Im Namen der: Beschwerdeführer
Name: Ian Brown
Nummer: 1
Beweisstück: IB1
Datum: 27. September 2013

Beschwerde Nr.: 58170/13

VOR DEM EUROÄISCHEN GERICHTSHOF FÜR MENSCHENRECHTE

(1)BIG BROTHER WATCH;
(2)OPEN RIGHTS GROUP;
(3)ENGLISH PEN;
(4)DR. CONSTANZE KURZ

Beschwerdeführer

- v -

VEREINIGTES KÖNIGREICH

Beschwerdegegner

ZEUGENAUSSAGE VON
DR. IAN BROWN

Ich, Doktor Ian Brown, **Oxford Internet Institute, University of Oxford, 1 St. Giles', Oxford OX1 3JS, Vereinigtes Königreich**, mache folgende Aussage:

EINFÜHRUNG

1. Ich bin Senior Research Fellow am Oxford Internet Institute der Universität Oxford und Stellvertretender Direktor am Cyber Security Centre der Universität Oxford. Ich mache diese Aussage, um die Beschwerde der Antragsteller zu unterstützen und um das

Gericht bei der Klärung von Fragen, die in meinen Fachbereich fallen, zu unterstützen. Ich versichere, dass die Inhalte dieser Aussage, die auf meinen Kenntnissen basieren, wahr sind. Für jene Inhalte, die nicht meinen direkten Kenntnissen entspringen, habe ich die Quellen der relevanten Informationen geprüft und versichere, dass sie nach meinem besten Wissen und meiner Überzeugung wahr sind.

2. Ich gehöre als Distinguished Scientist der Association for Computing Machinery (ACM) an und bin Mitglied (Chartered Fellow) des British Computer Society Chartered Institute (BCS). Ich gehöre außerdem dem Fachausschuss für Technologie bei der Datenschutzbehörde des Vereinigten Königreichs an (UK Information Commissioner's Technology Reference Panel). Ich war als Berater für das Ministerium für Innere Sicherheit der Vereinigten Staaten (DHS), das Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (UNOCD), den Europarat, die OECD, JP Morgan, die BBC, die Europäische Kommission, das Cabinet Office der britischen Regierung und andere große Behörden und Unternehmen tätig. Ich bin Berater der Open Rights Group und war in der Vergangenheit Beauftragter und Berater einer Reihe von Nichtregierungsorganisationen. Ich verfüge über besondere Sachkenntnis in den Bereichen Internettechnologien, Cybersicherheit, Überwachung und Regulierung. Mein ausführlicher akademischer Lebenslauf steht bei Bedarf zur Verfügung.

3. In dieser Aussage gehe ich kurz auf folgende Punkte ein:

   3.1. Den Anstieg der Internetüberwachung im Vereinigten Königreich

   3.2. Die unlängst veröffentlichten Enthüllungen des Guardian über die Aktivitäten der britischen Regierung im Bereich der Internetüberwachung und die Reaktion der britischen Regierung darauf

   3.3. Wie die offengelegten Programme aller Wahrscheinlichkeit nach funktionieren

   3.4. Die Rechtsgrundlage für diese Programme nach britischem Recht

3.5. Ein kurzer Kommentar zur Tragweite dieser Informationen

4. Die in jüngster Zeit enthüllten Informationen beziehen sich auch auf Programme der US-amerikanischen National Security Agency („**NSA**"). Meiner Kenntnis nach wird Cindy Cohn von der Electronic Frontier Foundation in einer separaten Zeugenaussage detailliert darauf eingehen. Ich werde dies dennoch nachfolgend ebenfalls kurz kommentieren, da die britische Zusammenarbeit mit den US-Programmen ebenfalls für die obengenannten Sachverhalte relevant ist.

5. Mir wird nun ein mit „IB1" beschriftetes, paginiertes Konvolut beglaubigter Dokumente überreicht und gezeigt. Sämtliche Verweise auf Dokumente beziehen sich in dieser Aussage, sofern nicht ausdrücklich anders festgestellt, in der Form [**IB1/Tab/Seite**] auf das Konvolut IB1.

INTERNETÜBERWACHUNG IM VEREINIGTEN KÖNIGREICH

6. Die Internetüberwachung obliegt im Vereinigten Königreich primär dem Government Communications Headquarters (GCHQ). Der GCHQ liefert der britischen Regierung Signals Intelligence (Fernmelde- und elektronische Aufklärung), kurz ‚SIGINT'. Seine Geschichte reicht bis vor den Ersten Weltkrieg zurück, als verschiedene Vorgängerorganisationen deutsche Nachrichten abfingen. Die Dechiffrierung verschlüsselter Nachrichten durch die Government Code and Cypher School spielte eine wichtige Rolle für den Ausgang des Zweiten Weltkriegs. Der GCHQ wurde in den Jahren darauf und insbesondere durch den aufkommenden Kalten Krieg für die folgenden Regierungen ein immer wichtigerer Lieferant geheimer Informationen. Mit der wachsenden Verbreitung des Personal Computing und des Internets hat der GCHQ seine Rolle und den Umfang seiner Aktivitäten kontinuierlich weiter ausgebaut.

7. In den vergangenen 20 Jahren hat sich das Internet von einem akademischen Spezialisten-Netzwerk für Forscher zu einem Kommunikationsapparat des Mainstream gewandelt. Laut der Statistikbehörde (Office for National Statistics) der britischen Regierung verfügten 83% aller britischen Haushalte (21 Millionen) im Jahr 2013 über Internetzugang. Neben den Entwicklungen im Bereich der Kommunikationstechnologien, die das Wachstum des Internets vorangetrieben haben, sehen wir auch weiter exponentielle Zuwächse in der Rechen- und Datenspeicherungskapazität. Die Rechenleistung hat sich alle zwei Jahre

grob verdoppelt und seit 1965 ungefähr vermillionenfacht. Die Bandbreite und die Speicherkapazitäten wachsen sogar noch schneller.

8. Mit der zunehmenden Nutzung des Internets ist auch der Bedarf von Polizei und Geheimdiensten, Internetanwender zu kontrollieren, gewachsen. Zu den neuen Überwachungstechnologien, die diesen Bedarf bedienen, gehören etwa „Wanzen" und Tracing-Technologien, die Zugang zu den geografischen Positionen von Mobiltelefonen ermöglichen und sich wie ferngesteuerte Abhörgeräte verhalten; oder (selbst mit Antiviren-Programmen) schwer aufspürbare „Spyware", die Behörden unbemerkt auf PCs von Verdächtigen installieren und die es ermöglicht, heimlich und aus der Ferne sämtliche Onlineaktivitäten eines Verdächtigen, seine Passwörter und E-Mails, sogar die Kamera und das Mikrophon im PC zu überwachen. Eine derartige Überwachungstechnologie ist naturgemäß in ihrem Einzugsbereich relativ zielgerichtet. Andere Überwachungstechnologien haben es dem GCHQ jedoch ermöglicht, weitaus weniger zielgerichtet und vielmehr sehr umfassend Aufzeichnungen von Milliarden von Telefon- und E-Mail-Aktivitäten aufzunehmen, zu filtern und auszuwerten. Im selben Maß ist die sogenannte „Dataveillance", die Datenüberwachung, gewachsen, also die massenweise Überwachung von „Datenspuren", die User bei ihren Nutzungsvorgängen im Internet hinterlassen per Zugriff auf Kommunikationsdaten und andere Datenbestände, in denen solche Spuren enthalten sind. Es ist inzwischen klar, dass sowohl E-Mail-Inhalte als auch Metadaten auf diese Weise überwacht wurden.

9. Laut dem Cheftechnologen der US-Aufsichtsbehörde (Federal Trade Commission, FTC), Professor Edward Felten, können Metadaten häufig „proxy for content", stellvertretend für den Inhalt, stehen. Mit seinem Einverständnis lege ich dieser Erklärung als Anlage **IB1/1/S.543-577** eine Kopie seiner Erklärung in einem laufenden Verfahren bei, das die Amerikanische Bürgerrechtsunion American Civil Liberties Union (ACLU) in Verbindung mit einigen der jüngsten Presseenthüllungen in den USA angestrebt hat. In diesem Dokument nennt er als Beispiel Anrufe an Notruf-Hotlines für Opfer von häuslicher und sexueller Gewalt, Menschen mit Suizidgedanken, Suchtkranke usw., sowie SMS-Spenden für bestimmte gemeinnützige Zwecke. Er erklärt:

> „46. Auch wenn es schwer ist, sensible Informationen, die Telefon-Metadaten über Einzelpersonen offenlegen können, zusammenzufassen, können sie außerordentlich viel über unsere Gewohnheiten und unsere Kontakte aussagen. Unser Anrufverhalten kann Aufschluss darüber geben, wann wir wach sind und wann wir schlafen; es kann unsere Religion verraten, wenn eine Person etwa regelmäßig am Sabbat nicht telefoniert oder an Weihnachten besonders viele

Anrufe tätigt; unsere Arbeitsgewohnheiten und unser Sozialverhalten, die Zahl unserer Freunde und selbst unsere private und politische Zugehörigkeit aufzeigen."

10. Er bemerkt außerdem zutreffend, dass gesammelte Metadaten noch weitaus mehr enthüllen können, wenn er im Folgenden feststellt:

> „48. Eine Auswertung von Metadaten in diesem Ausmaß kann das Netzwerk jener Personen, mit denen wir kommunizieren, sichtbar machen – das, was man gemeinhin einen Social Graph nennt. Mit einem Social Graph, der sämtliche Telefonate einer Organisation im Lauf der Zeit aufzeichnet, ließe sich ein Verzeichnis von Kontakten generieren, das einen substantiellen Teil der Mitglieder dieser Gruppe, ihrer Wohltäter, politischen Fürsprecher, vertraulichen Quellen usw. enthielte. Die Metadatenanalyse dieser einzelnen Anrufer könnte in einem weiteren „Schrittchen" wiederum dabei helfen, jeden einzelnen zu klassifizieren, was schließlich zu einer detaillierten Aufschlüsselung aller Beziehungen und Verbindungen einer Organisation führen würde …
>
> …52. Stellen Sie sich folgendes hypothetisches Beispiel vor: Eine junge Frau ruft ihren Frauenarzt an; danach ruft sie sofort ihre Mutter an; dann einen Mann, mit dem sie in den vergangenen Monaten wiederholt nach 23 Uhr telefoniert hat; und schließlich ein Familienplanungszentrum, das auch Abtreibungen vermittelt. Daraus lässt sich eine Geschichte ableiten, die durch die Aufzeichnung eines einzelnen Anrufs nicht so offensichtlich wäre.
>
> 53. Metadaten, die einen Anruf an ein Wettbüro erkennen lassen, legen vielleicht nahe, dass die Zielperson eine Wette abgibt; die Analyse von Metadaten über einen längeren Zeitraum könnte dagegen offenlegen, dass die Zielperson ein Problem mit Spielsucht hat, insbesondere, wenn die aufgezeichneten Anrufe auch wiederholte Telefonate mit Kleinkreditanbietern enthalten.

11. Er weist ferner darauf hin, dass die Kontrolle von Massendaten – sogenannten „Big Data" – einer noch aufdringlicheren Überwachung den Weg weist. Ich stimme ihm zu, wenn er festhält: „Die Macht der Metadatenanalyse und ihr potentieller Einfluss auf die Privatsphäre von Einzelpersonen nimmt entsprechend der Menge der gesammelten Daten zu." Daraus leitet er folgende Schlussfolgerung ab:

> „64. Die Beeinträchtigung der Privatsphäre durch die Sammlung aller Kommunikationsmetadaten einer einzelnen Person über lange Zeiträume hinweg hat eine andere Qualität als wenn dies nur über eine Zeitspanne von einigen Tagen geschieht. Ebenso ist die Beeinträchtigung der Privatsphäre, wenn die Anrufe jedes einzelnen US-Amerikaners aufgezeichnet werden, sehr viel größer als wenn Daten über eine einzelne Person oder selbst eine Gruppe von Personen gesammelt werden. Die massenhafte Erfassung ermöglicht es der Regierung nicht nur, Informationen über mehr Menschen zu erhalten, sondern erlaubt ihr auch, neue, bis dahin private Fakten, an die sie durch die einfache Sammlung von Informationen über einige spezifische Einzelpersonen nicht gelangt wäre, in Erfahrung zu bringen.

12. Professor Felten beschreibt den Prozess der Metadatenanalyse folgendermaßen:

> „22 … die Struktur von Metadaten macht es sehr einfach, riesige Datensätze mit hochentwickelten Data-Mining-Programmen und Programmen zur Linkanalyse auszuwerten. Diese Analyse ist in den vergangenen 35 Jahren durch die technologischen Fortschritte in der elektronischen Datenverarbeitung, der elektronischen Datenspeicherung und im Bereich Digital-Data-Mining enorm erleichtert worden. Diese Fortschritte haben unsere Möglichkeiten, persönlichen Kommunikationsverkehr einschließlich Metadaten aufzunehmen, zu speichern und auszuwerten, radikal begünstigt.
>
> 23. Innovative Neuerungen in der elektronischen Speicherung erlauben uns heute, kostengünstig und effizient riesige Datenmengen zu unterhalten. Die Möglichkeit, Daten in diesem Umfang zu speichern, ist an sich eine beispiellose Entwicklung – die eine digitale Aufzeichnung von Verlaufsdaten ermöglicht, wie sie Einzelpersonen, Unternehmen oder Regierungen bislang nicht ohne Weiteres möglich war.
>
> 24. Diese nie dagewesenen Kapazitäten zur Datenspeicherung haben zu ganz neuen Möglichkeiten bei der Nutzung digitaler Aufzeichnungen geführt. Hochentwickelte Anwendungen erlauben die Analyse großer Datensätze, um darin enthaltene Muster und Zusammenhänge zu identifizieren, einschließlich persönlicher Daten, Gewohnheiten und Verhaltensweisen. Daraus resultiert, dass einzelne Daten, die bisher kaum das Potenzial hatten, private Informationen zu enthüllen, jetzt im Verbund sensible Details über unseren Alltag offenlegen können – Details, die wir nie mitzuteilen erwartet oder gewünscht haben.

13. Als Beispiel führt er die kommerziell erhältliche Analysesoftware Pen-Link und die IBM-Software Analyst's Notebook an:

> „27…Pen-Link ist in der Lage, automatisierte ‚Call Pattern'-Analysen (Analysen von Anrufmustern) durchzuführen, die ‚automatisch Situationen identifizieren, in denen bestimme Sequenzen von Anrufen auftreten, außerdem wann dies der Fall ist und wie oft, zwischen welchen Nummern und zwischen welchen Namen.' Wie das Unternehmen in seinen Produktbroschüren schreibt, kann diese Anwendung, dem Analysten dabei helfen, festzustellen, wie oft Joe Steve angepiepst, Steve daraufhin Barabara angerufen und danach Joe zurückgerufen hat.'"

Abbildung 1: Screenshot des IBM-Programms Analyst's Notebook

14. Professor Felten überträgt diese Erkenntnisse auf eine Organisation wie die Amerikanische Bürgerrechtsunion ACLU:

> „55. Im Falle einer Organisation wie der ACLU können gesammelte Metadaten sensible Informationen über interne Abläufe sowie externe Kontakte und Beziehungen offenlegen. Die Metadatenspuren der ACLU spiegeln ihre Beziehungen mit Klienten, ihre Kontakte zu Vertretern der Legislative, Mitgliedern und potenziellen Whistleblowern, die die ACLU anrufen, wider. Eine Second-Order-Analyse der Telefon-Metadaten der Kontaktpersonen der ACLU würde über jeden dieser Kontakte weitere Einzelheiten erbringen. Wenn zum Beispiel ein Angestellter der Regierung plötzlich mehrere Telefonnummern verschiedener Medienvertreter anwählt, anschließend die ACLU und dann vielleicht einen Anwalt, der auf Strafrecht spezialisiert ist, anruft, lassen sich daraus Rückschlüsse ziehen, die diese Person als potenziellen Whistleblower identifizieren. Würde die Regierung die Anrufgewohnheiten der ACLU-Mitglieder untersuchen, könnte sie auch ein detailliertes Profil der Art von Menschen, die die Ziele der ACLU unterstützen, erstellen …
>
> … 57. Mit der Analyse von Metadaten könnten sogar juristische Strategien von Klägern aufgedeckt werden. Die Durchsicht der ACLU-Telefon-Metadaten könnte zum Beispiel zeigen, dass die Anwälte der Organisation etwa eine ungewöhnliche große Zahl von Menschen, die in einem bestimmten Staat als sexuelle Straftäter registriert sind, kontaktiert haben, oder eine scheinbar beliebige Auswahl von Eltern farbiger Kinder in einem Bezirk mit rassengetrennten Schulen, oder Personen, die in einer bestimmten Stadt oder Region mit einer Protestbewegung in Verbindung gebracht werden."

Meiner Meinung nach gelten diese Beobachtungen ebenso für die Antragsteller in diesem Fall, da sie sich für den Schutz von Bürgerrechten einsetzen und dies oft in anonymem Auftrag tun.

15. Die Enthüllungen der jüngsten Zeit verschaffen uns ein sehr viel besseres Verständnis vom Ausmaß der Internetüberwachungsprogramme des GCHQ. Ihre Größenordnung und ihre Verbreitung haben viele Experten überrascht. Unter den ins Visier genommenen Zielen finden sich auch ausländische Regierungen, selbst jene, die mit den USA und dem Vereinigten Königreich verbündet sind. Dennoch wissen wir noch immer nicht, welche Bürger überwacht worden sind und aus welchen Gründen dies geschehen ist. Dies unterstreicht wie wichtig es ist, zu gewährleisten, dass bekannte Praktiken und Systeme den Gesetzen entsprechen und verhältnismäßig sind. Nach meinem Verständnis ist dies der Zweck der Beschwerde der Antragsteller.

16. Vor den Enthüllungen durch den Guardian waren viele Experten der Auffassung, dass das anhaltend dramatische Wachstum des Internetverkehrs die Kapazitäten der Signals-Intelligence-Agenturen, diese Datenfluten zu kontrollieren, übersteige. Wir wissen jetzt, dass die NSA und der GCHQ Technologien entwickelt haben, die große Mengen an Internetverkehr aufzeichnen und filtern können; aus technologischer Sicht gibt es keinen Grund, warum sie dazu nicht auch weiterhin in der Lage sein sollten.

ENTHÜLLUNGEN DER JÜNGSTEN ZEIT ZUR INTERNETÜBERWACHUNG IM VEREINIGTEN KÖNIGREICH

17. In den Medien gab es jüngst eine ganze Reihe von Enthüllungen über Internet-Überwachungsprogramme im Vereinigten Königreich und in den USA. Der größte Teil davon resultierte aus den Offenlegungen des früheren Booz-Allen-Hamilton-Angestellten Edward Snowden. Nach meinem Verständnis liefern diese Enthüllungen die Grundlage für die Hauptbeschwerdepunkte der Antragsteller in diesem Verfahren. Ich habe die Enthüllungen nachfolgend in Form eines Zeitstrahls angeführt:

> **6. Juni 2013** – Das US-amerikanische Gericht für die Überwachung der Auslandsgeheimdienste (Foreign Intelligence Surveillance Court, FISC) verfügt, dass die Telefongesellschaft Verizon Corporation Metadaten zu Telefonaten von US-Bürgern auszuhändigen hat. („**IB1/2/S.578-587**")
> **6. Juni 2013** – Details des NSA-Programms PRISM werden bekannt, die

nahelegen, dass die NSA direkten Zugriff auf die Server großer US-Internetkonzerne erhielt. („**IB1/2/S.594-600**")

7. Juni 2013 – Präsident Obama ordnet an, dass die USA Listen potenzieller ausländischer Ziele für Cyber-Angriffe erstellen sollen. („**IB1/2/S.601-605**")

8. Juni 2013 – Enthüllung über das NSA-Programm „Boundless Informant", das globale Überwachungsdaten zusammenfasst. („**IB1/2/S.606-618**")

9. Juni 2013 – Edward Snowden gibt sich als Quelle der Enthüllungen zu erkennen. („**IB1/2/S.619-625**")

13. Juni 2013 – Die NSA hackt zivile Computernetze in Hongkong und auf dem chinesischen Festland. („**IB1/2/S.626-629**")

16. Juni 2013 – Die NSA und Großbritannien (Government Communications Headquarters (GCHQ)) überwachen ausländische Diplomaten. („**IB1/2/S.630-634**")

19. Juni 2013 – „Project Chess": Skype gestattet der NSA Zugang. („**IB1/2/S.635-638**")

20. Juni 2013 – Dokumente des FISC beschreiben, wie die NSA ohne richterliche Anordnung auf US-Daten zugreifen darf. („**IB1/2/S.639-657**")

21. Juni 2013 – Enthüllung über das GCHQ-Programm „Tempora", das Glasfaserkabel anzapft und Daten speichert. („**IB1/2/S.658-678**")

27. Juni 2013 – Enthüllung über Programme, mit denen die NSA Metadaten von Internetnutzern online ‚erntet' und wie vom GCHQ gesammelte Metadaten an die NSA übermittelt werden. („**IB1/2/S.679-681**")

29. Juni 2013 – Die USA hören EU-Büros in New York, Washington DC und Brüssel sowie Botschaften der europäischen Regierung ab. („**IB1/2/S.682-683**")

30. Juni 2013 – Die NSA überwacht monatlich 500 Millionen Verbindungen in Deutschland. („**IB1/2/S.684-685**")

6. Juli 2013 – Die USA nutzen das Programm „Fairview", um über Kooperationen ausländischer Telekommunikationsanbieter mit amerikanischen Anbietern Zugang zu Internet- und Telefondaten ausländischer Bürger zu erhalten. („**IB1/2/S.686-690; IB1/2/S.693-696**")

8. Juli 2013 – Australische Überwachungsstationen unterstützen die NSA bei der Datensammlung. („**IB1/2/S.691-692**")

10. Juli 2013 – Weitere Details über das NSA-Programm „Upstream", das

Glasfaserkabel anzapft, werden bekannt. („**IB1/2/S.697-701**")

20. Juli 2013 – Der deutsche Bundesnachrichtendienst arbeitet ebenfalls dem NSA-Netzwerk zur Datensammlung zu. („**IB1/2/S.702**")

31. Juli 2013 – Das NSA-Programm „Xkeyscore" verwendet zur Datensammlung über 500 Server in der ganzen Welt. („**IB1/2/S.703-713**")

1. August 2013 – Die NSA hat dem GCHQ zwischen 2010 und 2013 rund 155 Mio. US-Dollar gezahlt. („**IB1/2/S.714-718**")

2. August 2013 – Der GCHQ verfügt über direkten Zugang zu den Glasfaserkabel-Netzen von sieben Telekommunikationsfirmen (darunter British Telecommunications, Vodafone und Verizon). Der GCHQ bezahlt Compliance-Kosten. („**IB1/2/S.719-736**")

9. August 2013 – Abwandlungen des Grundsatzes der Datenminimierung durch die NSA gestatten möglicherweise die Durchsicht der Daten von US-Bürgern ohne richterliche Anordnung. („**IB1/2/pS.737-741**")

16. August 2013 – Verstöße der NSA gegen US-Gesetze und interne Bestimmungen. („**IB1/2/S.742-743**")

21. August 2013 – Die NSA gibt drei unter Verschluss gehaltene gerichtliche Stellungnahmen frei, die zeigen, dass auch zahlreiche US-Bürger, die nicht mit Terrorismus in Verbindung gebracht wurden, überwacht wurden. („**IB1/2/S.749-752**")

23. August 2013 – Eine GCHQ-Station im Nahen Osten fängt Informationen aus Glasfaserkabeln ab. („**IB1/2/S.753-755**")

30. August 2013 – Die NSA zahlt für den Zugang zu Glasfaser-Hubs hunderte Millionen US-Dollar an private Unternehmen. („**IB1/2/pp.756-757**")

30. August 2013 – Einzelheiten über die 231 Cyber-Angriffe seitens der USA im Jahr 2011 werden bekannt. („**IB1/2/S.758-763**")

31. August 2013 – Die NSA hat auch Al-Jazeera überwacht. („**IB1/2/S.766**")

1. September 2013 – Die NSA hat auch die brasilianischen und mexikanischen Präsidenten überwacht. („**IB1/2/S.767-775**")

5. September 2013 – NSA und GHCQ haben 2010 erfolgreich mehrere Verschlüsselungstechnologien geknackt („**IB1/2/S.776-806**")

7. September 2013 – Die NSA ist in der Lage, Smartphone-Daten auszuspähen, einschließlich E-Mails, Adressbüchern, Notizen und Standorten. („**IB1/2/S.807**")

9. September 2013 – Die NSA hat auch private Netzwerke von Google, Petrobas, dem französischen Außenministerium und SWIFT überwacht – dies widerspricht früheren Behauptungen, dass die NSA nicht in Wirtschaftsspionage verwickelt gewesen sei. („**IB1/2/S.808-811**")

11. September 2013 – Die NSA tauscht Daten mit Israel aus. Die entsprechende gemeinsame Absichtserklärung wird vollständig veröffentlicht. („**IB1/2/S.812-822**")

16. September 2013 – Ein NSA-Programm überwacht Finanznetzwerke, einschließlich VISA und SWIFT, dies verstößt gegen das Abkommen mit der EU aus dem Jahr 2010. („**IB1/2/S.823-825**")

18. Die signifikantesten Enthüllungen betreffen das britische Tempora-Programm, das PRISM-Programm der NSA, offensive Operationen und das Knacken kryptographischer Schutzsysteme durch technische und sogenannte ‚HUMINT'-Maßnahmen (Human Intelligence – Erkenntnisgewinnung aus menschlichen Quellen).

REAKTIONEN DER BRITISCHEN REGIERUNG

19. Die Reaktionen der britischen Regierung und des Parlaments auf diese Enthüllungen waren zurückhaltend. Am 7. Juni 2013 veröffentlichte der parlamentarische Ausschuss für Nachrichten- und Sicherheitsdienste (Intelligence and Security Committee, ISC) eine kurze Erklärung, die besagte, dass die Vorwürfe bezüglich der britischen Nutzung des NSA-Programms PRISM untersucht würden (zu diesem Zeitpunkt waren die Details über das Programm Tempora noch nicht bekannt geworden). Darauf folgte am 10. Juni 2013 eine Erklärung des Außenministers William Hague vor dem Parlament („**IB1/3/S.826-830**"), in der er auf die Enthüllungen einging. Er bekräftigte dabei die Aktivitäten des GCHQ und deren Rechtmäßigkeit, ging jedoch weder auf den Rechtsrahmen für diese Aktivitäten ein, noch auf die Aufsichtsmechanismen die dabei zur Anwendung kamen.

20. Am 1. Juli 2013 verschob der ISC eine geplante Anhörung der Geheimdienste über die Sommerpause hinaus; derweil gab der Vorsitzende des Ausschusses, Sir Malcolm Rifkind MP, am 17. Juli 2013 eine dreiseitige Erklärung heraus („**IB1/3/S.831-833**"), in der er über eine vom ISC eingeleitete Untersuchung der Vorwürfe bezüglich PRISM berichtete. Die Untersuchung sprach den GCHQ auf

Grundlage der geprüften Beweise von dem Vorwurf frei, mit der Nutzung von PRISM gesetzliche Bestimmungen umgangen zu haben. Der Bericht traf jedoch keine Aussage darüber, welche Mechanismen zur Anwendung gekommen waren und schien einzuräumen, dass das gesetzliches Rahmenwerk mangelhaft war, was zur Festlegung geheimer Zusatzregelungen durch den GCHQ- geführt habe:

> „7. In manchen Teilen ist die Gesetzgebung sehr allgemein gehalten, so dass zurecht detailliertere Richtlinien und Vorgehensweisen die Arbeit des GCHQ betreffend eingerichtet wurden, um deren Übereinstimmung mit den Vorgaben des Human Rights Act 1998 sicherzustellen…."

Der ISC kündigte an, dass diese Sachverhalte weiter geprüft würden. In einem Pressebriefing zu dem Bericht (vgl. *Inquiry into snooping laws as committee clears GCHQ,* Guardian, 18. Juli 2013 („**IB1/3/S.834-836**")) räumte der Vorsitzende des ISC ein, dass die Untersuchung sich nur auf geheimdienstliche Informationen über spezifisch verdächtigte Einzelpersonen konzentriert hatte, die der GCHQ mit entsprechenden Anordnungen gezielt aus den USA angefordert hatte. Der Bericht ging demnach nicht darauf ein, ob PRISM-Daten über andere Wege mit Großbritannien geteilt wurden, etwa im Rahmen von Anordnungen allgemeinerer Art oder indem die USA dem Vereinigten Königreich unaufgefordert Informationen zur Verfügung stellten. Die Untersuchung befasste sich auch nicht mit *Metadaten* aus Kommunikationen, die durch PRISM erfasst worden waren; untersucht wurde lediglich die Bereitstellung von Informationen zu *Inhalten*.

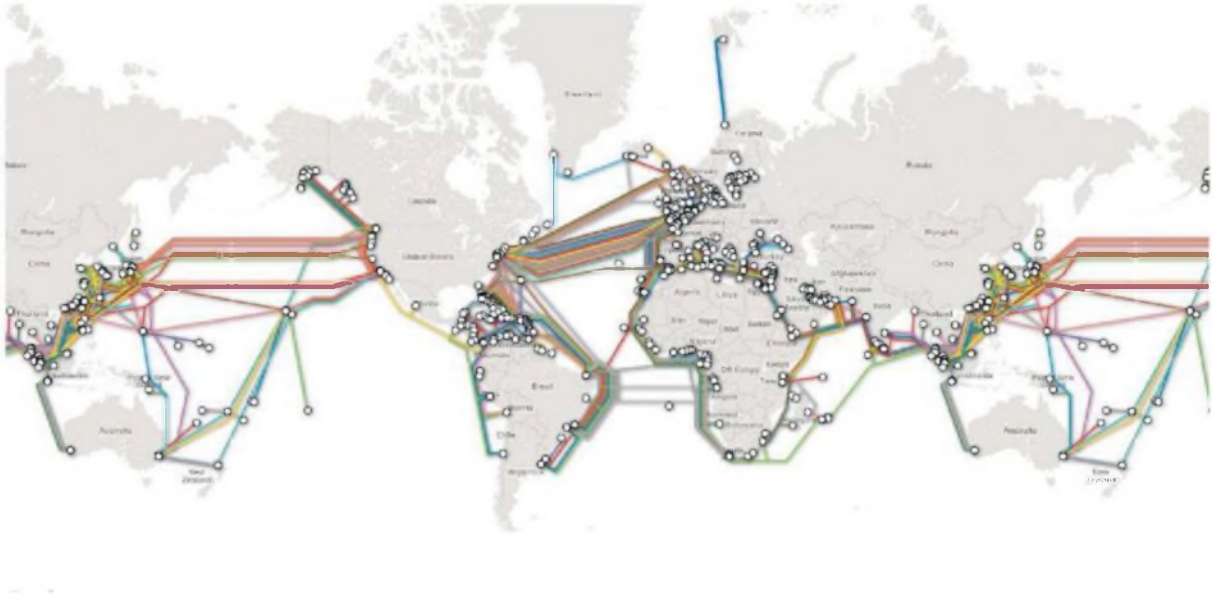
21. Seit damals ist es kontinuierlich zu weiteren Enthüllungen gekommen, insbesondere jenen vom 21. Juni 2013 bezüglich des Programms Tempora, es wurden jedoch kaum weitere öffentliche Kommentare abgegeben. Berichten zufolge vernichtete der *Guardian* am 20. Juli 2013 auf Anordnung der Regierung Festplatten, die GCHQ-Dateien enthielten („**IB1/2/S.744-748**"). In einer schriftlichen Erklärung des High Court zur Festsetzung des Lebenspartners eines der Guardian-Journalisten erklärte der stellvertretende nationale Sicherheitsberater für die Geheimdienste im Kabinett (Deputy National Security Adviser for Intelligence) Oliver Robbins, dass „*die nationale Sicherheit Großbritanniens durch die Enthüllungen der Medien faktisch bereits konkreten Schaden genommen habe*" („**IB1/2/S.764**"), untermauerte diese Behauptung jedoch nicht weiter.

DER EINSATZ DER PROGRAMME

Das Programm Tempora

22. Im Bericht des Guardian vom 21. Juni 2013 wurde enthüllt, dass der GCHQ an Glasfaserkabeln, die Internetdaten nach und aus dem Vereinigten Königreich leiten, Abfangvorrichtungen installiert hatte. Zu diesen im Vereinigten Königreich befindlichen Leitungen zählen auch transatlantische Kabelverbindungen zwischen den USA und Europa. Es wird davon ausgegangen, dass die Abfangvorrichtungen in mindestens 200 „Wellenlängen" (Datenkanälen) auf den Glasfaserkabeln platziert wurden, bis nah an die Punkte heran, an denen sie an die Küste gelangen. Dies scheint unter heimlicher Mitarbeit der Unternehmen, die die Kabel unterhalten, geschehen zu sein. Laut *Guardian* war das Programm seit 2011 im Einsatz.[1]

23. Weltweit verlegte Unterseekabel sind die Hauptschlagadern des globalen Internets. Gelingt es, sie anzuzapfen, werden sie zur „Schnellstraße" totaler Internetüberwachung, ohne, dass einzelne Nutzer mit spezielleren Methoden gezielt überwacht werden müssten. Ich lege hier eine Karte vor, die das Aufkommen dieser Kabel weltweit veranschaulicht („**IB1/4/S.848**").[2]

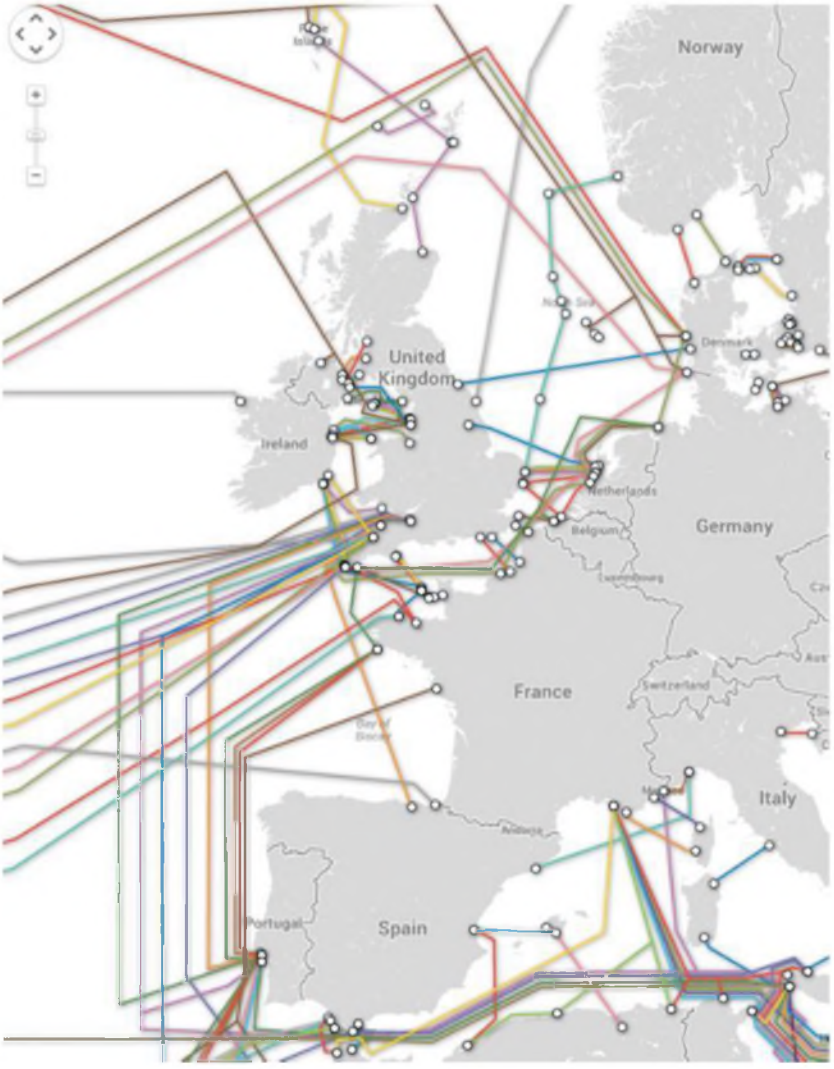


24. Die Überwachung der Kabel, die das Vereinigte Königreich erreichen und verlassen, bedeutet unter anderem, dass große Mengen von Kommunikationen, die den Rest der Welt betreffen, abgefangen werden können. Ein beträchtlicher

[1] *GCHQ taps fibre-optic cables for secret access to world's communications*, The Guardian, 21. Juni 2013 („**IB1/2/S.658-663**")

[2] Reproduktion mit der Erlaubnis von: Submarine Cable map, Telegeography © 2013 PriMetrica, Inc (http://www.submarinecablemap.com)

Teil des externen Internetverkehrs aus dem Rest von Europa führt durch das Vereinigte Königreich, da hier die meisten transatlantischen Glasfaserkabel ankommen. Die Vergrößerung der Karte aus Anlage **IB1/4/S.848** veranschaulicht diese Konzentration.

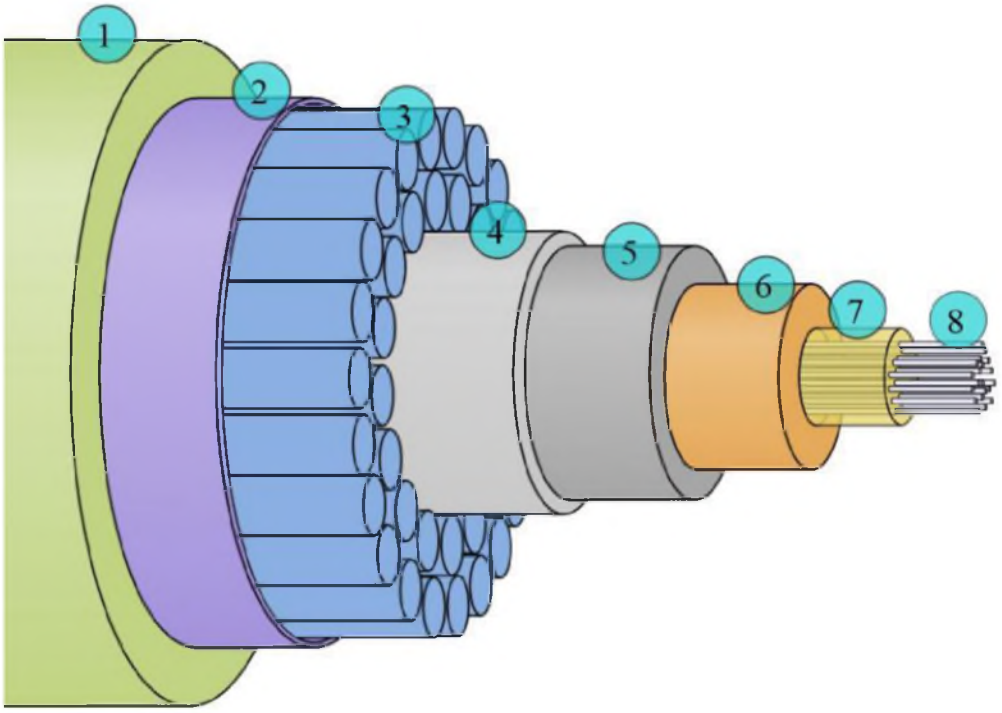


25. Viele ‚innereuropäische' Kommunikationen aus dem Vereinigten Königreich und dem restlichen Europa passieren dennoch Offshore-Kabel, da sie über Internet- und Kommunikationsserver in Übersee (häufig den USA) laufen. Eine anonyme Geheimdienst-Quelle erklärte gegenüber dem *Guardian* zwar, dass „*mit diesem Programm nicht die Absicht verfolgt wird, den nationalen Internetverkehr des Vereinigten Königreichs – also Unterhaltungen zwischen Briten – zu überwachen*“,[3] dies ist für den GCHQ jedoch durchaus möglich und es findet sich

[3] Fn. 1 oben

in den Quellen und Materialien, die der *Guardian* zitiert, auch kein Hinweis darauf, dass der ‚rein inländische' britische Internetverkehr ausgenommen würde.

26. Die Kabel selbst bestehen aus mehreren Schutzschichten, die sich um eine Reihe von Glasfaserkabeln schließen. Üblicherweise sind sie im Durchmesser rund 10 cm dick. Das folgende Schaubild zeigt den Aufbau eines typischen Kabels:



Die Glasfaserkabel selbst sind mit „8" markiert. Die weiteren Schichten setzen sich zusammen aus: 1. Polyethylen, 2. Folie aus Polyethylenterephthalat, 3. verdrillten Stahlseilen, 4. einer Aluminium-Wasserbarriere, 5. Polykarbonat, 6. Kupfer- oder Aluminiumrohr, 7. einer Vaselineschicht.

27. Man kann nur darüber spekulieren, wie genau der GCHQ diese Kabel anzapft. Möglich wäre dies etwa durch den Einsatz eines ‚optischen Splitters', der die Lichtsignale, die durch die Kabel fließen, dupliziert. Ich würde erwarten, dass diese duplizierten Signale über weitere Glasfaserkabel in die Speicher- und Rechenzentren des GCHQ in Bude, Cheltenham usw. umgeleitet werden.

28. Der *Guardian* berichtete, dass *„der GCHQ bis zum Sommer 2011 ca. 200*

Abfangvorrichtungen, je mit einer Übertragungsrate von 10 Gigabit pro Sekunde angebracht hatte."[4] Platziert wurden diese Vorrichtungen meiner Einschätzung nach in der Nähe jener Bereiche, in denen die Kabel an Land gehen (siehe unten). Der *Guardian* berichtete, dass die Abfangvorrichtungen in Kooperation mit den Unternehmen, denen die Kabel gehören, angebracht wurden. Laut dem Bericht *„wurden die Unternehmen für ihre Kooperation bezahlt und der GCHQ unternahm große Anstrengungen, ihre Namen geheim zu halten. Den Firmen wurden sogenannte ‚Sensitive Relationship Teams' (‚Teams für sensible Geschäftsbeziehungen') zugeteilt und Mitarbeiter wurden in einem internen Leitfaden angehalten, die Herkunft von Materialien der ‚speziellen Quelle' in ihren Berichten zu kaschieren, weil die Sorge bestand, dass die Rolle der Unternehmen als Überwachungspartner bei Bekanntwerden , Auseinandersetzungen auf höchster politischer Ebene' verursachen würde."*[5]

29. Der *Guardian* berichtete, dass dieser Überwachungsmodus dem GCHQ potentiell Zugang zu Daten im Umfang von 21 Petabyte am Tag verschafft.[6] Ein Petabyte entspricht ca. 1000 Terabyte (ein Terabyte wiederum entspricht 1000 Gigabyte). Um eine Vorstellung dieser Größenordnung zu vermitteln, hilft ein Vergleich mit der US Library of Congress: Diese verfügte 2009 über 15,3 Millionen abrufbare Online-Dokumente mit einer geschätzten Gesamtgröße von 74 Terabyte. Um diese Datenmenge zu erreichen, rechnete der *Guardian*, müsste die British Library sämtliche Inhalte ihrer gesamten Buchbestände alle 24 Stunden 192 Mal versenden. Berichten zufolge verfügt der GCHQ unter jenen Ländern, die in den geheimen Unterlagen der Gruppe der „Five Eyes" zugeordnet werden (Australien, Neuseeland, Kanada, die USA und das Vereinigte Königreich), mit seinem Programm über den größten Zugriff auf das Internet.[7]

30. Vermutlich fließen die Daten über die Abfangvorrichtung und durch weitere Glasfaserkabel in die Überwachungsstationen des GCHQ. Dort werden die Informationen Berichten zufolge über „Internet Buffer" des GCHQ zwischengespeichert.[8] Dabei dürfte es sich um enorme Speicherzentrenhandeln, die mit den GCHQ-internen Servern durchsucht werden. Selbst bei hoher

[4] Fn. 1 oben
[5] Fn. 1oben
[6] Fn. 1 oben
[7] Fn. 1 oben
[8] Fn. 1oben

Komprimierung und mit den Möglichkeiten moderner Datenspeicherung würde für die Speicherung von Daten in diesem Umfang und für die entsprechenden Anlagen sehr viel Platz benötigt. Es ist deshalb denkbar, dass die Speicherzentren insgesamt oder teilweise in den vier unterirdischen Rechenzentren des GCHQ in Cheltenham untergebracht sind, von denen drei größer als das Fußballfeld des Wembley-Stadion sind,[9] sowie möglicherweise auch an weiteren Standorten des GCHQ in anderen Teilen des Landes. Der *Guardian* nannte den GCHQ-Nebenstandort in Bude (Cornwall) und einen weiteren Standort im Ausland und zitierte in diesem Zusammenhang aus einem internen GCHQ-Dokument, das besagte, dass die NSA finanzielle Mittel in Höhe von 15,5 Millionen Pfund zur Verfügung gestellt habe, um „die Infrastruktur in Bude radikal zu verbessern."[10]

31. Der Guardian berichtete, dass die auf diese Art massenhaft erfassten Internetdaten für bis zu drei Tage (Inhalte) und dreißig Tage (Metainhalte) gespeichert werden könnten.[11] Mit „Inhalten" ist die Gesamtheit aller kommunizierten Daten gemeint (Inhalte von E-Mails oder Kurzmitteilungen, sämtliche besuchte Websites, sämtliche Informationen, auf die durch Social-Media-Netzwerke wie Facebook zugegriffen wurde oder die darüber geteilt wurden, Dokumente die in sogenannten Cloud-Diensten wie Google Docs bearbeitet wurden etc. – sämtliche Online-Aktivitäten von Einzelpersonen, also nicht nur „Kommunikation" im traditionellen Sinn). „Metainhalte" steht für ‚Daten über die Daten', also Daten, die die Umstände der Produktion von versendeten Daten aufzeichnen: Datum und Uhrzeit ihrer Entstehung, die Urheber, den Standort des Computernetzwerks, in dem sie produziert wurden und welche Standards dabei verwendet wurden. Metainhalte können dabei, wie oben ausgeführt, extrem aufschlussreich sein.

32. Im Rahmen des Tempora-Programms werden sowohl Metadaten als auch Inhaltsdaten mit einem Verfahren gefiltert, das man als Massive Volume Reduction (MVR) bezeichnet. Peer-to-Peer-Downloads von Musik, Filmen und Computerprogrammen werden beispielsweise als „Datenverkehr mit hohem Volumen und geringem Erkenntniswert" eingestuft und ausgefiltert, so dass sich das Volumen der Daten um 30% reduziert. Die verbleibenden Daten werden nach Stichwörtern, E-

[9] *GCHQ. Cracking the Code*, BBC Radio 4, 4. April 2010 (http://www.bbc.co.uk/programmes/b00rmssw)
[10] *GCHQ: inside the top secret world of Britain's biggest spy agency*, The Guardian, 1. August 2013 („**IB1/2/S.723-736**")
[11] Fn. 1oben

Mail- oder anderen Adressen, Namen, Pseudonymen oder Telefonnummern von Zielpersonen durchsucht. Wie der *Guardian* berichtete, wurden viele dieser Stichwörter von der US-Regierung bereitgestellt. Dem Bericht zufolge führen der GSCQ und die NSA ca. 40.000, bzw. 31.000 solcher zugeordneter „Selektoren".[12] Eine „Geheimdienst-Quelle" beschrieb den Ablauf dem Guardian gegenüber folgendermaßen:

> „‚Im Grunde genommen ermöglicht uns dieser Prozess, einige wenige Nadeln in einem Heuhaufen zu finden. Wir sehen uns nicht jeden Strohhalm an. Es gibt bestimmte Trigger, mit denen wir große Datenmengen aussortieren oder ignorieren können, so dass nur die Nadeln übrig bleiben. Wir lesen nicht, wie Sie vielleicht den Eindruck hatten, tausende von E-Mails.'
> Er erklärte, dass wenn solche ‚Nadeln' gefunden würden, ein Protokoll angefertigt werde, das der verantwortliche Überwachungsbeauftragte einsehen könne."[13]

33. Ich gehe davon aus, dass dieses Sichten ein teilautomatisierter Prozess ist, der mithilfe einer ständig wachsenden Liste von Stichwörtern und Selektoren vollzogen wird. Unklar ist, wann ein Protokoll angelegt wird – wenn die Person, die mit der Suche betraut ist, bestimmte Informationen liest oder wenn sie nützliche Informationen findet. Da automatisierte Auswertungen großer Datenmengen ohne menschliches Dazutun weniger streng überwacht werden, scheint es jedoch, dass diese Protokolle nicht alle Suchaktivitäten und Überwachungsmaßnahmen in ihrer Gesamtheit abbilden. Angesichts der Berichte des *Guardian* über das XKeyScore-Programm der NSA erscheint es naheliegend, dass auch die Angestellten des GCHQ abgefangene Daten in breiten Kategorien durchsuchen können und dabei mit Anwendungen ähnlich gewöhnlicher Internetsuchmaschinen arbeiten.

34. Große Teile des Internetverkehrs sind heute zum Schutz vor Überwachung verschlüsselt, besonders seit Konzerne wie Google und Microsoft für ihre E-Mail- und anderen Dienste Verschlüsselungen ermöglichen. Dem GCHQ und der NSA ist es Berichten zufolge dennoch gelungen, Daten, die mit üblichen Verschlüsselungsstandards (vgl. für weitere Einzelheiten [48]) geschützt worden waren, zu entschlüsseln. Kommunikationen, die während dieser Suchvorgänge identifiziert werden, müssen deshalb möglicherweise erst entschlüsselt werden, bevor sie gelesen und weiter verwendet werden können.

---

[12] Fn. 1 oben
[13] Fn. 1 oben

35. Laut dem *Guardian* sind rund 300 Mitarbeiter des GCHQ und 250 NSA-Mitarbeiter mit der Sichtung dieser Daten beauftragt. Die Zahl der Menschen, die anschließend Zugang zu diesen Daten bekommen, ist ohne Zweifel sehr viel größer. Der Zugang der NSA zu Daten wird als beträchtlich erachtet. Der *Guardian* berichtete mit Verweis auf Original-Dokumente:

> „Im Jahr 2011 brüstete die Agentur [GCHQ] sich damit, dass die Bereitstellung ihrer Datenbank an die Amerikaner nun ‚unseren einzigartigen Beitrag an die NSA' unterstreiche, der ‚wir Erkenntnisse zu einigen ihrer wichtigsten Überwachungsziele liefern können'. Der GCHQ brüstete sich auch mit der Bereitstellung von 36% aller unverarbeiteten Informationen, die die Briten aus überwachten Computern abgefangen hatten, an die NSA. Die Informationen seien ‚an die NSA weitergeleitet' worden, wie in dem Dokument ausgeführt wird. Weiter steht dort: ‚Wir können nun 100% aller GCHQ-End-Point-Projekte mit der NSA austauschen.' Das legt nahe, dass die NSA potentiell Zugang zu allen gesichteten und verarbeiteten Informationen des GCHQ hat …
> … Im Halbjahresbericht 2010/11 erklärte der GCHQ: ‚Auch unsere Partner haben unser Leistungsvermögen zu spüren bekommen, besonders die NSA ist begeistert von unserer einzigartigen Hilfe im Zusammenhang mit den vereitelten Bombenanschlägen am Times Square und in Detroit.' Wie sich diese Hilfe gestaltete, wurde nicht ausgeführt. Es ist bekannt, dass die NSA keine US-Bürger ausspähen darf; im Fall von Shahzad stellt sich weiterhin die Frage ob der GCHQ das für sie übernommen hat."[14]

36. Es ist nicht bekannt, welchen Gebrauch die NSA von Daten, an die sie durch ihren Zugang zum Tempora-Programm gelangt, macht. Es besteht jedoch eindeutig die Möglichkeit, dass Daten dieser Art in die Hände von Drittstaaten gelangen, seien es Mitglieder des „Five Eyes"-Netzes jener Staaten, die in der Internetüberwachung zusammenarbeiten (USA, Vereinigtes Königreich, Australien, Kanada und Neuseeland) oder Israel. Der *Guardian* berichtete am 11. September 2013, dass die NSA entsprechend einer gemeinsamen Absichtserklärung der beiden Länder dem israelischen Geheimdienst routinemäßig unbearbeitete ‚SIGINT'-Daten zur Verfügung stelle.[15]
37. Ein Artikel im Nachrichtenmagazin Der Spiegel vom 16. September 2013 über die Überwachung globaler Finanztransaktionen durch die NSA und den GCHQ verweist auf eine Passage in einer GCHQ-Veröffentlichung, in der eingeräumt wird, dass der

[14] Fn. 1 oben
[15] *NSA shares raw intelligence including Americans' data with Israel*, The Guardian, 11. September 2013 („**IB1/1/S.812-822**")

Datenaustausch mit den USA extrem weitreichend sei:

> *„… wie aus einem Dokument des britischen Nachrichtendienstes GCHQ hervorgeht, das sich aus rechtlicher Sicht mit „Finanzdaten" und der eigenen Zusammenarbeit mit der NSA befasst. Das Sammeln, Speichern und Teilen der „politisch sensiblen" Daten sei ein tiefer Eingriff, schließlich handle es sich um „Massendaten voller persönlicher Informationen", von denen „viele nicht unsere Ziele betreffen."*[16]

38. Die Tatsache, dass die USA Zugang zu dem Tempora-Programm haben, stellt auch die Möglichkeit in Aussicht, dass das Vereinigte Königreich der NSA – versehentlich oder mit Absicht – bei der Erhebung von Daten über Zielpersonen der USA im Vereinigten Königreich zuarbeitet. Ebenso könnte das Vereinigte Königreich im Gegenzug weitere Aufzeichnungen aus den USA über Bürger aus dem Vereinigten Königreich erhalten, die aus deren britischer Überwachung stammen (ohne dass dafür eine spezifische Anordnung erwirkt worden wäre). Die Aktivitäten der NSA fallen außerhalb der Bestimmungen des britischen Gesetzes zur Telekommunikationsüberwachung (Regulation of Investigatory Powers Act, RIPA), das unten skizziert ist und fallen auch nicht unter die Aufsicht des Geheimdienst- und Sicherheitsausschusses (Intelligence and Security Committee, ISC), des zuständigen Gerichts (Investigatory Powers Tribunal, IPT) oder des Beauftragten für Kommunikationsüberwachung (Interception of Communications Commissioner, IoCC, siehe unten).

39. Die Berichte des Guardian erscheinen mir glaubwürdig. Einige der Einzelheiten sind durch die US-Regierung sowie durch frühere Lecks (einschließlich Äußerungen von früheren leitenden NSA-Beamten wie William Binney) bestätigt worden. Ein Großteil der verwendeten Technologie (wie etwa die optischen Splitter) ist handelsüblich. Die erforderlichen Haushaltsmittel entsprechen den öffentlich bekannten Budgets der Geheimdienste des Vereinigten Königreichs und der USA. Wie vielfach berichtet, hat die NSA kürzlich den Bau eines neuen Rechenzentrums in Utah fertiggestellt, dessen Kosten sich auf schätzungsweise 1,5 bis 2 Milliarden US-Dollar belaufen und das über sehr große Datenspeicherungs- und Rechenleistungsvermögen verfügt.[17]

---

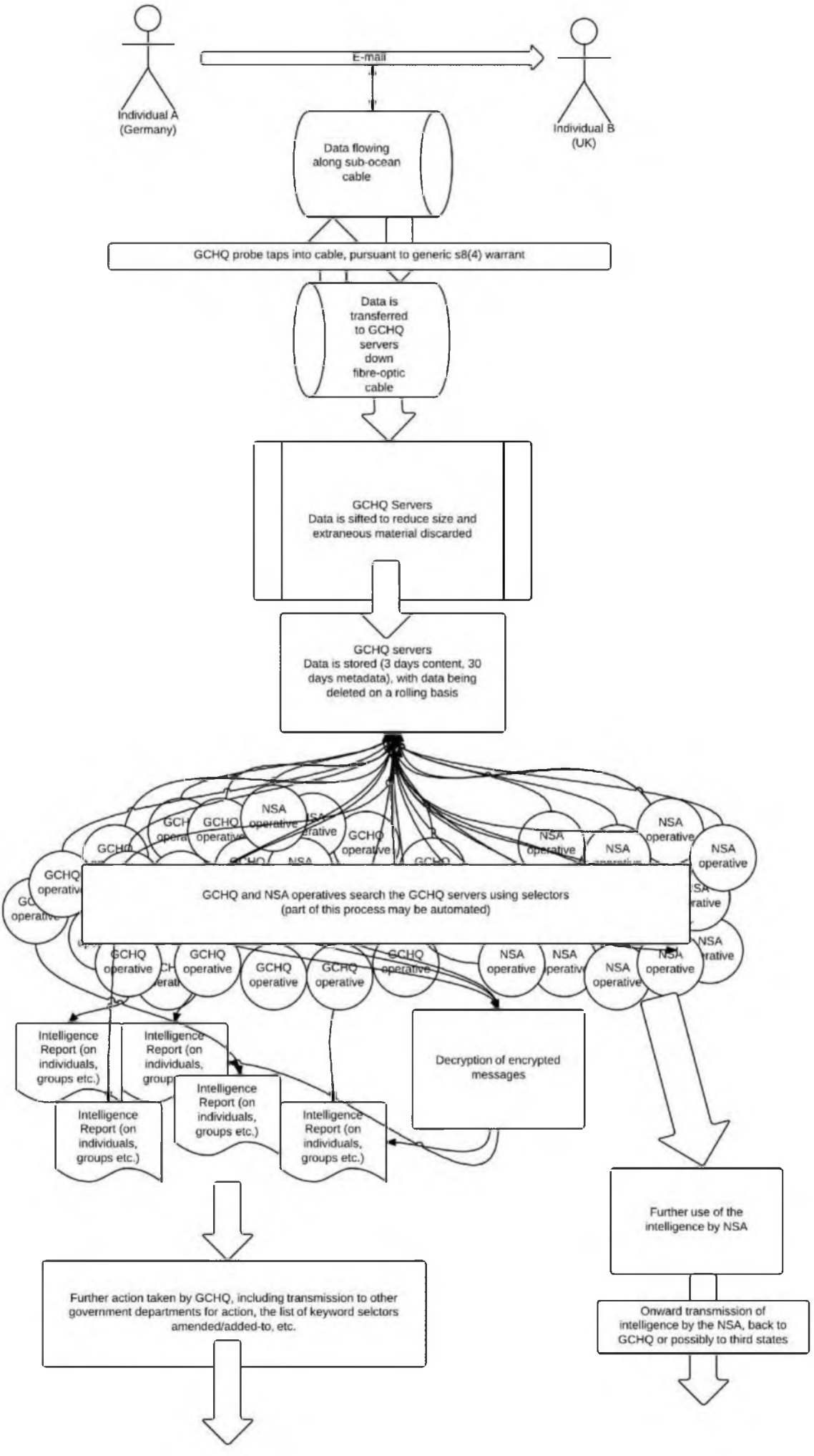
[16] *Folge dem Geld*, Der Spiegel, 16. September 2013 („**IB1/2/S.823-825**")

[17] *Welcome to Utah, the NSA's desert home for eavesdropping on America*, The Guardian, 14. Juni 2013 („**IB1/3/S.844-846**")

40. Ich habe umseitig ein einfaches Schaubild angefertigt, das zusammenfasst, wie der Prozess der Datensammlung mit dem Tempora-Programm aller Wahrscheinlichkeit nach und entsprechend der enthüllten Informationen abläuft. Das Diagramm greift auf meine Kenntnisse in den Bereichen Cybersicherheitstechnologien und Internetüberwachung zurück, basiert jedoch auf den Enthüllungen der jüngsten Zeit, da es nur sehr wenige anderweitige Informationen über die Vorgehensweisen des GCHQ gibt. Das nachfolgende Schaubild ist daher nicht als fundierte Veranschaulichung, sondern als Illustration eines wahrscheinlichen Überwachungsszenarios im Licht der aktuellen Erkenntnisse zu verstehen. In dem Diagramm kommuniziert eine Person in Deutschland mit einer Person im Vereinigten Königreich. Sie versendet eine E-Mail, die Daten fließen dabei, via Servern in den USA, durch Unterseekabel. Die Daten werden mit der Methode, die ich oben bereits erläutert habe, abgefangen und an GCHQ-Server umgeleitet, wo sie zusammen mit weiteren großen Datenmengen zwischengespeichert werden. Die Daten werden nun möglicherweise zunächst ‚ausgesiebt', bevor sie nach Stichworten/Indikatoren durchsucht werden. GCHQ-Mitarbeiter verfassen daraufhin auf Grundlage der Inhalte geheimdienstliche Berichte, die zur weiteren Verwendung an andere Stellen versandt werden. Es ist denkbar, dass ein solcher Kommunikationsvorgang gespeichert oder kopiert wird, bevor die ursprünglichen Inhaltsdaten, mit denen er gleichzeitig zwischengespeichert wurde, gelöscht werden. Die Metadaten stehen dagegen offenbar für einen längeren Zeitraum für eine Durchsuchung zur Verfügung, bevor sie gelöscht werden.

41. Wie der *Guardian* berichtete, besteht die Möglichkeit, dass auch US-Behörden die erhobenen E-Mail-Inhalte nutzen. Auch dies ist in dem Schaubild berücksichtigt. Tatsächlich könnte es sein, dass die USA an der deutschen Person im Diagramm interessiert sind und bereits eine spezifische Anfrage an das Vereinigte Königreich gestellt haben, um auf die mit der Person verbundenen Daten des Tempora-Programms zuzugreifen. Die Person könnte damit in die Liste der Stichwortselektoren zur Sichtung der Tempora-Daten aufgenommen werden. Die USA könnten dadurch Zugang zu weiten Teilen ihrer E-Mail-Inhalte, Kurzmitteilungen und anderen Verkehrsdaten erhalten, dies offenbar in unbegrenztem Umfang. Die Materialien würden gespeichert, möglicherweise auch dauerhaft, wenn absehbar ist, dass sie in Zukunft nützlich sein könnten.

42. Dies zeigt ein weiteres Problem auf, das mit der breit angelegten Sichtung von Tempora-Daten anhand von Stichwörtern einhergeht. In der Praxis können diese zur gezielten Überwachung zahlreicher Personen, die in die rapide wachsenden Stichwortlisten aufgenommen werden, führen. Es scheint jedoch, dass der allgemeine Rechtsrahmen für das Tempora-Programm derartige Durchsuchungen nicht als Abfangen von Inhalten spezifischer Zielpersonen entsprechend des Gesetzes zur Telekommunikationsüberwachung (RIPA) behandelt. Auch wenn RIPA Abschnitt 16 einen gewissen Schutz für Datenmaterial, das mit einer Genehmigung allgemeiner Art entsprechend RIPA Abschnitt 8 Absatz 4 gesammelt wurde und das andernfalls auch mit einer spezifischen Anordnung gesammelt hätte werden können, bietet, greift dieser Schutz nur für Personen, die sich zu diesem Zeitpunkt auf den britischen Inseln befinden. Für das Szenario, das ich hier skizziert habe, besteht mit Ausnahme der zeitlichen Beschränkung der Überwachung auf maximal sechs Monate kein Schutz.


Individual A
(Germany)
E-mail
Individual B
(UK)
Data flowing along sub-ocean cable
GCHQ probe taps into cable, pursuant to generic s8(4) warrant
Data is transferred to GCHQ servers down fibre-optic cable
GCHQ Servers
Data is sifted to reduce size and extraneous material discarded
GCHQ servers
Data is stored (3 days content, 30 days metadata), with data being deleted on a rolling basis
GCHQ and NSA operatives search the GCHQ servers using selectors
(part of this process may be automated)
Intelligence Report (on individuals, groups etc.)
Intelligence Report (on individuals, groups etc.)
Intelligence Report (on individuals, groups etc.)
Intelligence Report (on individuals, groups etc.)
Decryption of encrypted messages
Further action taken by GCHQ, including transmission to other government departments for action, the list of keyword selctors amended/added-to, etc.
Further use of the intelligence by NSA
Onward transmission of intelligence by the NSA, back to GCHQ or possibly to third states

Das Programm Global Telecoms Exploitation

43. Der *Guardian* berichtete auch über das GCHQ-Programm Global Telecoms Exploitation (zur Auswertung der globalen Telekommunikation). Es wird davon ausgegangen, dass auch dieses Programm auf dem Anzapfen von Glasfaserkabeln basiert. Der Guardian berichtete, dass der GCHQ im Jahr 2012 einen Durchsatz von „600 Millionen ‚Telefonereignissen' pro Tag" bewältigte.[18] Ob dies neben Metadaten auch Inhalte einschließt, ist für mich nicht klar. Wie ich jedoch bereits ausgeführt habe, können Metadaten ebenso aufschlussreich sein wie die Inhalte eines Telefonats oder andere relevante Informationen, die mit dem Anruf in Zusammenhang stehen.

Die Nutzung von PRISM seitens des Vereinigten Königreichs

44. Die Einzelheiten des PRISM-Programms sind meines Wissens Gegenstand einer gesonderten Zeugenaussage. Das Programm ermöglicht der NSA Zugang zu Daten auf den Servern bekannter privater, in den USA ansässiger Unternehmen wie Google, Facebook, Microsoft, Apple, Yahoo und das Microsoft-Tochterunternehmen Skype. Diese Unternehmen bestreiten, ‚Hintertüren' zu ihren Servern eingerichtet zu haben; stattdessen leiten sie auf richterliche Anordnungen (große) Mengen spezifischer Daten (die vermutlich den oben beschriebenen „Selektoren" entsprechen) weiter.[19] Das PRISM-Programm fängt also nicht Kommunikation ‚im Verkehr' ab, sondern verschafft sich über die Server der großen Internetkonzerne Zugang. Die Tatsache, dass auch das Vereinigte Königreich den Zugang zu PRISM sucht, legt nahe, dass es hier Daten gibt, die durch Tempora nicht erhoben werden können, entweder, weil die Informationen von den GCHQ-Servern gelöscht wurden, nicht durch britische Glasfaserkabel geflossen sind oder verschlüsselt übermittelt wurden.

45. Als der *Guardian* am 7. Juni 2013 Einzelheiten über das Programm enthüllte, berichtete er auch, dass der GCHQ Zugang dazu hatte und im Jahr 2012 insgesamt 197 geheimdienstliche Berichte daraus generiert hatte.[20] Daraufhin wurden Vorwürfe laut, dass das Vereinigte Königreich mit der Nutzung von PRISM den von dem

[18] Fn. 1 oben
[19] Vgl. z.B. *Google: There is no PRISM Back Door to Our Servers, No Open-Ended Access to User Data*, techcrunch.com, 7. Juni 2013 („**IB1/3/S.847**")
[20] Fn. 1 oben

Gesetz zur Regelung der Überwachung in der Telekommunikation (Regulation of Investigatory Powers Act, RIPA) vorgegeben Rechtsrahmen umgangen habe. Wie oben ausgeführt, machte der parlamentarische Ausschuss für Nachrichten- und Sicherheitsdienste (Intelligence and Security Committee, ISC) die Anschuldigung zum Gegenstand einer Untersuchung und kam zu dem Schluss, dass es keine Umgehung gegeben habe. Der ISC erklärte, dass der GCHQ bei jedem untersuchten Fall im Besitz einer Abfanganordnung gewesen sei, wobei über die Reichweite dieser Anordnungen nichts bekannt ist. Ebenso wenig ist bekannt, ob die britischen Behörden der Auffassung sind, dass Anfragen an das PRISM-Programm einer Anordnung bedürfen, noch hat sich die Untersuchung der Frage gewidmet, ob über PRISM gewonnene Erkenntnisse auch unaufgefordert oder auf Grundlage allgemeiner Anfragen der britischen Behörden zur Verfügung gestellt wurden. Darüber hinaus legten die öffentlichen Erklärungen des ISC nahe, dass der Ausschuss zuvor keine Kenntnis über das PRISM-Programm gehabt hatte.[21]

46. Neben Informationen, die auf Anfrage übermittelt werden, profitiert das Vereinigte Königreich möglicherweise auch dadurch von dem PRISM-Programm, dass ihm die US-Behörden unaufgefordert oder nur im Rahmen von Anfragen allgemeiner Art Informationen über britische und europäische Bürger zur Verfügung stellen. Würden die USA Informationen ‚freiwillig' bereitstellen, wäre der Empfang für das Vereinigte Königreich wohl an keinerlei gesetzlichen Rahmen gebunden. Der ISC stellte klar, dass er sich in seiner Untersuchung ausschließlich mit der britischen Verwendung von PRISM-Daten, für die eine spezifische Abfanganordnung angefragt worden und von den britischen Behörden ausgefertigt worden war, befasst hat. In der Praxis könnte zwischen Daten, die auf Anfrage geliefert und Daten, die ‚freiwillig' zur Verfügung gestellt werden, eine Grauzone liegen: Die britischen und die US-Behörden arbeiten effektiv als Team zusammen, weshalb die britische Seite der US-amerikanischen kaum spezifisch mitteilen muss, an welchen Informationen sie interessiert ist: Die USA wissen genau, welche Personen und Gebiete für die britischen Behörden ‚von Interesse' sind.

47. Diese Tatsachen verdeutlichen, wie beschränkt der durch das Gesetz zur Regelung der Überwachung in der Telekommunikation (RIPA) geschaffene Rechtsrahmen und

---

[21] Sir Malcolm Rifkind, Vorsitzender des ISC: *„No, I didn't know it, nor would I have expected to any more than I would any other country's process...." – „Nein, das habe ich nicht gewusst und hätte ich, wie auch bei den Verfahrensweisen eines jeden anderen Landes, auch nicht erwartet …"*. Frontline Club Debate, 9. Juli 2013 (http://www.frontlineclub.com/the-tradeoff-individual-privacy-and-national-security/ 58:30).

die Aufsichtsmechanismen in ihrer Wirkung sind. Unter den bekannt gewordenen Umständen besteht bei der britischen Nutzung des PRISM-Programms sowohl die Möglichkeit, bei den US-Behörden gezielt Daten anzufragen als auch, dass US-Behörden Daten im Rahmen einer Anfrage allgemeiner Art oder unaufgefordert zur Verfügung stellen. Diese Informationen werden vom GCHQ in irgendeiner Weise abgefangen worden sein, sind als externe Materialien aus dem Besitz der USA kaum durch US-amerikanische gesetzliche Bestimmungen zur Überwachung geschützt und können aus einer breit angelegten Datenerhebung stammen. Möglich wären auch Szenarien, in denen sich eine Zielperson im Vereinigten Königreich befindet oder sich der gesamte Datenverkehr im Vereinigten Königreich abspielt (aber auf US-Servern gespeichert wird). Für den Empfang, die Verwendung und die Verbreitung solcher Materialien gibt es keine ausreichenden Restriktionen.

Die Überwindung kryptografischer Schutzsysteme

48. Am 5. September 2013 veröffentlichte der *Guardian* weitere Enthüllungen darüber, wie der GCHQ und die NSA häufig genutzte Verschlüsselungstechnologien, die zum Schutz von E-Mails, beim Online-Banking, für medizinische Daten und andere private Informationen verwendet werden, geknackt haben. Diese Enthüllungen sind nicht nur wegen des weiteren Eindringens in internationale private Kommunikationen und Datenbestände von Einzelpersonen, sondern auch vor dem Hintergrund ihres historischen Kontexts und der Methoden, die dabei zum Einsatz kamen, bedeutsam. Die US-Regierung hatte seit den 1970ern und bis 2001 Versuche unternommen, den Gebrauch gängiger Verschlüsselungsverfahren einzuschränken, was stets rundheraus abgelehnt worden war.[22] Die Anschuldigungen legen jedoch nahe, dass allgemein gebräuchliche Verschlüsselungsverfahren in jedem Fall von dem GCHQ und der NSA überwunden worden sind. Auch die dabei verwendeten Methoden und Herangehensweisen sind bemerkenswert: über verdeckte Einflussnahme auf Verschlüsselungsstandards; die Zusammenarbeit mit Unternehmen, die der Regierung Produkte verkauften; ‚HUMINT' (Human Intelligence, Erkenntnisgewinnung aus menschlichen Quellen), das heißt Angestellte ausgewählter privatwirtschaftlicher Akteure; und hohe Investitionen in Rechenkapazitäten. Wie der *Guardian* berichtete, lässt das Budget für das Programm mit 254,9 Millionen US-Dollar im Jahr 2013 die jährlichen 20 Millionen US-Dollar für das PRISM-Programm verschwindend gering erscheinen.

[22] Vgl. z.B. *UK and US spy agencies undermined encryption standards,* Wired, 6. September 2013 („**IB1/3/S.837-840**")

49. Das berichtete Knacken gemeinhin verwendeter Verschlüsselungsstandards ist zweifellos auch für andere Programme wie Tempora von Bedeutung, da gespeicherte Kommunikationen möglicherweise entschlüsselt werden müssen, bevor ihr Inhalt ausgewertet werden kann.

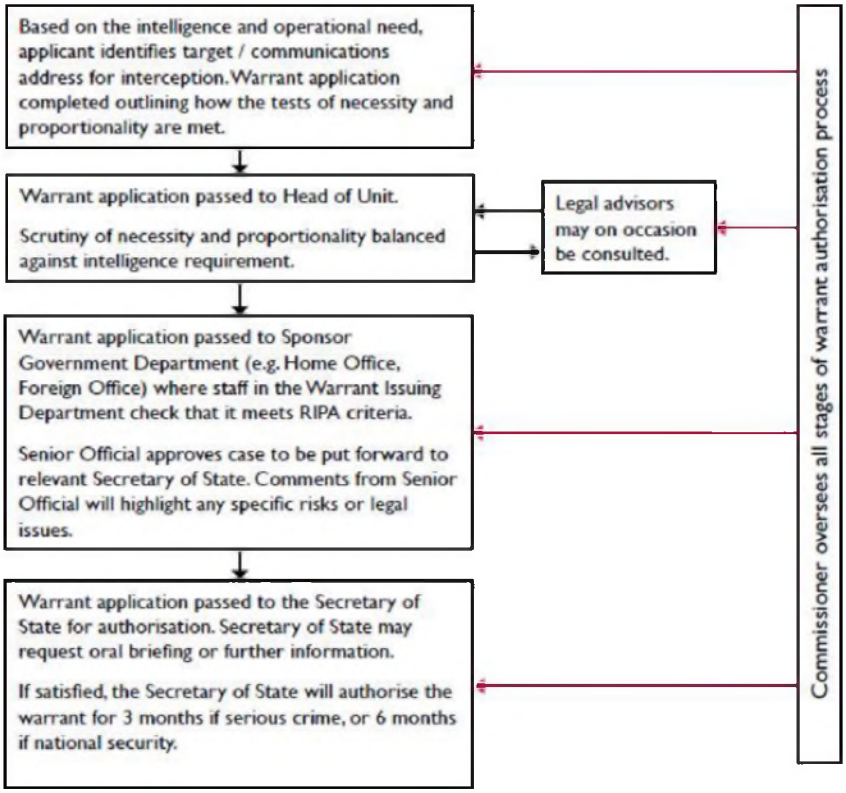
GESETZLICHE ERMÄCHTIGUNGEN

Das Anordnungsverfahren

50. Die Überwachung von Kommunikation gabelt sich in der Gesetzgebung des Vereinigten Königreichs in zwei Stränge. Das Abfangen von Inhalten (was in einem Brief, einem Anruf oder einer E-Mail gesagt wird) wird für drei bis sechs Monate genehmigt (je nach Absicht der Maßnahme), dafür bedarf es entsprechend des im Jahr 2000 verabschiedeten Regulation of Investigatory Powers Act (RIPA), Teil 1, Kapitel 1, einer vom Minister ausgestellten Anordnung, auf der die betreffende Zielperson oder der betreffende Zielort genannt sein muss. Der Zugriff auf „Kommunikationsdaten" – Kundeninformationen, Verzeichnisse getätigter oder empfangener Anrufe sowie gesendeter oder empfangener E-Mails, besuchter Websites, Standorte von Mobiltelefonen – ist in RIPA Teil 1, Kapitel 2 geregelt, wobei viele Behörden sich den Zugriff auf bestimmte derartige Daten selbst genehmigen dürfen. Das untenstehende Schaubild zeigt den Rechtsweg für die Genehmigung zur Überwachung von Inhalten entsprechend des Berichts des Beauftragten für Kommunikationsüberwachung (Interception of Communications Commissioner, IoCC):[23]

[23] Quelle: *2012 Annual Report of the Interception of Communications Commissioner* („**IB1/4/pp.851-920**").

Figure 2 - The Warrantry Authorisation Process



51. Im Jahr 2012 wurden laut des Jahresberichts des Beauftragten für Kommunikationsüberwachung (IoCC) 3372 Abfanganordnungen gemäß RIPA Teil 1, Kapitel 1 erwirkt. (Abs. 6.3 („**IB1/4/S.866**")).

52. Eine Abfanganordnung muss **keine** Angaben zur Zielperson oder zum Zielort enthalten, wenn Auslandskommunikationen abgefangen werden sollen und eine Bescheinigung vom Minister vorliegt, auf der die Art/Einstufung des zu untersuchenden Datenmaterials angegeben ist (RIPA Abschnitt 8, Absatz 4). Den Berichten des *Guardian* und Aussagen des Vorsitzenden des Ausschusses für Nachrichten- und Sicherheitsdienste (ISC)[24] nach zu schließen, scheint dies der Mechanismus zu sein, mit dem die Regierung den GCHQ ermächtigt, etwa mit dem Tempora-Programm automatisierte Erhebungen von Kommunikationen vorzunehmen, die außerhalb der britischen Inseln entspringen oder enden. „Externe" Kommunikationen könnten jedoch auch die Datenübermittlung von oder zu Servern außerhalb des Vereinigten Königreichs beinhalten. Dies würde also auch Internetverkehr zu den Einrichtungen der meisten großen Konzerne (wie

[24] Fn. 1 und 21 oben

Facebook, Google und Microsoft) einschließen, auf die sich das PRISM-Programm der NSA bezogen hat. Der *Guardian* zitierte einen internen Schriftsatz des GCHQ, in dem steht: *„Die Bescheinigung wird mit der Abfanganordnung ausgestellt, vom Minister unterzeichnet und klassifiziert die Arbeitsschritte, [die] wir im Rahmen dessen unternehmen können … [Sie] kann weder Zahlen noch Personen nennen, da dies zu einer endlosen Liste führen würde, die wir nicht verwalten könnten." Derartige Genehmigungen „decken das gesamte Spektrum der geheimdienstlichen Erkenntnisgewinnung des GCHQ ab*".[25] Laut *Guardian* „berichten die Anwälte von GCHQ von 10 grundlegenden Bescheinigungen, darunter eine ‚globale' für die Nebenstandorte der Dienststelle in Bude in Cornwall, Menwith Hill in North Yorkshire und in Zypern[26]." Dadurch wird es möglich, dass eine typische Abfanganordnung, die den Einsatz des Tempora-Programms genehmigt, sehr breit gefasste Formulierungen im Stil von „allen Datenverkehr, der durch ein bestimmtes Kabel zwischen dem Vereinigten Königreich und den USA verläuft" enthalten kann.

53. In der Praxis sind diese Anordnungen zwar gemäß RIPA Abschnitt 9 auf drei bis sechs Monate begrenzt, können effektiv aber auch zu „fortlaufenden" Anordnungen werden, wenn nämlich nach Ablauf der Frist sofort eine neue Anordnung erteilt wird. Der Grund dafür ist, dass sich Anordnungen allgemeiner Art der Zweckmäßigkeit halber nicht auf bestimmte Personen oder eine bestimme Bedrohung, sondern nur auf allgemeine Bedrohungen beziehen. Die britische Regierung hat eine Richtlinie für die Überwachung von Informationen (Code of Practice for the Interception of Communications **(„IB1/4/S.921-962")**) herausgegeben, deren fünftes Kapitel Weisungen für Anordnungen gemäß RIPA Abschnitt 8 Absatz 4 enthält. Darin findet sich unter anderem die Vorgabe (5.2.), dass *„jedes außergewöhnliche Maß an kollateraler Eindringung und die Gründe dafür, dass diese Eindringung unter den gegebenen Umständen gerechtfertigt ist, abzuwägen sind. Wenn die betreffenden Kommunikationen insbesondere das Religions- oder Arztgeheimnis, journalistischen Quellenschutz oder anwaltliche Vertraulichkeitspflichten beeinträchtigen, muss dies im Antrag spezifiziert werden."* Derartige Abwägungen konnten in der Praxis jedoch offenbar nicht das Aufkommen einer ganzen Reihe von fortlaufenden Anordnungen verhindern, die ein breit angelegtes „Big Data"-Programm wie Tempora zugelassen haben.

---

[25] *The legal loopholes that allow GCHQ to spy on the world*, The Guardian, 2. Juni 2013 („**IB1/2/S.664-668**").
[26] ebd.

54. Auf Grundlage des RIPA, des Code of Practice for the Interception of Communications und der Enthüllungen der jüngsten Zeit gehe ich von folgenden Vorgängen beim Erwirken einer Abfanganordnung nach Abschnitt 8 Absatz 4 aus:

    1. Der GCHQ beantragt beim Minister eine Anordnung zur Überwachung einer externen Kommunikationsverbindung, etwa eines oder mehrerer Unterseekabel zwischen dem Vereinigten Königreich und dem europäischen Festland. Diese wird gemäß RIPA Abschnitt 8 Absatz 4 erteilt.
    2. Der Minister stellt eine Bescheinigung aus, in der die Informationskategorien, nach denen gesucht werden soll, beschrieben sind. Der *Guardian* berichtete, dass es sich dabei um „breit gefasste Kategorien" handelte und hielt fest, dass „als Kategorien bezüglich der [zu sammelnden] Datenmaterialien etwa Betrug, Drogenhandel und Terrorismus" genannt wurden.[27] Die Bescheinigung wird höchstwahrscheinlich nicht die tausenden potenziellen Zielpersonen und Standorte namentlich anführen.
    3. Das Programm Tempora verschafft sich nun Zugang zu diesen Datenmaterialien. Auf den Einsatz vieler tausender Stichwörter und Selektoren wird in der Bescheinigung vermutlich nicht eingegangen.

55. Im Gegensatz hierzu muss eine Abfanganordnung für „landesinterne" Kommunikationen im Vereinigten Königreich gemäß RIPA Abschnitt 8, Absatz 1 entweder eine einzelne Zielperson oder eine Auswahl an Zielorten benennen sowie die Adressen, Nummern und weiteren Faktoren, anhand derer festzulegen ist, welche Kommunikationen überwacht werden sollen.

56. RIPA Abschnitt 12 ermächtigt den Innenminister, Telekommunikationsanbieter zur gesetzmäßigen Überwachung ihres Netzwerks zu verpflichten. Das dürfte Maßgaben wie die Installation von Abfangvorrichtungen mit speziellen Fähigkeiten, etwa zum Abfangen von Kommunikationen in Echtzeit, sowie Stillschweigen über die Existenz anderer simultaner Abfangvorgänge gegenüber den einzelnen

[27] Fn. 1 oben

Überwachungsorganen beinhalten. Telekommunikationsanbieter können gegen diese Anordnung bei einem technischen Beirat, der sich aus Vertretern der Überwachungsorganen und Vertretern von Telekommunikationsanbietern zusammensetzt und das den Minister über die technischen und finanziellen Konsequenzen der Anordnung informiert, Einspruch einlegen. Die Anordnung kann dann entweder zurückgezogen oder erneuert werden.

57. Gemäß Abschnitt 94 des Telecomunications Act von 1984 ist der Minister berechtigt, Anbietern von öffentlichen elektronischen Netzen „im Interesse der nationalen Sicherheit oder der Beziehungen zur Regierung eines Landes oder Territoriums außerhalb des Vereinigten Königreichs … Anordnungen allgemeiner Art zu erteilen", die vor Veröffentlichung geschützt werden dürfen.

58. Durch die Kombination verschiedener rechtlicher Bestimmungen (Abschnitt 10 des Computer Misuse Act 1990, RIPA Abschnitt 32, Teil III des Police Act 1997 und Abschnitt 5 des Intelligence Service Act 1994) können Regierungsbehörden auch ermächtigt werden, aus der Ferne in Computersysteme einzudringen und auf Daten in diesen Systemen zuzugreifen.

59. Überdies sind die Handlungen des GCHQ außerhalb des Vereinigten Königreichs gemäß Absatz 7 des Intelligence Service Act von 1994 von der zivil- und strafrechtlichen Verfolgung unter britischem Gesetz ausgeschlossen, sofern diese mit Genehmigung des Ministers gemäß dem genannten Absatz erfolgten.

60. Der GCHQ ist vielleicht nicht in der Lage, Beziehungen mit den größten Internetkonzernen zu nutzen wie die NSA es offenbar mit ihrem PRISM-Programm getan hat, da nur sehr wenige dieser Unternehmen ihren Hauptsitz im Vereinigten Königreich haben, wenngleich sie Standorte und Infrastrukturen im Vereinigten Königreich unterhalten. Dennoch hat er eindeutig großangelegte Überwachungen von Kommunikationen, die das Vereinigte Königreich erreichen oder verlassen, durchgeführt. Die Behörde hat Berichten zufolge bereits mehrere hundert Millionen Pfund in den Ausbau ihrer Kapazitäten zur Überwachung von ISP-Netzwerken investiert. Dies geschah im Zuge des Projekts „Mastering the Internet" (zu dem auch Tempora gehört), das angeblich über ein Gesamtbudget von über 1 Milliarde Pfund (1,23 Milliarden Euro) verfügt und das Analysten durch die „vollständige Sichtbarmachung des Internetverkehrs im Vereinigten Königreich" in die Lage versetzen soll, ihre Abfanganwendungen aus der Ferne so zu konfigurieren, dass sie

Daten (sowohl Kommunikationsdaten als auch Kommunikationsinhalte) nach dem „Deep-Packet-Inspection"-Prinzip auf Anfrage überwachen können."[28]

Einschätzung

Die Verhältnismäßigkeit der enthüllten Methoden

61. Als Experte für Internettechnologien, Cybersicherheit und Überwachung ist es nicht meine Rolle, zu beurteilen, ob die oben genannten Methoden eine verhältnismäßige Form von Überwachung darstellen oder nicht. Ich bin jedoch der Ansicht, dass ich die wesentlichen Merkmale der Rahmenbedingungen für die Überwachung und der Überwachungspraktiken, die nach meiner Einschätzung in dieser Frage von Bedeutung sind, hier festhalten kann. Die wichtigsten diesbezüglichen Aspekte sind meiner Meinung nach:

- das enorme (und vor Snowdens Enthüllungen ungeahnte) Ausmaß der Operationen;
- die Tatsache, dass die Verstöße und Aktivitäten, bezüglich derer Überwachungsmaßnahmen ergriffen werden dürfen (und eindeutig auch ergriffen werden), nicht klar und genau definiert sind;
- die Tatsache, dass die Überwachung nicht auf zuvor eindeutig festgelegte Personen oder wenigstens Kategorien von Personen abzielt: Im Rahmen des Tempora-Programms sind die Kommunikationen und Internetaktivitäten *aller* Bürger, deren Daten durch das vom Vereinigten Königreich ausgehende Glasfaserkabelnetz fließen, Gegenstand genauester Überprüfung (selbst wenn sie nicht von einem menschlichen Agenten gelesen oder geprüft werden);
- die Tatsache, dass es keine klaren Beschränkungen für die Dauer der Überwachung gibt; im Gegenteil, im Rahmen des Tempora-Programms werden effektiv und permanent *alle* Daten, die durch die „gesplitteten" Glasfaserkabel fließen, erhoben;
- die Tatsache, dass die „Richtlinien und Verfahren", die gegenwärtig die Überwachung regeln, wie die Behörden selbst einräumen, unklar und vage sind;
- die Tatsache, dass diese Richtlinien und Verfahren nicht veröffentlicht und nicht Gegenstand parlamentarischer oder öffentlicher, demokratischer Überprüfung

[28] *Jacqui's secret plan to 'Master the Internet'*, Christopher Williams, The Register, 3. Mai 2009 („**IB1/3/S.841-843**")

sind;

- die Tatsache, dass es keine ernsthaften Schutzmaßnahmen gegen Missbrauch gibt, derweil die aktuellen Aufsichtsmechanismen sich als unfähig erwiesen haben, das Wachstum der massiven, zügellosen Überwachung, die in Gang gesetzt wurde, in Schach zu halten;
- die Tatsache, dass es keine bekannten Vorschriften gibt, die den Gebrauch und die Offenlegung der erfassten Daten regulieren, ebenso wenig den Austausch dieser Daten mit anderen Behörden, einschließlich der NSA in den USA oder anderer Behörden des „Five Eyes"-Netzes;
- die Tatsache, dass es keine bekannten, eindeutigen Vorschriften gibt, die gewährleisten, dass die erhobenen Daten einerseits nicht unrechtmäßig zurückbehalten werden, wenn sie nicht länger gebraucht werden oder nicht mehr relevant sind, und anderseits nicht zu einem Zeitpunkt oder in einer Art und Weise vernichtet werden, die es unmöglich machen, Fehler nachträglich zu korrigieren;
- genauer: die Tatsache, dass es keine Auflagen gibt, Opfer von Überwachungsmaßnahmen darüber zu informieren, dass sie ausgespäht worden sind;
- die Tatsache, dass es (jenseits geheimer Untersuchungen des Ausschusses für Nachrichten- und Sicherheitsdienste (ISC)) keinerlei öffentliche oder parlamentarische Debatte über die Einrichtung und den Betrieb der massiven Überwachungsprogramme gegeben hat, und allgemeiner;
- die Tatsache, dass die meisten Schutzmaßnahmen, die für Nachrichtendienste des Vereinigten Königreichs mit Blick auf den Zugriff auf Daten, die aus großen Teilen des europäischen Internetverkehrs erhoben wurden, gelten, nicht einsehbar sind, so dass es unmöglich ist festzustellen, ob es ihnen gelingt, dieses Ziel zu erreichen;
- die Tatsache, dass der GCHQ in signifikantem Ausmaß europäische Bürger außerhalb des Vereinigten Königreichs überwacht (und diese Daten mit anderen Regierungen teilt), wobei es wegen des britischen Zugangs zu Unterseekabeln, der dem Vereinigten Königreich einen Vorteil verschafft, kaum effektive Aufsichtsmöglichkeiten für diese Personen gibt.

62. Von Bedeutung hinsichtlich der Konvention ist auch die Tatsache, dass die National Security Agency der Vereinigten Staaten Berichten zufolge direkten Zugriff auf die Daten von Tempora und anderen GCHQ-Programmen hat – zu Zwecken, die weit über jene hinausgehen, die der Europäische Gerichtshof für

Menschenrechte zur Rechtfertigung der Übergriffigkeit „strategischer" Überwachungssysteme als angemessen bestätigt hat (etwa in *Klass v. Germany*, *Weber and Saravia v. Germany* und anderen Entscheidungen). Beschränkungen für die Nutzung dieser Daten sind, soweit sie britische Bürger betreffen, in geheimen vertraglichen Abkommen festgehalten. Es ist schwer nachzuvollziehen, wie dies mit der positiven Pflicht des Vereinigten Königreichs, die Privatsphäre der Menschen unter seiner Rechtsprechung zu schützen, in Einklang zu bringen ist.

Alternativen, die zu weniger weitreichenden Beeinträchtigungen führen:

63. Ich habe sowohl Unternehmen als auch Regierungen in Fragen des Datenschutzes im Internet und der Cybersicherheit beraten. Meiner Meinung nach ist es möglich, ein System einzurichten, das die einzelnen Persönlichkeitsrechte hinreichend wahrt, während es andererseits verhältnismäßige, gezielte Überwachungsmaßnahmen für genau definierte Zwecke gestattet. Die Spannungsverhältnisse in einem solchen System können zwar nie ganz beseitigt werden, sie lassen sich jedoch durch Aufsichtsmechanismen, die eine öffentliche Überprüfung gestatten, verträglich handhaben.

64. Ein besserer Schutz könnte erreicht werden, durch Benachrichtigung der Personen, die Ziel von Überwachungsmaßnahmen geworden sind, nach Ende der Ermittlungen; durch richterliche statt behördlicher Anordnungen für gezielte Überwachungen; durch die Veröffentlichung gesammelter Informationsanfragen an die einzelnen Internetanbieter nach Ermittlungsart und -Zweck; und durch die Abschaffung von Geheimhaltungsbestimmungen, die Internetunternehmen daran hindern, Einzelheiten über ihre Vorgehensweisen bei Überwachungsanordnungen zu veröffentlichen.

65. Neben den Mängeln des durch Abschnitt 8, Absatz 4 festgelegten Rechtsrahmens, die ich oben ausgeführt habe, verdient auch die Tatsache Beachtung, dass „Metadaten"/„Kommunikationsdaten" unter RIPA Teil 1, Kapitel 2 nur zu einem sehr geringen Grad gesetzlich geschützt sind, obwohl sie sehr viel über das Privatleben von Menschen preisgeben können. Dies ist von der gegenwärtigen Regierung teilweise bereits erkannt worden, die mit dem Erlass des Protection of Freedoms Act 2012, Abschnitt 37 festgelegt hat, dass lokale Behörden sich den Zugriff auf Kommunikationsdaten von einem Amtsrichter (magistrate) gestatten lassen müssen.

Diese Vorgabe sollte für alle Behörden gelten.

66. Ein Beispiel dafür, wie ein System die Rechte Einzelner auf Privatsphäre hinreichend schützen kann, bieten die Internationalen Grundsätze für die Anwendung der Menschenrechte in der Kommunikationsüberwachung[29] **(„IB1/4/pp.963-982")**, die in viele Sprachen übersetzt worden sind. Sie sind das Ergebnis einer gemeinsamen Ausarbeitung von zivilgesellschaftlichen Gruppen, Wirtschaftsvertretern und internationalen Experten für Kommunikationsüberwachungsrecht, -politik und -technologie. In der Präambel werden das Aufkommen von Massenüberwachung infolge der öffentlichen Verbreitung des Internets sowie der Schwund logistischer Barrieren der Überwachung ausdrücklich angesprochen. Sie hebt die Grenzen veralteter Rechtsrahmen hervor. Die Grundsätze selbst setzen Standards, die meiner Ansicht nach mit den Praktiken, die ich in dieser Aussage beschrieben habe, oder durch die Regelung im RIPA nicht erreicht werden. Alle Grundsätze verdienen wie ich finde Aufmerksamkeit, insbesondere aber die folgenden:

„Gesetzmäßigkeit": Jede Beschränkung des Rechtes auf Privatsphäre muss gesetzlich vorgeschrieben sein. Der Staat darf in Abwesenheit eines bestehenden öffentlich verfügbaren Rechtsaktes, welcher den Standard der Klarheit und Genauigkeit erfüllt, und der ausreicht, um sicherzustellen, dass Einzelne eine Benachrichtigung erhalten und seine Anwendung vorhersehen können, keine Maßnahmen einführen oder durchsetzen, die das Recht auf Privatsphäre beeinträchtigen. Angesichts der Geschwindigkeit des technologischen Wandels sollten Gesetze, die das Recht auf Privatsphäre beschränken, regelmäßig durch Instrumente eines partizipativen legislativen und behördlichen Prozesses überprüft werden.

„Notwendigkeit":Gesetze, die Kommunikationsüberwachung durch den Staat erlauben, müssen die Überwachung darauf begrenzen, was zweifellos und nachweislich notwendig ist, um das legitime Ziel zu erreichen. Kommunikationsüberwachung darf nur durchgeführt werden, wenn es das einzige Mittel zur Erreichung eines rechtmäßigen Ziels ist, oder wenn es mehrere Mittel gibt, es das Mittel ist, welches am unwahrscheinlichsten die Menschenrechte verletzt. Der Nachweis der Begründung dieser Rechtfertigung in gerichtlichen sowie in Gesetzgebungsverfahren liegt beim Staat.

„Verhältnismäßigkeit": Kommunikationsüberwachung sollte als hochgradig invasive / (or: eindringende) Handlung angesehen werden, die in das Recht auf Privatsphäre und die Freiheit der Meinungsäußerung eingreift und die Grundlagen einer demokratischen Gesellschaft bedroht. Entscheidungen über Kommunikationsüberwachung müssen durch Abwägen der gesuchten Vorteile gegen die Schäden, die den Rechten des Einzelnen und anderen konkurrierenden Interessen zugefügt würden, getroffen werden, und sollten eine Betrachtung der Sensibilität der Informationen und der Schwere der Verletzung des Rechts auf Privatsphäre einbeziehen.

[29] https://en.necessaryandproportionate.org/text

Dies erfordert insbesondere: Sollte ein Staat Zugang zu oder die Nutzung von geschützten Informationen anstreben, die durch Kommunikationsüberwachung im Rahmen einer strafrechtlichen Untersuchung gesammelt wurden, dann muss dies auf der zuständigen, unabhängigen und unparteiischen gerichtlichen Entscheidung begründet sein, dass:

1. es eine hohe Wahrscheinlichkeit gibt, dass ein schweres Verbrechen begangen wurde oder begangen werden wird;
2. der Beweis eines solchen Verbrechens durch den Zugriff auf die geschützten Daten erhalten werden würde;
3. andere verfügbare und weniger invasive Ermittlungsmethoden ausgeschöpft sind;
4. die abgerufenen Informationen in vernünftiger Weise auf diejenigen begrenzt werden, die für die mutmaßliche Straftat relevant sind, und jede weitere gesammelte Information sofort vernichtet oder zurückgegeben wird; und
5. Informationen nur von der festgelegten Behörde abgerufen und nur für den Zweck, für den die Genehmigung erteilt wurde, verwendet werden.

Wenn der Staat mit Kommunikationsüberwachung Zugang zu geschützten Informationen zu einem Zweck erlangen will, der eine Person nicht der Strafverfolgung, Ermittlung, Diskriminierung oder Verletzung der Menschenrechte aussetzt, muss der Staat einer unabhängigen, unparteiischen und zuständigen Behörde Folgendes nachweisen:

1. andere verfügbare und weniger invasive Ermittlungsmethoden wurden in Betracht gezogen;
2. die abgerufenen Informationen werden in vernünftiger Weise auf die relevanten begrenzt und jede zusätzlich gesammelte Information wird sofort vernichtet oder dem betroffenen Individuum zurückgegeben; und
3. Informationen werden nur von der festgelegten Behörde abgerufen und nur für den Zweck verwendet, für den die Genehmigung erteilt wurde.

„Zuständige gerichtliche Behörden“: Bestimmungen in Bezug auf die Kommunikationsüberwachung müssen von zuständigen gerichtlichen Behörden, die unparteiisch und unabhängig sind, festgelegt werden. Die Behörde muss:

1. getrennt sein von der Behörde, welche die Kommunikationsüberwachung durchführt,
2. vertraut sein mit den relevanten Themen und fähig sein, eine gerichtliche Entscheidung über die Rechtmäßigkeit der Kommunikationsüberwachung, die benutzte Technologie und Menschenrechte zu treffen, und
3. über entsprechende Ressourcen verfügen, um die ihr übertragenen Aufgaben auszuführen.

„Rechtsstaatliches Verfahren“: Ein rechtsstaatliches Verfahren verlangt, dass Staaten die Menschenrechte jedes Einzelnen respektieren und garantieren, indem sie rechtmäßige Prozesse versichern, die jegliche Beeinträchtigung der Menschenrechte ordnungsgemäß und gesetzlich spezifiziert regeln, die konsistent durchgeführt werden, und die der allgemeinen Öffentlichkeit zugänglich sind. Insbesondere bei der Bestimmung seiner oder ihrer Menschenrechte hat jeder das Recht auf ein faires und

öffentliches Verfahren innerhalb einer angemessenen Frist von einem unabhängigen, zuständigen und unparteiischen rechtmäßig gegründeten Gericht, außer in Notfällen, wenn für Menschenleben Gefahr in Verzug ist. In solchen Fällen, muss innerhalb einer vernünftigen und realisierbaren Frist eine rückwirkende Autorisierung eingeholt werden. Lediglich das Risiko der Flucht oder Zerstörung von Beweismitteln soll niemals als ausreichend für eine rückwirkende Autorisierung angesehen werden.

„Benachrichtigung des Nutzers“: Personen sollten über die Entscheidung der Autorisierung einer Kommunikationsüberwachung informiert werden. Es sollten ausreichend Zeit und Informationen zur Verfügung gestellt werden, so dass die Person die Entscheidung anfechten kann. Des Weiteren sollte sie Zugang zu dem Material bekommen, welches für den Antrag der Autorisierung vorgelegt wurde. Eine Verzögerung der Benachrichtigung ist nur unter folgenden Bedingungen gerechtfertigt:

1. Die Benachrichtigung würde den Zweck, für den die Überwachung genehmigt ist, ernsthaft gefährden oder es besteht eine unmittelbare Gefahr für Menschenleben, oder
2. Die Erlaubnis einer Verzögerung der Benachrichtigung wird durch die zuständige Justizbehörde zum Zeitpunkt der Genehmigung der Überwachung erteilt; und
3. Die betroffene Person wird benachrichtigt, sobald die Gefahr aufgehoben ist, oder innerhalb einer vernünftigen realisierbaren Frist, je nachdem, welches zuerst zutrifft, aber in jeden Fall zu dem Zeitpunkt, zu dem die Kommunikationsüberwachung abgeschlossen ist. Die Verpflichtung zur Benachrichtigung liegt beim Staat, aber in dem Fall, dass der Staat dem nicht nachkommt, sollten Kommunikationsdiensteanbieter die Freiheit haben, Personen über die Kommunikationsüberwachung freiwillig oder auf Anfrage zu benachrichtigen.

„Transparenz“: Staaten sollten bezüglich der Nutzung und des Umfangs der Techniken und Befugnisse der Kommunikationsüberwachung transparent sein. Sie sollten mindestens die gesammelten Informationen über die Anzahl der genehmigten und abgelehnten Anfragen, eine Aufschlüsselung der Anfragen nach Dienstanbieter und nach Ermittlungsart und -zweck veröffentlichen. Staaten sollten Personen genügend Informationen liefern, um zu gewährleisten, dass sie den Umfang, die Art und Anwendung der Gesetze, welche die Kommunikationsüberwachung erlauben, verstehen. Staaten sollten Diensteanbieter befähigen, die von ihnen angewendeten Prozesse zu veröffentlichen, wenn sie staatliche Kommunikationsüberwachung bearbeiten, an diesen Prozessen festzuhalten und Berichte der staatlichen Kommunikationsüberwachung zu veröffentlichen.

„Öffentliche Aufsicht“: Staaten sollten unabhängige Aufsichtsmechanismen schaffen, die Transparenz und Verantwortung der Kommunikationsüberwachung gewährleisten. Aufsichtsmechanismen sollten die Befugnis haben, auf alle potenziell relevanten Informationen über staatliche Maßnahmen, wenn notwendig auch auf geheime oder als Verschlusssachen gekennzeichnete Informationen zuzugreifen; zu beurteilen, ob der Staat seine rechtmäßigen Fähigkeiten legitim nutzt; zu beurteilen, ob der Staat die Informationen über den Einsatz und den Umfang der Techniken und Befugnisse der Kommunikationsüberwachung transparent und genau veröffentlicht hat; und regelmäßige Berichte und andere für die Kommunikationsüberwachung relevante Informationen zu veröffentlichen. Unabhängige Kontrollmechanismen sollten in Ergänzung zur Aufsicht geschaffen werden, die bereits über einen anderen

Teil der Regierung zur Verfügung steht.

„Integrität der Kommunikation und der Systeme": Um die Integrität, Sicherheit und Privatsphäre der Kommunikationssysteme zu gewährleisten, und in Anerkennung der Tatsache, dass Abstriche bei der Sicherheit für staatliche Zwecke fast immer die Sicherheit im Allgemeinen infrage stellen, sollten Staaten die Dienstleister oder Hardware- oder Softwarehändler nicht zwingen, Überwachungs- oder Beobachtungsfunktionen in ihre Systeme einzubauen oder bestimmte Informationen lediglich für Zwecke der staatlichen Überwachung zu sammeln oder zu speichern. A priori Vorratsdatenspeicherung oder Sammlung sollte nie von Dienstleistern gefordert werden. Personen haben das Recht, sich anonym zu äußern; Staaten sollten daher auf die zwingende Identifizierung der Nutzer als Voraussetzung für die Leistungserbringung verzichten.

„Schutzmaßnahmen für die internationale Zusammenarbeit": Als Reaktion auf die Veränderungen der Informationsflüsse und Kommunikationstechnologien und -dienstleistungen, kann es notwendig sein, dass Staaten Hilfe von einem ausländischen Dienstleister anfordern. Dementsprechend sollten die gemeinsamen Rechtshilfeverträge und andere Vereinbarungen, die von den Staaten eingegangen wurden, sicherstellen, dass in Fällen, in denen die Gesetze mehr als eines Staates für die Kommunikationsüberwachung angewendet werden können, derjenige verfügbare Standard mit dem höheren Schutzniveau für den Einzelnen angewendet wird. Wo Staaten Unterstützung für Zwecke der Strafverfolgung suchen, sollte der Grundsatz der beiderseitigen Strafbarkeit angewendet werden. Staaten dürfen gemeinsame Rechtshilfeprozesse und ausländische Anfragen nach geschützten Informationen nicht nutzen, um inländische gesetzliche Beschränkungen der Kommunikationsüberwachung zu umgehen. Gemeinsame Rechtshilfeprozesse und andere Vereinbarungen sollten klar dokumentiert werden, öffentlich zugänglich sein und dem Schutz des fairen Verfahrens unterliegen.

67. Die deutsche Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat unlängst eine Entschließung verabschiedet, die sich kritisch mit Tempora und PRISM auseinandersetzt und Richtlinien ähnlich der oben angeführten fordert (siehe Zusammenfassung in („**IB1/4/S.983**")). Die Datenschutzbeauftragten sprechen sich für die Weiterentwicklung und Umsetzung von nationalem, europäischem und internationalem Recht aus, um umfassenden Schutz der Privatsphäre, zu gewährleisten. Sie fordern außerdem mit Blick auf gegenwärtige Praktiken die Beachtung grundrechtlicher Mindeststandards, die dem Schutzniveau des Art. 8 der Charta der Grundrechte der Europäischen Union entsprechen.

Die Folgen der Überwachung

68. Massive Überwachung kann das Vertrauen in Technologien beschädigen, soziale Mobilität und gesellschaftlichen Zusammenhalt verringern, Konformismus bestärken und eine signifikant hemmende Wirkung auf politische Debatten und Proteste

ausüben.

69. Aus Kommunikationsdaten lässt sich ein höchst detailliertes Bild von Einzelnen – und Gruppen von Menschen – erzeugen. Für die individuelle Privatsphäre oder die Freiheit der unbeobachteten Zusammenkunft bleibt wenig Raum, wenn staatliche Ermittler einsehen können, mit wem wir kommunizieren, was wir online lesen und ansehen und wohin wir mit unseren Mobiltelefonen reisen. Die Netzwerkanalyse von Kommunikationsdaten (einschließlich Daten von Standorten), also die Erzeugung großer Datenbestände, die Menschen über mehrere ‚Communication Hops' (mittels gemeinsamer Kontakte) miteinander in Verbindung bringen und Millionen von Menschen erfassen können, sind eine ernsthafte Beeinträchtigung des Grundrechts auf Versammlungsfreiheit. In einem Bericht für die britische Regierung habe ich vor Kurzem die Implikationen derartiger Überwachungstendenzen für die Identität aus psychologischer Sicht kommentiert („**IB1/4/pp.984-1002**").

70. Unmittelbar vor den jüngsten Enthüllungen der Presse veröffentlichte der UN-Sonderberichterstatter für das Recht auf Meinungsfreiheit und freie Meinungsäußerung, Frank La Rue, einen Bericht über Kommunikationsüberwachung („**IB1/4/pp.1003-1025**"), in dem er schreibt:

> „23. Damit Einzelne ihr Recht auf Privatsphäre [und vertrauliche] Kommunikation ausüben können, müssen sie sicher sein können, dass diese [Kommunikationen] vertraulich, geschützt und, wenn sie dies wünschen, anonym bleiben. Private Kommunikation bedeutet, dass Menschen Informationen und Ideen in einem Raum austauschen können, der sich außerhalb des Zugriffs der restlichen Gesellschaft, des Privatsektors und letzten Endes des Staats selbst befindet. Geschützte Kommunikation bedeutet, dass Einzelne in der Lage sein sollten, verifizieren zu können, ob ihre Kommunikation, ohne Eingriffe oder Veränderungen, ausschließlich beim beabsichtigten Empfänger ankommt und dass die Kommunikationen, die sie erhalten, ebenso wenig beeinträchtigt worden sind. Anonyme Kommunikation ist einer der wichtigsten Fortschritte, der durch das Internet ermöglicht wurde, sie erlaubt es Einzelnen, sich frei und ohne Furcht vor Strafe oder Verurteilung auszudrücken ...
>
> ... 33. Moderne Überwachungstechnologien und Arrangements, die es Staaten erlauben, in die Privatleben Einzelner einzudringen, bergen die Gefahr, die Grenze zwischen der privaten und der öffentlichen Sphäre zu verwischen. Sie ermöglichen eine invasive und wahllose Überwachung von Menschen, die möglicherweise nicht einmal wissen, dass sie Gegenstand derartiger Überwachungsmaßnahmen sind, geschweige denn dagegen vorgehen. Der technologische Fortschritt führt dazu, dass die Effizienz staatlicher Überwachung in ihrem Ausmaß und ihrer Dauer nicht länger eingeschränkt ist. Sinkende Kosten für die Technik und Datenspeicherung haben finanzielle und praktische Überwachungshürden aus dem Weg

geräumt. Der Staat als solcher ist heute mehr denn je in der Lage, simultane, invasive, gezielte und breitgefasste Überwachungen vorzunehmen."

71. Computer zur Datenüberwachung überwachen nicht nur: Sie lenken die Aufmerksamkeit von Polizisten und anderen Behörden auf „Ziele", die durch Algorithmen bestimmt wurden. Zur selben Zeit als die Enthüllungen über das Tempora-Programm erschienen, zitierte der *Guardian* eine nicht identifizierte Geheimdienstquelle, die sagte: *„Die Kriterien sind Sicherheit, Terror, organisiertes Verbrechen. Und wirtschaftliches Wohlergehen. Es gibt ein Kontrollverfahren, in dem man die Protokolle erneut überprüft, um zu sehen, ob sie gerechtfertigt waren oder nicht. Die große Mehrheit der Daten wird unbesehen entsorgt … wir haben schlicht nicht die Ressourcen."* [30] Sollte das zutreffen, handelt es sich nichtsdestotrotz um relativ breit gefasste Kriterien. Darüber hinaus dürften, wie ich unten ausführe, die beständig wachsenden Speicher- und Durchsuchungskapazitäten dazu verführen, die Suchparameter den Kapazitäten anzupassen. In seinem Artikel über das Tempora-Programm berichtete der *Guardian*: *„Ein Hinweis darauf, wie groß das Schleppnetz sein kann, schimmert in der Aussage der GCHQ-Juristen durch, die erklärten, es wäre unmöglich, die gesamte Zahl der Zielpersonen zu nennen, ‚da dies zu einer endlosen Liste führen würde, die wir nicht verwalten könnten.'"*[31]

In Bereichen wie der Terrorismusbekämpfung geht es darum, Verbrechen zu verhindern, die von einer Zielperson möglicherweise begangen werden könnten. Versuche, sehr seltene Ereignisse oder Ziele in einem sehr großen Datensatz automatisch zu identifizieren, führen jedoch mit hoher Wahrscheinlichkeit zu einer inakzeptablen Menge von „falschen Übereinstimmungen" (‚false positives'), die unschuldige Menschen als Verdächtige identifizieren oder „falschen Negativmeldungen" (‚false negatives'), die tatsächliche Kriminelle oder Terroristen nicht erkennen. Der wissenschaftliche Ausdruck hierfür lautet „Prävalenzfehler" (base-rate-fallacy); umgangssprachlich heißt das so viel wie: *„Wenn man nach einer Nadel im Heuhaufen sucht, bringt es nichts, noch mehr Heu hinzu zu schütten."* Die Tatsache, dass hier vermeintlich hochentwickelte Algorithmen derbe Stereotypen ersetzen, kann dies kaum verhindern. Weil selbst die, die sich darauf verlassen, es nicht verstehen und weil die, die damit ins Visier genommen werden, sich faktisch nicht dagegen wehren können, birgt derartiges „Data Mining" die Gefahr der Diskriminierung. Ein Bericht des US-amerikanischen National Research Council aus dem Jahr 2008 kommt zu dem Schluss, *„dass es weder im Kreis der relevanten Wissenschaftler, noch im Komitee einen*

[30] Fn 1 oben
[31] Fn 1 oben

Konsens darüber gibt, ob Maßnahmen zur Verhaltensüberwachung oder physische Überwachungstechniken angesichts des gegenwärtigen Stands der Wissenschaft im Kontext der Terrorismusbekämpfung überhaupt brauchbar sind." („**IB1/4/pp.1026-1055**").[32]

74. Es wird davon ausgegangen, dass sich die Rechenleistung von Computern entsprechend Moore's Law weiterentwickeln und alle 18-24 Monate verdoppeln – sich im nächsten Jahrzehnt also mindestens verdreißigfachen wird, wenngleich dann die fundamentalen Grenzen dessen, was die Silikonverarbeitung zu leisten vermag, abzusehen sein werden. Speicherkapazitäten von Computern und die Kommunikationsbandbreite werden wahrscheinlich ebenfalls weiterhin mindestens in derselben Geschwindigkeit zunehmen. Diese exponentiellen Zuwächse werden die Voraussetzungen für Organisationen, persönliche Daten zu erheben, zu speichern und zu verarbeiten erheblich verbessern und ebenso die technischen Hindernisse für Geheimdienste und Polizei für die Überwachung aller Aspekte des täglichen Lebens, die digitale Spuren hinterlassen, verringern.

Versagen der Aufsicht

75. In Anbetracht der Enthüllungen des *Guardian* haben die britischen Aufsichtsinstanzen und Behörden eindeutig mangelhaft gearbeitet. Für die Öffentlichkeit ist es schwer, darauf zu vertrauen, dass ihre Privatsphäre von einem derart intransparenten System, hinreichend geschützt wird. Fern jeglicher öffentlichen Debatte ist ein globales Überwachungssystem von atemberaubendem Ausmaß entstanden, das durch pauschale geheime Anordnungen des zuständigen Ministers ermächtigt wurde und lediglich geheim diskutiert und intern durch den Ausschuss für Nachrichten- und Sicherheitsdienste (ISC) überprüft wird. Das System interner Vorgaben für den GCHQ zur Wahrung der Menschenrechte ist ähnlich aufgebaut und weist entsprechend des Berichts des Beauftragten für Kommunikationsüberwachung (IoCC) nicht annähernd die Sorgfalt und Klarheit auf, die nötig wären, um das Vertrauen der Öffentlichkeit gewinnen.

76. Was die Aufsicht betrifft, ist bemerkenswert, dass der Guardian, wieder ein Originaldokument zitierend, berichtete, dass die NSA *„Richtlinien für den Gebrauch von [Tempora] erhielt, in juristischen Briefings jedoch von den GCHQ-Juristen gesagt bekam: ‚Wir haben hier verglichen mit den USA nur ein schwaches Aufsichtssystem'*[33]

[32] http://www.nap.edu/openbook.php?record id=12452

und dass „als es darum ging, die Notwendigkeit und Verhältnismäßigkeit dessen, was sie erheben dürften, zu beurteilen, die künftigen amerikanischen Nutzer gesagt bekamen, das sei ‚eure Entscheidung'". Die juristischen Berater des GCHQ erklärten der NSA Berichten zufolge, dass *‚der parlamentarische Ausschuss für Nachrichten- und Sicherheitsdienste (ISC), der die Arbeit der Behörden überwacht, ‚Verständnis für die Schwierigkeiten der Nachrichtendienste habe' und dass Beschwerden des Überwachungsbeauftragten über die Nachrichtendienste unter dem ‚Mantel der Verschwiegenheit' geschähen. Überdies habe das zuständige Gericht (Investigatory Powers Tribunal, IPT) Beschwerden über die Behörden , bisher immer zu unseren Gunsten entschieden.'"*

77. Für diese Überwachungspraktiken wird weitaus mehr Transparenz benötigt, einschließlich Veröffentlichungen über die Einzelheiten aller Programme (mit einem Minimum an Zurückhaltung von Informationen zum Schutz von Quellen und Methoden), damit die Medien, die Zivilgesellschaft und einzelne Personen die Vorgehensweisen der Regierung nachvollziehen und wenn nötig kritisieren können. Für die Ermächtigung groß angelegter Überwachungsmaßnahmen wäre eine parlamentarische Zustimmungspflicht – wie es sie in anderen Ländern, besonders Deutschland, gibt – angemessen.

78. Eine breitere Besetzung der Aufsichtsgremien wäre eine Möglichkeit, diesen zu helfen, unverhältnismäßiger Überwachung besser zu begegnen – insbesondere sollten die Aufsichtsgremien auch mit Personen besetzt sein, die über das nötige technische Fachwissen verfügen, um komplexe Überwachungssysteme zu verstehen. Dies ist, wie wir inzwischen aus zur Einsicht freigegebenen Anordnungen wissen, eine ernsthafte Herausforderung für das US-amerikanische Gericht für die Überwachung der Auslandsgeheimdienste (FISC) geworden. Strenge und aggressive Sicherheitsüberprüfungen als Auflage für die Beteiligung an Überwachungsmaßnahmen (außer für Mitglieder des Parlaments), würden die Zahl derer, die dazu bereit sind, reduzieren.

WAHRHEITSBEKUNDUNG

Ich glaube, dass die in dieser Aussage gemachten Angaben wahr sind.

[33] Fn. 1 oben

UNTERZEICHNET: (Ian Brown)

DATUM: (27/9/13)

Beschwerde Nr.: 58170/13

VOR DEM EUROPÄISCHEN GERICHTSHOF FÜR MENSCHENRECHTE

(1)BIG BROTHER WATCH;
(2)OPEN RIGHTS GROUP;
(3)ENGLISH PEN;
(4)DR. CONSTANZE KURZ

Beschwerdeführer

-v-

VEREINIGTES KÖNIGREICH

Beschwerdegegner

ZEUGENAUSSAGE
DR. IAN BROWN

Deighton Pierce Glynn Solicitors
Center Gate
Colston Avenue
Bristol BS1 4TR

Tel: 0117 317 8133
Fax: 0117 317 8093
REF: OC/2265/001
www.deightonpierceglynn.co.uk

S. 19

Person A (Deutschland) — E-Mail — Person B (Vereinigtes Königreich)

Daten fließen durch Unterseekabel

Vorrichtung des GCHQ fängt unter einer Anordnung allgemeiner Art gemäß RIPA Abschnitt 8, Absatz 4 Daten aus dem Kabel ab

Daten werden über Glasfaserkabel an die GCHQ-Server weitergeleitet

Sichtung der Daten auf den GCHQ-Servern zur Verringerung des Volumens, Entsorgung von irrelevantem Material

Speicherung der Daten auf den GCHQ-Servern (Inhalte 3 Tage, Metadaten 30 Tage lang), die Daten werden fortlaufend gelöscht

NSA-Mitarbeiter NSA-Mitarbeiter NSA-Mitarbeiter NSA-Mitarbeiter

GCHQ-Mitarbeiter GCHQ-Mitarbeiter GCHQ-Mitarbeiter GCHQ-Mitarbeiter

GCHQ- und NSA-Mitarbeiter durchsuchen die Server des GCHQ unter Anwendung von Selektoren (ein Teil dieses Arbeitsprozesses ist möglicherweise automatisiert)

Geheimdienstbericht (über Einzelne, Gruppen, etc.)

Entschlüsselung verschlüsselter Nachrichten

Weitere Verwendung der Information durch die NSA

Zusätzliche Schritte des GCHQ, darunter Weiterleitung an andere Behörden zwecks weiterer Maßnahmen, Korrekturen/Ergänzungen der Stichwortlisten etc.

Weiterleitung gewonnener Erkenntnisse der NSA an den GCHQ und möglicherweise an Drittstaaten

S. 23

Abbildung 2: Rechtsweg für die Genehmigung zur Überwachung von Inhalten

Auf Grundlage geheimdienstlicher Informationen und Handlungsbedarfs nennt der Antragsteller die zu überwachende Adresse des Ziels/der Kommunikationen. Der Antrag auf eine Überwachungsanordnung wird durch eine Begründung, warum die Grundsätze der Notwendigkeit und Verhältnismäßigkeit erfüllt sind, vervollständigt.

Der Antrag auf eine Überwachungsanordnung wird an den Bereichsleiter übermittelt.

Gegebenenfalls wird juristischer Rat eingeholt

Notwendigkeit und Verhältnismäßigkeit werden gegen den geheimdienstlichen Erkenntnisbedarf abgewogen

Der Antrag auf eine Überwachungsanordnung wird an das zuständige Ministerium (z.B. Innenministerium, Außenministerium) weiter geleitet, wo Mitarbeiter der Anordnungsabteilung überprüfen, ob die Kriterien gemäß RIPA erfüllt sind.
Ein leitender Beamter erteilt die Genehmigung für die Weiterleitung an den zuständigen Minister. Auf spezifische Risiken oder rechtliche Fragen wird durch entsprechende Kommentare hingewiesen.

Der Antrag auf eine Überwachungsanordnung wird zur
Genehmigung an den Minister weitergeleitet. Der Minister kann eine
mündliche Unterrichtung oder weitere Informationen verlangen.
Bei Einverständnis erteilt der Minister
eine Überwachungsanordnung, die bei schweren Verbrechen
für 3 Monate, bei einer Gefährdung der nationalen Sicherheit für 6 Monate gilt.

Der Beauftragte für Kommunikationsüberwachung (IoCC) überwacht alle Stadien des Genehmigungsverfahrens