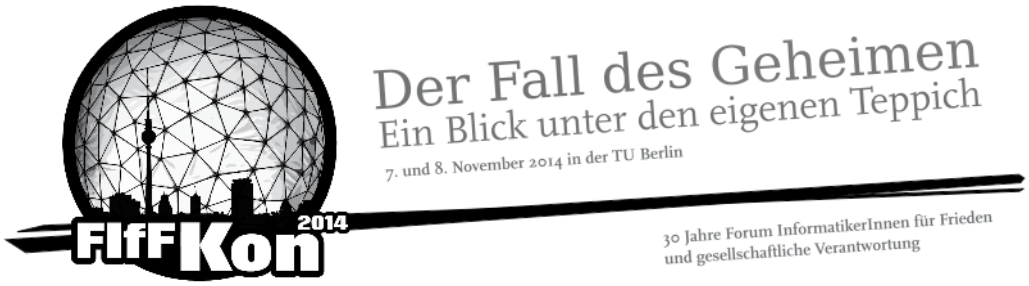

FIfF-Konferenz 2014

Der Fall des Geheimen – Ein Blick unter den eigenen Teppich

Wir haben die Rolle Deutschlands und der deutschen Geheimdienste im Kontext der älteren und jüngeren Erkenntnisse – von Echelon über Prism bis Eikonal – zusammen mit rund 400 Besucherinnen und Besuchern beleuchtet und Handlungsoptionen erarbeitet. Natürlich muss die Bearbeitung nun weitergehen.

Am 7. und 8. November 2014 lud das FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung – zur FIfF-Konferenz 2014 ein. Dabei warfen wir den längst überfälligen Blick unter Deutschlands eigenen Geheimdienst-Teppich, denn spätestens nach den jüngsten Enthüllungen zur Rolle Deutschlands im globalen Geheimdienstroulette ist es absurd, nur mit dem Finger über den Atlantik oder auf die Britischen Inseln zu zeigen. Insbesondere Deutschland agiert willentlich als Dreh- und Angelpunkt globaler geheimdienstlicher Aktivitäten und treibt die flächendeckende Überwachung voran.

Wir wollten die Rolle der deutschen Geheimdienste beschreiben und verstehen, wie die Überwachungssysteme gebaut sind, nach welchen Menschen- und Weltbildern sie konzipiert und in welchen Kontexten sie verwendet werden. Mit Experten, Betroffenen, Politikern und der Öffentlichkeit wurden technische, politische, rechtliche, wirtschaftliche und historische Aspekte betrachtet – von Echelon über Prism bis Eikonal. Die Zusammenarbeit von Geheimdiensten, deutschen Telekommunikationsanbietern und Technikern bedarf der besonderen Aufmerksamkeit.

Nötig ist der Blick unter den eigenen Teppich auch, weil die deutsche parlamentarische Aufklärungsarbeit zu den Machenschaften von NSA, GCHQ, BND und Co. nur schleppend vorankommt und angesichts der systematischen Missachtung von Menschenrechten und Grundrechten durch die deutschen Geheimdienste halbherzig wirkt. Zudem sabotiert die Bundesregierung das parlamentarische Unterfangen absichtsvoll und maßgeblich: Sei es durch fast durchgehend geschwärzte oder gänzlich zurückgehaltene Dokumente, durch die Verhinderung von Zeugenvernehmungen oder durch monatelange Verzögerungen. Die Regierung und ihre Geheimdienste haben offenbar aktiv vergessen, dass sie eigentlich vom Parlament kontrolliert werden sollten und nicht andersherum.

Ute Bernhardt, Matthias Bäcker, Wolfgang Coy, Hans-Jörg Kreowski, Constanze Kurz, Wolfgang Nešković, Frank Rieger, Anne Roth, Ingo Ruhmann, Peter Schaar, Erich Schmidt-Eenboom, Patrick Sensburg, Hans-Christian Ströbele, Gregor Wiedemann und Andy Müller-Maguhn trugen mit ihren Vorträgen zum Gelingen der Konferenz bei. Das *Nö-Theater* führte am Samstagabend das Stück *V wie Verfassungsschutz* auf.

Auf den folgenden Seiten dokumentieren wir die Beiträge unserer Referentinnen und Referenten zur Konferenz. Dazu haben wir ihre Vorträge zusammengefasst. Natürlich gilt wie immer das gesprochene Wort: Alle Vorträge wurden aufgezeichnet und sind über die Konferenz-Web-Seite *https://fiffkon.de* unter *https://fiffkon.de/medien.html* zugänglich.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

FIfF-Konferenz 2014

Strategische Telekommunikationsüberwachung auf dem Prüfstand

Zusammenfassung des Vortrags von Matthias Bäcker

Nach wie vor hält sich in Deutschland die Forderung, fremde Geheimdienste mögen doch deutsche Bürgerinnen und Bürger nicht mehr abhören. Dies zielt natürlich direkt in Richtung USA und Großbritannien, weil deren Geheimdienste NSA und GCHQ spätestens seit den Snowden-Veröffentlichungen für ihre globalen Überwachungsaktivitäten in heftiger Kritik stehen. Allerdings hängt die Glaubwürdigkeit solcher Forderungen wesentlich davon ab, wie die eigenen deutschen Dienste das Ausland überwachen, also wie Deutschland selbst mit den Rechten von Nichtdeutschen verfährt.

Was also tun die deutschen Nachrichtendienste diesbezüglich? Um eine sinnvolle Antwort zu bekommen, wird hier nur der Ausschnitt betrachtet, der den „skandalösen" Aktivitäten von NSA und GCHQ am stärksten ähnelt. Darüber hinaus wird es eine rein rechtliche Analyse.

Strategische Fernmeldeüberwachung

Die *strategische Fernmeldeüberwachung* entspricht den kritisierten Überwachungsprogrammen der NSA am ehesten, da es dort ebenfalls um nicht-individuelle Massenerfassung geht.

In Deutschland darf nur der BND strategische Fernmeldeüberwachung durchführen. Dies ist ein Mittel zur Verdachts- und Verdächtigengewinnung, wobei keine Einzelfallbetrachtung stattfindet. Die Maßname ist folglich anlasslos. Dabei gibt es drei strategische Beschränkungen: bezüglich des Gefahrenbereichs, der geographischen Region und der Übertragungswege. Diese Wege müssen jeweils vorab benannt werden, um sie zu überwachen.

1. Erlaubte Gefahrenbereiche sind z. B. internationaler Terrorismus oder organisierte Kriminalität.

2. Die möglichen geographischen Regionen oder Staaten umfassen einen Großteil der Erde, ca. 150 von 200 Staaten können benannt werden.

3. Zuletzt müssen die zu überwachenden Übertragungswege spezifiziert werden. Das können bestimmte Kabel sein oder auch Satelliten.

Um an den Rohdatenstrom zu kommen, kann der BND entweder die Übertragungswege selbst anzapfen oder aber die Provider dazu bringen, dem BND die Daten zuzuleiten. Dieser Rohdatenstrom wird dann gefiltert bzw. durchsucht. Die dabei nutzbaren Suchbegriffe werden in zwei Kategorien unterteilt: einerseits inhaltliche Begriffe wie Bombe oder Anschlag und andererseits formale Begriffe, die vorgangsbezogen funktionieren, also Web-Adressen, E-Mail-Adressen oder Telefonnummern. Sind die Treffer nachrichtendienstlich relevant, werden sie gespeichert, ansonsten werden sie gelöscht.

Im Jahre 1999 hat das Bundesverfassungsgericht das G10-Gesetz evaluiert. Die Begrenzungen waren demnach grundsätzlich angemessen. Doch seitdem gibt es technische und sonstige Neuerungen, die die Beschränkungen ganz offensichtlich sinnlos machen. Bei der folgenden Betrachtung wird nur zwischen internationaler und ausländischer Kommunikation unterschieden, denn im Inland darf der BND nicht aktiv werden. Internationale Kommunikation ist so definiert, dass mindestens ein Endpunkt im In- und einer im Ausland sein muss, ausländische Kommunikation geht folglich von Ausland zu Ausland.

Internationale Kommunikation

Die oben beschriebenen Beschränkungen gelten nur für die internationale Kommunikation, aber selbst diese Beschränkungen sind in den aktuellen technischen Gegebenheiten sehr schwierig zu operationalisieren. In der Praxis gelten daher wohl nur Faustregeln. Technisch denkbar sind Filter, die auf Top-Level-Domains (TLD) von Emailadressen basieren (.de) oder Telefonnummernpräfixe, doch die Effektivität dieser Filter muss aus offensichtlichen Gründen stark bezweifelt werden.

Ursprünglich erlaubte die strategische Fernmeldeüberwachung nur, nicht-leitungsgebundene Kommunikation zu betrachten – also Satellitenverbindungen – doch diese Beschränkung wurde bald aufgehoben. Dadurch entfiel faktisch die so umgesetzte nötige Volumenreduktion, also war eine neue gesetzliche Beschränkung nötig: Es sollten nun höchstens 20 % der Kapazität der überwachten Wege pro Überwachungsaufgabe abgefangen werden. Allerdings können sehr viele Übertragungswege angegeben werden, wodurch 20 % trotzdem sehr großen Datenmengen entsprechen. Zusätzlich kann ein Übertragungsweg auch aufgrund mehrerer Gefahrenbereiche überwacht werden, wodurch sich die erlaubten Prozente summieren.

Andererseits ist die Beschränkung auf Übertragungswege auch aufklärungstechnisch fragwürdig, denn eine digitale IP-basierte Datenübertragung kann ja auf unterschiedlichen Wegen stattfinden. Also ist es auch „ein bisschen Zufall, ob [der Dienst] seine Aufgabe erreicht", denn die Beschränkung „begrenzt die Überwachung, aber möglicherweise nicht in besonders sinnvoller Weise." Zusammengefasst: „Die Begrenzungswirkung steht in Frage – die Sinnhaftigkeit steht stark in Frage."

Nun zu den Modalitäten der Überwachung. Es existiert ein Verbot bestimmter formaler Suchbegriffe, die gezielt Telekommunikationsanschlüsse erfassen, damit gerade keine Einzelfallbetrachtung stattfinden kann. Telekommunikationsanschlüsse im Inland oder von Deutschen anzuzapfen ist „unstreitig verfassungswidrig", aber der Fokus auf Anschlüsse ist generell hochgradig fragwürdig, denn Teilnehmer könnte man demnach gezielt überwachen.

Bei „sportlichem Zugriff der Auslegung" wäre also eine Suche nach individuellen Telefonnummern verboten (Anschluss), aber die Suche nach E-Mailadressen (Teilnehmern) erlaubt.

Das Zwischenfazit lautet also: „Die Begrenzungen, die das Gesetz enthält, sind heute zum Teil kaum noch operationalisierbar, teilweise laufen sie unter heutigen technischen Bedingungen leer. Insgesamt ist ihre Begrenzungswirkung gering zu veranschlagen. [Es ist zu beweifeln], ob das G10-Gesetz heutzutage unter den rechtlichen und technischen Bedingungen noch den verfassungsrechtlichen Anforderungen genügt oder ob nicht inzwischen dieses Gesetz auch durch seine Veränderungen und durch Änderungen des tatsächlichen Umfeldes verfassungswidrig geworden ist."

Ausländische Kommunikation

Die allgemein von deutschen Geheimdiensten vertretene These lautet, dass die Zielbestimmung *Auslandsaufklärung* des BND ihm nach Belieben das Recht [gibt], Kommunikation zu überwachen. Diese Auffassung hat allerdings die verfassungsrechtliche Prämisse, dass das GG Art. 10 (Post- und Fernmeldegeheimnis/Telekommunikationsgeheimnis) nicht für alle Menschen gleichermaßen gilt. Diese Rechtsauffassung wird übrigens auch von den Amerikanern vertreten, wofür wir Deutsche sie immer scharf kritisieren.

Auch die Bundesregierung ist der Ansicht, dass das Grundgesetz nur im Inland gilt, wodurch Auslandsüberwachung unbeschränkt möglich wäre. Bezüglich genau dieser Frage ließ das Bundesverfassungsgericht zwar offen, ob ein territorialer Bezug grundsätzlich nötig ist. Aber es sagte ganz klar, dass sich Auslandsaufklärung zumindest immer dann nach GG Art. 10 richten muss, wenn die Überwachungsanlagen territorial in Deutschland stehen.

Umfassende Grundgesetzbindung

Diese Ansicht ist allerdings hinfällig, denn es ist verfassungsrechtlich allgemein anerkannt, dass alle Staatsgewalt eine umfassende Bindung an das Grundgesetz hat. Für den BND gilt das folglich ebenso zwingend, daher ist ein eventueller territorialer Bezug für die Beachtung von GG Art. 10 überhaupt nicht erforderlich.

Die Aussage des BND-Präsidenten Gerhard Schindler, Satellitenüberwachungsdaten würden ja im Weltraum abgefangen, ist demnach seit 15 Jahren doppelt falsch und grob fahrlässig, denn die Anlagen stehen in Deutschland und werden einzig von deutschen Stellen durchgeführt. Auch die Funktionsträgertheorie entbehrt jeglicher verfassungsrechtlicher Grundlage. Die „aktuelle Praxis ist demnach rechts- und verfassungswidrig und muss gestoppt werden."

Datenübermittlung an andere Dienste

Es gibt zwei mögliche rechtliche Grundlagen für eine Datenübermittlung an andere Dienste:

Matthias Bäcker

Matthias Bäcker ist Professor für Staats- und Verwaltungsrecht an der LMU München und war vorher Professor für Öffentliches Recht an der Universität Mannheim. Er war zudem Wissenschaftlicher Mitarbeiter am Bundesverfassungsgericht. Er schreibt u. a. für die *Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht* (HRRS) und stellte dem NSA-Untersuchungsausschuss kürzlich seinen rechtswissenschaftlichen Sachverstand zur Verfügung.

Einerseits ermöglicht das G10-Gesetz eine Übermittlung, aber nur unter sehr strengen Bedingungen der strategischen Beschränkung. Diese Möglichkeit wird allerdings kaum genutzt; es waren weniger als zehn Fälle seit der Einführung.

Andererseits legitimiert die Aufgabenzuweisung *Auslandsaufklärung* scheinbar eine Datenübermittlung an das Ausland nach Belieben, wenn es den sicherheitspolitischen und außenpolitischen Interessen der Bundesrepublik dienlich ist, so das Verständnis der Dienste. Auch diese Sicht „beruht auf irrigen Annahmen über das grundrechtliche Schutzniveau und führt deswegen zu rechts- und verfassungswidriger behördlicher Praxis."

Fazit und Ausblick

Ganz offensichtlich herrscht eine unzureichende Regulierung der strategischen Überwachungen. Dies erzeugt erhebliche verfassungsrechtliche Bedenken, zumal die oben angeführten Punkte Pars-proToto-Argumentationen sind. Die Geheimdienstgesetze enthalten überall Regelungen, die „mindestens genauso schrecklich" sind wie die präsentierten Sachverhalte. „Dieser ganze Regelungskorpus bedarf grundlegend der Überarbeitung. Man kann das auch nicht mehr punktuell retten. Das einzige, was man mit den Nachrichtendienstgesetzen machen kann, ist wegwerfen und neuschreiben."

„Dies bedarf einer Interdisziplinären Zusammenarbeit von Wissenschaftlern und Praktikern sowohl aus der Ministerialverwaltung als auch aus den Nachrichtendiensten, sowie einer Beteiligung der Zivilgesellschaft, insbesondere von Bürgerrechtsorganisationen und auch Juristen und Technikern; sonst wird das nicht gelingen können."

Letztendlich ist eine solche Reform auch unabdingbare Bedingung, um im Ausland gegen die Praxis von NSA und GCHQ zu argumentieren.

FIfF-Konferenz 2014

Snooping and Bugging

Zusammenfassung des Vortrags von Constanze Kurz

Die Veröffentlichungen zu Snowden in einem Vortrag auch nur zu nennen, würde vier Stunden dauern. Mit Sicherheit könnte man eine ganze Vorlesungsreihe zu diesem Thema aufbauen. An dieser Stelle soll es darum gehen, was grundsätzlich ans Licht gekommen ist, welche Reaktionen es darauf gab, und welche juristischen Schritte diese nach sich zogen.

Der Anfang

Der *Verizonfall*, der den Beginn der Skandalserie darstellte, schaffte es kaum in die europäische Presse und wurde auch in Deutschland kaum wahrgenommen. Verizon wurde verpflichtet, Meta-, Inhalts- und Positionsdaten der Kommunikation amerikanischer Kunden herauszugeben. Die Veröffentlichungen zu PRISM fanden dann jedoch weltweit Beachtung. Der Skandal um PRISM wurde so groß, weil alle großen amerikanischen Internetdienstleister, die weltweit benutzt werden, betroffen waren und dadurch auch die Betroffenheit der Menschen so vollständig und individuell war. Erst durch PRISM rückte überhaupt auch die FISA-Erlaubnis in die öffentliche Diskussion. Erst danach wurden die Urteile des Geheimgerichts, welches nach geheimen Verhandlungen geheime Urteile in Bezug auf Überwachungserlaubnisse der Dienste erlässt, überhaupt einer juristischen Debatte öffentlich zugänglich.

Ein weiterer Strang, der sich in der Debatte immer wiederholt, ist die Unterscheidung zwischen Rechten der Inländer und denen der Ausländer. Im Senat und Kongress der USA wurden im Wesentlichen nur Vorschläge debattiert, die Rechte von Amerikanern betreffen und nicht die von Ausländern. Nach nur zwei Wochen *NSA-Skandal* gerieten dann auch GCHQ und andere 5-Eyes-Dienste in den Fokus – insbesondere durch das Abhören des G20-Treffens 2009 in London. Hiernach wurden zum ersten Mal Sabotage- und Spionagetechniken sowie Hacking-Angriffe thematisiert. Für die Teilnehmer des Treffens wurden eigens präparierte Internetcafés geschaffen, in denen Tastatureingaben mitgeschnitten und Mobiltelefone gehackt wurden, um an Passwörter zu gelangen. Daran wurde sehr deutlich, dass Terrorabwehr nicht das Ziel der Überwachungsmaßnahmen sein kann.

An den *Tempora*-Veröffentlichungen wurde klar, dass die Briten mit der NSA kooperieren und ihre geografische Position ausnutzen, indem Internetkabel, die zum größten Teil über die Britischen Inseln verlegt wurden, abgeschnorchelt werden und der gesamte Traffic für mehrere Tage zwischengespeichert wird. Daraufhin kamen auch die kooperierenden Telekommunikationsunternehmen und Backbone-Provider in die Debatte (z. B. British Telecom, Global Crossing, Interroute, Level 3, Viatel, Verizon Business und Vodafone), die das Abschnorcheln überhaupt erst ermöglichen. In der Folgezeit gaben diese eine Vielzahl überspezifischer Dementi ab, die Weiteres erahnen lassen.