18. Wahlperiode

Deutscher Bundestag
1. Untersuchungsausschuss
nach Artikel 44 des Grundgesetzes

Nur zur dienstlichen Verwendung

Stenografisches Protokoll
der 122. Sitzung
- endgültige Fassung* -

1. Untersuchungsausschuss
Berlin, den 15. Dezember 2016, 9.00 Uhr
Paul-Löbe-Haus, Europasaal (4.900)
10557 Berlin, Konrad-Adenauer-Str. 1

Vorsitz: Prof. Dr. Patrick Sensburg, MdB

Tagesordnung - Öffentliche Beweisaufnahme

Tagesordnungspunkt

* Hinweis:
Die Sachverständigen King und Wilson Palow haben keine Korrekturwünsche übermittelt.

Mitglieder des Ausschusses

	Ordentliche Mitglieder	**Stellvertretende Mitglieder**
CDU/CSU	Sensburg, Prof. Dr. Patrick Lindholz, Andrea Schipanski, Tankred Warken, Nina	Marschall, Matern von Wendt, Marian
SPD	Flisek, Christian Mittag, Susanne	Zimmermann, Dr., Jens
DIE LINKE.	Renner, Martina	Hahn, André, Dr.
BÜNDNIS 90/DIE GRÜNEN	Notz, Dr. Konstantin von	Ströbele, Hans-Christian

Fraktionsmitarbeiter

CDU/CSU	Feser, Andreas, Dr. Allers, Fried-Heye Fischer, Sebastian D. Schrot, Jacob Wehrl, Wolfgang, Dr.
SPD	Ahlefeldt, Johannes von Dähne, Harald, Dr. Hanke, Christian Diego Weiß, Benjamin
DIE LINKE.	Halbroth, Anneke Martin, Stephan
BÜNDNIS 90/DIE GRÜNEN	Kant, Martina Hortolani, Johanna

Beauftragte von Mitgliedern der Bundesregierung

Bundeskanzleramt	Jipp, Daniel Heinemann, Martin Kämmerer, Marie Metscher, Andreas Wolff, Philipp Neist, Dennis Pachabeyan, Maria
Bundesministerium des Innern	Akmann, Torsten Blidschun, Jürgen Arthur Brandt, Karsten, Dr. Darge. Tobias, Dr. Kiehn, Eva Hofmann, Christian Matthes, Thomas Weiss, Jochen
Bundesministerium für Wirtschaft und Energie	Krüger, Philipp-Lennart
Bundesministerium für Verteidigung	Theis, Björn Voigt, Rüdiger
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	Kremer, Dr. Bernd

Teilnehmer Bundesrat

LV Hessen	Steinbach, Arvid

Original

(Beginn: 9.06 Uhr)

Vorsitzender Dr. Patrick Sensburg: Meine Damen und Herren, ich eröffne die 122. Sitzung des 1. Untersuchungsausschuss der 18. Wahlperiode. Ich stelle fest, die Öffentlichkeit ist hergestellt. Die Öffentlichkeit und die Vertreter der Presse darf ich an dieser Stelle ganz herzlich begrüßen.

Ich frage jetzt mal ganz kurz unsere Sachverständigen: Haben Sie Ton, die Übersetzung auf dem Ohr? Do you hear the interpreter? Hören Sie die Übersetzung?

(Die Sachverständigen nicken)

- Beide können die Übersetzung gut hören. - Gut. Dann seien auch Sie noch mal ganz herzlich begrüßt.

Bevor ich zum eigentlichen Gegenstand der heutigen Sitzung komme, gestatten Sie mir einige Vorbemerkungen.

Ton- und Bildaufnahmen sind während der öffentlichen Beweisaufnahme grundsätzlich nicht zulässig. Wegen des besonderen öffentlichen Interesses haben die Obleute vorgeschlagen, nach § 13 des Untersuchungsausschussgesetzes von der heutigen Sitzung ausnahmsweise eine Videoaufzeichnung durch die Bundestagsverwaltung fertigen zu lassen. Diese wird im Hauskanal des Deutschen Bundestages live übertragen. Hierzu ist nach § 13 PUAG neben dem Einverständnis der Sachverständigen, das diese bereits erteilt haben, auch ein Beschluss des Ausschusses mit der Mehrheit von zwei Dritteln der anwesenden Mitglieder erforderlich. Wir sollten dies nach meiner Meinung so beschließen, dass wir live im Hauskanal übertragen. Deswegen frage ich: Wer dafür ist, dass die Sachverständigenanhörung im Bundestagskanal übertragen wird, den bitte ich um

Übersetzung

Original

das Handzeichen. - Herzlichen Dank. - Gegenstimmen? - Enthaltungen? - Keine. Damit ist dies mit Einstimmigkeit so beschlossen.

Sonstige Bild-, Ton-und Filmaufzeichnungen sind nicht zulässig; entsprechende Geräte sind abzuschalten. Ein Verstoß gegen dieses Gebot kann nach dem Hausrecht des Bundestages nicht nur zu einem dauernden Ausschluss von den Sitzungen dieses Ausschusses, sondern auch des ganzen Hauses führen sowie gegebenenfalls auch strafrechtliche Konsequenzen nach sich ziehen. Ich bitte, dies also zu berücksichtigen. Die Live-Übertragung findet ja im Bundestagskanal statt.

Ich rufe den **einzigen Punkt der Tagesordnung** auf:

> Öffentliche Anhörung von Sachverständigen
>
> **Eric King,** „Don't spy on uns"
> (Beweisbeschluss SV-17)
>
> **Caroline Wilson Palow,**
> Privacy International
> (Beweisbeschluss SV-17)

In der 122. Sitzung des 1. Untersuchungsausschuss findet die öffentliche Beweisaufnahme aufgrund des Beweisbeschlusses SV-17 statt. Danach wird Beweis erhoben zum Untersuchungsauftrag - Bundestagsdrucksachen 18/843 und 18/8683 - durch Anhörung von Sachverständigen aus dem Vereinigten Königreich. Diese Anhörung findet ausschließlich öffentlich statt.

Wir werden die Anhörung gegen circa 10.10 Uhr für eine namentliche Abstimmung im Plenum unterbrechen müssen. Das lässt sich leider nicht verhindern, weil dann alle Ausschussmitglieder zur Abstimmung den Saal verlassen müssen. Wir kommen aber sofort nach der Abstimmung wieder, und dann setzen wir die Anhörung fort.

An dieser Stelle darf ich unsere heutigen Sachverständigen in alphabetischer Reihenfolge herzlich begrüßen, zuerst Herrn Eric King, Director der Nichtregierungsorganisation „Don't spy on us", und Frau Caroline Wilson Palow, General

Übersetzung

Original

Council bei der Nichtregierungsorganisation Privacy International. Schön, dass Sie zu uns gekommen sind. Frau Wilson Palow, Herr King, ganz herzlichen Dank, dass Sie meiner Einladung gefolgt sind, den weiten Weg auf sich genommen haben und dem Ausschuss für diese Anhörung zur Verfügung stehen. Das ist der einzige parlamentarische Untersuchungsausschuss, der sich mit den von Edward Snowden veröffentlichten Vorgängen beschäftigt. Daher freue ich mich sehr, dass Sie uns bei der Aufklärung unterstützen, die ja nicht nur eine rückwärtsgewandte ist, sondern immer auch wieder den Blick in die Zukunft wagt, welche Dinge wir empfehlen müssen. Es gibt hinterher in unserem Abschlussbericht einen Empfehlungsteil. Daher ist es für mich eine besondere Freude, dass Sie uns vielleicht auch Hinweise mit Blick in die Zukunft geben, was besser gemacht werden kann.

Die Situation im Vereinigten Königreich war bereits Gegenstand einer Sachverständigenanhörung am 1. Dezember 2016. Dass Sie heute hier sind, gibt uns Gelegenheit, unsere dabei gewonnenen Erkenntnisse gemeinsam mit Ihnen zu vertiefen.

Ich habe Sie darauf hinzuweisen, dass die Bundestagsverwaltung nicht nur eine Video-Liveübertragung, sondern auch eine Tonbandaufnahme der Sitzung fertigt. Diese dient ausschließlich dem Zweck, die stenografische Aufzeichnung der Sitzung zu erleichtern. Die Aufnahme wird nach Erstellung des Protokolls gelöscht.

Das Protokoll dieser Anhörung wird Ihnen nach Fertigstellung zugestellt. Sie haben dann, falls dies gewünscht ist, die Möglichkeit, innerhalb von zwei Wochen Korrekturen und Ergänzungen vorzunehmen und uns dann diese zurückzusenden. - Haben Sie hierzu Fragen?

(Die Sachverständigen schütteln den Kopf)

- Okay. - Sie haben die Gelegenheit erhalten, ein schriftliches Gutachten einzureichen. Soweit Sie davon Gebrauch gemacht haben, wird dieses

Übersetzung

Original

dann auf der Website des Ausschusses veröffentlicht werden.

Frau Wilson Palow, Herr King, vor Ihrer Anhörung habe ich Sie zunächst zu belehren. Sie sind als Sachverständige geladen worden. Als Sachverständige sind Sie verpflichtet, die Wahrheit zu sagen. Ihr Gutachten ist unparteiisch und nach bestem Wissen und Gewissen zu erstatten.

Ich habe Sie außerdem auf die möglichen strafrechtlichen Folgen eines Verstoßes gegen diese Wahrheitspflicht hinzuweisen. Wer vor dem Untersuchungsausschuss uneidlich falsch aussagt, kann gemäß § 162 in Verbindung mit § 153 des Strafgesetzbuches mit Freiheitsstrafen von drei Monaten bis zu fünf Jahren oder mit Geldstrafe bestraft werden.

Nach § 28 in Verbindung mit § 22 Absatz 2 des Untersuchungsausschussgesetzes können Sie die Auskunft auf solche Fragen verweigern, deren Beantwortung Sie selbst oder Angehörige im Sinne des § 52 Absatz 1 der Strafprozessordnung der Gefahr aussetzen würde, einer Untersuchung nach einem gesetzlich geordneten Verfahren ausgesetzt zu werden. Dies betrifft neben Verfahren wegen einer Straftat oder Ordnungswidrigkeit auch gegebenenfalls Disziplinarverfahren, wenn dies bei Ihnen in Betracht kommen könnte. Auf jeden Fall können Sie in solchen Fällen von Ihrem Aussageverweigerungsrecht Gebrauch machen. - Haben Sie hierzu Fragen?

(Die Sachverständigen schütteln den Kopf)

Sachverständige Caroline Wilson Palow: No.

Vorsitzender Dr. Patrick Sensburg: Okay, danke schön. - Nach diesen notwendigen Vorbemerkungen darf ich Ihnen den geplanten Ablauf kurz darstellen. Zu Beginn haben Sie nach § 28 in Verbindung mit § 24 Absatz 4 des Untersuchungsausschussgesetzes die Gelegenheit, zum Beweisthema im Zusammenhang vorzutragen. Die Reihenfolge richtet sich nach dem Alphabet bzw. damit auch nach Ihrer Sitzordnung. Ich bitte Sie, sich bei Ihren einführenden Statements jeweils in

Übersetzung

Sachverständige Caroline Wilson Palow: *Nein.*

Original

einem Zeitrahmen von zehn Minuten zu bewegen. Also, zehn Minuten für ein Eingangsstatement.

Danach haben die vier Fraktionen die Möglichkeit, Fragen zu stellen. Zunächst darf jeder Abgeordnete entweder zwei Fragen an einen Sachverständigen stellen oder zwei Sachverständige jeweils mit einer Frage befragen. Nach der Beantwortung dieser Fragen in der ersten Runde schließt sich eine weitere Fragerunde an, sodass jede Fraktion ausreichend Gelegenheit erhält, mit ihren Mitgliedern Fragen an Sie zu stellen, und Sie ausreichend Gelegenheit haben, Antworten zu geben. Das ist das übliche Prozedere bei Sachverständigenanhörungen.

Wir werden versuchen, die Anhörung gegen circa 10.50 Uhr zu beenden, da sich um 11 Uhr eine Beratungssitzung anschließt, der dann eine Zeugenvernehmung folgt, die wahrscheinlich nicht ganz um 11.30 Uhr beginnen wird, sondern, ich sage mal, um 12 Uhr/12.30 Uhr. Da müssen wir gucken, wie schnell wir mit der Beratungssitzung durchkommen.

Für Sie ist entscheidend, dass wir um circa 10.50 Uhr mit dieser Sachverständigenanhörung durch sind. - Gibt es hierzu Fragen Ihrerseits?

Sachverständige Caroline Wilson Palow: No.

Vorsitzender Dr. Patrick Sensburg: Herzlichen Dank. - Gemäß dem Beweisbeschluss, der unserer heutigen Anhörung zugrunde liegt - ich hatte es eben gesagt, es ist der Beweisbeschluss SV-17 -, führen wir eine Anhörung durch zur

> parlamentarischen, öffentlichen und wissenschaftlichen Debatte im Vereinigten Königreich zu den Fragen der Tätigkeit der Nachrichtendienste des Vereinigten Königreichs im Bereich der Fernmeldeaufklärung …

- des sogenannten SIGINT -,

> deren parlamentarischer Kontrolle und des Schutzes der Freiheit und

Übersetzung

Sachverständige Caroline Wilson Palow: *Nein.*

Original

Privatheit insbesondere zu relevanten Änderungen der Rechtslage seit den Enthüllungen von Edward Snowden im Jahre 2013 mit Blick auf

- die gesetzlichen Ermächtigungen … zur … und

- den rechtlichen Schutz … vor der Erhebung, Speicherung auf Vorrat und Weitergabe von Daten aus und über Telekommunikationsvorgänge und Internetnutzung

und deren Bewertung aus Sicht im Vereinigten Königreich tätiger Forschungs- und Beratungsinstitutionen.

Das ist der Inhalt des Beweisbeschlusses.

Zu diesen Fragen hat der Ausschuss bereits am 1. Dezember - ich hatte es gesagt - vier Sachverständige gehört, nämlich Professor Richard Aldrich von der University of Warwick, den Independent Reviewer of Terrorism Legislation David Anderson, Silkie Carlo von der Nichtregierungsorganisation Liberty und den Prozessrechtsanwalt Ben Jaffey. Alle vier werden Sie vermutlich kennen. Das war eine ganz, ganz spannende Sachverständigenanhörung. Dabei sind viele interessante Punkte zur Sprache gekommen.

Wir freuen uns, dass wir jetzt mit Ihnen diese Themen vertiefen können. Frau Wilson Palow und Herr King, wir erhoffen uns nun zahlreiche Erkenntnisse von Ihnen. Ich darf Sie, wie ich es gerade gesagt habe, jetzt um Ihre Eingangsstatements bitten. Wir fangen alphabetisch an, ausnahmsweise mal nicht „ladys first“, sondern alphabetisch, und wir würden mit Ihnen, Herr King, anfangen, und Sie hätten jetzt Gelegenheit für Ihr Eingangsstatement. Zehn Minuten Zeit haben Sie dafür, und wir sind schon ganz gespannt. - Herr King, Sie haben das Wort.

Sachverständiger Eric King: Hello, good morning! I wish to thank the committee of inquiry for giving me this opportunity to testify. My work is

Übersetzung

Sachverständiger Eric King: *Hallo und guten Morgen! Ich danke dem Untersuchungsausschuss für die Gelegenheit, hier heute vor Ihnen zu sprechen. Meine*

Original	*Übersetzung*
focused around human rights and signals intelligence, but for the last year, as you noted, I have acted as director of the Don't Spy on Us coalition of UK NGOs working around the reform of surveillance laws in the UK. Prior to that, I was deputy director at Privacy International. It's important to note I don't represent either of those entities today, I instead appear in my own capacity as an independent expert.	*Arbeit bezieht sich in erster Linie auf Menschenrechte und Signalaufklärung [SIGINT]. Seit einem Jahr bin ich jedoch, wie Sie erwähnten, als Leiter der Koalition „Don't spy on us" tätig, in der sich britische NGOs zusammengeschlossen haben, die sich mit der Reform der Überwachungsgesetzgebung in Großbritannien beschäftigen. Davor war ich stellvertretender Direktor von Privacy International. Es ist mir wichtig, darauf hinzuweisen, dass ich vor diesem Ausschuss keine dieser Organisationen vertrete. Ich bin vielmehr in meiner Eigenschaft als unabhängiger Experte hier.*
As was mentioned, I understand the committee has received evidence on the recent changes to UK surveillance law with the passing of the Investigatory Powers Act 2016. I also understand the committee has heard from witnesses on the state of UK-based litigation from parties including Privacy International. I don't wish to duplicate that evidence. Instead, I have noted an interest on behalf of the committee regarding the so-called "no-spy pact" that exists within the Five Eyes' alliance and other partnerships. So, we'll use this introductory opportunity to set out a very brief summary of the conclusions of my work in this area.	*Mir ist bekannt, dass dem Ausschuss bereits Informationen zu den jüngsten Änderungen der britischen Überwachungsgesetze vorliegen, die mit der Verabschiedung des Investigatory Powers Act 2016 in Kraft getreten sind. Mir ist auch bekannt, dass der Ausschuss Aussagen zum Stand der Gerichtsverhandlungen gehört hat, die in Großbritannien von Klägern wie Privacy International angestrengt wurden. Ich möchte diese Aussagen hier nicht wiederholen. Stattdessen würde ich gerne auf das Interesse des Ausschusses an dem so genannten No-Spy-Abkommen eingehen, das innerhalb der Allianz der Five-Eyes-Staaten sowie innerhalb anderer staatlicher Partnerschaften besteht. Nutzen wir die Gelegenheit dieser einführenden Stellungnahme also für eine kurze Zusammenfassung der Ergebnisse meiner Arbeit auf diesem Gebiet.*
Documents released by Edward Snowden provide some of the early insight into how these original terms have been interpreted by the various parties and applied to modern-day practices. It seems there is, instead, a general understanding that citizens will not be directly targeted where the communications are incidentally intercepted. There will be an effort to minimise the use and analysis thereof by the intercepting state. A leaked copy of the US National Security Agency Directive on Collection, Processing and Dissemination of Allied Communications states that "under the UKUSA arrangement, both governments agree to exchange communications intelligence, products, methods, techniques, as applicable, so long as it was not prejudicial to national interests". This agreement has evolved to	*Die von Edward Snowden veröffentlichten Dokumente bieten frühe Erkenntnisse darüber, wie diese ursprünglichen Vertragsbedingungen von den verschiedenen Parteien interpretiert und auf moderne Geheimdienstpraktiken angewendet wurden. Danach scheint es statt einer Verpflichtung die allgemeine Übereinkunft zu geben, dass im Falle eines zufälligen Abfangens von Kommunikationsdaten Bürger [der Vertragsstaaten] nicht gezielt Gegenstand der Signalaufklärung werden. Der Staat, der die Daten abgefangen hat, wird sich bemühen, deren Nutzung und Analyse auf ein Minimum zu beschränken. In einer durchgesickerten Kopie der Direktive der US National Security Agency zur Erfassung, Bearbeitung und Weitergabe von Kommunikationsdaten von Verbündeten heißt es, dass „im Rahmen der UKUSA-Vereinbarung beide Regierungen übereinkommen, dass sie Daten sowie Produkte, Methoden und Techniken der*

Original	*Übersetzung*
include a common understanding that both governments will not target each other's citizens or persons. The head of the New Zealand intelligence service, the GCSB, has said in public that he also views the arrangement as providing a similar set of protections. He stated publicly,	*Fernmeldeaufklärung soweit zutreffend austauschen, sofern dies nicht dem jeweiligen nationalen Interessen entgegensteht.“ Diese Vereinbarung wurde weiterentwickelt und umfasst das Einvernehmen, dass keiner der beiden Staaten gezielt Bürger oder Aufenthaltsberechtigte des jeweils anderen Staats abhört. Der Leiter des neuseeländischen Geheimdienstes GCSB erklärte öffentlich, dass die Vereinbarung seiner Ansicht nach einen ähnlichen Schutzrahmen [wie ein No-Spy-Abkommen] bietet. Er erklärte öffentlich:*
you cannot read the UKUSA arrangement without coming to the conclusion that the full sharing which is described can only be done if there is no deliberate targeting against each other's governments or nationals.	*Man muss beim Lesen der UKUSA-Vereinbarung zu dem Schluss kommen, dass der volle Informationsaustausch, der darin beschrieben wird, nur dann stattfinden kann, wenn es keine gezielten Abhöraktionen gegen die Bürger oder Regierungen des jeweils anderen Staates gibt.*
It is assumed, but not known, that the other parties to the Five Eyes arrangement, Canada and Australia, view the arrangement in the same light. Numerous documents disclosed as part of the Snowden revelations show that this underlying agreement manifests itself not just in policy documents but in the underlying technical architecture of the actual SIGINT collection systems themselves. So, even with these bulk interception systems there are technical rules that are put in place by all parties that minimise metadata in content from IP addresses known to be in UKUSA countries.	*Es wird davon ausgegangen, auch wenn es nicht mit Sicherheit bekannt ist, dass die anderen Parteien der Five-Eyes-Vereinbarung, Kanada und Australien, dies ähnlich sehen. Zahlreiche Dokumente, die Teil der Snowden-Enthüllungen waren, belegen, dass diese grundlegende Vereinbarung nicht nur in Strategiepapieren, sondern auch in der zugrundeliegenden technischen Architektur der SIGINT-Datenerfassungssysteme zum Tragen kommt. Es gibt also sogar in diesen Systemen zur massenhaften Erfassung von Daten technische Regeln, die von allen Parteien eingeführt wurden und die dafür sorgen, dass aus Kommunikationsinhalten, die von IP-Adressen in UKUSA-Ländern stammen, weniger Metadaten erfasst werden.*
However, this general understanding does not prevent Five Eye states from targeting each other's nationals or collaborating to analyse information about their own citizens collected by a second party on a bulk scale. When a Five Eye's partner wants to target the citizens of another country, they first attempt to do so with the other country's consent. It is unclear on what basis this consent may be given or withheld, but the same directive referenced earlier explains:	*Dieses grundlegende Einvernehmen hindert die einzelnen Five-Eyes-Staaten jedoch nicht daran, Kommunikationsdaten von Bürgern der jeweils anderen Staaten zu erfassen oder darin zusammenzuarbeiten, Daten ihrer eigenen Bürger zu analysieren, die massenhaft von einer „zweiten Partei“ erfasst wurden. Wenn ein Mitglied der Five Eyes Kommunikationsdaten von Bürgern eines anderen Mitglieds erfassen möchte, wird es zunächst versuchen, dies mit dem Einverständnis des betreffenden Staates zu tun. Es ist unklar, auf welcher Grundlage dieses Einverständnis*

Nur zur dienstlichen Verwendung

Original

> There are circumstances when targeting of second-party persons and communications systems, with the full knowledge and cooperation of one or more second parties, is allowed when it is in the best interests of both nations.

The directive goes on to make clear that these circumstances may include targeting a UK citizen located in London using a British telephone system, targeting a UK person located in London using an internet service provider in France, or targeting a Pakistani person located in the UK using a UK internet service provider. These leaked GCHQ documents also show that additional authorisation is needed by British intelligence services should they wish to target the citizens of a Five Eyes country. This importantly applies no matter where that citizen is in the world.

There have also been incidents where Five Eye states have consented to other parties in the Five Eyes alliance making use of material intercepted under bulk intercept programs related to their own systems. Previous practice across the Five Eyes would require that minimisation or the immediate deletion of such incidentally collected material was a requirement to comply with UKUSA. Such a practice could mean removing the names of identifiable UKUSA citizens from finalised intelligence reports, or when conducting analysis of large datasets that include UKUSA citizens replacing personally identifiable information with a hash or a pseudonymous tag related to them. Then, in such individual cases, permission could be sought by the relevant government to seek to unminimise such material. But this policy, in practice, that has existed for a long time, is appearing to be relaxed in some areas. One example of this is a UK change in policy in 2007 to permit the NSA to unminimise all incidentally collected UK contact identifiers, in-

Übersetzung

erklärt oder verweigert wird, aber in der zuvor zitierten Direktive heißt es:

> *Es gibt Umstände, unter denen die Erfassung von Kommunikationsdaten von Bürgern und Kommunikationssystemen einer zweiten Partei mit Kenntnis und in Zusammenarbeit von einer oder mehreren zweiten Parteien zulässig ist, wenn dies zum Vorteil beider Staaten ist.*

Die Direktive erläutert im Folgenden Beispiele für derartige Umstände, so das Abhören eines britischen Bürgers in London, der über das britische Telefonnetz telefoniert, das Abhören eines britischen Bürgers in London, der einen Internetanbieter in Frankreich nutzt, oder das Abhören eines pakistanischen Bürgers in Großbritannien, der einen britischen Internetanbieter nutzt. Die durchgesickerten Dokumente des GCHQ belegen weiterhin, dass die britischen Geheimdienste weitere Genehmigungen benötigen, falls sie Kommunikationsdaten von Bürgern eines anderen Five-Eyes-Staates erfassen wollen. Wichtig ist, dass dies unabhängig davon gilt, wo sich dieser Bürger aufhält.

Es gab auch Fälle, in denen Five-Eyes-Mitglieder es anderen Five-Eyes-Mitgliedern gestattet haben, Material aus Programmen zur massenhaften Datenerfassung zu nutzen, die auf ihre eigenen Systeme abzielten. Die bisherige Praxis in den Five-Eyes-Staaten sah so aus, dass zufällig erfasstes Datenmaterial dieser Art sofort gelöscht oder „minimiert“ werden musste, um den Bestimmungen der UKUSA-Vereinbarung Folge zu leisten. Das hieß, dass beispielsweise die Namen von identifizierbaren UKUSA-Bürgern aus den endgültigen Geheimdienstberichten gelöscht wurden oder bei der Analyse großer Datenmengen, die auch Daten von UKUSA-Bürgern enthielten, personenbezogene Daten durch Rautenzeichen oder Pseudonyme ersetzt wurden. In Einzelfällen konnte dann von der betreffenden Regierung die Genehmigung beantragt werden, dieses Datenmaterial wiederherzustellen und vollständig zu nutzen. Diese Regeln, die es in der Praxis bereits seit langem gibt, scheinen in einigen Bereichen gelockert worden zu sein. Ein Beispiel hierfür ist die Änderung der britischen Richtlinien aus dem Jahr 2007, die der NSA gestattet, alle zufällig erfassten Identifikatoren von

Original	*Übersetzung*
cluding IP and email addresses, fax and cell-phone numbers, for use in analysis. Given the reported extraordinary scale of NSA collection, this change in policy means that for many UK citizens their communications are being intercepted by the NSA, and the NSA has had express permission to analyse them, even identifying those UK citizens within it. This policy essentially permits the analysis of information relating to UK citizens by allied countries - which information the UK intelligence agencies would not themselves be permitted to analyse without additional authorisations. The NSA could then share that information derived from the analysed communications with foreign and, potentially, British intelligence agencies, potentially circumventing UK authorisation procedures.	*britischen Kontakten wiederherzustellen und für Datenanalysen zu nutzen, darunter auch IP- und E-Mail-Adressen sowie Fax- und Telefonnummern. Angesichts des immensen Datenvolumens, das die NSA Berichten zufolge erfasst, bedeutet diese Richtlinienänderung für viele britische Bürger, dass ihre Kommunikationsdaten von der NSA abgefangen werden und die NSA die ausdrückliche Genehmigung hat, diese Daten zu analysieren, einschließlich der darin enthaltenen personenbezogenen Daten, mit denen sich britische Bürger identifizieren lassen. Im Kern gestattet es diese Richtlinie befreundeten Staaten, die Daten britischer Bürger zu analysieren - Daten, die der britische Geheimdienst selbst nur mit zusätzlicher Genehmigung auswerten dürfte. Die NSA dürfte die so gewonnenen Informationen aus den analysierten Kommunikationsdaten dann an ausländische - und damit potenziell auch an die britischen - Geheimdienste weitergeben. Damit könnten die britischen Genehmigungsverfahren potenziell umgangen werden.*
As all policy relating to intelligence exchange in the UK is subjected to a “neither confirm nor deny” policy, this change in policy has not been officially acknowledged by the government. There is no reason given or further detail provided as to why the UK permitted such a radical change in policy. While there is a preference and understanding that Five Eyes' governments will not target each other's citizens, if consent isn't provided then states do reserve the right to act unilaterally. The directive I've mentioned already states:	*Da die britische Regierung in Bezug auf die Richtlinien zum Austausch geheimdienstlicher Informationen nach der Regel „weder bestätigen noch dementieren“ verfährt, wurde diese Änderung nicht offiziell bestätigt. Es gibt weder eine offizielle Begründung dafür, warum Großbritannien eine derart radikale Änderung der Richtlinien genehmigt hat, noch nähere Einzelheiten zur Änderung. Obwohl es unter den Five-Eyes-Staaten ein Einvernehmen und eine bevorzugte Vorgehensweise gibt, wonach die Bürger der jeweils anderen Partnerstaaten nicht Objekt der Überwachung werden, behalten sich die Staaten das Recht eines unilateralen Vorgehens für den Fall vor, dass eine Zustimmung nicht erteilt wird. Die oben zitierte Direktive erklärt hierzu:*
When it is in the best interest of each other's nations, each reserve the right to conduct unilateral Comint	*Falls es im besten Interesse der jeweiligen Staaten ist, behält sich jeder der Staaten das Recht vor, unilateral COMINT*
- collection of signals intelligence -	*- die Erfassung von SIGINT-Daten -*
against each other's citizens and persons. Therefore under certain circumstances it may be advisable and allowable to target second-party persons and second-party	*gegen Bürger und Aufenthaltsberechtigte der jeweils anderen Staaten durchzuführen. Unter gewissen Umständen kann es daher ratsam und gestattet sein, unilateral Bürger und*

Original

> communication systems unilaterally when it is in the best interests of the US and necessary for US security.

For this reason, any suggestion that the UKUSA arrangement, the Five Eyes arrangement, creates a no-spy pact could be seen as misleading. Certainly, the arrangement makes it clear that there is no absolute prohibition on the targeting of Five Eyes allied parties. It's perhaps for this reason that President Obama felt able to state: "There is no country where we have a no-spy arrangement". And former NSA director, Michael Hayden, supported this statement explaining:

> No, we are not going to do no spy arrangements, it's just too hard to do, not even with the British.

Outside these Five Eyes states there are other countries that have agreed to the exchange of intelligence known as “third parties”. This, of course, includes Germany, which is a third party to the UKUSA arrangement. There are 41 such third parties. In Europe alone there are 23 such third-party countries. Of these, 14 countries have formed a group called SIGINT Seniors Europe. Beyond the existence of the group, there is very little known about the exchange between these parties or whether any attempt has been made to provide for similar protections for each other's citizens as exists between the second parties of the UKUSA arrangement. However, there should be no ambiguity about the policy regarding the targeting of third-party countries like Germany by second parties. An internal NSA presentation makes clear: We can and often do target the signals of most third-party foreign partners.

So, in conclusion, the UKUSA arrangement does not, in my view, amount to a no-spy pact. It does, however, in practice, afford some greater safeguards to those Five Eyes citizens who would otherwise be afforded none. My view is that a

Übersetzung

> *Kommunikationssysteme von zweiten Parteien zu überwachen, sofern dies im Interesse der USA liegt und für die Sicherheit der USA erforderlich ist.*

Die Annahme, dass die UKUSA-Vereinbarung - die Übereinkunft der Five-Eyes-Staaten - ein No-Spy-Abkommen darstellt oder beinhaltet, kann aus diesem Grund als irregeleitet betrachtet werden. Die Übereinkunft stellt eindeutig klar, dass es kein absolutes Verbot einer Überwachung von Bürgern der Five-Eyes-Partnerstaaten gibt. Dies mag der Grund sein, weshalb Präsident Obama sagen konnte: „Es gibt kein Land, mit dem wir ein No-Spy-Abkommen haben.“ Und der ehemalige Direktor der NSA, Michael Hayden, untermauerte diese Erklärung, als er erklärte:

> *Nein, wir schließen keine No-Spy-Abkommen, noch nicht einmal mit den Briten; das ist einfach zu schwierig zu bewerkstelligen.*

Außerhalb des Kreises dieser Five-Eyes-Staaten gibt es weitere Nationen, die so genannten „dritten Parteien“ [Third Parties], die einem Austausch von Geheimdienstinformationen zugestimmt haben. Hierzu zählt natürlich auch Deutschland, das eine dritte Partei im Sinne der UKUSA-Vereinbarung ist. Von diesen dritten Parteien gibt es insgesamt 41. In Europa sind es 23, von denen sich 14 zu den so genannten SIGINT Seniors Europe zusammengeschlossen haben. Wir wissen zwar, dass diese Gruppe existiert; aber darüber hinaus ist wenig darüber bekannt, wie und welche Informationen die Partnerstaaten austauschen oder ob versucht wurde, den Bürgern der jeweils anderen Partnerstaaten einen ähnlichen Schutzrahmen zu bieten, wie er zwischen den zweiten Parteien der UKUSA-Vereinbarung besteht. Das grundlegende Vorgehen bezüglich der Überwachung von Bürgern dritter Parteien wie Deutschland durch zweite Parteien ist jedoch eindeutig. Wie eine NSA-interne Präsentation deutlich macht, können wir die Kommunikationssignale der meisten dritten Parteien abfangen und tun dies auch.

Zusammenfassend kann ich also sagen, dass die UKUSA-Vereinbarung in meinen Augen kein No-Spy-Abkommen ist oder beinhaltet. In der Praxis bietet sie jedoch einen stärkeren Schutzrahmen für Bürger von Five-Eyes-Staaten, die andernfalls gar

Original	*Übersetzung*
better way of achieving this same goal is to respect the privacy rights of every individual no matter where in the world they may be and furnish them with the same statutory protections that a country's own citizens are entitled to. This needn't be constrained just to the Five Eyes countries, indeed I would encourage all states to provide such protections and encourage other states to do the same.	*nicht geschützt wären. Meiner Meinung nach ließe sich dies sehr viel besser dadurch erreichen, dass man die Persönlichkeitsrechte jedes Menschen achtet, ganz egal wo auf der Welt er sich aufhält, und indem jeder Staat allen Menschen denselben gesetzlichen Schutzrahmen bietet, den die eigenen Bürger genießen. Dies muss sich nicht auf die Five-Eyes-Staaten beschränken. Vielmehr würde ich alle Staaten dazu aufrufen, einen solchen gesetzlichen Schutz zu bieten und andere anzuregen, dasselbe zu tun.*
Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Dann machen wir mit dem zweiten Statement weiter. Ganz herzlichen Dank, dass auch Sie bei uns sind, Frau Wilson Palow. Sie haben jetzt zehn Minuten für Ihr Statement Zeit. Bitte schön.	
Sachverständige Caroline Wilson Palow: Thank you. And thank you to the committee for inviting me here today. - I am the general counsel of Privacy International, a charity based in London which is dedicated to defending the right to privacy around the world. As general counsel, I lead PI's legal team and I'm representing Privacy International here today.	***Sachverständige Caroline Wilson Palow:*** *Vielen Dank. Ich danke auch dem Ausschuss für die Einladung. - Ich bin General Counsel der gemeinnützigen Organisation Privacy International, die ihren Sitz in London hat und sich weltweit für den Schutz der Persönlichkeits- und Datenschutzrechte einsetzt. Als General Counsel leite ich die Rechtsabteilung von Privacy International und spreche hier und heute als Vertreterin der Organisation.*
You have asked us to speak about the changes that have taken place in the parliamentary, public and academic spheres since the revelations made by Edward Snowden, on issues concerning the activities of the UK intelligence services including any parliamentary oversight of their activities and, of course, the protection of privacy.	*Sie hatten darum gebeten, dass wir etwas über den Wandel im parlamentarischen, öffentlichen und universitären Bereich berichten, der seit den Snowden-Enthüllungen stattgefunden hat, sowie zu Fragen nach Aktivitäten der britischen Geheimdienste einschließlich der parlamentarischen Aufsicht über diese Aktivitäten und natürlich zum Datenschutz.*
I started at Privacy International in 2013, shortly before we all learned about the Snowden revelations, which has given me a front row seat to how they have affected the debate in the UK.	*Ich habe 2013 bei Privacy International angefangen, kurz bevor die Snowden-Enthüllungen bekannt wurden. Ich habe also aus nächster Nähe miterlebt, welche Auswirkungen sie auf die Debatte in Großbritannien hatten.*
So, I'm going to begin today with a short story about my own experiences with the evolving nature of transparency and oversight in the UK regarding the activities of the UK intelligence services. While there have been some improvements on both fronts, from a human rights perspective	*Lassen Sie mich daher mit einer kurzen Geschichte über meine eigenen Erfahrungen mit der sich verändernden Transparenz und Geheimdienstkontrolle in Großbritannien beginnen. Obwohl es in beidem Bereichen Fortschritte gab, gibt es aus Menschenrechts-*

Nur zur dienstlichen Verwendung

Original

there is still much work to be done. Along the way I've experienced some of the same frustrations that I understand this committee has at times experienced when faced with, sometimes the extremely strong, reluctance of the United Kingdom to discuss the activities of its intelligence services so that there can be a public debate around those activities. At times, it has taken significant effort to overcome this reluctance. And, even today, as admittedly much more has gone into the public domain, during the debate surrounding the Investigatory Powers Act, much is still shrouded in secrecy in a way that I think has hindered the public debate and a full understanding of the surveillance powers now enshrined in that act.

The initial reaction to the Snowden revelations in the UK was mixed. Several of the earliest news stories implicated the UK intelligence services, both as receiving intelligence from the US, that was gathered under what was identified at the time as the Prism program, and also as collecting vast amounts of data themselves through programs like Tempora, which was the mass interception of communications travelling under undersea fibre-optic cables. The initial reaction of the UK government, despite significant public attention at the time, was to rely on its "neither confirm nor deny" policy under which it refused to admit whether the programs referenced in the Snowden documents, even at the most abstract level, were actually being undertaken by the UK intelligence services. The hand of the UK government was forced, somewhat, when the US government admitted that Prism was in fact a real program being undertaken by the NSA and that information obtained under Prism was being shared with the UK. After this admission, the UK parliamentary oversight committee, the Intelligence and Security Committee, which oversees the intelligence services, released a short report in July 2013 stating that, while the UK had received intelligence from the US obtained via the Prism program, that sharing was entirely lawful and had been properly authorised under the laws

Übersetzung

perspektive noch viel zu tun. Angesichts der teils extrem starken Widerstände der britischen Regierung, über die Aktivitäten der Geheimdienste zu sprechen und so eine öffentliche Debatte zu diesem Thema zu ermöglichen, habe ich in dieser Zeit ähnlich frustrierende Erfahrungen gemacht wie dieser Ausschuss. Manchmal war erheblicher Aufwand nötig, um diese Widerstände zu überwinden. Und selbst heute, da im Rahmen der Debatte zum Investigatory Powers Act mehr öffentlich bekannt gemacht wurde, wird immer noch vieles in Schweigen gehüllt, und dies auf eine Weise, die meiner Meinung nach eine öffentliche Auseinandersetzung und ein umfassendes Verständnis der in diesem Gesetz enthaltenen Überwachungskompetenzen behindert.

Die Reaktionen auf die Snowden-Enthüllungen waren in Großbritannien zunächst sehr gemischt. Einige der frühesten Medienberichte beschuldigten die britischen Geheimdienste zum einen, nachrichtendienstliche Informationen von den USA erhalten zu haben, die im Rahmen des damals als PRISM identifizierten Programm erfasst wurden, und zum anderen, selbst riesige Datenmengen durch Programme wie Tempora erfasst zu haben, bei dem massenhaft Kommunikationsdaten aus Tiefsee-Glasfaserkabeln abgefangen wurden. Trotz der zu diesem Zeitpunkt bedeutenden öffentlichen Aufmerksamkeit folgte die britische Regierung weiterhin ihrer Strategie „weder bestätigen noch dementieren" und weigerte sich, einzuräumen, ob die in den Snowden-Dokumenten genannten Programme tatsächlich, und sei es auf der abstraktesten Ebene, von den britischen Geheimdiensten durchgeführt wurden. Etwas unter Druck gesetzt wurde Großbritannien, als die US-Regierung einräumte, dass es sich bei Prism tatsächlich um ein Programm handelt, das von der NSA durchgeführt wird, und dass Daten, die im Rahmen von Prism erfasst wurden, an Großbritannien weitergegeben wurden. Nach diesem Eingeständnis veröffentlichte das britische Intelligence and Security Committee (ISC), das für die Geheimdienstkontrolle zuständige parlamentarische Aufsichtsgremium, im Juli 2013 einen kurzen Bericht, der besagte, dass Großbritannien zwar nachrichtendienstliche Informationen von den USA erhalten habe, die durch das Prism-Programm gewonnen wurden, dass diese Datenweitergabe jedoch vollkommen rechtmäßig gewesen sei und entsprechend der

Nur zur dienstlichen Verwendung

Original

currently in place, including the Intelligence Services Act of 1994 and the regulations of the Investigatory Powers Act 2000.

This conclusion would come back to haunt the ISC when in February 2015, in response to a lawsuit filed by Privacy International, Liberty, Amnesty International and seven other NGOs, the UK Investigatory Powers Tribunal which also oversees the activities in the intelligence services ruled that the sharing of information between the US and the UK had been unlawful prior to December 2014 due to a lack of a publicly accessible legal framework governing that sharing. This lawsuit was the first in a series filed by Privacy International and other NGOs in the UK challenging the activities of the intelligence services. As you have already heard from experts who have appeared before this committee before, including Ms Carlo and Mr Jaffey, these lawsuits that were filed between July 2013 and June 2015 addressed the following types of surveillance: bulk interception of content in metadata, which is often referred to as communications data in the UK; intelligence sharing between the US and the UK; targeted and bulk hacking by the UK intelligence services; the collection of bulk personal datasets, which are large sets of data that can contain personally identifiable information; and the obtaining of communications data in bulk. The Snowden revelations provided some of the foundation for these lawsuits.

While these lawsuits were proceeding, and, we suspect, in some cases as a result of these lawsuits, the UK began to slowly release more information about the activities of the intelligence services. For instance, in February 2015, on the same day on which the UK government was to respond to the lawsuit on hacking, they released a draft code of practice on what they call "equipment interference", which encompasses hacking by the intelligence services. While far from perfect, that draft code was one of the first glimpses into the way the UK was establishing policies

Übersetzung

geltenden Gesetze - darunter der Intelligence Services Act von 1994 und die Richtlinien des Investigatory Powers Act von 2000 - korrekt autorisiert wurde.

Diese Erklärung sollte noch auf das ISC zurückfallen, denn im Februar 2015 entschied das UK Investigatory Powers Tribunal, das ebenfalls die Aktivitäten der Geheimdienste beaufsichtigt, anlässlich einer von Privacy International, Liberty, Amnesty International und sieben weiteren NGOs eingereichten Klage, dass die Weitergabe von Informationen zwischen den USA und Großbritannien vor dem Dezember 2014 unrechtmäßig war, da es zu diesem Zeitpunkt keinen öffentlich zugänglichen Rechtsrahmen für eine solche Weitergabe gab. Es war das erste einer Reihe von Gerichtsverfahren, die von Privacy International und weiteren NGOs in Großbritannien gegen die Aktivitäten der Geheimdienste angestrengt wurden. Wie Sie bereits von anderen Experten wissen, die vor diesem Ausschuss ausgesagt haben, darunter auch Ms. Carlo und Mr. Jaffey, ging es bei diesen Klagen, die zwischen Juli 2013 und Juni 2015 eingereicht wurden, um die folgenden Arten von Überwachung: die massenhafte Erfassung von Inhalten in Metadaten, die in Großbritannien oft als Kommunikationsdaten bezeichnet werden, der Austausch von Daten zwischen den USA und Großbritannien, gezieltes und massenhaftes Hacken durch die britischen Geheimdienste, die Erfassung von personenbezogenen Massendatensätzen, also von großen Datensätzen, die personenbezogene Informationen enthalten können, sowie die massenhafte Beschaffung von Kommunikationsdaten. Die Snowden-Enthüllungen lieferten zum Teil die Grundlagen für diese Gerichtsverfahren.

Im Laufe dieser Verfahren - und wir nehmen an, in einigen Fällen auch als Resultat der Verfahren - begann Großbritannien langsam damit, mehr Informationen über die Aktivitäten der britischen Geheimdienste freizugeben. So veröffentlichte die britische Regierung im Februar 2015 - am selben Tag, an dem sie auf die Klage wegen Hackens reagieren musste - den Entwurf eines Leitfadens zum so genannten „equipment interference", dem Eingriff in technische Anlagen und Geräte, der auch das Hacken durch Geheimdienste umfasst. Auch wenn er noch lange nicht ideal war, ließ dieser Leitfaden-Entwurf einen ersten Blick darauf zu, wie in

Original

and, potentially, safeguards surrounding this type of surveillance activity.

As you've already heard, over the next few months in 2015, a series of reports were released regarding the intelligence services' activities, including by the ISC, the parliamentary committee, by the independent reviewer of terrorism legislation, Mr David Anderson, from whom you've heard, and by the Royal United Services Institute. Those reports provided additional insight into some of the surveillance capabilities being exercised and revealed, including revealing one new type of surveillance, that of the collection of the bulk personal datasets that I already mentioned.

The reports uniformly criticised the confusing and outdated legal regime governing surveillance powers of the UK intelligence agencies at the time and recommended reform. The UK government's response was to publish the draft Investigatory Powers Bill in November 2015. The bill, which is now an act, was a step forward in transparency because it included explicit reference to and rules governing certain surveillance powers, such as hacking and the collection of bulk personal datasets. But up until that point these powers were being authorised under a very old and vague set of laws that we argued, and in some cases the IPT agreed, were so broad as to fail to provide the necessary transparency and foreseeability required in order to intrude upon privacy. When it published the bill, the government also admitted for the first time it had been using another very old and vague power, Section 94 of the Telecommunications Act of 1984, to obtain bulk communications data about people within the UK. This is the same practice that was rather roundly criticised in the US following the very first Snowden disclosure of the famous Verizon order and which led the US Congress to reign in the practice under the US Freedom Act. The IPT has since agreed with us that the use of Section 94 for the bulk collection of communications data was in fact a violation of Article 8 of the European Convention on Human Rights. Yet the practice of collecting communications data in

Übersetzung

Großbritannien Richtlinien und möglicherweise auch Schutzmaßnahmen zu dieser Art von Überwachungsaktivitäten festgelegt werden.

Wie Sie bereits gehört haben, wurde in den folgenden Monaten des Jahres 2015 eine Reihe von Berichten zu den Aktivitäten der Geheimdienste veröffentlicht, unter anderem vom ISC (dem parlamentarischen Ausschuss), vom unabhängigen Gutachter für Antiterrorgesetze, Mr. David Anderson, der vor Ihnen gesprochen hat, und vom Royal United Services Institute. Diese Berichte lieferten weitere Erkenntnisse über einige der Überwachungskompetenzen, die ausgeübt und offengelegt wurden. Unter anderem zeigten sie auf, dass es eine neue Art von Überwachung gab, nämlich die von mir erwähnte Erfassung von personenbezogenen Massendatensätzen.

Alle diese Berichte kritisierten den verwirrenden und veralteten Rechtsrahmen, durch den die Überwachungsbefugnisse und -kompetenzen zum damaligen Zeitpunkt geregelt wurden, und alle forderten Reformen. Die britische Regierung reagierte, indem sie im November 2015 den Gesetzesentwurf der Investigatory Powers Bill vorlegte. Der Gesetzentwurf, der inzwischen verabschiedet wurde, stellt einen Schritt in Richtung höherer Transparenz dar, weil er sich ausdrücklich auf bestimmte Überwachungsbefugnisse bezieht und entsprechende Regeln enthält, so zum Hacken und zur Erfassung von personenbezogenen Massendatensätzen. Bis zu diesem Zeitpunkt jedoch wurden diese Befugnisse im Rahmen eines sehr alten und schwammigen gesetzlichen Regelwerks erteilt, das unserer Argumentation zufolge - und das Investigatory Powers Tribunal stimmte uns darin in einigen Fällen zu - so weit gefasst war, dass es nicht die Transparenz und Vorhersehbarkeit bot, die ein Eingreifen in die Privatsphäre erfordert. Als die Regierung den Gesetzesentwurf vorlegte, räumte sie auch zum ersten Mal ein, dass sie mit Section 94 des Telecommunications Act von 1984 bisher eine sehr alte und schwammige Grundlage für die Genehmigung der massenhaften Erfassung von Kommunikationsdaten von Menschen in Großbritannien genutzt hatte. Dabei handelt es sich um dasselbe Vorgehen, das in den USA nach den allerersten Snowden-Enthüllungen zum berühmten Verizon-Befehl recht einhellig kritisiert wurde und das den US-Kongress dazu veranlasste, die Praxis

Original	*Übersetzung*
bulk will continue in the UK because it is now explicitly permitted under the Investigatory Powers Act and that, from our perspective, has been one of the major flaws with the act and the debate surrounding it.	*mit dem US Freedom Act einzuschränken. Das Investigatory Powers Tribunal hat seither in unserem Sinne entschieden, dass die Nutzung von Section 94 als Grundlage für die massenhafte Erfassung von Kommunikationsdaten gegen Artikel 8 der Europäischen Menschenrechtskonvention verstößt. Doch in Großbritannien werden weiterhin massenhafte Datenerfassungen durchgeführt, weil dies im Rahmen des Investigatory Powers Act jetzt ausdrücklich gestattet ist. Unserer Ansicht nach ist dies einer der Hauptmängel des Gesetzes und der dazugehörigen Debatten.*
While transparency has undeniably been increased over the last few years, transparency is not the sole criterion for a human rights compliant surveillance regime. We disagree that merely enshrining bulk surveillance in the act makes bulk surveillance legal. There is a long-standing precedent under UK law and the European Convention on Human Rights that requires that any interference with privacy, among other things, be based on reasonable suspicion. This is lacking from both the bulk powers provisions of the bill and the so-called thematic warrants, which I think you've heard about before, which authorise large-scale collection under the targeted powers of interception and hacking contained in the bill.	*Zwar wurde die Transparenz in den vergangenen Jahren zweifellos erhöht, doch Transparenz ist nicht das einzige Kriterium für ein Überwachungssystem, das mit den Menschenrechten vereinbar ist. Wir sind nicht der Meinung, dass Massenüberwachung rechtmäßig wird, wenn sie in ein entsprechendes Gesetz gehüllt wird. Es gibt im britischen Recht und gemäß der Europäischen Menschenrechtskonvention ein langwährendes Präjudiz, wonach jedem Eingriff in die Privatsphäre unter anderem ein begründeter Verdacht vorausgehen muss. Diese Voraussetzung fehlt in den Bestimmungen zur Genehmigung von Massendatenkompetenzen und zu den so genannten themenbezogenen Befugnissen, von denen Sie, so denke ich, ebenfalls schon etwas gehört haben und die die großangelegte Datenerfassung im Rahmen der im Gesetz enthaltenen Abfang- und Hacking-Kompetenzen autorisiert.*
The question of whether bulk surveillance is proportionate was also never fully tackled during the UK debate. While, as you've heard, David Anderson published a report earlier this year concluding some of the bulk powers had, in his opinion, been shown to be useful, he did not tackle the more nuanced question of proportionality - which is whether, even if the powers are useful, does that usefulness outweigh the significant intrusion into privacy that they cause and the potential threat to a democratic society caused by their very existence? There is also an open question as to whether admitting to the broad powers, without tackling the more specific implementations of those powers, has sufficiently given the	*Die Frage nach der Verhältnismäßigkeit von Massenüberwachung wurde in den britischen Debatten ebenfalls nie vollständig erörtert. David Anderson hat, wie Sie bereits erfahren haben, in diesem Jahr einen Bericht veröffentlicht, in dem er zu dem Schluss kommt, dass einige der Befugnisse zur Massenüberwachung sich seiner Meinung nach als nützlich erwiesen haben. Er geht dabei jedoch nicht auf die etwas differenziertere Frage der Verhältnismäßigkeit ein - die Frage danach, ob der möglicherweise bestehende Nutzen dieser Befugnisse den mit ihnen verbundenen, signifikanten Eingriff in die Privatsphäre überwiegen, ebenso wie die potenzielle Bedrohung der Demokratie, die durch die bloße Existenz derartiger Befugnisse gegeben ist. Offen bleibt auch die*

Original	*Übersetzung*
public a full understanding of what can be undertaken now by the UK intelligence services and is enough to sanction the surveillance capabilities now permitted under the Investigatory Powers Act. For instance, while the act broadly permits bulk interception of content, we know from the Snowden documents, that such interception can take a variety of forms, most of which were never explicitly addressed during the parliamentary debates because of the unwillingness of the UK government to engage in that level of detail. For instance, we do not know if the bulk interception power will be used to capture the webcam feeds of millions of people, as has allegedly happened under the Optic Nerve program revealed by Mr Snowden. Nor do we know if the bulk hacking power will be used to authorise the hacking of overseas service providers such as Google and Yahoo as purportedly happened under the program codenamed Muscular.	*Frage, ob dadurch, dass das Bestehen dieser weitreichenden Kompetenzen und Befugnisse zwar eingeräumt, ihre genaue Umsetzung jedoch nicht erklärt wurde, die Öffentlichkeit ausreichend darüber aufgeklärt wurde, was die britischen Geheimdienste jetzt tun können. Es ist nicht klar, ob dies ausreicht, um die Überwachungskompetenzen zu sanktionieren, die gemäß dem Investigatory Powers Act nunmehr erlaubt sind. So enthält das Gesetz zwar beispielsweise eine sehr weitgefasste Erlaubnis zum massenhaften Abfangen von Kommunikationsinhalten; doch wir wissen aus den Snowden-Dokumente, dass ein solches Abfangen auf unterschiedliche Arten stattfinden kann, von denen die meisten in den parlamentarischen Debatten niemals ausdrücklich zur Sprache kamen, weil die britische Regierung keine derart detaillierte Diskussion führen wollte. Wir wissen zum Beispiel nicht, ob die Befugnis zum massenhaften Abfangen von Daten dazu genutzt wird, die Webcam-Feeds von Millionen Menschen anzuzapfen, wie es im Rahmen des von Mr. Snowden bekanntgemachten „Optic Nerve“-Programms angeblich geschehen ist. Wir wissen auch nicht, ob die Befugnis zum massenhaften Hacken dazu genutzt wird, das Hacken von Internetdienstleistern in Übersee - Unternehmen wie Google und Yahoo - zu autorisieren, wie es vermutlich im Rahmen des Programms mit dem Codenamen Muscular geschehen ist.*
For all of these reasons, while I think there has been some progress in how the UK governs its intelligence services, there is still significant room for improvement. Many of the powers that now form part of the Investigatory Powers Act, including data retention, bulk interception and hacking, are currently subject to legal challenges at the European level. It will be interesting to see how the government reacts to those judgements, one of which I understand is expected next week, which will of course set a precedent across Europe.	*Aus all diesen Gründen denke ich, dass bei allen Fortschritten der britischen Regierung hinsichtlich der Kontrolle ihrer Geheimdienste nach wie vor deutlicher Verbesserungsbedarf besteht. Gegen viele der Kompetenzen, die jetzt Inhalt des Investigatory Powers Act sind, darunter die Datenspeicherung, die massenhafte Datenerfassung und das Hacking, wird derzeit auf europäischer Ebene geklagt. Es wird spannend sein, zu beobachten, wie die Regierung auf diese Urteile reagieren wird, von denen eines, soweit ich weiß, in der kommenden Woche erwartet und natürlich einen europaweiten Präzedenzfall schaffen wird.*
Thank you for inviting me here and I'm happy to answer questions.	*Ich danke Ihnen für Ihre Einladung und beantworte gerne weitere Fragen.*

Original

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Wir würden dann jetzt direkt mit den Fragerunden anfangen. Ich schaue mal in die Reihen der Ausschussmitglieder. - Herr Kollege Wendt und Frau Kollegin Renner haben sich gemeldet. Ich sammle erst, sodass jede Fraktion eine Frage stellen kann, und dann geht es in die Beantwortungsrunden. Da würden übrigens Sie wieder anfangen, Frau Wilson Palow; dann gehen wir von der anderen Seite durch. - Kollege Wendt.

Marian Wendt (CDU/CSU): Vielen Dank, Herr Vorsitzender. - Meine Damen und Herren Sachverständige, vielen Dank für Ihr Kommen und für den Austausch miteinander.

Ich habe jetzt zwei Fragen an Herrn King. Sie hatten das No-Spy-Paket von 1995 erwähnt. Sie haben dargestellt, dass es das gibt. Aber Sie sind leider nicht näher darauf eingegangen, warum es das vielleicht gibt. Warum ist es aus Ihrer Sicht notwendig, dass diese Staaten vielleicht solch ein Abkommen abgeschlossen haben? Das beinhaltet ja nicht nur das gegenseitige Nicht-Abhören, sondern im Bedarfsfall natürlich auch das Abhören von - gegebenenfalls - Terroristen, Straftätern, Kriminellen, auch eigenen Staatsbürgern. In Deutschland ist es zum Beispiel möglich, eigene Bürger - Straftäter, Schwerstkriminelle - nach entsprechenden rechtlichen Vorgaben abzuhören. Vielleicht könnten Sie das noch ein bisschen mehr erörtern, gerade auch vor dem Hintergrund der weltweiten Bedrohungslagen, die wir haben. Wir hatten gestern eine Aktuelle Stunde im Bundestag zu den Anschlägen in Istanbul, in Kairo, in Nigeria. Allein letzte Woche sind über 300 Menschen durch Terror weltweit umgekommen, und die Terrorlage - Sie kennen sie - hat sich seit 1995 ja sehr verschlechtert.

Die zweite Frage ist: Gibt es konkrete - Sie haben ja auch die Situation kritisiert - Fälle, wo Menschen zu Unrecht abgehört wurden? Gibt es da eine Beschwerdestelle bei Ihnen in Großbritannien, oder sind Sie da Ansprechpartner in Ihrer NGO, wo man sich ganz konkret hinwenden kann? - Vielen Dank.

Übersetzung

Original

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Frau Kollegin Renner hatte sich gemeldet.

Martina Renner (DIE LINKE): Von mir zuerst eine Frage an Herrn King. Sie haben ja sehr eindrücklich mit dem Beispiel aus 2007 dieses System, wie wir es nennen, des „Ringtausches“, des Datenaustausches zwischen - in Ihrem Beispiel - Großbritannien, USA und zurück, beschrieben. Was wissen Sie über solche gemeinsamen Datentransfers zwischen Großbritannien und Deutschland, also unseren deutschen Diensten, und sind Ihnen da vielleicht auch einzelne Beispiele, Operationen bekannt? - Das wäre meine erste Frage.

Die zweite Frage würde ich an Frau Palow richten, insofern Sie etwas dazu sagen können. Gegebenenfalls würde ich die Frage dann weiterreichen an Herrn King. In den Dokumenten, die veröffentlicht wurden im Zusammenhang mit Edward Snowden, werden ja auch einzelne Operationen beschrieben; Prism wurde eben schon genannt. Welche dieser beschriebenen Operationen, aber auch Komponenten wie Hardware und Software, die dort genannt werden, haben sich in den Aufklärungsbemühungen in Großbritannien nach 2013 bestätigt? Haben Sie dort Erkenntnisse erlangt, dass einzelne dort beschriebene Vorgänge, Techniken tatsächlich auch angewandt wurden? - Danke.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Herr Kollege Flisek als Nächster.

Christian Flisek (SPD): Herzlichen Dank, Herr Vorsitzender. - Auch von meiner Seite an die beiden Sachverständigen erst einmal einen guten Morgen. - Ich möchte Sie gerne noch mal fragen in Bezug auf Geheimdienstkooperationen und den Rechtsrahmen von Geheimdienstkooperationen aus britischer Sicht. Das ist ein Thema, das uns natürlich hier sehr beschäftigt, insbesondere unter dem Aspekt, dass man jeweils für die Arbeit des eigenen Dienstes nationales Recht schaffen kann, das dafür sorgt, dass die Arbeit ja restriktiv ist im Rahmen der Arbeitsaufträge, dass es auch kontrolliert werden kann. Aber immer

Übersetzung

Original

dann, wenn es sozusagen den nationalen Bereich verlässt und wenn es in den Bereich von Geheimdienstkooperation geht, kommen wir in einen Graubereich hinein. Mich würde interessieren: Wie ist der rechtliche Rahmen und wie ist der Kontrollrahmen in Großbritannien für die britischen Dienste, wenn es darum geht, Verantwortlichkeit bei Geheimdienstkooperationen britischer Dienste sicherzustellen? - Das wäre meine erste Frage, durchaus an beide gerichtet, wenn es möglich ist.

Und die zweite Frage - -

Vorsitzender Dr. Patrick Sensburg: Dann geht keine zweite Frage mehr.

Christian Flisek (SPD): Ja, okay. - Gut, dann passt es. Dann machen wir es so. Alles easy.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Herr Kollege von Notz.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Jetzt muss ich kurz überlegen, wie ich das jetzt mache, dass ich meine zwei Fragen unterbringe.

(Christian Flisek (SPD): Alter Taktiker!)

Vorsitzender Dr. Patrick Sensburg: Das geht auch nicht anders.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Erst mal einen guten Morgen und vielen Dank für Ihre Statements und Ihre Arbeit. - Ich will vielleicht mal so beginnen und Sie fragen, inwieweit Sie auch Einblick haben in die technische Umsetzung dessen, was Sie beschrieben haben. Da stelle ich die Frage an Sie beide: Wie würde es eigentlich funktionieren, wenn es so etwas wie ein No-Spy-Verständnis zwischen den einzelnen Mitgliedern der Five Eyes gäbe? Da müsste man ja Filter haben, die an jedem Datenpaket feststellen „Oh, Achtung, das ist ja ein britisches“, „Oh, Achtung, das - - Wie würde sozusagen die technische Umsetzung funktionieren bei der Erfassung, nicht erst bei der Bearbeitung

Übersetzung

Original

von Daten, sondern schon bei der Erfassung? Haben Sie eine Idee davon, wie es praktisch zwischen den Five Eyes läuft? Also, tauschen alle die Erfassungen komplett aus, und gibt es bei jedem der Five-Eyes-Staaten jeweils einen großen Datenpool, oder gibt es eine zentrale Speicherung der „bulked data“? - Vielleicht fangen wir so an. Ich stelle die Frage an Sie beide.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Jetzt gucke ich noch mal in die Runde. - Damit haben alle Fraktionen Fragen gestellt, und ich würde anfangen bei Frau Wilson Palow zur Beantwortung der an sie gestellten Fragen. - Sie haben das Wort.

Sachverständige Caroline Wilson Palow: Yes, thank you. - I'll begin with the question regarding the Snowden documents and whether or not any of the individual operations have been confirmed by the UK government. The UK government did confirm that they are receiving intelligence obtained by the NSA under the Prism program, that that is being shared. I think that is one of the only explicit confirmations from the Snowden documents of a program - maybe Mr King will have further insight into this. But, that being said, there have been confirmations at a higher level. I mentioned the program codenamed Tempora, which is the bulk interception program. And while the UK government has never admitted to that particular code word, we do know that under the prior legal regime, the Regulation of Investigatory Powers Act, now under the current Investigatory Powers Act, there is a bulk interception capability available under law and that the UK government engages in that activity, which is essentially what we understand Tempora to be. So, we understand that there is bulk interception, we understand also, from some of the reports that have come out since, that the UK government, the intelligence services, engage in hacking, which was revealed in a variety of the different Snowden documents. We understand that they have engaged in the past and will continue to engage in the bulk collection of communications data both outside the UK and within the UK.

Übersetzung

Sachverständige Caroline Wilson Palow: *Ja. Vielen Dank. - Ich beginne mit der Frage nach den Snowden-Dokumenten und danach, ob die britische Regierung die Durchführung einzelner Operationen bestätigt hat. Die britische Regierung hat bestätigt, dass sie nachrichtendienstliche Informationen erhält, die von der NSA im Rahmen des Prism-Programms erfasst wurden, dass diese Informationen weitergegeben werden. Ich denke, das ist eine der wenigen expliziten Bestätigungen eines Programms, die sich aus den Snowden-Dokumenten ergeben haben. Vielleicht kann Mr. King noch mehr hierzu sagen. Davon abgesehen gab es jedoch Bestätigungen auf abstrakterer Ebene. Ich habe vorhin das Programm mit dem Codenamen Tempora erwähnt. Dabei handelt es sich um das Programm zur massenhaften Datenerfassung. Zwar hat die britische Regierung nie eingeräumt, dass es ein Programm mit diesem bestimmten Codenamen gibt; aber wir wissen, dass das vorherige Gesetz, der Regulation of Investigatory Powers Act, ebenso wie das aktuelle Gesetz, der Investigatory Powers Act, eine Kompetenz zur massenhaften Datenerfassung vorsieht und dass die britische Regierung solcherlei Aktivitäten durchführt - was im Kern genau dem entspricht, was Tempora unserem Wissen nach ist. Wir wissen also, dass es eine massenhafte Datenerfassung gibt, wir wissen weiterhin, aus einigen der seither erschienenen Berichte, dass die britische Regierung, die Geheimdienste, Geräte und Systeme hacken, was durch verschiedene der Snowden-Dokumente enthüllt wurde. Wir wissen, dass die britischen Geheimdienste in der Vergangenheit massen-*

Original

So, there has been quite a bit of confirmation at the more abstract level of what was released in the Snowden documents even if it wasn't the particular operations or code words. Although as I mentioned, there hasn't necessarily been confirmation of some of the real specifics of the program besides the idea that bulk interception is taking place. What type of material? We know that it is content, and that's a very broad descriptor, but does that mean necessarily that all the video feeds are coming in and being analysed? There are still some open questions along those lines.

With regard to the UK framework on cooperation between the intelligence services, I think that there continue to be large questions about how that framework works because of the point that you just made, which is that it can be very difficult to effectively oversee them given the restrictions that other countries may place on the information that is being shared with the UK intelligence services. The framework in the UK right now is relatively sparse when it comes to intelligence sharing. We understand that it can be permitted under the Investigatory Powers Act, and we understand that in the fairly narrow circumstance of sharing between the US and the UK - this came out during our lawsuit - that the UK should be obtaining, if possible, a warrant-like authorisation to obtain the data from the US. And, again I think Mr King may be able to describe this in a bit more detail, but we do believe that there are actually quite large - and this feeds into the second question that was asked on this area - databases that are being shared at least between the Five Eyes and perhaps other governments of data - essentially raw data that has been unprocessed or unfiltered - and that they, at least the US and the UK, have access to those databases and that what rules are applied during processing is not entirely clear from the national laws of either country as to how they can get access to that data.

Übersetzung

haft Kommunikationsdaten erfasst haben, sowohl außerhalb als auch innerhalb Großbritanniens, und dass sie dies auch weiterhin tun werden.

Es wurde also auf einer abstrakteren Ebene ziemlich viel von dem bestätigt, was durch die Snowden-Dokumente offenbart wurde, wenn auch nicht die genauen Operationen oder Codenamen. Doch wie ich zuvor sagte, wurden außer der generellen Tatsache, dass eine massenhafte Datenerfassung stattfindet, keine echten Einzelheiten des Programms bestätigt. Um welche Art von Datenmaterial handelt es sich? Wir wissen, dass es Inhalte sind, und das ist eine sehr umfassende Bezeichnung. Aber bedeutet dies, dass all die Video-Feeds abgefangen und analysiert werden? Diese und weitere Fragen sind noch offen.

Was das britische Rahmenwerk für die geheimdienstliche Zusammenarbeit betrifft, so denke ich, dass es auch hier wichtige Fragen dazu gibt, wie dieser Rahmen funktioniert, genau aus dem Grund, den Sie gerade nannten: Angesichts der Auflagen und Restriktionen, mit denen andere Länder die Daten versehen, die sie an die britischen Geheimdienste weitergeben, kann es sehr schwierig sein, die Geheimdienste effektiv zu kontrollieren. Das britische Rahmenwerk für die Weitergabe von geheimdienstlichen Informationen ist derzeit relativ dürftig. Wir wissen, dass eine Weitergabe nach dem Investigatory Powers Act erlaubt sein kann. Wir wissen ebenfalls, dass es im relativ enggefassten Fall einer Weitergabe zwischen den USA und Großbritannien so aussieht, dass Großbritannien nach Möglichkeit eine Art richterliche Genehmigung einholen sollte, um die Daten von den USA einzufordern. Dies ging aus unserem Gerichtsverfahren hervor. Auch hier denke ich, dass Mr. King möglicherweise genauere Einzelheiten erklären kann. Wir sind jedoch überzeugt, dass es sehr große Datenbanken gibt - und das beantwortet zum Teil auch die zweite Frage zu diesem Thema –, die mindestens von den Five-Eyes-Staaten und vielleicht noch von weiteren Regierungen genutzt werden und die im Wesentlichen unbearbeitete, ungefilterte Rohdaten enthalten. Wir sind der Meinung, dass zumindest die USA und Großbritannien Zugriff auf diese Datenbanken haben und dass die Regeln, nach denen die Daten

Nur zur dienstlichen Verwendung

Original

Übersetzung

verarbeitet werden, sich nicht eindeutig aus den nationalen Gesetzen der beiden Länder zum Zugriff auf diese Daten ergeben.

Sachverständiger Eric King: I'm just trying to consolidate the questions to answer them in the most helpful way. Perhaps just taking them in order is simplest.

Sachverständiger Eric King: *Ich versuche gerade, die Fragen so zu bündeln, dass ich sie möglichst zielführend beantworten kann. Vielleicht gehe ich sie einfach der Reihe nach durch.*

The question was asked why did the Five Eyes no-spy arrangement come into practice. I think we should be clear here about what the no-spy arrangement does - it doesn't prohibit targeting of each other's citizens. What it seems to provide is a process upon which you get authorisation to target individuals and, in almost all circumstances, that's the appropriate course when we're talking about surveillance. It's not a prohibition of the practice of acquiring communications that may be necessary for preventing terrorism or pertaining to an individual that threatens a country's national security, but it's about what is the lawful process that regulates that to prevent abuse and to ensure that the targeting is done in an appropriate manner. The reason why the no-spy pact, as it's dubbed, came into existence was, the best I can ascertain, a matter of practicality. The Five Eyes signals intelligence agencies are so interlinked. Their staff sits next to each other. One officer told me at one point that the lunch pass at GCHQ gets you into the lunch room at NSA, you know, such is the level of integration. As a result, it's pretty obvious that it would be inappropriate to permit one officer to the left to do something that they would not be able to do. And so, as such, they simply collaborated to say, look, while we're sitting in the same room, we need to put in place some restrictions to make sure that we can't be directly targeting each other's citizens - and it's grown from there.

Es wurde gefragt, warum es die No-Spy-Übereinkunft der Five Eyes gibt. Ich denke, wir sollten uns darüber im Klaren sein, was diese No-Spy-Übereinkunft tut - sie verbietet nicht das Ausspionieren der Bürger von Partnerstaaten. Sie scheint jedoch ein Verfahren zu liefern, durch das man die Genehmigung erhält, Einzelpersonen zu überwachen, und in fast allen Fällen ist dies das angemessene Vorgehen, wenn es um Überwachung geht. Die Übereinkunft verbietet es nicht, Kommunikationsdaten zu beschaffen, die benötigt werden könnten, um terroristische Angriffe abzuwehren, oder die sich auf eine Person beziehen, die eine Gefahr für die nationale Sicherheit eines Staates darstellt. Es geht darin vielmehr darum, das rechtmäßige Verfahren zu beschreiben, das diese Praktiken regelt, um einen Missbrauch zu verhindern und sicherzustellen, dass die Überwachung auf angemessene Weise durchgeführt wird. Nach allem, was ich weiß, wurde dieses so genannte No-Spy-Abkommen aus rein praktischen Gründen geschlossen. Die Geheimdienste der Five-Eyes-Staaten sind eng miteinander verbunden. Ihre Mitarbeiter sitzen Seite an Seite. Ein Mitarbeiter erzählte mir einmal, dass man mit der Cafeteria-Karte vom GCHQ auch in den Speiseraum der NSA kommt. So eng sind sie verflochten. Es ist demzufolge ziemlich klar, dass es unangemessen wäre, dem Mitarbeiter einen Platz weiter etwas zu gestatten, was man selbst nicht darf. Also arbeiteten sie einfach zusammen und sagten: Nun, solange wir im selben Raum sitzen, müssen wir ein paar Restriktionen einführen, damit sichergestellt ist, dass keiner von uns die Bürger des anderen überwachen kann. - Und von da aus hat es sich dann weiterentwickelt.

You asked whether people were targeted unlawfully. We have some information about that. Amnesty International were found by British courts to have had their communications unlawfully interfered with. Importantly, the court didn't find

Sie fragten, ob Menschen widerrechtlich überwacht werden. Uns liegen dazu einige Informationen vor. Britische Gerichte haben entschieden, dass die Kommunikationsdaten von Amnesty International widerrechtlich abgefangen wurden. Wichtig ist dabei, dass

Nur zur dienstlichen Verwendung

Original

that it was unlawful for them to be targeted in the first instance, but internal procedures inside GCHQ were not followed in this instance. It resulted in the fact that material was held for too long and selected inappropriately and, as such, the court found that that was unlawful. There are other circumstances where it hasn't gone to court, but I think you could test the lawfulness of it. *Le Monde* published an article, I think last week, perhaps the week before, where it is described how GCHQ were targeting telecommunications companies across Europe. They were targeting technical staff at these companies. They were not national security threats, these staff, they were not committing any sort of serious crime. The reason they were targeted is because they hold privileged information which GCHQ wanted and once that information was acquired it would allow them to hack or to target the communications of other people. Now, under British law, the agencies would say that that's lawful. It's lawful to target someone who is innocent, who is not a national security threat, nor is suspected of committing any crime, so long as they hold information that might be relevant to Britain. Now, for me, I find that deeply unsettling and not a practice that should be encouraged.

The question was asked about the exchange of material. Again, as is often in this area, we don't have the full picture that we would like. Privacy International requested updated versions of the Five Eyes intelligence sharing arrangement, sent out freedom of information requests in some circumstances and has gone to court in others to try and obtain them. GCHQ's position at this point is that they apply in practice the same protections that they would to material received from a foreign partner as if they had intercepted it themselves. I think that only begins to scratch the surface of how the arrangements actually work in practice.

Übersetzung

das Gericht nicht zu dem Schluss kam, dass die Überwachung von Amnesty International grundsätzlich unrechtmäßig war. Vielmehr lag die Unrechtmäßigkeit darin, dass die internen Verfahren des GCHQ in diesem Fall nicht befolgt worden waren. Das führte dazu, dass das Datenmaterial zu lange gespeichert und unangemessen gefiltert wurde, und das war nach Ansicht des Gerichts ein Rechtsverstoß. Es gibt andere Fälle, in denen es nicht zu einem Gerichtsverfahren kam, bei denen die Rechtmäßigkeit jedoch meiner Meinung nach infrage steht. In Le Monde *erschien kürzlich ein Artikel, in der letzten oder vorletzten Woche, der beschrieb, wie der GCHQ Telekommunikationsanbieter in ganz Europa überwacht. Sie überwachten die technischen Mitarbeiter dieser Unternehmen. Diese Leute stellten keine Bedrohung der nationalen Sicherheit dar und begingen auch keinerlei schwere Verbrechen. Sie wurden nur deshalb überwacht, weil sie im Besitz sensibler Informationen waren, an die der GCHQ herankommen wollte und mit denen es die Möglichkeit hätte, die Kommunikationsverbindungen anderer Menschen zu hacken oder zu überwachen. Nach britischem Recht, so würden die Geheimdienste argumentieren, ist das legal. Es ist legal, einen unschuldigen Menschen zu überwachen, der weder eine Gefahr für die nationale Sicherheit ist noch eines Verbrechens verdächtigt wird, solange diese Person Informationen hat, die möglicherweise von Relevanz für Großbritannien sind. In meinen Augen ist dies zutiefst beunruhigend. Eine solche Praxis sollte nicht begünstigt werden.*

Es wurde nach dem Austausch und der Weitergabe von Datenmaterial gefragt. Auch hier, wie so oft in diesem Bereich, haben wir nicht den Gesamtüberblick, den wir gerne hätten. Privacy International hat aktuelle Fassungen der Five-Eyes-Vereinbarung zur gemeinsamen Nutzung geheimdienstlicher Informationen angefordert. Die Organisation hat in einigen Fällen Anträge im Rahmen des Informationsfreiheitsgesetzes gestellt und ist in anderen Fällen vor Gericht gegangen, um diese Dokumente einzufordern. Der Standpunkt des GCHQ ist derzeit, dass bei Material, das von einem ausländischen Partner beschafft wurde, in der Praxis genau dieselben Schutzmaßnahmen gelten wie bei selbst erfassten Daten. Ich denke, dass damit nur an der Oberfläche der tatsächlichen

Original	*Übersetzung*
	praktischen Umsetzung dieser Übereinkommen gekratzt wird.
One of the clearer examples that I can provide to you is the situation we have at the minute between the UK and the Dutch. The Dutch intelligence services are not allowed to tap undersea fibre-optic cables, as I understand it. Their legislation only permits the interception of communications from satellite off the air and they are strictly prohibited from tapping cables. So, the question that came up after the Snowden revelations is, could they receive information from foreign partners that they know to have come from these undersea cables that they themselves are prohibited from tapping? And the oversight body, in this instance, undertook a thematic review, it was a very detailed one. But they concluded that it would be impractical to try and put in place such a restriction because there would be no way to know what material has come from what source. I can see how that argument can be made but I don't think it acknowledges the reality of intelligence cooperation as it stands between longstanding partners, certainly between NSA and GCHQ. They have a full understanding, for example, of which program works in what way and, in many circumstances, they built the programs together, they built the technology together. And I imagine that there will be areas where the same will be for Germany and Britain, and the NSA and Germany as well, although perhaps not quite so comprehensively.	*Ein Beispiel, bei dem diesbezüglich mehr Klarheit herrscht, ist die aktuelle Situation zwischen Großbritannien und den Niederlanden. Die niederländischen Geheimdienste dürfen, soweit ich weiß, keine Untersee-Glasfaserkabel anzapfen. Ihre Gesetzgebung gestattet lediglich das Abfangen von Kommunikationsinhalten, die über Satellit übermittelt werden, während das Anzapfen von Kabeln strengstens verboten ist. Nach den Snowden-Enthüllungen kam die Frage auf, ob die niederländischen Geheimdienste Informationen von ausländischen Partnern annehmen dürfen, von denen ihnen bekannt ist, dass sie aus Unterseekabeln stammen, die sie selbst nicht anzapfen dürfen. Das Aufsichtsgremium führte in diesem Fall eine sehr detaillierte Auswertung nach thematischen Gesichtspunkten durch. Sie kamen jedoch zu dem Schluss, dass eine solche Einschränkung praktisch undurchführbar sei, weil man nicht wissen könne, welches Datenmaterial aus welcher Quelle stamme. Ich kann die Argumentation nachvollziehen, denke jedoch nicht, dass sie die Wirklichkeit einer geheimdienstlichen Zusammenarbeit erkennt, wie sie zwischen langjährigen Partnern und ganz sicher zwischen NSA und GCHQ besteht. Sie wissen ganz genau, wie beispielsweise die einzelnen Programme funktionieren, die sie in vielen Fällen gemeinsam aufgebaut haben. Sie haben die Technologie gemeinsam entwickelt. Und ich kann mir vorstellen, dass es Bereiche gibt, in denen es sich mit Deutschland und Großbritannien oder der NSA und Deutschland ganz ähnlich verhält, wenn auch vielleicht nicht in einem so umfassenden Ausmaß.*
The other area where it is controlled much more strictly is with finalised intelligence reporting. I think this is a legacy of how spying used to be done, which was mostly human intelligence, analysing material and then providing that back. These days, as we all know, it's raw SIGINT collection. So there are better controls in place for the exchange of finalised intelligence reports. None of that applies to raw exchange of that raw material, and that's where protections need to go.	*Der andere Bereich, in dem dies sehr viel strenger kontrolliert wird, ist der Bereich der finalen Geheimdienstberichte. Ich denke, das geht auf die traditionelle Art der Spionage zurück, bei der geheimdienstliche Informationen größtenteils durch Agenten gewonnen, analysiert und zur Verfügung gestellt wurden. Heute handelt es sich, wie wir alle wissen, um die Erfassung von Rohdaten durch Signalaufklärung. Es gibt also bessere Kontrollmechanismen für den Austausch und die Weitergabe finaler Geheim-*

Original

Finally, Dr von Notz, the question about the practical ways that filters are applied, and then the no-spy arrangement. I'm afraid it's not at the collection stage as you correctly assumed. Once collected, the material has to be processed in some way to determine what it is. And it's at that stage that material is deselected. I think they call it a Five Eyes blind, which is that anything that they can identify coming from a British IP address or even a British organisation, and some of that is quite generously put, as I understand it, is then subtracted from the material as it continues to be processed, or minimised - which, in practice, simply means that it's flagged such that it would require additional authorisation to begin to look at it. Most of the protections then apply when a human searches for material relating to someone inside the UK or pertaining to the Five Eyes. The reason for why safeguards have developed towards that latter end of the process, though, is because that's where our law and policy has constrained them up until this point. I am of the view that should a greater appreciation of the level of intrusion that occurs earlier on in the process be made, i. e. if intelligence agencies begin to acknowledge the level of invasion of privacy that occurs simply at the point of collection, then you would necessarily have to improve the level of technical protections that could be afforded at that point. - I think that's addressed all the questions.

Vorsitzender Dr. Patrick Sensburg: Ich hoffe. - Ich gucke mal gerade in die Runde. - Das ist der Fall. Dann beginnen wir mit der zweiten Runde.

Übersetzung

dienstberichte. Keiner davon findet jedoch Anwendung beim reinen Austausch bzw. der Weitergabe des Datenmaterials, und hier bedarf es eines Schutzes.

Zum Schluss zur Frage von Dr. von Notz zu der praktischen Verwendung von Filtern und zum No-Spy-Abkommen. Ich fürchte, Sie haben Recht mit der Annahme, dass nicht schon bei der Erfassung gefiltert wird. Nach der Erfassung muss das Datenmaterial zunächst irgendwie bearbeitet werden, damit man weiß, worum es sich handelt. In dieser Phase wird Material aussortiert. Ich glaube, sie nennen es „Five-Eyes-Scheuklappe", was bedeutet, dass alles, von dem sie feststellen können, dass es von einer britischen IP-Adresse oder sogar einem britischen Unternehmen bzw. einer britischen Organisation stammt - und das wird meines Wissens teilweise recht großzügig ausgelegt -, vor der weiteren Verarbeitung aus dem Datenmaterial entfernt bzw. minimiert wird. In der Praxis bedeutet das einfach, dass diese Daten gekennzeichnet werden und dass sie nur nach einer weiteren Autorisierung angesehen werden dürfen. Die meisten dieser Schutzmaßnahmen werden dann befolgt, wenn ein menschlicher Mitarbeiter nach Datenmaterial zu einer Person in Großbritannien oder zu den Five-Eyes-Staaten sucht. Dass die Schutzmaßnahmen erst in diesen späten Phasen des Verfahrens eingebaut wurden, liegt jedoch daran, dass unsere Gesetze und Richtlinien sie bisher auf diese Phase beschränkt haben. Ich bin der Meinung, dass das Ausmaß stärker anerkannt werden sollte, zu dem schon viel früher in diesem Verfahren in die Privatsphäre eingegriffen wird. Wenn zum Beispiel die Geheimdienste damit anfangen würden, einzuräumen, wie sehr die Privatsphäre schon bei der bloßen Datenerfassung verletzt wird, dann würde das notwendigerweise eine Verbesserung der rechtlichen und technischen Schutzmaßnahmen nach sich ziehen, die in dieser Phase befolgt werden müssen. - Ich glaube, damit bin ich auf alle Fragen eingegangen.

Original

(Marian Wendt (CDU/CSU): Um 10.03 Uhr kommt der letzte Redner!)

- Wir haben es auf dem Schirm, wie in jeder Sitzung der letzten drei Jahre. - Herr Kollege Schipanski.

Tankred Schipanski (CDU/CSU): Herr Vorsitzender, vielen Dank. - Meine Dame und mein Herr Sachverständiger, wir hatten ja nun Zeugen hier und auch Sachverständige in der letzten Sitzungswoche. Ich möchte - an Sie beide gerichtet - noch mal das Thema Ringtausch aufgreifen. Bisher hat kein Zeuge ausgesagt, dass ein solcher Ringtausch stattfindet, auch kein Sachverständiger in der letzten Sitzungswoche. Sie sind jetzt die Ersten, die sagen, dass es diesen Ringtausch gibt, dass also die Five Eyes hier Daten austauschen, gemeinsam verarbeiten. Jetzt bin ich aber ob Ihrer Wortwahl etwas skeptisch geworden. Sachverständiger King sagt: „Ich habe gehört …“ - dann haben Sie das von den Kantinenausweisen erzählt - „…, dass da eine Kooperation mit Daten ist.“ Sie wurden gefragt, wie die Daten gemeinsam ausgetauscht und verarbeitet werden. Das konnten Sie jetzt auch nicht aus eigenem Wissen beschreiben. Und Frau Palow hat gesagt: Wir glauben, dass Datensätze ausgetauscht werden. - Nun sind Sie heute als Sachverständige hier, und uns interessiert natürlich, was Sie zu diesem Vorwurf ganz konkret wissen, weil Sie heute die ersten Sachverständigen sind, die sagen: Ich weiß, es findet ein Ringtausch statt, und es funktioniert so und so. - Da möchte ich Sie beide noch mal bitten, dass Sie uns konkret belegen: Woher kommt dieses Wissen, und wie funktioniert das Ganze? Weil Sie heute die Ersten sind, die das hier behaupten. - Vielen Dank.

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Das sind die Ersten, die wir heute überhaupt hören!)

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Ich sehe, da ist eine Frage vom Kollegen von Notz. - Nein? - Dann Kollege Hahn.

Übersetzung

Original	*Übersetzung*
Dr. André Hahn (DIE LINKE): Vielen Dank, Herr Vorsitzender. - Anders als der Kollege habe ich schon viele Hinweise erhalten hier in den Zeugenvernehmungen bezüglich eines möglichen oder tatsächlichen Ringtausches. Da muss man wahrscheinlich auch etwas genauer zuhören, was Zeugen hier aussagen.	
Aber unabhängig davon möchte ich gerne ein Wort aufgreifen, das Sie eben mehrfach verwandt haben, nämlich Datenhacking. Es ist auch das Stichwort Unterseekabel gefallen. Ich möchte beide fragen, was Sie dort über die Praxis des GCHQ wissen, wie der Abgriff an Unterseekabeln erfolgt, in welchem Umfang das stattfindet und wie die internationale Kommunikation seitens der britischen Dienste abgefischt oder abgefangen wird, also welche Erkenntnisse oder welches Wissen Sie dazu haben.	
Vorsitzender Dr. Patrick Sensburg: Herzlichen Dank. - Ich schaue gerade mal. Wenn es keine weiteren Fragen mehr gibt, würde ich die beiden Fragen beantworten lassen, weil wir dann zur namentlichen Abstimmung müssen. Wäre das okay? - Jetzt würde ich Herrn King beginnen lassen.	
Sachverständiger Eric King: Perhaps you use the word circular exchange or perhaps it holds a slightly different connotation to the one that we mean here. I mean, it's not contested by the British government that they exchange information with foreign partners at all. Indeed, all intelligence services practice it - it should be encouraged, in my view. There is absolutely nothing wrong with intelligence exchange so long as it's authorised by law, properly done, and able to be overseen by the respective parliaments. The threats we face are global and our intelligence agencies need to respond as such.	***Sachverständiger Eric King:*** *Vielleicht verwenden Sie den Begriff Ringtausch anders bzw. vielleicht ist er ein wenig anders konnotiert, als das, was wir hier meinen. Die britische Regierung bestreitet keineswegs, dass sie Informationen mit ausländischen Partnern austauscht. Vielmehr tun dies alle Geheimdienste - und diese Praxis sollte meiner Meinung nach auch gefördert werden. Es ist nichts Falsches daran, wenn Geheimdienste Informationen gemeinsam nutzen, solange dies gesetzlich genehmigt ist, korrekt durchgeführt wird und durch die betreffenden Parlamente kontrolliert werden kann. Die Bedrohungen, denen wir ausgesetzt sind, sind globaler Natur, und entsprechend müssen auch unsere Geheimdienste reagieren.*
Perhaps the narrower issue that you are asking is whether or not there are activities that exist between allied partners in which they attempt to	*Vielleicht geht es Ihnen um die engergefasste Frage, ob es zwischen verbündeten Partnern vorkommt, dass sie die nationalen Gesetze ihres jeweiligen Landes durch den Informationsaustausch zu umgehen*

Original

circumvent the domestic laws of their own countries? Perhaps it's that point that is kind of sharper here. An example of this, which I think is one of the clearer ones, is the fact that when the National Security Agency ran a program called Muscular - this was intercepting the cables between data centres of American companies, Google and Yahoo included - they didn't tap those cables in the United States, that's where the majority of the data servers are - they didn't tap them there. Instead, they asked GCHQ to tap them, and they were tapped between the UK and Ireland. I don't know why they did that. It doesn't make any sense to me beyond the fact that there will have been political and policy reasons for why they will have asked a foreign partner to do something that, I think, would have been difficult for them to justify domestically. That's not an example of a breaking of law, necessarily, a court hasn't looked at that or ruled on that, but that's the sort of thing that I believe happens. If you'd like I could give it more thought and perhaps prepare an additional note pulling together every example with the facts that I am able to draw up - if that's a particular point of concern.

The only other thing that I would very briefly say: There's a fantastic old book called *UK Eyes Alpha* which is British, which is written by the old BBC foreign service correspondent and, in it, he interviews a number of Five Eyes officers. There's three quotes in there that I think paint an interesting picture - these aren't quotes I've acquired, they're in a published book - in which he describes the level of cooperation. He says:

> The national product between the Five Eyes arrangements is often indistinguishable. SIGINT customers in both capitals seldom know which country generated either the access or the product itself.

Another one says:

Übersetzung

versuchen. Vielleicht ist das die genauere Zuspitzung der Frage. Ein Beispiel hierfür, das meiner Ansicht nach zu den eindeutigeren zählt, ist das so genannte Muscular-Programm der National Security Agency, bei dem die Kabel zwischen den Datenzentren US-amerikanischer Unternehmen, darunter auch Google und Yahoo, angezapft wurden. Die NSA zapfte diese Kabel nicht in den Vereinigten Staaten an, wo sich der Großteil der Server befand. Stattdessen baten sie den GCHQ darum, diese Verbindungen anzuzapfen, und das geschah dann zwischen Großbritannien und Irland. Ich weiß nicht, warum sie das taten. Für mich ergibt es keinen Sinn, außer dass sie politische und strategische Gründe dafür gehabt haben werden, einen ausländischen Partner zu bitten, etwas zu tun, was sich meiner Ansicht nach im eigenen Land nur schwer hätte rechtfertigen lassen. Das ist nicht unbedingt ein Beispiel für einen Gesetzesverstoß - kein Gericht hat dieses Vorgehen untersucht oder hierzu geurteilt. Aber es ist ein Beispiel für etwas, das meiner Meinung nach geschieht. Wenn Sie möchten, denke ich gerne noch weiter hierüber nach und erstelle vielleicht eine Zusammenfassung der bekannten Beispiele mit den mir verfügbaren Fakten, falls daran besonderes Interesse besteht.

Ein weiterer Punkt, den ich gerne ganz kurz ansprechen würde: Es gibt ein großartiges britisches Buch mit dem Titel UK Eyes Alpha, *das schon etwas älter ist. Es wurde von einem ehemaligen Auslandskorrespondenten der BBC geschrieben und enthält eine Reihe von Interviews mit Geheimdienstmitarbeitern der Five-Eyes-Staaten. Drei Zitate aus dem Buch, in denen er das Ausmaß der Zusammenarbeit beschreibt, zeichnen ein, wie ich finde, sehr interessantes Bild. Diese Zitate stammen aus dem veröffentlichten Text; ich habe sie nicht auf anderem Wege erhalten. Er schreibt:*

> *Die jeweiligen nationalen Produkte innerhalb dieser Five-Eyes-Übereinkünfte sind oft nicht auseinanderzuhalten. SIGINT-Empfänger in beiden Hauptstädten wissen selten, von welchem Staat der Zugang oder das Datenprodukt selbst stammt.*

Und an anderer Stelle:

Nur zur dienstlichen Verwendung

Original	*Übersetzung*
The cooperation between the two countries, particularly in SIGINT, is just so close that it becomes very difficult to know who is doing what, it's just organisational mess.	*Die Zusammenarbeit zwischen den beiden Ländern, insbesondere bei der Signalaufklärung, ist so eng, dass es sehr schwer zu erkennen ist, wer was tut. Es ist ein organisatorisches Chaos.*
Now, when you have agencies working so closely but you don't have oversight bodies working as closely, you get into all sorts of problems. I imagine you'll have seen evidence to this committee about the problem of treating oversight parties as third partners - that is when intelligence agencies enter into exchange arrangements they limit the exchange to only the agency that's receiving them and prohibit sharing to any other third party. In many circumstances, the further sharing of that with third parties would include making that material available to oversight bodies themselves. I don't know if that's a problem in Germany, I haven't looked at the examples here. But, certainly, it's a well-recognised international problem.	*Wenn Geheimdienste so eng zusammenarbeiten, ohne dass die entsprechenden Kontrollgremien ähnlich eng kooperieren, ergeben sich alle möglichen Probleme. Ich kann mir vorstellen, dass Sie vor diesem Ausschuss Aussagen über die Schwierigkeit gehört haben, die entstehen, wenn Kontrollgremien als Drittpartner [Drittparteien?] behandelt werden - wenn also Geheimdienste Übereinkünfte zum Informationsaustausch schließen und den Austausch allein auf den Geheimdienst beschränken, der die Informationen erhält, unter Ausschluss jeglicher Dritter. In vielen Fällen fällt das Verfügbarmachen des Materials für die Kontrollgremien auch unter die Weitergabe von Informationen an Dritte. Ich weiß nicht, ob das in Deutschland ein Problem ist; ich habe mich nicht eingehend mit den Beispielen hier beschäftigt. Aber auf internationaler Ebene ist es ein bekanntes Problem.*
Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Ich muss jetzt unterbrechen, weil wir zur namentlichen Abstimmung müssen. - Wir kommen dann zu Ihren Ausführungen gleich im Anschluss, wenn wir wieder zurück sind.	
Die Sitzung ist für die namentliche Abstimmung unterbrochen.	
(Unterbrechung von 10.06 bis 10.24 Uhr)	
Vorsitzender Dr. Patrick Sensburg: Meine Damen und Herren, die unterbrochene Sitzung des 1. Untersuchungsausschuss wird fortgesetzt. - Wir kommen jetzt zu den Ausführungen von Frau Wilson Palow zu den beiden gestellten Fragen. Sie haben das Wort.	
Sachverständige Caroline Wilson Palow: Thank you. - I would agree with what Mr King has already said regarding the circular exchange. It is	***Sachverständige Caroline Wilson Palow:*** *Vielen Dank. Ich stimme Mr. King bezüglich des Ringtauschs zu. Es ist wahr, dass wir nicht viele explizite*

Nur zur dienstlichen Verwendung

Original

true that we don't have many explicit examples - if what you mean by that is the violation of sharing of information, explicitly against UK law with, for instance, the UK government. But what we do have is evidence of, for instance, the raw unanalysed sharing. You can look back all the way to the public version of the Five Eyes agreement, which dates from the late 1940s, early 1950s, and the type of information that it said in that agreement would be shared between the Five Eyes. It includes the sort of unanalysed data and, actually, in the course of our lawsuit - ten human rights organisations versus the UK, which is currently pending at the European Court of Human Rights - we have gathered together quite a bit of information because the sharing between the US and the UK is one of the questions in the lawsuit, and what sort of safeguards and regulations surround that sharing. We've gathered together quite a bit of information surrounding that analysed sharing and what safeguards are in place, and we'd also be happy to share the submissions that we have made there as well, if it would be helpful to the committee.

With regard to how fibre-optic undersea cables are intercepted, what precise information we have. There again, from my perspective, I would point to what we've learned in that particular lawsuit because that has been discussing the bulk interception power in the UK. And, again, the UK government has not been terribly forthcoming as to exactly how that bulk interception power works but we do have some information that we have been able to glean from the Snowden documents and also from what has been admitted during the course of the lawsuit. We know that, initially, large amounts of information are obtained. And the UK government has said that while they have a legal obligation, ultimately, to try to split what are called "foreign communications", which are communications between the UK and abroad, or happening entirely abroad, which may be travelling over these cables, and communications that are entirely internal to the UK. They have said, technically, they are incapable of doing that. And that is one of the reasons that when they intercept these fibre-optic cables they pick

Übersetzung

Beispiele hierzu haben - falls Sie damit eine Informationsweitergabe zum Beispiel an die britische Regierung meinen, die ausdrücklich gegen britisches Recht verstößt. Uns liegen jedoch Beweise für die gemeinsame Nutzung nicht analysierter Rohdaten vor. Sie können bis zur öffentlich einsehbaren Version der Five-Eyes-Vereinbarung aus den späten 1940er- oder frühen 1950er-Jahren zurückgehen und sich ansehen, welche Informationen laut dieser Vereinbarung von den Five-Eyes-Staaten gemeinsam genutzt wurden. Dazu zählt auch diese Art nicht analysierter Daten, und im Laufe unserer Klage - zehn Menschenrechtsorganisationen gegen die britische Regierung, die derzeit vor dem Europäischen Gerichtshof für Menschenrechte anhängig ist - haben wir ziemlich viele Informationen hierzu zusammengetragen; denn diese Datenweitergabe zwischen den USA und Großbritannien gehört zu den Fragen, die gerichtlich geklärt werden sollen, ebenso wie die zu dieser Weitergabe gehörenden Schutzmaßnahmen und Richtlinien. Wir haben eine Menge Informationen zur Weitergabe von analysierten Daten und den dabei geltenden Schutzmaßnahmen zusammengetragen, und wir leiten auch gerne unsere Eingaben in diesem Verfahren weiter, wenn dies für den Ausschuss nützlich ist.

Was die Frage zum Anzapfen der Unterwasser-Glasfaserkabel betrifft sowie zu den genauen Informationen, die wir hierzu haben: Von meinem Standpunkt aus würde ich auch hier auf die Erkenntnisse aus dem genannten Gerichtsverfahren verweisen, denn darin wurde die Befugnis zur massenhaften Datenerfassung in Großbritannien erörtert. Wie gesagt, die britische Regierung war nicht besonders auskunftsfreudig, was die genaue Funktionsweise dieser Massenerfassungsbefugnis betrifft; aber wir konnten einige Erkenntnisse aus den Snowden-Dokumenten gewinnen sowie aus dem, was im Laufe dieses Verfahrens eingeräumt wurde. Wir wissen, dass zunächst eine große Menge an Daten erfasst wird. Die britische Regierung hat erklärt, dass sie zwar rechtlich verpflichtet ist, die so genannten „ausländischen Kommunikationsdaten" - das sind Daten aus Kommunikationsverbindungen zwischen Großbritannien und dem Ausland bzw. Kommunikationsverbindungen, die ganz im Ausland stattfinden und über diese Kabel laufen - letzten Endes von den Kommunikationsinhalten zu trennen, die vollständig innerbritisch sind. Sie erklärte jedoch, dass sie hierzu nicht die

Original	*Übersetzung*
out all of the communications at the same time and then they will later apply a filtering process and later apply selectors - but that is much later down the line. What might initially be filtered out could be information that is thought to be not particularly helpful like large video files or other information that is unlikely to contain the communications content that they are interested in. But then we know that, potentially for quite a period of time, both the content and the communications data, or the metadata associated with that content, can be stored and then selectors may later be applied. But within the UK, at least, those selectors, when they are referring to those foreign communications, can be quite broad and don't require additional approval. Whereas it's only if they were to attempt to target someone who is believed to be located within the United Kingdom that additional protections apply. And that is true both under the previous legal regime and under the current Investigatory Powers Act.	*technischen Möglichkeiten habe. Und das ist ein Grund, weshalb beim Anzapfen der Glasfaserkabel alle Kommunikationsdaten gleichzeitig erfasst und erst später durch ein Filterverfahren geleitet und noch später durch Selektoren eingegrenzt werden - dies jedoch erst zu einem viel späteren Zeitpunkt. Bei den Daten, die zunächst ausgefiltert werden, könnte es sich um solche handeln, die als nicht sonderlich hilfreich betrachtet werden, beispielsweise große Videodateien oder andere Daten, die wahrscheinlich nicht die Inhalte enthalten, an denen die Geheimdienste interessiert sind. Wir wissen jedoch, dass sowohl die Inhalte als auch die Kommunikationsdaten bzw. die zu den Inhalten gehörigen Metadaten zunächst gespeichert werden können, und dies möglicherweise für einen ziemlich langen Zeitraum, bevor dann später Selektoren angewendet werden. Doch innerhalb Großbritanniens können diese Selektoren, sofern sie sich auf ausländische Kommunikationsdaten beziehen, recht weit gefasst sein, ohne eine zusätzliche Genehmigung zu erfordern. Zusätzliche Schutzmaßnahmen greifen nur dann, wenn jemand überwacht werden soll, von dem davon ausgegangen wird, dass er sich in Großbritannien aufhält. Das war nach vorherigem Recht so und gilt auch unter dem aktuellen Investigatory Powers Act.*
Aside from that, we have actually been able to learn a little bit about the bulk interception process from some of the reports coming out of the US - which I'm sure you are aware of. Particularly from the Privacy and Civil Liberties Oversight Board, which has described the way in which the NSA conducts this bulk interception under Section 702 of the FISA Amendments Act, which in the US is often referred to - or as one of the Snowden codenames is - Upstream for that program, and it seems to be a somewhat similar process which is: large unanalysed data is first collected and selectors are applied at a later point. - Thank you.	*Davon abgesehen konnten wir aus den Berichten, die aus den USA kamen und die Sie sicher kennen, ein wenig über das Verfahren zur massenhaften Datenerfassung lernen, besonders aus dem Bericht des Privacy and Civil Liberties Oversight Board, in dem beschrieben wird, wie die NSA diese massenhafte Datenerfassung im Rahmen von Section 702 des FISA Amendments Act durchführt. In den USA wird dieses Verfahren oft als „Upstream" bezeichnet bzw. ist dies einer der Snowden-Codenamen für das Programm, in dem ähnlich verfahren wird: Große Mengen nicht analysierter Daten werden zunächst erfasst, und zu einem späteren Zeitpunkt werden Selektoren darauf angewendet. - Vielen Dank.*
Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Herr Kollege Hahn, eine Nachfrage?	

Original

Dr. André Hahn (DIE LINKE): Nein, wir hatten vor der Unterbrechung, die wir eben gemacht haben wegen der namentlichen Abstimmung, -

Vorsitzender Dr. Patrick Sensburg: Ich erinnere mich.

Dr. André Hahn (DIE LINKE): - Herrn King erst nur zum Ringtausch gehört. Ich hatte meine Frage an beide gestellt, was die Unterseekabel, die Praxis usw. angeht.

Vorsitzender Dr. Patrick Sensburg: Okay. Dazu hat er aber eben was gesagt.

Dr. André Hahn (DIE LINKE): Nein, habe ich nicht gehört.

Vorsitzender Dr. Patrick Sensburg: Ach so, dann Entschuldigung.

Dr. André Hahn (DIE LINKE): Ich wollte nur mal fragen, ob er auch dazu etwas sagen kann.

Vorsitzender Dr. Patrick Sensburg: Na klar, deshalb meinte ich „Nachfrage?“. - Dazu Herr King.

Sachverständiger Eric King: Sure, of course. - An additional report that Caroline didn't mention as well is the US National Academy of Sciences' report, which is a 300-page report that explains in pretty significant detail the process by which fibre optics are tapped, the material ingested, processed and analysed. My only criticism of that report is that it is simplistic in its nature. This is, in part, because whereas 30 years ago the way that signals intelligence was collected followed a pretty straightforward route. That is: identifying what it is you are trying to collect, working out how to collect it, looking at the material you have then collected, processing it and then matching it against what you were trying to collect, leading to a finalised intelligence report. That method was a perfectly satisfactory one when you're dealing with kind of concrete human intelligence, you know, files, documents that you were trying to steal, that sort of thing. With signals intelligence, at the scale it's run today, that chain is

Übersetzung

Sachverständiger Eric King: *Ja, natürlich. - Ein weiterer Bericht, den Ms. Wilson Palow nicht erwähnte, stammt von der US National Academy of Sciences. Dieser Bericht ist 300 Seiten lang und beschreibt ziemlich detailliert das Verfahren, mit dem Glasfaserkabel angezapft werden und das Datenmaterial aufgenommen, bearbeitet und analysiert wird. Meine einzige Kritik an diesem Bericht gilt seinem stark vereinfachenden Ansatz. Zum Teil liegt das zwar daran, dass die Informationserfassung in der Signalaufklärung vor 30 Jahren ziemlich simpel war. Es lief so ab: Man stellte fest, welche Informationen man erfassen wollte, überlegte sich einen Weg, sie zu erfassen, sah sich dann die erfassten Informationen an, verarbeitete sie und verglich sie mit dem, was man erfassen wollte. Daraus ergab sich der finale Geheimdienstbericht. Diese Methode war absolut befriedigend, wenn es um die konkrete geheimdienstliche Nachrichtengewinnung durch Agenten ging, also Dateien, Dokumente, die man zu stehlen versuchte, so etwas in der Art. Bei der Signalaufklärung im heutigen*

Original

essentially permanently looped, i.e. material once decided to be collected is got in bulk. When it's processed, it's processed to understand what information was acquired and then re-matched against it. In the United Kingdom, there's a particular type of process called query-focused datasets that are created from this raw SIGINT. To the extent that your committee has analysed the equivalent here in Germany or the US, I would suggest you focus on this in great detail. The importance of it, to my mind, is that query-focused datasets acquire large amounts of raw material. It processes them and ties them to identifiable individuals, essentially creating the modern version of a dossier on a person. Thus, when they are stored, even if they are never looked at by an intelligence officer, the level of intrusion is far greater than simply storing it in an unindexed form. It's much more profiling - something that the European Courts of Strasbourg and Luxembourg have both attached more significance and importance to. And I think it's that area that probably requires much greater safeguards and it's the area where our law has not done enough to acknowledge that change in technical capability in that way. - I can speak a lot more about this issue but perhaps I should stop there.

Übersetzung

Maßstab ist diese Kette im Grunde eine ewige Schleife. Das heißt, das Material, von dem früher gezielt entschieden wurde, dass es erfasst werden soll, wird jetzt massenhaft erfasst. Wenn diese Daten verarbeitet werden, dann um zu verstehen, welche Informationen beschafft wurden, und sie anschließend zu vergleichen. In Großbritannien gibt es ein besonderes Verfahren, das als „query-focused datasets" beschrieben wird, „fragebezogene Datensätze", die aus den Rohdaten der Signalaufklärung gewonnen werden. Sofern Sie ein entsprechendes Verfahren hier in Deutschland oder den USA untersucht haben, empfehle ich Ihnen, ihm sehr eingehende Aufmerksamkeit zu widmen. Das Wichtige daran ist meiner Ansicht nach, dass beim Verfahren der fragebezogenen Datensätze große Mengen von Rohdaten erfasst werden. Sie werden verarbeitet und mit identifizierbaren Personen in Verbindung gebracht, wodurch im Grunde eine moderne Art von personenbezogenem Dossier entsteht. Wenn diese Datensätze gespeichert werden, ist dies ein sehr viel größerer Eingriff in die Privatsphäre, als wenn die Daten einfach nicht indexiert gespeichert würden, selbst dann, wenn sie kein Geheimdienstmitarbeiter jemals ansieht. Sie lassen in viel stärkerem Ausmaß die Erstellung von Persönlichkeitsprofilen zu - und das ist etwas, dem die Europäischen Gerichtshöfe in Straßburg und Luxemburg eine größere Bedeutung beimessen. Ich denke, dass in diesem Bereich sehr viel stärkere Schutzmaßnahmen benötigt werden und dass es der Bereich ist, in dem unser Gesetz den Veränderungen der technischen Möglichkeiten nicht ausreichend Rechnung trägt. - Ich könnte noch viel mehr zu diesem Thema sagen, aber ich denke, ich sollte es hierbei belassen.

Vorsitzender Dr. Patrick Sensburg: Gut. - Dann kommen wir jetzt zum Kollegen von Notz.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. - Ich wollte noch mal zwei Fragen stellen, und zwar im Hinblick auf vielleicht Ihre Kenntnisse zu Aktivitäten der Five Eyes in Deutschland oder auch Kooperationen mit dem Bundesnachrichtendienst. Im Grunde würde ich das gerne so weit halten, wie es geht, aber vielleicht zwei Stichworte nennen. Also einmal: Wie verhält es sich eigentlich mit dem TAT-

Original

14-Kabel und eventuell gemeinsamen Kooperationen, die im Jahr 2013 zumindest begonnen wurden, zwischen dem GCHQ und dem Bundesnachrichtendienst? Haben Sie vielleicht von einzelnen Operationen gehört, wie „Glotaic“ oder Ähnliches, oder nur über unseren Ausschuss? Dann brauchen Sie das nicht zu berichten; denn das wissen wir ja selbst. Aber vielleicht haben Sie eigene Erkenntnisse, was für eine Rolle in den letzten Jahren der Bundesnachrichtendienst und Deutschland für die Five Eyes und den GCHQ im Speziellen gespielt haben. - Vielen Dank.

Vorsitzender Dr. Patrick Sensburg: Ich würde sagen, jetzt beginnen Sie wieder, Herr King. Oder wie hatten wir es letztes Mal? - Andersherum. - Dann sind Sie dran, Frau Wilson Palow. Sie beginnen.

Sachverständige Caroline Wilson Palow: I may actually defer to Mr King on this one. I'm afraid I do not have much more information than what we already know has been revealed by this committee.

Sachverständiger Eric King: I'm afraid, while I would love to answer that question in full, the extent of the knowledge that I have I'm sure is shared by the committee here. I've read the *Der Spiegel* report and the codename, I think, was "Monkeyshoulder". I have attempted to find out information in the UK about it - its relationship, how it was regulated, whether or not it was simply bilateral, whether or not it was part of a broader set of undertakings which GCHQ might have been trying to establish also with the Dutch in a similar way, exchanging material. A similar sort of programs are run by the NSA under the RAMPART codename. I regret I haven't been able to obtain any further information from the British government. Of course, this is a point that is deeply frustrating. Our oversight reports in this area protect national security by not referencing specific codenames. While that is of course proper, in principle, it is frustrating when you are trying to understand the legal requirements and whether or not policy is being lawfully followed. We've had a number of oversight reports

Übersetzung

Sachverständige Caroline Wilson Palow: *Ich möchte diese Frage gerne an Mr. King weitergeben, denn ich fürchte, ich weiß darüber nicht mehr, als dem Ausschuss bereits bekannt ist.*

Sachverständiger Eric King: *Ich würde diese Frage sehr gerne vollumfänglich beantworten, fürchte jedoch, dass ich nicht mehr darüber weiß als die Mitglieder des Ausschusses. Ich habe den Bericht im* Spiegel *gelesen, und ich glaube, der Codename lautete „Monkeyshoulder“. Ich habe versucht, in Großbritannien Informationen hierüber zu erhalten - dazu, wie die Beziehung aussah, wie es reguliert wurde, ob es sich um ein rein bilaterales Programm handelte, ob es Teil einer größeren Reihe von Operationen war, die der GCHQ möglicherweise auf ähnliche Weise auch mit den Niederländern zum Austausch von Material etablieren wollte. Ähnliche Programme werden von der NSA unter dem Codenamen RAMPART durchgeführt. Ich bedaure, dass es mir nicht gelungen ist, von der britischen Regierung weitere Informationen hierüber zu erhalten. Das ist natürlich zutiefst frustrierend. Die Berichte unserer Kontrollgremien zu diesem Bereich nennen zum Schutz der nationalen Sicherheit keine bestimmten Codenamen. Das ist natürlich grundsätzlich korrekt, aber dennoch frustrierend, wenn man versucht, die rechtlichen Vorgaben zu verstehen und zu erkennen,*

Original

in the last three years none of which clearly addresses this issue despite efforts. I wish that wasn't the case but that's where we are.

Übersetzung

ob die Richtlinien rechtmäßig befolgt wurden. Es gab in den vergangenen drei Jahren eine Reihe von Kontrollberichten, von denen keiner klar auf diese Fragen eingegangen ist, trotz aller Bemühungen. Ich wünschte, es wäre anders. Aber so sieht es aus.

Vorsitzender Dr. Patrick Sensburg: Okay, gut. - Dann würden wir die nächste Runde machen. Kollege Schipanski hatte sich schon gemeldet, Kollege von Notz und Kollege Flisek. Danke.

Tankred Schipanski (CDU/CSU): Herr King, ich darf vielleicht einfach noch einmal anknüpfen bei der Beantwortung der Ringtausch-Frage. In der Tat haben Sie das noch mal konkretisiert. Wir verstehen unter Ringtausch eben, dass angeblich die inländischen Gesetze umgangen werden, um eben an entsprechende Informationen zu kommen.

Jetzt will ich da einfach nur noch mal in der Hinsicht fragen: Sie sind als Sachverständiger hier. Woher stammt Ihr Wissen? Sie hatten jetzt Bücher angebracht, die Sie zitiert haben. Kommt das aus Gesprächen mit Mitarbeitern von Nachrichtendiensten? Ist das Forschung an Universitäten? Ist das Zeitungswissen? Sie haben jetzt den *Spiegel* erwähnt. Es ist nur wichtig, dass wir einordnen können, woher diese Informationen stammen, die Sie heute uns hier nennen.

Die zweite Frage geht an die Frau Palow, die jetzt in mehreren Antworten die Snowden-Dokumente als eine Art Beweis angeführt hat. Wir konnten jetzt im Rahmen dieser Ausschussarbeit noch nicht klären, ob diese Unterlagen, die da von Edward Snowden stammen, tatsächlich echt sind, welchen Stellenwert diese haben.

(Dr. André Hahn (DIE LINKE): Das ist doch Unsinn! So ein Unsinn!)

Wir haben verschiedenen Zeugen diese Sachen vorgelegt und gezeigt. Sie haben gesagt, das ist technisch gar nicht möglich, was da drinsteht, und Ähnliches.

Original

(Dr. André Hahn (DIE LINKE): Das ist eine glatte Lüge!)

Und jetzt ist die Frage an Sie: Wie haben Sie das authentifiziert? Wie haben Sie festgestellt: „Aha, das sind wirkliche Unterlagen. Das ist richtig. Genau das passiert eigentlich“?

(Dr. André Hahn (DIE LINKE): Glatte Lüge!)

Vorsitzender Dr. Patrick Sensburg: Herr Kollege Hahn, bitte unterlassen Sie solche Zwischenrufe.

Tankred Schipanski (CDU/CSU): Ja.

(Dr. André Hahn (DIE LINKE): Nein! Wenn er lügt, dann muss man das doch sagen!)

Vorsitzender Dr. Patrick Sensburg: Nein, bitte unterlassen Sie solche Zwischenrufe.

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Das ist ein falscher Vorhalt!)

Tankred Schipanski (CDU/CSU): Das ist überhaupt kein falscher Vorhalt.

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Na logo!)

Vorsitzender Dr. Patrick Sensburg: Nein.

Tankred Schipanski (CDU/CSU): Überhaupt nicht.

Vorsitzender Dr. Patrick Sensburg: Ich würde jetzt sofort die Sitzung unterbrechen. Dann machen wir eine Beratungssitzung.

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, bitte schön! Los geht’s!)

Übersetzung

Original

Die Sitzung ist unterbrochen. Wir machen eine Beratungssitzung. Ich bitte die Zuhörer und auch die Sachverständigen, den Saal zu verlassen. Wir müssen an dieser Stelle beraten.

(Unterbrechung des Sitzungsteils Sachverständigenanhörung: 10.39 Uhr - Folgt Sitzungsteil Beratung)

(Wiederbeginn des Sitzungsteils Sachverständigenanhörung: 10.47 Uhr)

Vorsitzender Dr. Patrick Sensburg: Meine Damen und Herren, wir setzen die unterbrochene Sitzung des 1. Untersuchungsausschusses fort. Die Vorweihnachtszeit hat schnellen Frieden gebracht. - Ich nehme jetzt die Frage des Kollegen von Notz sowie die offenen Fragen vom Kollegen Flisek und von Frau Kollegin Renner mit dazu, und dann kommen wir in die Beantwortungsrunde. - Herr Kollege von Notz.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ich wollte noch mal fragen, ob Sie uns erklären können, was metadatenzentrierte Erfassung ist - also nicht Metadatenerfassung, das sage ich jetzt auch für die Dolmetscher, sondern metadatenzentrierte Erfassung - und wohin die Reise in diesem Bereich geht.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Herr Kollege Flisek.

Christian Flisek (SPD): Ich möchte dann noch eine Frage anschließen. Und zwar gibt es ja vor dem Europäischen Gerichtshof für Menschenrechte insgesamt drei Beschwerden britischer NGOs. Vielleicht - ich möchte die Frage nicht an irgendjemanden speziell adressieren; Sie können gerne zusammen darauf antworten - können Sie uns noch mal einen kurzen Sachstand geben: Worum geht es dort? Was ist der aktuelle Stand dieser Verfahren? Das wäre für uns vielleicht ganz informativ. - Danke.

Vorsitzender Dr. Patrick Sensburg: Und last but not least Frau Kollegin Renner.

Übersetzung

Original

Martina Renner (DIE LINKE): Ich habe noch mal eine etwas speziellere Frage. Wir haben hier im Untersuchungsausschuss auch die Zusammenarbeit deutscher Dienste mit dem amerikanischen Militärgeheimdienst DIA untersucht bei der Befragung von Flüchtlingen, die nach Deutschland gekommen sind oder noch kommen. Meine Frage geht in die Richtung: Haben Sie Erkenntnisse, ob es so eine Zusammenarbeit auch mit britischen Geheimdiensten gab, also ob britische Geheimdienste in Deutschland systematisch Flüchtlinge, möglicherweise unter Legende, also ohne dass die Betroffenen wussten, wem sie gegenübersitzen, befragt haben?

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Wir beginnen jetzt aber, ich glaube, bei Ihnen, Herr King. - Genau.

Sachverständiger Eric King: I'm afraid I might need some clarification on your questions, Dr von Notz. I don't think I'm familiar with the term metadata-centred collection but perhaps it's a translation error. Could you ask the question a different way, perhaps I can better understand.

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Erteilen Sie mir noch mal das Wort?)

Vorsitzender Dr. Patrick Sensburg: Auf die Nachfrage gerne.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Also, während man früher die großen Datenmengen mit Selektoren und den Personal Identifiern durchforstet hat, nimmt man heute - so viel hoffe ich verstanden zu haben - bestimmte Parameter, Verhaltensparameter und erfasst damit aus der Datenmenge: „Wer schaltet zu welcher Uhrzeit wo ein Handy an?“, „Wer wechselt zu welcher Uhrzeit wo eine SIM-Karte aus?“, „Wer telefoniert immer mit den drei Leuten?“ usw., sodass sozusagen die Fernmeldeaufklärung eben in diesen Bereich hineinwächst. Was bedeutet das vor allen Dingen für die Datenmengen, die man vorhält, also die Rohdaten, in denen man

Übersetzung

Sachverständiger Eric King: *Ich befürchte, ich benötige eine Erklärung zu Ihrer Frage, Dr. von Notz. Der Begriff „metadatenzentrierte Erfassung“ ist mir nicht bekannt, glaube ich; aber vielleicht handelt es sich auch um einen Übersetzungsfehler. Könnten Sie die Frage umformulieren, damit ich sie eventuell besser verstehe?*

Original

das dann praktizieren muss? - Wenn Sie es nicht wissen, dann ist das auch total okay. Ich dachte nur, vielleicht wissen Sie es.

Sachverständiger Eric King: Yes, I can speak to that. I mean, certainly, the way that signals intelligence works today is, as you described, to focus on metadata. That's for practical reasons. For a long time, in the United Kingdom, our protections were provided to the content of communications rather than to the metadata. There were significantly reduced protections for metadata. Remarkably, our oversight bodies in the United Kingdom didn't understand, actually, that the metadata was the more important aspect for signals intelligence technologies. And, to their credit, the oversight body acknowledged that in their report two years ago. They said: "We were surprised to learn, after talking to the intelligence agencies, how important metadata is to the collection of signals intelligence". There's a variety of ways in which you can understand the importance. In the US, former directors of the NSA have boasted about how important metadata is. I believe the former director of NSA boasted that they kill people on the basis of metadata alone. Stewart Baker, the former General Counsel of NSA, has also said: "Metadata tells you all you need to know about anybody". And it's for obvious reasons. It's because very often the fact of a communication is much more important than the content of it, particularly when you are trying to analyse material of thousands, hundreds of thousands, millions, of people. It's a structured way of achieving those goals. I don't expect that to decrease in the future. In fact, with the rise of transit-based encryption, the content of communications is likely to be more protected in future resulting in a push by signals intelligence agencies to focus even harder on the acquisition and analysis of metadata.

Vorsitzender Dr. Patrick Sensburg: Okay. - Die weiteren Fragen.

Übersetzung

Sachverständiger Eric King: *Ja, dazu kann ich etwas sagen. Die Arbeit der heutigen Signalaufklärung konzentriert sich, wie Sie beschrieben haben, auf Metadaten. Dies geschieht aus praktischen Gründen. In Großbritannien galten unsere Schutzmaßnahmen lange Zeit den Kommunikationsinhalten und nicht so sehr den Metadaten. Für die Metadaten gab es deutlich geringeren Schutz. Es ist bemerkenswert, dass unsere Kontrollgremien in Großbritannien nicht erkannten, dass die Metadaten in Wirklichkeit der für die Signalaufklärungstechnologien wichtigere Teil waren. Man muss ihnen jedoch zugestehen, dass sie dies vor zwei Jahren in ihrem Bericht eingeräumt haben. Dort heißt es: „Wir waren überrascht, in den Gesprächen mit den Geheimdiensten zu erfahren, wie wichtig Metadaten für die geheimdienstliche Nachrichtengewinnung durch Signalaufklärung sind." Es gibt verschiedene Hinweise auf die hohe Bedeutung von Metadaten. In den USA haben ehemalige Leiter der NSA damit geprahlt, wie wichtig Metadaten sind. Ich glaube, der ehemalige Direktor der NSA behauptete, dass allein auf Grundlage von Metadaten Menschen getötet würden. Stewart Baker, der ehemalige General Counsel der NSA, erklärte ebenfalls: „Metadaten verraten einem alles, was man über einen Menschen wissen will." Die Gründe hierfür liegen auf der Hand. In sehr vielen Fällen ist die bloße Tatsache, dass eine Kommunikation stattfindet, wichtiger als der eigentliche Inhalt. - ganz besonders dann, wenn man das Datenmaterial von Tausenden, Hunderttausenden oder gar Millionen Menschen zu analysieren versucht. Metadaten bieten eine strukturierte Herangehensweise zur Erreichung dieser Ziele. Ich denke nicht, dass das in Zukunft weniger werden wird. Mit der Verbreitung der übertragungsbasierten Verschlüsselung werden die Kommunikationsinhalte zukünftig besser geschützt sein, was dazu führen dürfte, dass sich die Geheimdienste noch stärker auf die Beschaffung und Analyse von Metadaten konzentrieren werden.*

Original	*Übersetzung*
Sachverständige Caroline Wilson Palow: I might just add to that that in the case currently pending before the European Court of Justice - it's both the referral from Sweden and from the United Kingdom - - The United Kingdom case is Watson and others versus the United Kingdom regarding data retention. There's actually quite an interesting passage from the Advocate General in the case, describing the ways in which metadata can be used and are very helpful in this regard, and he describes how it is quite a useful tool for looking very quickly at large populations, being able to discern patterns in the exact way that you just described.	***Sachverständige Caroline Wilson Palow:*** *Ich möchte dem nur hinzufügen, dass in dem derzeit vor dem Europäischen Gerichtshof anhängigen Verfahren - sowohl in dem aus Schweden an den Europäischen Gerichtshof verwiesenen Verfahren als auch in dem aus Großbritannien - - Bei dem Verfahren aus Großbritannien handelt es sich um die Klage von Watson und Nebenklägern gegen Großbritannien in der Sache der Datenspeicherung. Es gibt eine sehr interessante Passage in der Einlassung des Generalanwalts in diesem Verfahren, in dem er Möglichkeiten beschreibt, wie Metadaten genutzt werden und die in dieser Hinsicht sehr hilfreich sein können. Er erläutert, wie sich Metadaten als nützliches Werkzeug einsetzen lassen, um sehr schnell sehr große Bevölkerungsgruppen zu betrachten und dabei Muster zu erkennen, genau wie Sie es gerade beschrieben haben.*
Maybe I'll just briefly address the question regarding the three cases currently pending before the European Court of Human Rights. I think you maybe mentioned that the three cases are joined together. Yes, one of which is the ten human rights organisations which I mentioned earlier, in which Privacy International is a claimant, along with Liberty - Ms Carlo's from Liberty whom you've already heard earlier -, Amnesty International and seven other NGOs, along with another related case which is Big Brother Watch, Open Rights Group and several other UK NGOs, and then, finally, a third related case where they are all dealing with the same general issues, which are two: one is the question of whether or not the bulk interception regime in the United Kingdom is lawful under the European Convention on Human Rights, and the second is whether or not the sharing of information between the US and the United Kingdom was lawful under the legal regime that was in place in the United Kingdom at the time that that occurred. And so in that case, at the moment, observations have been submitted by the United Kingdom and the claimants have responded to them and then we are waiting for the next phase. - Okay.	*Vielleicht gehe ich kurz auf die Fragen zu den drei Klagen ein, die derzeit vor dem Europäischen Gerichtshof für Menschenrechte anhängig sind. Ich glaube, es wurde bereits erwähnt, dass die drei Verfahren zusammenhängen. Ja, bei einem handelt es sich um die Klage der zehn Menschenrechtsorganisationen, die ich zuvor erwähnte. Hier tritt Privacy International gemeinsam mit Liberty - Ms. Carlo von Liberty haben Sie bereits in einer früheren Sitzung angehört -, Amnesty International und sieben weiteren als Kläger auf, neben einem zweiten, damit verbundenen Verfahren, in dem die Kläger Big Brother Watch, Open Rights Group und mehrere weitere britische NGOs sind, und schließlich einem dritten, ebenfalls damit verbundenen Verfahren. In allen drei Verfahren geht es um dieselben beiden allgemeinen Fragen: Erstens, ob die britische Gesetzgebung zur massenhaften Datenerfassung mit der Europäischen Menschenrechtskonvention vereinbar ist, und zweitens, ob der Austausch nachrichtendienstlicher Informationen zwischen den USA und Großbritannien nach dem zum damaligen Zeitpunkt in Großbritannien geltendem Recht gesetzeskonform war. Der aktuelle Stand in diesem Verfahren ist der, dass die britische Regierung eine Stellungnahme abgegeben hat, auf die die Kläger reagiert haben, und jetzt warten wir auf die nächste Phase. - Okay.*

Nur zur dienstlichen Verwendung

Original

Vorsitzender Dr. Patrick Sensburg: Okay. - Ich sehe jetzt, dass zwei Fragen noch nicht beantwortet sind: eine vom Kollegen Schiplanski und eine von Frau Renner. Die beiden Fragen sind noch offen.

Sachverständiger Eric King: I'm afraid, Ms Renner, I'm not familiar with news related to that. I apologise.

Mr Schipanksi, your question, was that the one asking where I get my information from? So, I'm an academic on this topic at the moment. I teach a law course in the United Kingdom looking at intelligence collection and surveillance as it applies to law. I've spent the last seven years looking exclusively at this issue of signals intelligence. My sources are varied, as they are in all research: that's oversight reports, provided by governments, that's speaking with law enforcement bodies, former intelligence officers, former lawyers at intelligence agencies, government departments, our Home Office, and others that have looked at this, leaked material from Snowden and from a wide variety of other sources some of which are confirmed to individuals and some of which are not, autobiographies and biographies from former intelligence officers, academic studies written in collaboration with intelligence bodies, international organisations' reports on oversight from the Council of Europe and others who have worked with intelligence officers. So, a broad spectrum of material. And, so, I have based my analysis on my research using that sort of material, if that's helpful.

Vorsitzender Dr. Patrick Sensburg: Okay. - Gut, die Antwort auf die Frage von Frau Kollegin Renner war jetzt nicht ergiebig.

(Martina Renner (DIE LINKE): Ja, ist okay!)

Übersetzung

Sachverständiger Eric King: *Ich befürchte, Frau Renner, dass mir hierzu nichts Neues bekannt ist. Ich bitte um Nachsicht.*

Herr Schipanski, Ihre Frage war die danach, woher ich meine Informationen habe? Nun, ich befasse mich momentan als Wissenschaftler mit diesem Thema. Ich unterrichte in einem juristischen Seminar in Großbritannien, in dem es um die rechtlichen Aspekte der nachrichtendienstliche Datenerfassung und Überwachung geht. Ich habe mich in den vergangenen sieben Jahren ausschließlich mit dem Thema Signalaufklärung beschäftigt. Meine Quellen sind vielfältig, wie sie es in der Forschung immer sind: Dazu zählen Berichte von Kontrollgremien, die von Regierungen verfügbar gemacht werden, Gespräche mit Vertretern von Sicherheitsbehörden, ehemaligen Geheimdienstmitarbeitern, ehemaligen Anwälten bei Geheimdiensten, Regierungsbehörden, unserem Innenministerium und mit anderen, die sich mit diesem Thema befassen, außerdem die Materialien der Snowden-Enthüllungen sowie eine breite Vielfalt weiterer Quellen, von denen einige Personen zuzuordnen sind und andere nicht, Autobiografien und Biografien ehemaliger Geheimdienstmitarbeiter, wissenschaftliche Untersuchungen, die in Zusammenarbeit mit Geheimdienstbehörden verfasst wurden, Berichte internationaler Organisationen zur Geheimdienstkontrolle, vom Europarat und anderen, die mit Geheimdienstmitarbeitern zusammengearbeitet haben. Also eine große Bandbreite an Material. Ich gründe meine Analyse in meiner wissenschaftlichen Forschung, die ich unter Nutzung all dieser Materialien betreibe, wenn das hilfreich ist.

Original

Kollege von Notz noch zur letzten Frage? Oder geht es schon wieder in eine neue Runde?

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Neue Runde!)

- Okay, dann gibt es eine neue Runde. Es beginnt Kollege von Notz.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Genau. - Ich wollte vielleicht noch einmal nachhaken im Hinblick auf diese Frage zu Metadaten, die wir eben hatten. Wir haben uns ja hier im Ausschuss auch sehr intensiv mit der Frage der Selektoren beschäftigt. Also, ich würde sagen, im Grunde schon eine leicht überholte, aber immer noch praktizierte Art, eben aus den großen Metadatenmengen Inhalte herauszufiltern. Sie haben das vielleicht medial verfolgt: Der Bundesnachrichtendienst hat selbst eine ganze Reihe von Selektoren, die er steuert, und da ging es um Fragen der Zulässigkeit. Das ist hier sehr intensiv bewegt worden. Aber vor allen Dingen hat der Bundesnachrichtendienst auch für die NSA viele Millionen Selektoren über viele Jahre in Deutschland gesteuert. Deswegen die Frage: Ist das Thema Selektoren in Großbritannien ein Thema? Und wenn ja: Wie sieht eigentlich die parlamentarische Kontrolle dieser Selektoren aus? Gibt es darüber eine Diskussion „Was darf man steuern, was nicht?“, „Sind Journalisten in Ordnung?“, „Gibt es Tabus?“ oder „Gibt es bestimmte Zeiträume, für die man Selektoren unter bestimmten Voraussetzungen steuern kann?“, oder machen die Dienste einfach in dem Bereich, was sie wollen?

Vorsitzender Dr. Patrick Sensburg: Herzlichen Dank. - Frau Kollegin Renner habe ich noch. Dann müssten wir gucken, ob es die letzte Runde ist, weil die Zeit dann um ist.

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Eine Frage habe ich noch!)

- Ja, wollen wir die noch mit dazupacken?

Übersetzung

Original

(Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Wenn das okay ist!)

- Klar, wenn wir dann die letzte Runde schaffen, ist es so am besten.

Dr. Konstantin von Notz (BÜNDNIS 90/DIE GRÜNEN): Ja, gut. - Dann ist meine letzte Frage vielleicht noch mal konkret auf das TAT-14-Kabel und Bude bezogen. Was passiert da? Was macht der britische Dienst sozusagen an diesem Glasfaserkabel mit europäischem Datenverkehr? Gibt es da Indikatoren? Dass man das nicht exakt weiß, okay; aber wir haben inzwischen schon eine Idee, was da passiert. Vielleicht können Sie das ergänzen mit Wissen von Ihnen, was sozusagen speziell bei der Glasfaseranlandung in Großbritannien an den Kabeln gemacht wird, insbesondere am TAT-14.

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Frau Kollegin Renner.

Martina Renner (DIE LINKE): Ich hätte abschließend zwei Fragen. Zum einen: Uns wird gelegentlich aus Regierungskreisen entgegengehalten, dass bei zu detaillierter Auseinandersetzung mit einzelnen Operationen, die im Bereich geheimdienstlicher Kooperationen stattfinden, dies möglicherweise auf der Gegenseite derartiges Missfallen auslösen könnte, dass dann die Zusammenarbeit gänzlich infrage gestellt würde. Mit Blick auf Ihre Kenntnis, insbesondere Herrn Kings, über den GCHQ, halten Sie es für realistisch angesichts der Bedeutung der Zusammenarbeit der Five Eyes, dass man aus Verstimmungen heraus die Zusammenarbeit abbrechen würde?

Und das Zweite - ich glaube, Frau Palow, da bin ich bei Ihnen richtig -: Welche Rechte haben denn Nicht-Briten und -Britinnen mit Blick auf Datenerfassung durch Geheimdienste in Großbritannien hinsichtlich der Frage „Wer kann dort Auskunft verlangen, welche Daten zu ihm erhoben und verarbeitet wurden?“, „Wer hat Anspruch darauf, wenn er eine solche Auskunft erhalten hat, dass Daten auch gelöscht werden?“

Übersetzung

Original

und Ähnliches? Also, gibt es dort eine Gleichberechtigung mit zum Beispiel EU-Bürgern, mit Bürgern anderer Staaten, oder gibt es spezielle Rechte, die nur eigenen Staatsbürgern und -bürgerinnen zukommen würden?

Vorsitzender Dr. Patrick Sensburg: Ganz herzlichen Dank. - Ich glaube, das waren die letzten Fragen an Sie. Und jetzt würde ich mit Frau Wilson Palow beginnen.

Sachverständige Caroline Wilson Palow: Yes, thank you. - With regard to the question on selectors and oversight, and I'm sure Mr King will have more to say on this as well. In the UK, the specific question of selectors and how those will be used was not something that was specifically addressed in the Investigatory Powers Act. There is now a new scheme of broad authorisations for different types of interception and, in a relatively new scheme, of having an additional judicial commissioner who will sign off on the warrants but selectors are never specifically mentioned. There are also certain protections - they may not go far enough - but there are certain protections for groups like journalists, legally privileged material, Members of Parliament, but again, there is no specific mention of selectors in that process. That's something that we certainly brought up during the course of the debate as an area where safeguards might actually be useful to be applied but, ultimately, that's not something that is explicitly mentioned in the law.

With regard to what rights do non-UK citizens have in the United Kingdom - it's not so much based on citizenship but on location. So, anyone who is located - this is what the Investigatory Powers Tribunal, the oversight body of the UK intelligence services, has said - within the United Kingdom can take a claim to the Investigatory Powers Tribunal requesting that there be an assessment of whether or not they were unlawfully subject to surveillance. Until recently, it seems apparent that anyone in the world could come to the Investigatory Powers Tribunal, but there was a decision this year where the tribunal said that only those people within the UK have rights to

Übersetzung

Sachverständige Caroline Wilson Palow: *Ja, vielen Dank. - Zur Frage nach den Selektoren und der Geheimdienstkontrolle - und ich bin sicher, dass Mr. King hierzu auch etwas zu sagen hat -: Der britische Investigatory Powers Act geht nicht explizit auf Selektoren und den Einsatz von Selektoren ein. Aktuell gibt es ein neues System weitgefasster Genehmigungen für verschiedene Arten der Datenerfassung und ein relativ neues System, bei dem Genehmigungen durch einen weiteren Gerichtskommissar unterzeichnet werden müssen. Selektoren werden dabei jedoch nicht eigens erwähnt. Es gibt auch gewisse Schutzmaßnahmen, die möglicherweise nicht weitreichend genug sind; aber es gibt Schutzmaßnahmen für bestimmte Gruppen wie zum Beispiel Journalisten, für Kommunikationsdaten, die unter das anwaltliche Berufsgeheimnis fallen, für Parlamentsangehörige. Doch auch hier werden Selektoren nicht eigens erwähnt. Das ist ein Punkt, den wir im Laufe der Debatten angesprochen und als Bereich ausgemacht haben, in dem Schutzmaßnahmen sinnvollerweise gelten sollten; aber es wurde letztlich nicht ausdrücklich in das Gesetz aufgenommen.*

Was die Rechte betrifft, die ausländische Bürger in Großbritannien genießen: Das hängt nicht so sehr von der Staatsbürgerschaft ab, sondern vom Aufenthaltsort. Das Investigatory Powers Tribunal, das Kontrollgremium für die britischen Geheimdienste, hat dazu erklärt, dass jeder, der sich in Großbritannien aufhält, vor dem Investigatory Powers Tribunal eine Beurteilung darüber einfordern kann, ob er oder sie unrechtmäßig überwacht wurde. Bis vor kurzem schien es offensichtlich, dass jeder Mensch auf der Welt sich an das Investigatory Powers Tribunal wenden kann; aber es gab in diesem Jahr ein Urteil, in dem das Tribunal entschied, dass nur Menschen, die

Original

bring these claims under the European Convention on Human Rights. So I should be specific about that. So, the tribunal has said that anything under the European Convention on Human Rights, they only have jurisdiction to hear those claims if it's about someone who is located in the UK at the time the claim occurred. If it is a violation of UK law, it is still possible for anyone to come to the tribunal and allege a violation of UK law in the course of their surveillance.

Sachverständiger Eric King: To take the questions in turn. Dealing with TAT-14 - I'm afraid I would have to look back at my notes. I recall that there were a number of publications relating to specific cables that were being intercepted by GCHQ and the percentage of egress - that is the percentage that was taken in from the cable - was published, as well as the projections for how that would grow over multiple years. I'm afraid the list was very long and I can't remember TAT-14 specifically within that. One of the takeaways of that publication that I did note, however, was that over the course of four years, GCHQ's capability to intercept from undersea fibre-optic cables increased by 7 000 percent. I make this point because when we talk about our statutory framework regulating this, concepts of necessity and proportionality become essentially tied to technical capability and they are pushed to their limit, in my view, when you can have a 7 000-percent increase in an activity over four years and not need to change the statutory framework limiting collection. This was in 2009. I imagine it's increased from this point. I think at around that time GCHQ had the ability to intercept from almost all cables coming into the UK but, in practice, in 2009 at least, and this is dated information, they were collecting off about a quarter of those at any one time.

Übersetzung

sich in Großbritannien aufhalten, ihre Ansprüche gemäß der Europäischen Menschenrechtskonvention vor dem Tribunal geltend machen können. Um es noch genauer zu sagen: Das Tribunal hat entschieden, dass es für Ansprüche auf Grundlage der Europäischen Menschenrechtskonvention nur dann zuständig ist, wenn die Person, die den Anspruch erhebt, sich zum Zeitpunkt des gerügten Tatbestands - der Überwachung - in Großbritannien aufhielt. Wenn es sich um einen Verstoß gegen britisches Recht handelt, kann nach wie vor jeder vor dem Tribunal geltend machen, dass im Laufe der Überwachung gegen britisches Recht verstoßen wurde.

Sachverständiger Eric King: *Ich gehe die Fragen der Reihe nach durch. Zum Verfahren beim TAT-14 - ich fürchte, da muss ich in meinen Aufzeichnungen nachsehen. Ich erinnere mich, dass es eine Reihe von Veröffentlichungen zu bestimmten Kabeln gab, die vom GCHQ angezapft wurden. Der Austrittsprozentsatz, also der Prozentsatz, der aus dem Kabel entnommen wurde, wurde darin veröffentlicht, ebenso wie Vorhersagen über die Zunahme im Laufe mehrerer Jahre. Ich befürchte, dass es eine sehr lange Liste war, und kann mich leider nicht an spezifische Informationen zu TAT-14 darin erinnern. Ein Punkt in dem Artikel, den ich mir jedoch gemerkt habe, ist, dass die Möglichkeiten des GCHQ, Daten von Unterwasser-Glasfaserkabeln zu erfassen, in vier Jahren um 7 000 Prozent gewachsen sind. Ich erwähne dies, weil bei den Diskussionen zu unserem rechtlichen Rahmen, der diese Erfassung regelt, Aspekte von Notwendigkeit und Verhältnismäßigkeit essenziell mit den technischen Möglichkeiten verknüpft werden. Und meiner Ansicht nach werden diese Aspekte an ihre Grenzen geführt, wenn man eine Aktivität im Laufe von vier Jahren um das 70-fache steigert, ohne den Rechtsrahmen anzupassen, der die Datenerfassung einschränkt. Die Zahlen stammen aus dem Jahr 2009. Ich nehme an, es ist seither noch mehr geworden. Ich glaube, damals hatte der GCHQ Möglichkeiten, fast alle nach Großbritannien laufenden Kabel anzuzapfen, aber in der Praxis haben sie nur etwa aus einem Viertel davon Daten erfasst, jedenfalls 2009, und diese Informationen sind mittlerweile veraltet.*

Nur zur dienstlichen Verwendung

Original

In terms of limits on selection, as Caroline explained, there's nothing in our statutory framework that regulates the selection of material. I think this is clearly problematic as it doesn't reflect how intelligence officers do their job. We almost have a completely separate legal framework and a completely separate set of rules to what the day-to-day activities of an officer is. My view is that our laws should be drafted to reflect what it is that our officers do and the collections systems that take place. What we do know from the Intelligence and Security Committee, and this is in their public reports, is that Britain has two separate collection systems. The first is a major processing system targeted at bearers as we call them in the United Kingdom, these undersea fibre-optic cables. The system compares the traffic against a list of simple selectors, that's a term we use in the UK - I don't know if it's the same in here, these are specific identifiers relating to a known target. Any communications which match these are collected. That's one major processing system. From there there's a tri-arch process. But there's another major processing system, which isn't called Tempora in the official documents but is widely understood in the United Kingdom to be Tempora. In this instance, it says that bearers make up the Internet, GCHQ applies selection rules and, as a result, the processing system begins to sift through that material. Now, the distinction between those two is quite important. The first is a simple selector which is about a known target that is your email address, my phone number, something of that nature. And the second processing system is a selection of rules - that is a string, a number of different variables put together. This is what you would otherwise call trawling for information not tied to a known specific individual. And it's that second processing system that I think is much more problematic.

Übersetzung

Was die Begrenzung von Selektoren angeht, so gibt es, wie Ms. Wilson Palow bereits erläuterte, in unseren rechtlichen Rahmenbedingungen nichts, wodurch dies geregelt wird. Dies ist meiner Ansicht nach eindeutig problematisch, da es nicht die Arbeitsweise von Geheimdienstmitarbeitern abbildet. Unser rechtlicher Rahmen und unser Regelwerk sind vollkommen abgetrennt von dem, was die Geheimdienstmitarbeiter tagtäglich tun. Ich bin der Meinung, dass unsere Gesetze so formuliert sein sollten, dass sie die Arbeitsweise unserer Geheimdienste und die Erfassungssysteme, die verwendet werden, widerspiegeln. Aus den öffentlich verfügbaren Berichten des Intelligence and Security Committee wissen wir, dass es in Großbritannien zwei verschiedene Erfassungssysteme gibt. Das erste ist ein groß angelegtes Verarbeitungssystem, das auf die in Großbritannien so genannten „Träger" abzielt, die Unterwasser-Glasfaserkabel. Dieses System vergleicht den Datenverkehr mit einer Liste einfacher Selektoren; „simple selectors" ist der Begriff, den wir hierfür in Großbritannien verwenden, ich weiß nicht, ob es hier derselbe ist. Es handelt sich dabei um bestimmte Identifikatoren, die sich auf ein bekanntes Überwachungsziel beziehen. Alle damit übereinstimmenden Kommunikationsdaten werden erfasst. Es handelt sich um ein einziges, sehr großes Verarbeitungssystem. Ab diesem Punkt gibt es dann ein Triage-Verfahren. Es gibt jedoch noch ein weiteres großes Datenverarbeitungssystem, das in den offiziellen Unterlagen zwar nicht als Tempora bezeichnet wird, bei dem aber in Großbritannien allgemein davon ausgegangen wird, dass es sich um Tempora handelt. In diesem Fall heißt es, dass das Internet aus „Trägern" besteht. Der GCHQ wendet dann Auswahlregeln an, und das Verarbeitungssystem beginnt das Material dementsprechend zu durchsuchen. Der Unterschied zwischen diesen beiden Vorgehensweisen ist ziemlich bedeutend. Im ersten Fall gibt es einen einfachen Selektor, der sich auf ein bekanntes Überwachungsziel bezieht, also zum Beispiel Ihre E-Mail-Adresse oder meine Telefonnummer oder etwas in der Art. Das zweite Verarbeitungssystem geht nach einer Reihe von Regeln vor, also einer Folge oder Kombination verschiedener Variablen. Dieses Vorgehen könnte man auch als Schleppnetz-Datenerfassung bezeichnen, die sich nicht auf ein bekanntes und bestimmtes Überwachungsziel beschränkt. Dieses

Nur zur dienstlichen Verwendung

Original

Ms Renner asked about whether or not it's likely that an intelligence agency would stop sharing material. I think it would be quite short-sighted of any agency to break entirely contact with another service. Certainly, Britain has relationships with hundreds of different countries. I think in the last evidence session from UK experts, the number of 168 was provided, I think, by Mr Anderson. In my experience, there is only one circumstance that I can think of amongst allies where that stopped happening, and that was when New Zealand was nuclear-free, this was in the late 70s, early 80s, and had a very strong policy position which prevented American nuclear power ships from landing in New Zealand waters. The dispute was so significant that they did stop sharing material, I think, for a period of six months. Soon after that it picked up again and resumed.

There are, however, two quotes that I would like to provide to you which I think provide a bit of a picture about how intelligence agencies see their intelligence sharing relationships. The first is a NSA Foreign Affairs Directorate leaked document - they say:

> For a variety of reasons our intelligence relationships are rarely disrupted by foreign political perpetrations, international or domestic. In many of our foreign partners' capitals, few senior officials outside of their defence and intelligence apparatus are witting to any SIGINT connection to the US.

In another story that was published by *Signal Magazine*, which is signals intelligence magazine in the US, Admiral Michael Rogers said:

Übersetzung

zweite Datenverarbeitungssystem halte ich für das weitaus problematischere.

Frau Renner fragte, wie wahrscheinlich es ist, dass ein Geheimdienst aufhört, Informationen an andere weiterzugeben. Ich denke, es wäre ein für jeden Geheimdienst sehr kurzsichtiger Schritt, den Kontakt zu einem anderen Geheimdienst komplett abzubrechen. Großbritannien unterhält [nachrichtendienstliche] Beziehungen zu Hunderten verschiedener Staaten. Ich glaube, in der letzten Anhörung britischer Experten wurde die Zahl 168 genannt, ich glaube, durch Mr. Anderson. Meiner Erfahrung nach gab es nur einen Fall, in dem die Zusammenarbeit zwischen Verbündeten unterbrochen wurde, das war in den späten 70er- und frühen 80er-Jahren, als Neuseeland atomwaffenfrei wurde und öffentlich eine sehr klare politische Position bezog, die ausschloss, dass US-amerikanische atomgetriebene Schiffe in neuseeländische Hoheitsgewässer einfahren. Der Streit hatte eine solche Tragweite, dass die beiden Staaten vorübergehend - ich glaube, für einen Zeitraum von sechs Monaten - keine Informationen mehr miteinander austauschten. Kurz darauf wurde die Zusammenarbeit jedoch wieder aufgenommen.

Ich möchte Ihnen aber zwei Zitate nennen, die meiner Meinung nach verdeutlichen, wie die Geheimdienste ihre Kooperationsbeziehungen einschätzen. Das erste stammt aus einem durchgesickerten Dokument des NSA Foreign Affairs Directorate (NSA-Direktion für Auswärtige Angelegenheiten). Darin heißt es:

> *Aus verschiedenen Gründen werden unsere Geheimdienstbeziehungen selten durch politische Vergehen ausländischer Regierungen - sei es auf nationaler oder internationaler Ebene - gestört. In zahlreichen Regierungssitzen unserer ausländischen Partner haben nur wenige hochrangige Amtsträger außerhalb des Verteidigungsapparats und der Geheimdienste Kenntnis einer SIGINT-Verbindung mit den USA.*

In einem Artikel, der in der US-amerikanischen Zeitschrift für Signalaufklärung, Signal Magazine, *erschien, erklärte der US-Admiral Michael Rogers:*

Original	*Übersetzung*
Clearly we have some nations that have been very vocal, very visible in their frustration and their unhappiness, …	*Es gibt eindeutig Staaten, die ihre Frustration und ihre Unzufriedenheit sehr deutlich zum Ausdruck gebracht haben …*
And he goes on to say,	*Und er fährt fort:*
… but we have a level of capability and a reach that literally few, if any, can replicate. The value that NSA in this instance provides them in terms of information that we share is almost irreplaceable.	*… doch wir verfügen über Möglichkeiten und eine Reichweite, die uns buchstäblich kaum einer, wenn überhaupt irgendjemand, nachmachen kann. Der Nutzen in Form einer Informationsweitergabe, den die NSA ihnen in diesem Fall bietet, ist so gut wie unersetzlich.*
You know, my view of looking at those together suggests that intelligence sharing is a practice that will survive almost all political disruptions. - I hope that's of assistance.	*Gemeinsam betrachtet legen diese Aussagen meiner Ansicht nach den Schluss nahe, dass die geheimdienstliche Zusammenarbeit eine Praxis ist, die nahezu jede politische Umwälzung überleben wird. - Ich hoffe, ich konnte Ihnen damit weiterhelfen.*

Vorsitzender Dr. Patrick Sensburg: Okay. - Ich schaue mal in die Runde; aber ich sehe keine weiteren Wortmeldungen. - Damit sind wir schon am Ende der Anhörung.

Ich hatte es Ihnen am Anfang gesagt: Nach Fertigstellung wird Ihnen ein stenografisches Protokoll dieser Sitzung zugesandt. Sie haben dann zwei Wochen Zeit, Korrekturen und Richtigstellungen oder Ergänzungen Ihrer Aussage vorzunehmen, falls das nötig sein sollte, und uns dann das Protokoll zurückzuschicken.

Auch diese Sachverständigenanhörung hat uns wieder zahlreiche Erkenntnisse gebracht. Wir werden das zusammen mit den anderen Sachverständigenanhörungen sicherlich in ein Gesamtbild setzen. Ich glaube, dass insbesondere der Blick nach Großbritannien unseren Blick auch noch einmal schärft, weil wir bisher sehr stark in die USA geschaut haben. Aber auch das, was im Vereinigten Königreich stattfindet - ich will es mal sehr zurückhaltend sagen -, sollte doch intensiv unsere Betrachtung finden. Dafür haben Sie uns noch einmal den Blick geschärft - ohne da etwas bewerten zu wollen; deswegen hatte ich mich so ausgedrückt. Es ist eben bei einer der Aussagen angeklungen: Wir sind ja immer noch -

Original

und ich hoffe, es bleibt so - in einem gemeinsamen Rechtsraum in Europa, und da kann man vielleicht auch einen guten Ansatz finden nach der Rechtsprechung zur Vorratsdatenspeicherung, um irgendwo auf ein gewisses Grundniveau auch im Bereich der Privatheit bei Nachrichtendiensten zu kommen.

Ganz herzlichen Dank für Ihre Ausführungen. Danke, dass Sie den weiten Weg auf sich genommen haben und alle Fragen gut beantwortet haben. Ich wünsche Ihnen einen guten Nachhauseweg. Danke schön.

(Beifall)

Die öffentliche Sachverständigenanhörung ist damit geschlossen.

(Schluss: 11.15 Uhr)

Übersetzung