellt, die Hauptakteure im Drama der NSA-Affäre. Als nächstes folgen Informationen über seinen ehemaligen Arbeitgeber der NSA und dessen Verbündete. Es werden danach die Anfänge erläutert, wie es zum ersten Kontakt mit dem Whistleblower kam, welche Schwierigkeiten vorlagen und es wird die Frage behandelt, was genau ein Whistleblower ist und welche Gefahren das Veröffentlichen von geheimen Regierungsdaten mit sich bringt (anhand von expliziten Beispielen aus den USA). Daraufhin wird die Flucht Snowdens näher betrachtet und welche Konsequenzen und Vorfälle damit verbunden waren. Das letzte Kapitel beschäftigt sich einerseits mit dem NSA-Überwachungsprogramm PRISM, sowie dem Tempora-Programm der britischen Sicherheitsbehörde GCHQ.

2 Die Hauptakteure der NSA-Affäre

2.1 Edward Snowden

Edward Joseph „Ed“ Snowden, wurde am 21.06.1983 in der Stadt Elizabeth City im Bundesstaat North Carolina geboren und ist ein US-amerikanischer IT-Spezialist, Whistleblower und ehemaliger CIA-Mitarbeiter.

Abbildung 1: Edward Snowden (Quelle: http://time.com/)

Snowden belegte 1999 ein Informatikstudium in den USA, welches er für seinen Militärdienst im Jahr 2003 unterbrach. Snowden wollte im Irak dienen, um andere von ihrer Unterdrückung zu befreien. (Beitzer & Klasen, 2013)

Jedoch brach er sich während seiner Zeit beim Militär bei einem Training seine beiden Beine, woraufhin er den aktiven Militärdienst beenden und die US-Army verlassen musste.

Nach seiner Entlassung nahm er 2004 sein Informatikstudium wieder auf, brach es aber, ohne einen Abschluss absolviert zu haben, nach einem Jahr wieder ab. Während dieser Zeit arbeitete er bereits als eine Sicherheitskraft für die NSA und schon im Jahr 2005 wurde er, obwohl er kein abgeschlossenes Informatikstudium hatte, von der CIA für ihre IT-Sicherheit eingestellt. Dies zeigte bereits, dass Snowden hervorragende IT-Kenntnisse besaß, die ihm außerdem dazu verhalfen im Jahr 2007 die USA als IT-Sicherheitsfachmann in Genf zu vertreten. (Connor, 2013)

In der Zeit, in der sich Snowden in Genf aufhielt, kamen ihm die ersten Zweifel an den Praktiken seiner Regierung. So schildert Snowden, dass die CIA ein Interesse an den geheimen Bankinformationen einer Schweizer Bank in Genf gehabt haben. Um diese zu erhalten, motivierten CIA-Agenten einen Schweizer Banker massiv Alkohol zu konsumieren und mit dem eigenen Auto nach Hause zu fahren. Als nächstes sorgten sie dafür, dass er in seinem alkoholisierten Zustand in eine Polizeikontrolle geriet und dadurch festgenommen wurde. Nun nutzten die Agenten die Gunst der Stunde und boten ihm an, ihn aus dieser Situation zu befreien im Austausch für eine Zusammenarbeit und die von ihnen gewünschten Daten. Seit dieser Zeit gelangten geheime Bankdaten aus Genf an die USA.

Dies war der Zeitraum in dem Snowden anfing darüber nachzudenken, geheime Regierungsinformationen preiszugeben, da er das Vertrauen aufgrund unethischer Vorgehensweisen in seine eigene Regierung immer mehr verlor. (Fritz, 2013)

2009 begann Edward Snowden seine Karriere bei dem führenden Technologieberater der USA, Booz Allen Hamilton, wodurch er eine Anstellung als Systemadministrator einer NSA-Einrichtung auf Hawaii erlangte. Jene Stelle verschaffte Snowden Zugang zu geheim eingestuften Informationen der NSA und anderen global agierenden Geheimdiensten, wie z.B. Informationen über das PRISM-Programm der NSA, das dazu dient elektronische Medien und elektronisch gespeicherte Daten auszuwerten und zu überwachen oder dem Tempora-Programm des britischen Geheimdienstes, bei dem ein Datenabgriff an Unterseekabeln erfolgt, wodurch sie den weltweiten Telekommunikations- und Internet-Datenverkehr überwachen können. Was es genau auf sich hat mit den Programmen und wie sie funktionieren, wird in Kapitel 7 detailliert behandelt.

Snowden arbeitete als externer Systemadministrator von Booz Allen Hamilton für die NSA und sammelte während dieser Zeit die umstrittenen Daten über die Überwachungsprogramme und ermöglichte 2013 der Welt durch ihre Veröffentlichung einen Einblick in die Vorgehensweise und Praktiken der Geheimdienste und wie sie die Daten der Menschen für sich nutzen. (Networks, kein Datum)

Und das obwohl er ein üppiges Jahreseinkommen von bis zu 200.000 $ erhielt.

Seine Überzeugung für die Sache und sein Motiv, drückte er mit dem folgenden Satz aus:

„I don't want to live in a society that does these sort of things " (Beitzer & Klasen, 2013)

Durch die Entwendung und Veröffentlichung dieser sensiblen Daten, mit Hilfe von Dokumentarfilmerin Laura Poitras und dem Reporter Glenn Greenwald, erlangte Edward Snowden unausweichlich den Status eines Whistleblowers und wurde 2013 zum Staatsfeind und zum Gejagten der USA.

Die daraus resultierenden Folgen für ihn, sowie sein weiteres Vorgehen und die Zusammenarbeit mit Laura Poitras und Glenn Greenwald, werden in den folgenden Kapiteln erläutert.

2.2 Laura Poitras

Laura Poitras, geboren am 02.02.1964 in Boston, ist eine US-amerikanische Dokumentarfilmerin, die sich in ihren Filmen mit sozialen und politische Missständen befasst. (ExpressVPN, kein Datum)

Abbildung 2: Laura Poitras (Quelle: https://www.mintpressnews.com)

Bekanntheit erlangte Poitras zuerst durch ihren Oskar nominierten Film „My Country, My Country" (2006), der von der Nachkriegszeit im Irak und der amerikanischen Besatzung des Landes nach 2003, handelt. In diesem Film erfährt der Zuschauer die

Umstände des Konflikts aus der Perspektive der irakischen Bevölkerung. (My Country, 2006)

Ihr Film und die durch dessen Dreharbeiten entstandenen Kontakte, katapultierten Poitras Namen auf eine amerikanische Watchlist (Beobachtungsliste), was dazu führte, dass sie von dort an als terrorverdächtig galt und bei Ein- und Abreisen aus den USA erschwerte Sicherheitskontrollen durchlaufen musste. Die Begründung basierte auf einem vagen Verdacht und zwar könnte Poitras Informationen über einen drohenden Angriff auf eine US-amerikanische Militärbasis verschwiegen haben, um diesen im Anschluss filmen zu können. (Richter, 2017)

Die Kontrollen gingen so weit, dass man ihre Elektronischen Geräte konfiszierte, sowie die darauf enthaltenen Daten, außerdem ihre Kreditkartenrechnungen und sogar Befragungen zu Kontaktpersonen durchführte. Man hatte sie außerdem jedes Mal mehrere Stunden festgesetzt und ihr elektronisches Gerät erst nach mehreren Wochen wiedergegeben. Dies musste die Dokumentarfilmerin über sich ergehen lassen, obwohl sie ein leeres Strafregister vorzuweisen hatte. (Greenwald, 2012)

Ein prägendes Ereignis für sie war die Kontrolle an einem Flughafen in New Jersey, wo ihr gedroht wurde ihr Handschellen anzulegen, da sie ihren für Notizen genutzten Bleistift, als Waffe hätte nutzen können. (Richter, 2017)

Diese Kontrollen und Schikanen erfolgten mehr als 50 Mal, woraufhin sie auf Grundlage des „Freedom of Information Act“, der jedem das Recht und den Zugang zu Dokumenten der staatlichen Behörden gibt, Auskunft über die Gründe ihrer Festhaltung erfahren wollte. Diese Anfrage wurde nie beantwortet, woraufhin Poitras die US-Regierung im Jahr 2015 verklagte. (McLaughlin, 2013)

Als Konsequenz der Kontrollen, trat Poitras die Flugreisen nur noch mit so wenig elektronischen Geräten wie möglich an und nutze alternative Wege, um ihre Aufnahmen zu transportieren und betrieb darüber hinaus einen großen Aufwand um ihre Daten zu verschlüsseln. (Greenwald, 2012)

Da unter ihren Quellen unter anderem bekannte Personen wie der Gründer der Enthüllungsplattform WikiLeaks Julian Assange und auch Whistleblower Edward

Snowden sind und beide Personen von der amerikanischen Behörde verfolgt werden, vermeidet sie es seitdem in den USA mit ihren Kontakten zu telefonieren, um der Überwachung ihrer Gespräche zu umgehen.

Am 10.02.2014 ging die publizistische Website „The Intercept“ online (SpiegelOnline, 2014), wovon Laura Poitras unter anderem mit Glenn Greenwald Mitbetreiberin ist. Das Prinzip hinter der Website ist das Zugänglichmachen von Informationen zu Themen wie die Verletzung von Bürgerrechten, Justizmissbrauch, Korruption und soziale Ungerechtigkeit. Die Seite soll Journalisten dazu dienen, die bereits aufgearbeiteten Informationen nutzen zu können, ohne einen Verlust ihrer Anstellung befürchten zu müssen. Angehörigen des US-Militärs wurden von Seite der Regierung aus angewiesen, die Seite nicht zu aufzusuchen. (Gallagher, 2014)

Weltweite Bekanntheit erhielt die Filmerin durch ihre Zusammenarbeit mit Edward Snowden und Glenn Greenwald und der Aufdeckung der geheimen Informationen der Geheimdienste, sowie für ihren Dokumentarfilm „Citizenfour“, der die Geschehnisse rund um die NSA-Affäre und Edward Snowden behandelt und zu dem den Oskar in der Kategorie Bester Dokumentarfilm erspielte. (Pulver, 2015)

2.3 Glenn Greenwald

Glenn Greenwald, geboren am 06.03.1967 in New York City, ist ein US-amerikanischer Journalist, Schriftsteller, Blogger und Rechtsanwalt mit dem Schwerpunkt sicherheits- und gesellschaftspolitische Themen.

Abbildung 3: Glenn Greenwald (Quelle: https://www.si.com)

Weltweite Bekanntheit erhielt der Journalist Greenwald als erster Publizist durch die von Snowden entwendeten Daten, wie unter anderem durch die Veröffentlichung vom NSA-Programm PRISM am 07.06.2013. (Greenwald & MacAskill, 2013)

Greenwald war mehrere Jahre als Anwalt tätig, bevor er sich auf seine journalistischen Tätigkeiten konzentrierte. Er erhoffte sich dadurch, einen größeren Einfluss auf die Gesellschaft ausüben zu können, als er es durch seine Arbeit als Anwalt jemals könnte.

So befasste er sich mit Themen wie der Plame-Affäre, einem politischen Skandal der USA rund um den Irakkrieg, der von gefälschten Dokumenten bis hin zur Veröffentlichung von Geheimdienstmitarbeiternamen reichte. Sowie über die Anthrax-Anschläge von 2001, bei denen mehrere Nachrichtensender und Politiker mit Milzbrandsporen versetzte Briefe erhielten. Diese Anschläge waren neben dem 9/11-Anschlag einer der Hauptgründe zur Durchführung des umstrittenen PATRIOT ACT's der USA, dem Gesetz für den Krieg gegen den Terrorismus.

Durch diesen wurde bei einem Terrorverdacht z.B. das Erfordernis eines Richters bei Telefon- und Internetüberwachung weitgehend aufgehoben. Die Offenlegung von Daten durch Internetprovider und Telefongesellschaften ist ebenso Teil des PATRIOT ACT's, auch wenn ein Richter pro forma entscheidet, müssen die Aktionen dennoch genehmigt werden. Auch Hausdurchsuchungen dürfen ohne Wissen des Betroffenen durchgeführt werden. (Gough, 2011)

2015 wurden Teile des PATRIOT ACT's durch den Freedom Act aufgehoben (Foitzick, 2015), jedoch wurde im Falle der Datenspeicherung nur umverteilt. So speichern die Geheimdienste die Daten nicht mehr selber, sondern können sie beim speichernden Anbieter einsehen.

Seit 2012 ist Greenwald Angestellter der britischen Tageszeitung „The Guardian", die er auch im Jahr 2013 nutzte, um die von Snowden übergebenen Informationen zu veröffentlichen.

Auch Greenwald wurde nach den Veröffentlichungen Ziel der Geheimdienste und auch von seinen eigenen Berufskollegen. (Pitzke, 2013)

Die New York Times veröffentlichte einen Artikel, der Greenwald einen Antiamerikanismus und eine Besessenheit von Überwachungsprogrammen unterstellte. Auch andere Stimmen aus den USA verurteilten den Journalisten und forderten für seine Beihilfe eine Gefängnisstrafe. (Cohen & Kaufman, 2013)

Auch sein Lebenspartner David Miranda wurde zur Zielscheibe nach einem Treffen mit Laura Poitras. Er wurde für fast 9 Stunden am Heathrow Flughafen festgehalten und verhört, während sie alle seine elektronischen Geräte konfiszierten. Sie vermuteten, dass er Informationen von Edward Snowden bei sich führen würde. Der Zweck war etwas über die entwendeten Daten herausfinden und weitere Recherchen bzw. Veröffentlichung die den GCHQ betrafen zu verhindern. Eine Grundlage dafür lieferte der Paragraf 7 des „Terrorism Act 2000“, der es ermöglicht Personen die einer Terrororganisation nahestehen könnten, ohne formale Begründung oder richterliche Überprüfung festzuhalten. (Harding, 2014)

Natürlich war ihnen bewusst, dass David Miranda keiner Terrororganisation nahesteht. Diesem war selber nicht bewusst, welche Daten er dort mit sich trug, da er obwohl er der Lebensgefährte von Glenn Greenwald ist, nicht in die Recherchen involviert war. Angesichts seines Berlin Aufenthaltes, dem Ort an dem Laura Poitras sich aufhielt und dass er der Partner von Greenwald ist, ließ die britischen Agenten ihre eigenen Schlüsse zehen. (TheGuardian, 2013)

Die anschließende Klage gegen dieses Vorgehen der Behörden blieb jedoch erfolglos (SpiegelOnline, 2014), da der High Court beschloss, dass die Daten die er bei sich trug die Sicherheit Großbritanniens hätten gefährden können und das Festhalten somit legitim gewesen sei.

Abbildung 4: Greenwald und Miranda nach der Befragung (Quelle: https://www.telegraph.co.uk)

3 Der Geheimdienst und seine Verbündeten

3.1 Die NSA

Die National Security Agency (NSA) ist der größte Auslandsgeheimdienst der USA.

Abbildung 5: NSA Headquarter in Fort Meade, Maryland
(Quelle: https://de.wikipedia.org)

Mit mehr als 35.000 Mitarbeitern (im Vergleich hat der Bundesnachrichtendienst nur ca. 6300) und bis zu 500 externe Partner wie Booz Allen Hamilton (mit ca. 24.000 Mitarbeitern) (Thoma, 2013), liegen die Zuständigkeiten der NSA in der weltweiten Überwachung, Entschlüsselung und Auswertung elektronischer Kommunikation, wie z.B. Emails, Telefonate, Chats etc. (www.rp-online.de, kein Datum) und ist damit ein Teil der Intelligence Community, dem Zusammenschluss von 17 Nachrichtendiensten der Vereinigten Staaten (u.a. CIA, FBI, DEA etc.). (Naß, 2013)

Ihre Anfänge hatte die NSA im zweiten Weltkrieg, wo sie unter dem damaligen Namen TICOM (Target Intelligence Committee) lief und sich mit der Suche, Bergung und dem Transport von geheimdienstlich relevanten Dingen wie z.B. der deutschen Enigma-Maschine befasste.

Die offizielle Gründung der NSA war am 04.11.1952 und seitdem gewann sie immer mehr an Einfluss, bis sogar Ende der 1970er Jahre die ersten Stimmen laut wurden, dass die Behörde zu einflussreich geworden und kaum kontrollierbar sei.

Die damalige Hauptaufgabe der NSA bestand darin, Informationen der Sowjetunion zu Zeiten des kalten Krieges zu erlangen um sich so einen Vorteil verschaffen zu können. Beispielweise belieferte die NSA das südafrikanische Apartheitsregime in den 1970er Jahren mit modernster Abhörtechnik, damit diese eingesetzt werden kann um Sowjetische Schiffe, die entlang der Küste fuhren, abzuhören. (de.wikipedia.org, kein Datum)

Nach dem Ende des Kalten Krieges, verlor die NSA an Bedeutung, da ihre Notwendigkeit durch den Fall der Sowjetunion anfänglich wegfiel. Als Resultat wurden Budgets und Mitarbeiterstellen gestrichen.

Erst seit dem 11.September.2001 und dem darauffolgenden PATRIOT ACT, erhielt die NSA im „Kampf gegen den Terrorismus“ erneut großen Einfluss, der mit dem stetigen Ausbau von Netzwerken und der Digitalisierung zunahm.

Die Vorgehensweise der NSA lässt sich dabei mit folgender Aussage beschreiben:

„Rather than look for a single needle in the haystack, let’s collect the whole haystack. Collect it all, tag it, store it and whatever it is you want, you go searching for it. “ (Nakashima & Warrick, 2013)

Anstatt die Nadel im Heuhaufen zu suchen, sollte man den ganzen Haufen nehmen und verstauen und bei Bedarf einfach nach dem Teil suchen, welches man braucht.

Nach diesem Motto sammelt die NSA bis heute jegliche Information die ihr in die Hände fällt.

3.2 Die Five-Eyes

Aufgrund des immensen Datenverkehrs im digitalen Zeitalter und den damit anfallenden Kosten und dem benötigten Equipment, handelt die NSA nicht nur auf eigene Faust, sondern kooperiert bei ihrer Arbeit mit anderen Geheimdiensten.

Ein erwähnenswerter Zusammenschluss diverser Geheimdienste ist das sogenannte Five-Eyes.

Seit 1946 bestand eine beidseitige Zusammenarbeit vom amerikanischen und britischen Geheimdiensten und diente der Überwachung des Ostblocks.

Weitere sekundäre Staaten die im Kampf gegen den Terrorismus miteinbezogen wurden sind Australien, Kanada und Neuseeland. Die Allianz dieser 5 Länder gründeten die Five-Eyes.

Israel erhielt vom Zusammenschluss einen Beobachterstatus (Fishman, 2017) und auch Singapur kooperiert mit den Five-Eyes. (Dorling, 2013)

Die erste große mediale Enthüllung der Five-Eyes war das Projekt „ECHELON“. Das Ziel war eine globale Überwachung zu etablieren und mit gleichgesinnten Partner, diese Daten zu teilen. Das weltweite Spionagenetz wurde anfangs genutzt um die Sowjetunion auszuspionieren, was mit dessen Fall 1990 keine Notwendigkeit mehr mit sich trug. Als Reaktion wurde die Begründung zur Nutzung auf den Kampf gegen den Terrorismus gelenkt, um das milliardenteure Unterfangen fortlaufen zu lassen.

Es wird davon ausgegangen, dass ECHELON jedoch stark genutzt wurde, um Wirtschaftsspionage unter den eigenen Verbündeten zu betreiben. (Hoenig, 2001)

Abbildung 6: ECHELON Kuppel in Bad Aibling (Quelle: https://de.wikipedia.org)

Ein weiterer Punkt ist die Tatsache, dass den Geheimdiensten in Großbritannien sowie der USA zur damaligen Zeit gesetzlich verboten war, die Kommunikation der eigenen Bevölkerung zu überwachen. Es kamen Gerüchte auf, dass diese das ECHELON-

System nutzten um sich gegenseitig zu überwachen und dann die Daten auszutauschen um das Gesetz zu umgehen. (www.whatreallyhappened.com, kein Datum)

Durch die Enthüllungen von Snowden kamen noch weitere Partner ans Licht: Dänemark, Frankreich, Norwegen und die Niederlande. Zusammen bildeten sie die „9-Eyes“. (www.cphpost.dk, 2013)

Belgien, Italien, Spanien, Schweden und auch Deutschland bildeten mit den 9-Eyes die sogenannten „14-Eyes“. (www.sueddeutsche.de, 2013)

Der Zweck des Zusammenschlusses und der Kooperation dieser vielen Regierungen, ist das Austauschen von Informationen und dem Kampf gegen den internationalen Terrorismus.

Hierfür werden Anlagen, Computer und Software gemeinsam genutzt und es wurden regionale Schwerpunkte festgelegt. Die Briten sind für Europa und Afrika, die USA für Lateinamerika und Ostasien zuständig. Neuseeland überwacht den Westpazifik und Australien Südasien. Kanada übernahm die weltweite Botschaftskommunikation, die nicht nur die Kommunikation von Regierungen, sondern auch von militärischen Kräften und Personen, Behörden und Dienststellen umfasst. (Volmer, 2013)

4 Das Zusammenkommen von Snowden, Poitras und Greenwald

Snowden war bereits ein erhebliches Risiko eingegangen und hatte es geschafft, Daten der Behörde unbemerkt zu entwenden. Jedoch musste er einen Weg finden, diese auch an die Öffentlichkeit zu bringen. Er entschied sich dafür, die Daten durch die Presse veröffentlichen zu lassen, anstatt sie einfach direkt frei ins Internet zu stellen.

Die Erste Person die Snowden kontaktierte war Glenn Greenwald. Der Journalist war durch seine bisherige Arbeit und Themengebiete aufgefallen. Jedoch gab es ein Problem und das waren seine fehlenden Kenntnisse über entsprechende Verschlüsslungsmaßnahmen. Snowden hatte Greenwald unter dem Pseudonym „Cincinnatus“ angeschrieben und monatelang versucht ihm Material zukommen zu lassen, was jedoch an dem erwähnten fehlenden Wissen über Verschlüsselungssysteme scheiterte (Bartels, 2014). Greenwald hatte diese Emails zu dieser Zeit nicht wirklich für ernst genommen und wollte sich nicht mit dem zeitintensiven Thema auseinandersetzen. (FAZ, 2013)

Also musste sich Snowden umorientieren und entschied sich für eine Person, die sich nicht nur inhaltlich mit solchen Themengebieten auseinandersetzt, sondern auch einer Person, die selber eine Verschlüsselung nutzt. Hierbei entschied er sich für die Dokumentarfilmerin Laura Poitras. Doch auch hier ergab sich eine Schwierigkeit, denn Snowden hatte keinen Zugriff zu ihrem Public Key (Öffentlicher Schlüssel). Dieser Public Key, war Voraussetzung für eine sichere Kommunikation mit Laura Poitras, denn Edward Snowden kannte die Möglichkeiten der Behörden und seines alten Arbeitgebers nur zu gut und musste deshalb extrem vorsichtig vorgehen. Da er vom Ausmaß der Internetüberwachung wusste, konnte und wollte er ihr keine unverschlüsselte Nachricht zukommen lassen, da er ansonsten sein gesamtes Vorhaben hätte auffliegen lassen können.

Durch den öffentlichen Schlüssel, hätte sich Snowdens Email nur durch den „Private Key“ (Privater Schlüssel) von Laura Poitras entschlüsseln lassen können, sprich nur sie wäre in der Lage gewesen seine Nachrichten zu lesen.

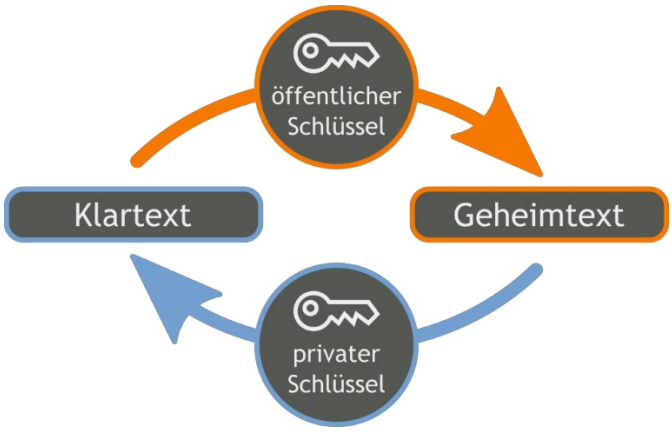

Abbildung 7: Public-Key-Verschlüsselungsprinzip (Quelle: https://de.wikipedia.org)

Deshalb musste Snowden erneut umdenken und jemanden finden, der sowohl ein Verschlüsselungssystem benutzt und zugleich den Private Key von Laura Poitras erlangen konnte.

Diese Person war der spätere Intercept-Mitarbeiter Micah Lee. Dieser erhielt am 11.01.2013 eine anonyme Email, die ihn um Hilfe beim Erwerb des Public Keys von Laura Poitras bat.

> From: anon108@■■■■■■■■■■
> To: Micah Lee
> Date: Fri, 11 Jan 2013
>
> Micah,
>
> I'm a friend. I need to get information securely to Laura Poitras and her alone, but I can't find an email/gpg key for her.
>
> Can you help?

Abbildung 8: Email von Edward Snowden an Micah Lee (Quelle: https://theintercept.com)

Der Bitte kam Lee nach und leitete es an Poitras weiter

> From: Micah Lee
> To: Laura Poitras
> Date: Sat, 12 Jan 2013
>
> Hey Laura,
>
> This person just send me this GPG encrypted email. Do you want to respond? If you want to, and you need any help with using crypto, I'm happy to help.

Abbildung 9: Micah Lee's Nachfrage an Poitras (Quelle https://theintercept.com)

Poitras war der Umgang mit anonymen Quellen gewohnt und erlaubte Lee die Weitergabe.

> From: Laura Poitras
> To: Micah Lee
> Date: Sat, 12 Jan 2013
>
> Hey Micah,
>
> Thanks for asking. Sure, you can tell this person I can be reached with GPG at: laurapoitras@gmail.com
>
> I'll reply with my public key.
>
> I'm also on jabber/OTR at:
> l.p.@jabber.org
>
> I hope all is good with you!
>
> Laura

Abbildung 10: Poitras Antwort auf Lee's Nachfrage (Quelle: https://theintercept.com)

Micah Lee hatte nun die Erlaubnis dem Anonymen den private Key weiterzugeben, jedoch sind auch die Experten nur Menschen und es folgte das nächste Problem.

Snowden hatte bei seiner Anfrage vergessen, seinen eigenen Public Key mitzugeben, woraufhin Micah Lee ihm eine unverschlüsselte Nachricht schicken musste.

Diese unverschlüsselte Aktion hatte aber keinen weiteren Einfluss auf die Personen und stellte nur eine temporäre Gefahr dar.

Micah Lee übergab der anonymen Quelle Poitras Public Key und dieser schrieb Poitras dann unter dem Pseudonym „Citizenfour“ an. (Lee, 2014)

Citizenfour wollte die Sicherheit noch weiter erhöhen und so erstellte sich Poitras einen anonymen Email-Account über den Tor Browser, der die Identität des Nutzers weitgehend verschleiert. Zu dem erstellte sie einen neuen Schlüssel, der nur für ihre Quelle Citizenfour gedacht war. Er riet ihr auch dazu, ihren Private Key durch einen starken passphrase (langes Passwort aus mehreren Wörtern) zu sichern, anstatt ein einziges Passwort zu nutzen, da der Gegenspieler in der Lage wäre eine Billion mögliche Anfragen pro Sekunde zu stellen. (Greenberg, 2014)

Kurze Zeit später sollte klarwerden, wofür all die Sicherheitsmaßnahmen gedacht waren, denn Citizenfour überreichte Poitras Daten über existierenden Überwachungsprogramme der Behörden und versicherte ihr auch, das er Beweise für dessen Existenz in Besitz habe.

Viele dieser Programme waren zu dem damaligen Zeitpunkt noch unbekannt und wenn es bereits Vermutungen über deren Existenz gab, so gab es keine expliziten Beweise.

Zu jener Zeit arbeitete Poitras bereits an einer Dokumentation zu dem Thema Überwachung, wodurch sie, wie bereits erwähnt, auch Informationen überprüfte und nutzte für ihre Arbeit, die aus anonymen Quellen stammten.

Poitras machte sich jedoch auch Gedanken darüber, ob die Quelle wirklich ein Insider sei oder ob es ein verdeckter Ermittler der CIA oder einer anderen behördlichen Organisation sein könnte, der versucht an Informanten über ihre anderen Quellen, wie z.B. den Wikileaks-Gründer Assange den sie für ihre Dokumentation interviewte, zu kommen.

Anfangs wusste Laura Poitras noch nicht, dass ihr Informant der IT-Spezialist Edward Snowden ist. Sie wusste nichts über ihren Informanten, außer dass er geheime Regierungsinformationen besaß. (Maass, 2013)

Um die Ungewissheit zu beseitigen und um die Zusammenarbeit weiter auszubauen, entschieden sich Poitras und Greenwald, nach Hongkong zu reisen, wo sich Citizenfour bereits aufhielt.

Zusammen mit einem weiteren Reporter des Guardian, Ewen MacAskill, hatten sie einen Treffpunkt ausgemacht. Dieser war im Kowloon Distrikt, wo sie vor einem Restaurant nahe dem „Mira-Hotel“ nach einem Mann Ausschau halten sollten, der einen Zauberwürfel in der Hand habe. Sie sollten die Person fragen, ob er wüsste, wann das Restaurant öffnen würde. Wenn alles nach Plan verliefe, hätte der Mann auf ihre Frage reagiert und ihnen von dem gefragten Restaurant abgeraten. Er würde sie aber an die Lounge weiterempfehlen und ihnen anbieten, sie dort hinzuführen. (Citizenfour, 2014)

Dies war das abgemachte Prozedere, um unentdeckt und ohne verdächtig zu wirken, gemeinsam das Hotelzimmer betreten zu können.

5 Exkurs

5.1 Was ist ein Whistleblower?

Edward Snowden erlangte durch sein Handeln den Status eines Whistblowers, jedoch ist vielen Menschen unklar, was es genau auf sich hat mit dem Titel und was genau dieser aussagt und bedeutet.

Der Begriff des Whistleblowers wird abgeleitet vom Englischen „to blow the whistle on“, was übersetzt wird mit „vor jemanden warnen“ oder „jemanden verpfeifen“. (Stefanowitsch, 2011)

Das Motiv der Whistleblower ist meist jenes, dass diese nicht darüber Schweigen wollen oder können, bzw. es nicht mit ihrem Gewissen vereinbaren können, dass Ihnen Informationen vorliegen, die ein illegales Handeln, Missstände oder Gefahren für Menschen oder Tiere beinhalten.

Dabei kann die Veröffentlichung der Informationen innerhalb ihres eigenen Betriebes, ihrer Dienststelle, ihrer Organisation oder der zuständigen Behörde erfolgen. Viele bekannte Whistleblower haben sich auch an externe Dritte wie z.B. der Presse gewandt und ihre gesammelten Daten mit deren Hilfe an die Öffentlichkeit gebracht, wie es auch im Falle Snowden stattfand. (WhistlerblowerNetzwerk, kein Datum)

Im deutschen Sprachraum ist ein Whistleblower ein „Enthüller“ oder „Skandalaufdecker“, wobei der englische Begriff „Whistleblower“ in den Medien noch gegenwärtig ist und genutzt wird.

Auch wenn Whistleblower vom Großteil der Bevölkerung Unterstützung erhalten, so haben ihre Taten, trotz moralischer Überlegenheit, juristische Folgen für sie. Diese Folgen werden im nächsten Abschnitt anhand von Beispielen aufgezeigt.

5.2 Die möglichen Gefahren eines Whistleblowers

Dieser Abschnitt befasst sich explizit mit den Konsequenzen und Gefahren von US-amerikanischen Whistleblowern, die Regierungsinformationen in der Vergangenheit entwendet und veröffentlicht bzw. weitergegeben haben.

Es gab in der Geschichte der USA viele Personen, die den Status eines „Whistleblower“ erhalten haben. Einer davon war Daniel Ellsberg, der die Pentagon-Papers 1971 durch die New York Times veröffentlichte und somit bewies, dass die USA entgegen ihrer Aussagen schon lange vor ihrem offiziellen Eingreifen im Vietnamkrieg geplant hatten, einen Krieg im Vietnam zu führen um gegen den Kommunismus zu kämpfen.

Oder der bekannte Fall Chelsea Manning (geboren als Bradley Manning) im Jahr 2010.

Manning übergab tausende Dateien und Informationen an die Enthüllungsplattform WikiLeaks, worunter sich auch ein Video befand, in welchem Amerikanische Soldaten aus einem Kampfhubschrauber aus, Reporter der Reuter Agentur und Zivilisten erschossen (Collateral Murder, 2007). Des Weiteren bewiesen die Informationen mehr als 300 Fälle von Folterungen im Jahr 2010, durch die amerikanischen Besatzungstruppen im Irak. (Korge, 2013)

Als Konsequenz seines Handelns und dem Veröffentlichen von geheimen Informationen, die der Meinung der Regierung nach, die Verteidigung und Sicherheit der USA betreffen würden, wurde Manning zu 35 Jahren Haft verurteilt. (Fischer, 2013)

Das Gesetz auf das sich berufen wird um Whistleblower anzuklagen, ist der „Espionage Act of 1917“, welches zur Zeit des 1. Weltkrieges entstand und welches die Offenlegung von Informationen, die den Vereinigten Staaten von Amerika schaden oder einem fremden Land einen Vorteil verschaffen würde, unter Strafe stellt. (Borger, 2013)

Daniel Ellsberg wurde 1971 auch auf Grundlage des Epsionage Act of 1917 angeklagt und ihm drohten bis zu 115 Jahre Haft. Jedoch kam es in seinem Fall damals zu einem Freispruch durch den Richter, da Geheimdienstmitarbeiter illegal in die Praxis von Ellsbergs Psychiater eingebrochen waren und er außerdem illegal überwacht wurde. (McDuffee, 2017)

Auch wenn Barack Obama seinerzeit als Präsidentschaftskandidat (2009), das Aufdecken von Missständen als „patriotischen Akt“ gelobt hatte, so kam es bereits in

seiner ersten Amtszeit (2009-2013) zu 6 Anklagen durch den Espionage Act of 1917, unter denen auch Manning war. (Leyendecker, 2013)

Von den angesetzten 35 Jahren, musste Manning jedoch nur 7 Jahre in einem Militärgefängnis verweilen (2010-2017), denn sie erhielt 2017 einen Straferlass (keinen Gnadenerlass) vom Präsidenten Barack Obama, kurz vor dessen Amtszeitende. (SpiegelOnline, 2017)

Auch Edward Snowden wurde 2013 auf Basis des Espionage Act of 1917 angeklagt (Finn & Horwitz, 2013), jedoch hatte er seinen Arbeitsplatz auf Hawaii bereits verlassen und sich nach Hongkong aufgemacht, damit er sich einer Festnahme entziehen konnte. Die Details seiner Flucht und wieso er Hongkong wählte, werden im folgenden Kapitel behandelt.

6 Die Flucht

6.1 Hawaii - Hongkong

Edward Snowden war durch die vergangenen Fälle und Urteile für Whistleblower bewusst, dass man auch ihn des Verrats bezichtigen und verhaften würde.

Snowden entschloss sich dafür, seinen Posten auf Hawaii zu verlassen. Um nicht den Verdacht seiner Vorgesetzten zu erwecken, benutzte er den Vorwand, eine Epilepsieuntersuchung durchführen zu lassen, da seine Mutter an dieser Krankheit leide. Dies war schon ein risikobehaftetes Unterfangen, denn NSA Mitarbeiter müssen Auslandsreisen im Normalfall 30 Tage vorher anmelden. (Reißmann, 2014)

Er entschied sich für Hongkong, der Sonderverwaltungszone der Volksrepublik China, obwohl Hongkong und die USA ein Auslieferungsabkommen besitzen. Einer der Gründe dafür ist, dass beide Seiten im Falle eines politischen Deliktes die Möglichkeit haben, die Auslieferung von Personen zu verhindern. Weiterhin besitzt Hongkong, seit seiner Übergabe an die Chinesen durch die Briten, im Vergleich zu China Pressefreiheit, sowie politische Toleranz, da es als Sonderzone unter dem Motto „Ein Land, zwei Systeme“ geführt wird. Auch die Mentalität der Hongkonger Bevölkerung ist stark an den freiheitlichen Gedanken gebunden. So kam es immer wieder bei den Versuchen der chinesischen Regierung Pekings, mehr Kontrolle über Hongkong zu erlangen, zu Protesten seitens der Hongkonger Bevölkerung. Ein bekanntes Beispiel dafür ist das Gedenken an das „Tian’anmen-Massaker“ von 1989, bei dem das chinesische Militär im Zentrum Pekings gewaltsam den Protest der Bevölkerung gegen die Politik des Landes niederschlug und woraufhin im Laufe der Woche in den weiteren Protesten mehrere Tausend Menschen umkamen. Während dieser Vorfall und alle Informationen darüber in China unter die Zensur fallen und auch die Informationen im Internet durch die Internetkontrolle Chinas geblockt werden (Ser, 2016), so gibt es in Hongkong jedes Jahr eine Gedenkveranstaltung an das damalige Ereignis.

Ein weiterer Punkt ist die Tatsache, dass man als Amerikanischer Staatsbürger für einen Aufenthalt in Hongkong von unter 90 Tagen, kein Visum benötigt, wodurch die Einreise für Snowden kein Problem darstellte.

Wenn es trotz politischer Verfolgung nicht möglich gewesen wäre in Hongkong zu bleiben, so wäre ein Asylantrag eine weitere Option für Snowden gewesen. Beide Möglichkeiten hätten ihm, auch im Falle eines Scheiterns, Zeit eingespielt, die er für eine weitere Flucht hätte nutzen können. (Borger, 2013)

Abgesehen von der Politischen Ebene, bietet Hongkong durch seine internationale und sehr große Bevölkerungsdichte einen weiteren Schutz, da man leicht in den Menschenmassen untertauchen könnte, denn Hongkong besitzt eine Bevölkerungsdichte von 6648 Einwohner pro km² (im Vergleich besitzt Deutschland eine Bevölkerungsdichte von 231 Einwohner pro km²) (Laenderdaten, kein Datum) und ist als bedeutender Finanz-und Handelsplatz zudem sehr international, wodurch Snowden unwahrscheinlicher zu entdecken gewesen wäre.

Aber für die Entscheidung waren die liberale Einstellung und die Souveränität ausschlaggebend, um Hongkong als idealen Veröffentlichungsort zu wählen. Snowden war fest davon überzeugt, dass Hongkong einer der wenigen Orte der Welt sei, der sich dem US-Diktat widersetzen können und widersetzen würden. (Borger, 2013)

In Hongkong stieg der Whistleblower im Fünf-Sterne-Hotel „The Mira“ ab, welches er aus Angst vor der Verfolgung der CIA nur ganze drei Male in einem dreiwöchigen Zeitraum verließ. (Reißmann, 2013)

Wie bereits im Kapitel 3 erwähnt, war dies der Ort an dem Snowden die Dateien an die Reporter übergab und sie in seine Pläne einweihte.

6.2 Hongkong - Russland

Die ersten Enthüllungen begannen am 06.06.2013, als der Guardian und die Washington Post über Zugriffe auf Telefonverbindungsdaten durch die NSA und über das Spähprogramm PRISM berichteten.

Erst 3 Tage später, am 09.06.2013, erklärte sich Snowden als Quelle der Informationen, um zu beweisen, dass dies keine unseriösen oder gar gefälschten Berichte seien. Snowden hatte bewusst damit gewartet sich als Quelle zu outen, da er den Fokus auf die Geschichten und nicht auf seine Person lenken wollte. (Greenwald, et al., 2013)

Nun war der Welt und auch der NSA das Gesicht sowie der Name bekannt, dass hinter den Enthüllungen steht.

Snowden wusste, dass die Geheimdienste schon bald in Hongkong nach ihm suchen würden und verließ daraufhin das Hotel Mira.

Der Whistleblower machte sich auf den Weg zum UN-Gebäude, wo er seinem Anwalt Robert Tibbo traf und gemeinsam mussten sie sich einen Weg überlegen, wie sie weiter vorgehen sollen. Wie bereits in Kapiel 5.1 erwähnt, war die Asylanfrage ein möglicher Weg. Jedoch hätte dies seinen Zugang zu Computern und seine Freiheit im Allgemeinen stark eingeschränkt. Bis zur einer möglichen Lösungen der problematischen Situation, musste Snowden untertauchen.

Tibbo arbeitete in Hongkong als Anwalt für viele Flüchtlinge die einen Asylantrag an Hongkong gestellt haben und riet Snowden an einem Ort unterzutauchen, an dem ihn niemand vermuten würde. Dieser Ort war in den Wohnungen der Flüchtlinge, die Tibbo bereits vertrat.

Am 21.06.2013, an seinem 30. Geburtstag, wurde Edward Snowden offiziell durch den Espionage Act of 1917 angeklagt. Nach 12 Tagen des Versteckens mussten Snowden und sein Anwalt handeln, da beiden klar wurde, dass der Aufenthalt in Hongkong immer ungewisser wurde. Also suchten sie auch außerhalb nach Hilfe und sein Anwalt wendete sich an Julian Assange und seinem bestehenden Wikileaks Netzwerk. Sarah Harrison eine britische Mitarbeiterin von Wikileaks und enge Vertraute von Assange trat in Kontakt mit Tibbo und sie entwickelten einen Plan zusammen, wie sie per Flugzeug aus Hongkong entkommen könnten. Sie fingen an mehr als ein Dutzend Tickets für verschiedenste Flüge und Ziele zu bestellen, um die Behörden zu verwirren und ihren wahren Zielort zu verschleiern.

Als junges Paar getarnt, betraten Snowden und Harrison den Flughafen in Hongkong und nahmen einen Flug nach Moskau. Eine Tatsache die die US-amerikanischen Behörden in Rage versetzte war, dass die Hongkonger Autoritäten erst nach dem Verlassen des Chinesischen Luftraumes bekannt gaben, dass Snowden das Land verlassen hat. Als Konsequenz entzogen die USA dem Whistleblower den Pass um seine weitere Reise zu behindern.

Durch den Entzug, war Snowden nun in Russland gestrandet und musste im Transitbereich bleiben, bis eine Lösung für das Problem gefunden wurde. (Tedesco, kein Datum)

6.3 Snowdens Asylanträge

Während seines Aufenthaltes im Transitbereichs, stellte Snowden 21 Asylanträge sowohl an europäische, asiatische und südamerikanische Regierungen. (SpiegelOnline, 2013)

Länder wie z.B. Deutschland, Österreich und Frankreich lehnten sein Ersuchen ab. Der Großteil der Länder begründete es damit, dass es nur möglich sei einen Antrag zu stellen, wenn man in dem jeweiligen Land sei. Das Auswärtige Amt und das Innenministerium Deutschlands, sahen die Voraussetzungen für eine Aufnahme als nicht erfüllt. Für Frankreich war die Freundschaft zu den USA sehr wichtig und sie hätten von ihrem Auslieferungsabkommen Gebrauch gemacht.

Lediglich Venezuela, Bolivien und Russland bestätigten Snowdens Anträge offiziell.

Im letzteren verweilt Snowden an einem unbekannten Ort, seit seiner Transitzeit.

Während seiner Transitzeit, war auch der bolivianische Präsident Evo Morales in Moskau auf dem Gipfel der gasexportierenden Länder präsent. Nach dessen Abflug kamen Gerüchte auf, dass sich Snowden in seiner Maschine befinden würde, da Snowden von Anfang an das Ziel hatte, nach Südamerika zu gehen und Morales in einem Interview bekannt gab, dass Bolivien bereit wäre ihn aufzunehmen.

Als Konsequenz übten die amerikanischen Behörden Druck auf Frankreich und Spanien aus und die Präsidentenmaschine wurde so gezwungen in Österreich zwischenzulanden. Ihnen wurde die Erlaubnis entzogen, den französischen- sowie den spanischen Luftraum zu durchqueren. Auf der Suche nach Edward Snowden durchsuchten die Behörden in Wien anschließend die Maschine. (derStandart, 2015)

Dieser Vorfall führte zu Spannungen zwischen den Parteien, da sie durch das Flugverbot das Leben des Staatspräsidenten gefährdeten und sie gegen die Immunität, die jedem Präsidenten zusteht, verstoßen haben. (SpiegelOnline, 2013)

Russland erteilte Snowden am 01.08.2013 Asyl für 1 Jahr, dass im Juli 2014 um 3 Jahre verlängert wurde. Auch nach Ablaufen dieser Frist im Januar 2017, wurde sein Asyl um weitere 3 Jahre verlängert bis 2020 (Kalischewski, 2017). Nach 5 Jahren Aufenthalt wäre es Snowden möglich, eine russische Staatsbürgerschaft zu beantragen, wodurch er nicht mit einer Ablehnung und einer dadurch möglichen Abschiebung fürchten müsste.

Der russische Präsident Putin bot Snowden das Asyl unter der Bedingung, den USA durch seine Enthüllungen keinen weiteren Schaden zuzufügen, an. (Westfalenpost, 2013)

7 Die Überwachungsprogramme

7.1 PRISM

PRISM steht für „Planning tool for Resource Integration, Synchronization, and Management“ („Planungswerkzeug für Ressourcenintegration, Synchronisation und Management") und wird seit 2007 genutzt, um Daten aus zentralen Rechnern mehrerer Internetfirmen anzuzapfen.

Abbildung 11: PRISM Logo (Quelle: https://openclipart.org)

Das PRISM-Programm betrifft dabei neun der größten Internetkonzerne der USA: Microsoft (u.a. mit Skype), Google (u.a. mit Youtube), Facebook, Yahoo, Apple, AOL und Paltalk.

Dieser direkte Zugriff ermöglicht es dem FBI und der NSA die Internetaktivitäten von Personen die jene Angebote nutzen zu überwachen und auf deren Fotos, Emails, Videos- und Textchats sowie anderen Daten wie Logins zuzugreifen. Die übermittelten Daten unterscheiden sich dabei von Anbieter zu Anbieter. Der Zugriff auf die Daten beschränkt sich auch nicht nur auf amerikanische Server, sondern betrifft auch Daten, die über US-Rechenzentren von Facebook und den anderen Anbietern weitergeleitet werden.

Offiziell ist der NSA durch den „Protect America Act“ nur erlaubt Nichtamerikaner die im Zusammenhang mit Terrorismus stehen, zu überwachen. Die amerikanischen Bürger sind weitgehend geschützt gegen die Datenzugriffe.

Um eine Überwachung durchzuführen, muss die Anfrage durch einen Mitarbeiter abgesegnet werden und darüber hinaus kontrolliert werden, ob es einen triftigen Grund bzw. dass ein geheimdienstlich notwendiger Grund existiert. Außerdem muss sichergestellt werden, dass es sich bei der betreffenden Person nicht um einen US-Bürger oder eine in den USA aufhaltende Person handelt. (ZeitOnline, 2013)

Dabei stößt die NSA aber auf ein Problem, und zwar ist es ihnen nicht vollkommen möglich, zwischen Amerikaner und nicht-amerikaner zu unterscheiden, weshalb Analytiker Wahrscheinlichkeiten nutzen, um einen Fall zu beurteilen. Beträgt die Wahrscheinlichkeit 51% (dem niedrigsten erlaubten Wert), dann liegt der Datenauswertung nichts im Wege. Im Falle eines Irrtums haben die Mitarbeiter pro Quartal Rechenschaft abzulegen aber müssen laut Trainingshandbuches nicht mit weiteren Konsequenzen rechnen. (Kuhn, 2013)

Die betroffenen Firmen nahmen nach den Veröffentlichungen Stellung und dementierten, dass die NSA einen direkten Zugang und Zugriff zu ihren Servern besitzt.

Jede Herausgabe erfolgte im rechtlichen Rahmen und auf Grundlage von richterlichen Beschlüssen.

Einzig allein Yahoo hatte im Jahr 2008 Klage gegen die Herausgabe von ihren Daten eingereicht. Diese Klage wurde am 22.08.2008 entschieden und Yahoo drohten hohe Geldbußen im Falle der Kooperationsverweigerung.

Im Jahr 2016 wurde Yahoo jedoch bezichtigt für die US-Dienste eine Software geschrieben zu haben, die sie ohne das Wissen ihrer Security-Abteilung installiert hatten. Diese Software ermöglichte Echtzeitscanns von den Kundenmails und eine Weiterleitung zu den Geheimdiensten die diese online lesen konnten. (Sokolov, 2016)

Auch Antivirenhersteller wie die deutsche Avira wurden von der NSA bespitzelt und es wurden Wege gesucht wie man den Virenschutz umgehen könne. (Scherschel, 2015)

Es wird davon ausgegangen das die NSA ihr 2013, ca. 100.000 Quadratmeter großes neu gebautes Datenzentrum in Utah für die Speicherung der Daten aus dem PRISM-Programm nutzt. Das 2 Milliarden Dollar teure Bauwerk soll Kapazitäten für ca. 12000 Petabyte (entspricht 5 Millionen Terabyte bzw. 5 Milliarden Gigabyte) besitzen (Hill, 2013) und die Kühlkosten der Server sollen sich auf ca. 40 Millionen Dollar pro Jahr belaufen. (Rosenbach, et al., 2013)

Abbildung 12: Utah Datencenter (Quelle: https://de.wikipedia.org)

7.2 Tempora

Wie man schon aus der UKUSA-Kooperation aus Kapitel 3.2 entnehmen konnte, existiert eine starke Zusammenarbeit zwischen der NSA und dem GCHQ.

Am 21.06.2013 erschien im Guardian ein Artikel, der über das „Tempora-Programm“ des britischen Geheimdienstes GCHQ berichtete. Bis dahin waren die Enthüllungen Snowdens nur auf die NSA bezogen, jedoch veränderte der neue Bericht die Situation, da nun klar war, dass die Überwachung viel weitgreifender war als gedacht.

Das Tempora Programm wird von GCHQ und NSA genutzt, um gezielt transatlantische Glasfaserkabel anzuzapfen und so geführte Telefonate und Internetverbindungen zu überwachen.

In bereits 200 Glasfaserkabel hat der Geheimdienst Sonden zum Abzapfen der Daten installiert. Jedes Kabel leitet dabei zehn Gigabit Daten pro Sekunde ab, was bedeutet das sie insgesamt 2000 Gigabit pro Sekunde aufnehmen (entspricht 250 Gigabyte). (Kleinz, 2013)

Die gesammelten Metadaten, z.B. IP-Adressen, Telefonnummern oder Verbindungsdaten werden bis zu 30 Tage und die Inhalte werden bis zu 3 Tage gespeichert und von 550 Analysten betreut, von denen ca. 250 NSA-angehörig sind.

Der GCHQ brüstet sich mit dem Fakt, dass nicht einmal die NSA, so viele Daten wie sie sammle und dass sie den größten Internetzugang innerhalb des Five-Eyes Zusammenschlusses hätten (Reißmann, 2013). Edward Snowden erklärte, dass das Tempora-System das erste System mit der Absicht alles zu speichern darstelle (ein sogenanntes „full take“ System) und das das GCHQ in der Hinsicht schlimmer als ihr Kollege NSA sei.

Die einzige Möglichkeit dem System zu entgehen, wäre die Rücksprache mit dem eigenen Anbieter, die Übertragungen nicht über Großbritannien laufen zu lassen, da alles was über die Insel läuft erfasst wird. Doch dies ist fast unmöglich, da die Verbindungen sich täglich ändern können. Zudem sind die meisten wichtigen Dienste für Privatnutzer, wie Social Medias und Cloudanbieter, in den USA angesiedelt und wie bereits in Abschnitt 7.1 erläutert, somit sowieso vom PRISM-Programm betroffen.

Ein weiteres Problem ist die Tatsache, dass die wichtigsten Kabel meistens über die britische Insel verlaufen (Stöcker, 2013), wodurch eine Absicherung noch schwieriger zu erreichen ist. Das folgende Bild macht die Misere noch einmal deutlich, da man klar erkennen kann, dass die meisten Kabel vom europäischen Festland, über Großbritannien verlaufen.

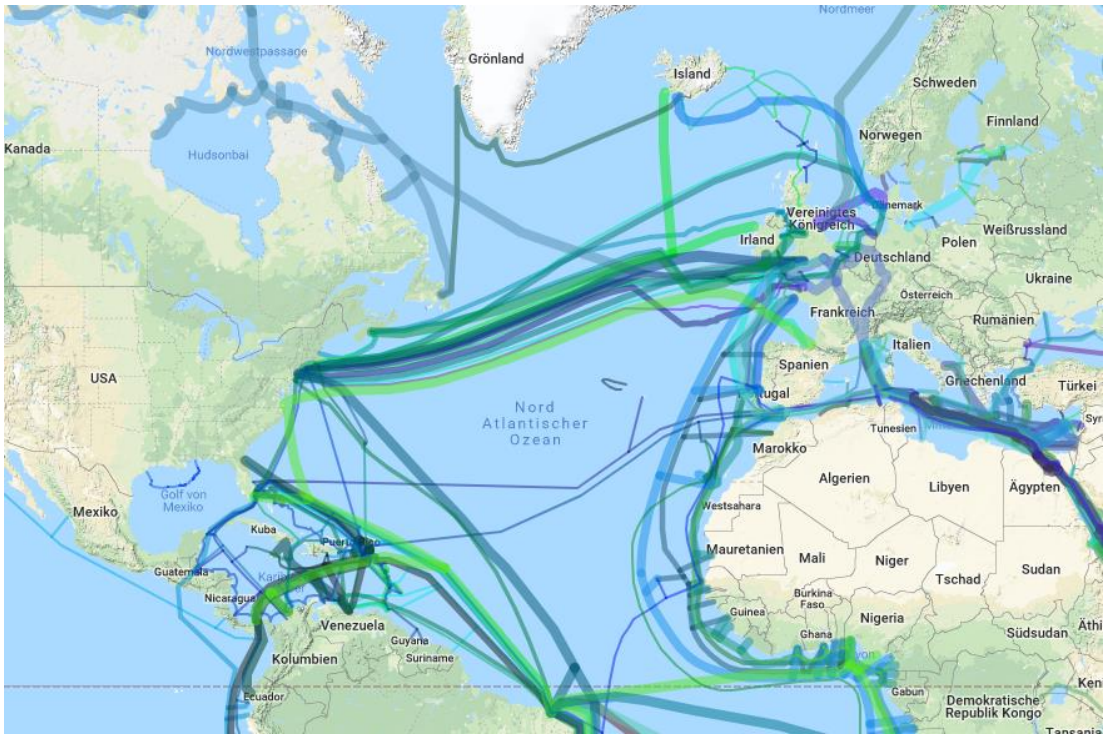

Abbildung 13: Transatlantische Kabelkarte (Quelle: https://netzpolitik.org)

Literaturverzeichnis

Anon., 2014. *www.spiegel.de.* [Online] Available at: http://www.spiegel.de/netzwelt/netzpolitik/the-intercept-enthuellungs-website-geht-online-a-952467.html

Bartels, G., 2014. *www.tagesspiegel.de.* [Online] Available at: https://www.tagesspiegel.de/kultur/glenn-greenwalds-buch-die-globale-ueberwachung-verstecken-ist-nicht/9915748.html

Beitzer, H. & Klasen, O., 2013. *www.Sueddeutsche.de.* [Online] Available at: http://www.sueddeutsche.de/politik/whistleblower-edward-snowden-allein-gegen-die-supermacht-1.1692537

Borger, J., 2013. *www.theguardian.com.* [Online] Available at: https://www.theguardian.com/world/2013/jun/11/edward-snowden-defence

Borger, J., 2013. *www.theguardian.com.* [Online] Available at: https://www.theguardian.com/world/2013/jun/09/edward-snowden-hong-kong-gamble

Citizenfour. 2014. [Film] Regie: Laura Poitras. s.l.: s.n.

Cohen, N. & Kaufman, L., 2013. *www.nytimes.com.* [Online] Available at: https://www.nytimes.com/2013/06/07/business/media/anti-surveillance-activist-is-at-center-of-new-leak.html?pagewanted=all&_r=0

Collateral Murder. 2007. [Film] s.l.: s.n.

Connor, T., 2013. *NBCnews.com.* [Online] Available at: https://web.archive.org/web/20130921183018/http:/usnews.nbcnews.com/_news/2013/06/10/18882615-what-we-know-about-nsa-leaker-edward-snowden

de.wikipedia.org, kein Datum *de.wikipedia.org.* [Online] Available at: https://de.wikipedia.org/wiki/National_Security_Agency

derStandart, 2015. *www.derstandard.at.* [Online] Available at: https://derstandard.at/2000010318614/Dokumentation-USA-zwangen-Oesterreich-2013-zu-Durchsuchung-von-Morales-Flugzeug

Dorling, P., 2013. *www.smh.com.au.* [Online] Available at: https://www.smh.com.au/technology/singapore-south-korea-revealed-as-five-eyes-spying-partners-20131124-2y433.html

ExpressVPN, kein Datum *www.expressvpn.com.* [Online] Available at: https://www.expressvpn.com/de/education/biography/laura-poitras

FAZ, 2013. *www.faz.net.* [Online] Available at: http://www.faz.net/aktuell/feuilleton/glenn-greenwald-erzaehlt-ueber-seine-arbeit-mit-edward-snowden-13300668.html

Finn, P. & Horwitz, S., 2013. *www.washingtonpost.com.* [Online] Available at: https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html?utm_term=.ec1050dab98c

Fischer, S., 2013. *www.spiegel.de.* [Online] Available at: http://www.spiegel.de/politik/ausland/urteil-im-fall-bradley-manning-35-jahre-haft-fuer-wikileaks-enthueller-a-917863.html

Fishman, A., 2017. *www.ynetnews.com.* [Online] Available at: https://www.ynetnews.com/articles/0,7340,L-4963869,00.html

Foitzick, K., 2015. *www.activemind.de.* [Online] Available at: https://www.activemind.de/magazin/freedom-act-datenschutz/

Fritz, D., 2013. *www.netzwoche.ch.* [Online] Available at: http://www.netzwoche.ch/news/2015-03-01/nsa-whistleblower-was-ich-in-genf-sah-hat-mich-desillusioniert

Gallagher, R., 2014. *www.theintercept.com.* [Online] Available at: https://theintercept.com/2014/08/20/u-s-military-bans-the-intercept/

Gough, J., 2011. *www.lto.de.* [Online] Available at: https://www.lto.de/recht/hintergruende/h/zehn-jahre-patriot-act-the-american-way-of-terrorbekaempfung/

Greenberg, A., 2014. *www.wired.com.* [Online] Available at: https://www.wired.com/2014/10/snowdens-first-emails-to-poitras/

Greenwald, G., 2012. *www.salon.com.* [Online] Available at: https://www.salon.com/2012/04/08/u_s_filmmaker_repeatedly_detained_at_border/

Greenwald, G. & MacAskill, E., 2013. *www.theguardian.com.* [Online] Available at: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Greenwald, G., MacAskill, E. & Poitras, L., 2013. *www.theguardian.com.* [Online] Available at: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Harding, L., 2014. *www.theguardian.com.* [Online] Available at: https://www.theguardian.com/world/2014/feb/02/david-miranda-detention-chilling-attack-journalism

Harding, L., 2014. *www.theguardian.com.* [Online] Available at: https://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract

Hill, K., 2013. *www.forbes.com.* [Online] Available at: https://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought/#4d9346a07457

Hoenig, J., 2001. *www.handelsblatt.com.* [Online] Available at: http://www.handelsblatt.com/archiv/echelon-dient-zur-wirtschaftsspionage/2047436.html

Kalischewski, J., 2017. *www.morgenpost.de.* [Online] Available at: https://www.morgenpost.de/politik/article209316483/Edward-Snowden-darf-zwei-weitere-Jahre-in-Russland-bleiben.html

Kleinz, T., 2013. *www.zeit.de.* [Online] Available at: http://www.zeit.de/digital/datenschutz/2013-06/gchq-tempora-internet/seite-1

Kleinz, T., 2013. *www.zeit.de.* [Online] Available at: http://www.zeit.de/digital/datenschutz/2013-06/gchq-tempora-internet/seite-2

Korge, J., 2013. *www.spiegel.de.* [Online] Available at: http://www.spiegel.de/politik/ausland/bericht-von-amnesty-international-entlarvt-foltersystem-im-irak-a-887470.html

Kuhn, J., 2013. *www.sueddeutsche.de.* [Online] Available at: http://www.sueddeutsche.de/digital/prism-programm-der-nsa-so-ueberwacht-der-us-geheimdienst-das-internet-1.1690762

Laenderdaten, kein Datum *www.laenderdaten.info.* [Online] Available at: https://www.laenderdaten.info/bevoelkerungsdichte.php

Lee, M., 2014. *www.theintercept.com.* [Online] Available at: https://theintercept.com/2014/10/28/smuggling-snowden-secrets/

Leyendecker, H., 2013. *www.sueddeutsche.de.* [Online] Available at: http://www.sueddeutsche.de/politik/barack-obama-treibjagd-auf-whistleblower-1.1739636

Maass, P., 2013. *www.nytimes.com.* [Online] Available at: https://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html?ref=magazine

McDuffee, A., 2017. *www.timeline.com.* [Online] Available at: https://timeline.com/pentagon-papers-famous-leak-prison-9772ec594f73

McLaughlin, J., 2013. *www.theintercept.com.* [Online] Available at: https://theintercept.com/2015/07/13/laura-poitras-sues-u-s-government-find-repeatedly-stopped-border/

My Country, M. C., 2006. *www.viennale.at.* [Online] Available at: https://www.viennale.at/de/film/my-country-my-country

Nakashima, E. & Warrick, J., 2013. *www.washingtonpost.com.* [Online] Available at: https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html?noredirect=on&utm_term=.f338d70b3c8b

Naß, M., 2013. *www.zeit.de.* [Online] Available at: http://www.zeit.de/2013/33/nsa-hauptquartier-fort-meade

Networks, A. T., kein Datum *www.biography.com.* [Online] Available at: https://www.biography.com/people/edward-snowden-21262897

n-tv.de, 2013. *www.n-tv.de.* [Online] Available at: https://www.n-tv.de/politik/Edward-Snowden-auf-der-Flucht-article10798311.html

Peres, R., 2011. *www.lto.de.* [Online] Available at: https://www.lto.de/recht/hintergruende/h/zehn-jahre-patriot-act-the-american-way-of-terrorbekaempfung/

Pitzke, M., 2013. *www.spiegel.de.* [Online] Available at: http://www.spiegel.de/kultur/gesellschaft/hetzjagd-auf-guardian-reporter-glenn-greenwald-a-908495.html

Pulver, A., 2015. *www.theguardian.com.* [Online] Available at: https://www.theguardian.com/film/2015/feb/23/edward-snowden-documentary-citizenfour-wins-oscar

Reißmann, O., 2013. *www.spiegel.de.* [Online] Available at: http://www.spiegel.de/netzwelt/netzpolitik/edward-snowdens-flucht-rekonstruktion-a-907709.html

Reißmann, O., 2013. *www.spiegel.de.* [Online] Available at: http://www.spiegel.de/netzwelt/netzpolitik/internetueberwachung-tempora-geheimdienst-zapft-glasfaserkabel-an-a-907283.html

Reißmann, O., 2014. *www.spiegel.de.* [Online] Available at: http://www.spiegel.de/netzwelt/netzpolitik/edward-snowden-enthuellungen-whistleblower-auf-der-flucht-chronik-a-973378.html

Richter, D., 2017. *www.netzpolitik.org.* [Online] Available at: https://netzpolitik.org/2017/laura-poitras-acht-jahre-lang-ein-hochsicherheitsrisiko-ohne-es-zu-wissen/

Rosenbach, M., Stark, H. & Stock, J., 2013. *www.spiegel.de.* [Online] Available at: http://www.spiegel.de/international/world/prism-leak-inside-the-controversial-us-data-surveillance-program-a-904761.html

Scherschel, F. A., 2015. *www.heise.de.* [Online] Available at: https://www.heise.de/security/meldung/NSA-und-GCHQ-spionieren-Anti-Viren-Hersteller-aus-2719443.html

Ser, K. K. K., 2016. *www.pri.org.* [Online] Available at: https://www.pri.org/stories/2016-06-03/how-china-has-censored-words-relating-tiananmen-square-anniversary

Siemons, M., 2013. *www.faz.net.* [Online] Available at: http://www.faz.net/aktuell/feuilleton/debatten/edward-snowden-in-hongkong-die-tragik-des-whistleblowers-12216774.html

Snowden, E., 2013. *www.truth-out.org* [Interview] (11 Juni 2013).

Sokolov, D. A., 2016. *www.heise.de.* [Online] Available at: https://www.heise.de/newsticker/meldung/Alle-Mails-gescannt-Yahoo-arbeitete-fuer-Geheimdienste-3340778.html

SpiegelOnline, 2013. *www.spiegel.de.* [Online] Available at: http://www.spiegel.de/politik/ausland/snowden-asyl-fuer-den-nsa-enthueller-pruefen-diese-laender-a-909022.html

SpiegelOnline, 2013. *www.spiegel.de.* [Online] Available at: http://www.spiegel.de/politik/ausland/snowden-geruechte-boliviens-praesidentenmaschine-muss-in-wien-landen-a-909108.html

SpiegelOnline, 2014. *www.spiegel.de.* [Online] Available at: http://www.spiegel.de/politik/ausland/festnahme-von-david-miranda-in-london-war-laut-high-court-rechtens-a-954437.html

SpiegelOnline, 2017. *www.spiegel.de.* [Online] Available at: http://www.spiegel.de/netzwelt/netzpolitik/chelsea-manning-whistleblowerin-ist-laut-bbc-frei-a-1148103.html

Stefanowitsch, A., 2011. *scilogs.spektrum.de.* [Online] Available at: https://scilogs.spektrum.de/sprachlog/whistleblower/

Stöcker, C., 2013. *www.spiegel.de.* [Online] Available at: http://www.spiegel.de/netzwelt/web/edward-snowden-ueber-tempora-macht-der-britischen-datensauger-a-909849.html

Tedesco, T., kein Datum *www.nationalpost.com.* [Online] Available at: http://nationalpost.com/features/how-edward-snowden-escaped-hong-kong

TheGuardian, 2013. *www.theguardian.com.* [Online] Available at: https://www.theguardian.com/world/2013/aug/19/david-miranda-interview-detention-heathrow

Thoma, J., 2013. *www.golem.de.* [Online] Available at: https://www.golem.de/news/geheimdienste-nsa-hauptquartier-groesser-als-das-pentagon-1307-100560.html

Volmer, H., 2013. *www.n-tv.de.* [Online] Available at: https://www.n-tv.de/politik/Five-Eyes-wollen-unter-sich-bleiben-article11636886.html

Westfalenpost, 2013. *www.wp.de.* [Online] Available at: https://www.wp.de/politik/snowden-verzichtet-nach-kreml-angaben-

auf-asyl-in-russland-id8139149.html?seite=2&displayDropdownTop=block&displayDropdownBottom=none

WhistlerblowerNetzwerk, kein Datum *www.whistleblower-net.de.* [Online] Available at: https://www.whistleblower-net.de/whistleblowing/

www.cphpost.dk, 2013. *www.cphpost.dk.* [Online] Available at: http://cphpost.dk/news/international/denmark-is-one-of-the-nsas-9-eyes.html

www.rp-online.de, kein Datum *www.rp-online.de.* [Online] Available at: http://www.rp-online.de/thema/nsa/

www.sueddeutsche.de, 2013. *www.sueddeutsche.de.* [Online] Available at: http://www.sueddeutsche.de/politik/spionage-kooperation-five-eyes-fuenf-augen-sehen-mehr-1.1807258

www.whatreallyhappened.com, kein Datum *www.whatreallyhappened.com.* [Online] Available at: http://www.whatreallyhappened.com/RANCHO/POLITICS/ECHELON/echelon.html

ZeitOnline, 2013. *www.zeit.de.* [Online] Available at: http://www.zeit.de/news/2013-07/01/geheimdienste-hintergrund-wie-prism-im-detail-funktioniert-01150602

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides Statt, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen oder direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

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

Ort, Datum Unterschrift (Vor- und Nachname)