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

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
über das grundrechtliche Schutz
rechts- und verfassungswidriger

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

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 Wis-
sowohl aus der Ministerialver-
achrichtendiensten, sowie einer
, insbesondere von Bürgerrechts-
n 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

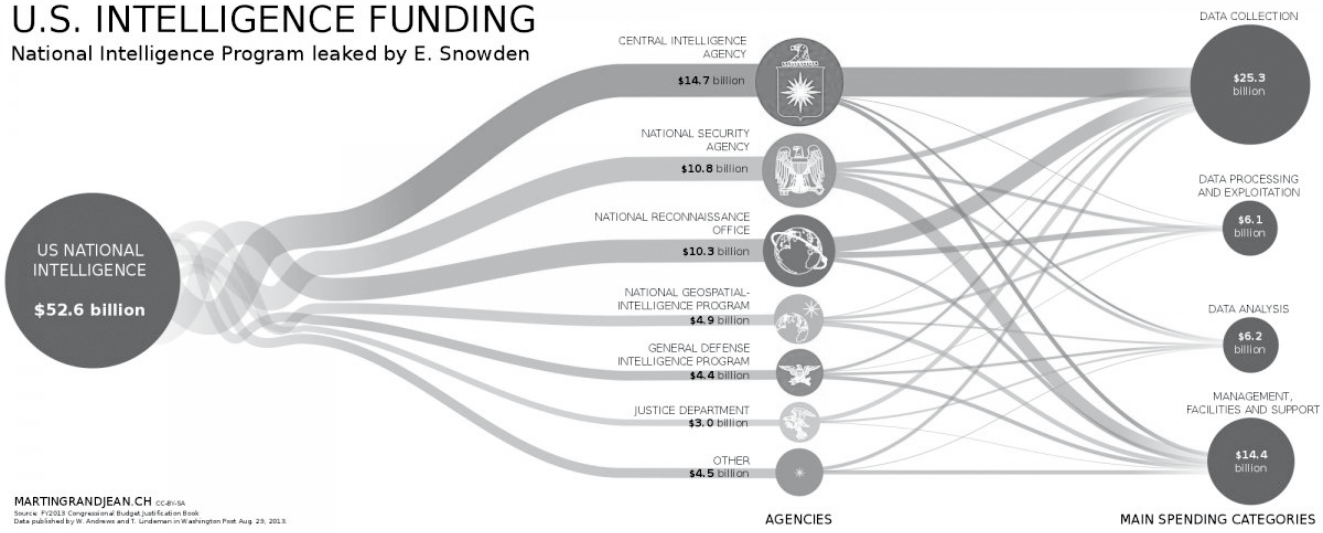
Die Veröffentlichungen zu Snowden in einem Vortrag auch nur zu nennen, würde vier Stunden dauern. Mit Sicherheit könnte man eine ganze Vorlesungsreihe zu diesem Thema aufbauen. An dieser Stelle soll es darum gehen, was grundsätzlich ans Licht gekommen ist, welche Reaktionen es darauf gab, und welche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



http://static4.businessinsider.com/image/5225baf069bedd3d09eca9f9-1200-522/usintelligencefunding.png

Reaktionen

Die *Intelligence Community* reagierte relativ offensiv und versuchte, die nicht mehr zu leugnende massenhafte Überwachung mit der Heuhaufenmetapher zu begründen: „If you're looking for the needle in the haystack, you have to get the haystack first." Immer wieder ganz zentrales Element der Begründungen für die Überwachungsprogramme und Eingriffsbefugnisse ist die Terrorismusbekämpfung. Eine andere Strategie des Rückzugs aus der Debatte ist die Behauptung, dass zwar große Datenmengen erhoben werden, jedoch der größte Teil der gesammelten Daten nie von einem Menschen betrachtet wird.

Missbrauchsfälle

Noch im Herbst 2013 kamen Missbrauchsfälle durch einzelne Mitarbeiter sowie Mitarbeiter von Vertragspartnern der Dienste ans Tageslicht. In vielen einzelnen Berichten wurde deutlich, dass auch die *Achselzucker*, die dachten, mit ihnen hätte die Überwachung nichts zu tun, ganz konkret von der Überwachung betroffen waren. Allein die bekanntgewordenen Berichte über Missbrauchsfälle in der deutschen, englischen und spanischen Presse summieren sich auf mindestens 84 Fälle.

Black Budget

In Deutschland sind die Budgets der Geheimdienste bekannt – in den USA waren sie es bis zu den Veröffentlichungen des sogenannten *Black Budget* nicht. In geheimen Dokumenten wird die Höhe des Budgets für das *National Intelligence Program* im Steuerjahr 2013 mit rund 53 Milliarden Dollar angegeben. Tatsächlich, so NSA-Whistleblower William Binney bei einem Besuch in Berlin, seien 80 Milliarden Dollar realistischer zu veranschlagen, da Teile davon im Militärbudget versteckt liegen.

Es war zu beobachten, dass sich Communities von Aktivisten und Datenjournalisten mit der Thematik beschäftigten. Inzwischen wurde damit gerechnet, dass es weitere Veröffentlichungen geben würde, und so wurden diese der Übersichtlichkeit wegen z. B. in visueller Form aufbereitet. Außerdem begannen politische Organisationen und Gruppen wie z. B. *Big Brother Watch*, die *Open Rights Group* und PEN, juristische Verfahren vorzubereiten und Beschwerden beim Europäischen Gerichtshof für Menschenrechte einzureichen.

Die abgehörte Kanzlerin

Das Interessanteste am Fall der Überwachung des Mobiltelefons von Angela Merkel war, dass danach ganz neu über die Aufbauten auf den Dächern der Botschaften und über die deutschen Liegenschaften debattiert wurde. Nach diesem medial sehr präsenten Vorfall wurden die folgenden Veröffentlichungen nicht mehr so stark skandalisiert. Zu beobachten war eher eine Auffächerung der Debatte in sehr unterschiedliche Diskussionsbereiche – später noch einmal verstärkt durch den NSA-Untersuchungsausschuss.

Priority Framework

Kronjuwel der Veröffentlichungen wurde neben dem *Black Budget* das *Priority Framework*, welches beschreibt, welche Ziele aus welchen Gründen in welchen Ländern überwacht

Constanze Kurz

Constanze Kurz ist Informatikerin, Sachbuchautorin und Aktivistin. Sie forscht aktuell zu den Themen Datenschutz und gesellschaftliche Auswirkungen von Automatisierung. Sie ist im Beirat des FIfF.

wurden und werden. Ziele, die die USA in Deutschland inhaltlich verfolgen, sind *Cyber Attack, Counterespionage, emerging strategic technologies, international trade policy, arms export, arms control and treaty monitoring, foreign policy objectives, economic and financial stability* (Cyber-Angriffe, Auslandsspionage, neue strategische Technik, Außenhandelspolitik, Rüstungsexport, Rüstungskontrolle und Vertragskontrolle, Außenpolitik, Wirtschafts- und Finanzstabilität). Wie auch für andere mitteleuropäische Länder geht aus dieser Aufzählung hervor, dass es überhaupt nicht, wie immer wieder behauptet, um Terrorismus geht!

Hackende Geheimdienste

Die Veröffentlichungen zu *Taylored-Access*-Operationen, die automatisierte Infiltration und Schwächung von kryptographischen Methoden, machen deutlich, dass es nicht nur um Überwachung geht, sondern um offensive Hackingmethoden. Informationen darüber sind in der Presse eher unterrepräsentiert. Deutlich wird, dass Firmen wie Google über das gesetzlich gezwungene Maß hinaus mit den Geheimdiensten zusammenarbeiten.

RSA und Cisco, die ebenfalls eng mit den Diensten zusammenarbeiteten, erlitten nach den Veröffentlichungen einen entscheidenden Imageverlust und Gewinneinbrüche – vor allem im Ausland. US-Firmen merken nun immer mehr, wie wichtig Sicherheitsaspekte wie z. B. Verschlüsselung sind.

Erfolge der NSA-Überwachung

Präsident Obama setzte im letzten Jahr eine Expertenkommission ein, die prüfen sollte, wie die Erfolge der massenhaften Überwachung einzuschätzen sind. Obwohl die Kommission fast nur aus Geheimdienstlern besteht, wofür sie stark kritisiert wurde, ist der veröffentlichte Bericht sehr bemerkenswert. Nicht nur, weil empfohlen wurde, die Manipulation der Finanzmärkte durch Geheimdienste rechtlich zu regulieren (worüber noch gar nichts veröffentlicht worden war), sondern vor allem, weil die Experten sich mit dem Terrorargument beschäftigten. Es wurde zu Protokoll gegeben, dass die massenhafte Metadatenanalyse nur einen bescheidenen Beitrag für die nationale Sicherheit leistet. Es hätte keinen einzigen Fall gegeben, bei dem die NSA mit Sicherheit sagen könnte, dass das Ergebnis einer Untersuchung zu Terror auf irgendeine Art anders gewesen wäre, wenn keine Metadaten zur Verfügung gestanden hätten. Sie konnten also keinen einzigen Fall anführen, um die zentrale Argumentation für diesen riesenhaften Geheimdienstkomplex zu begründen. In Anbetracht der Gelder, die den Diensten zur Verfügung stehen, haben diese stark an Legitimation verloren.

Resümee

Es gibt dadurch im Moment eine gute Chance, die Geheimdienste nicht nur durch eine öffentlich geäußerte Kritik, sondern auch juristisch anzugreifen. Viele juristische Prozesse laufen bereits. Constanze Kurz selbst ist Beschwerdeführerin vor dem Europäischen Gerichtshof für Menschenrechte, der die Wichtigkeit erkannt hat und sogar ein Schnellverfahren einleitete. Der *Chaos Computer Club* begab sich außerdem in Großbritannien vor das IPT *(Investigatory Powers Tribunal)* – die innerbritische Geheimdienstkontrolle. Auch in Frankreich und Ungarn laufen Verfahren.

Constanze Kurz zieht ein sehr positives Resümee aus den vergangenen zwei Jahren: „Die Chance, durch Snowden über die Geheimdienstaktivitäten Bescheid zu wissen, ermöglicht es uns, ein informiertes Urteil zu treffen und uns gegen diesen Komplex zu wehren – was wir auch tun sollten. Die Dienste sind nicht sankrosankt. Wir bezahlen sie, also können wir das auch beenden – wir müssen nur einen langen Atem haben."

FIfF-Konferenz 2014

Nachrichtendienstliche Zugriffe und ihre Auswirkungen auf digitale Souveränität

Zusammenfassung des Vortrags von Andy Müller-Maguhn

Zu Beginn erfolgte eine kurze Bestandsaufnahme mit der Entwicklung, dass Paranoia nun durch Gewissheit abgelöst wurde und weitgehende Telekommunikationsüberwachung existiert. Ebenso aber auch freier Informationsfluss, Anonymisierungs- und Verschlüsselungswerkzeuge, welche im Falle der Snowden-Evakuierung ihre Wirkkraft gezeigt haben. Die Politik war darüber freilich nicht erfreut, und gerade die erzwungene Landung der Morales-Maschine unter dem Verdacht, Snowden zu transportieren, war ein Vorfall, dessen Gewicht besonders betont wurde.

Nachrichtendienstliche Arbeit ist unterteilbar nach Überwachungsart. Das Anzapfen von Glasfaserkabeln fällt unter *Global Access Operations*; *Special Collection Service* und HUMINT (*human intelligence*) finden auch mit der CIA statt und enthalten Angriffe wie Verwanzungen; unter *Cryptoanalysis and Exploitation Services* können die Programme gefasst werden, welche darauf abzielen, Verschlüsselung zu brechen (BULLRUN, GENIE, TURBINE, TURMOIL, QUANTUM) oder Datenzugriff zu ermöglichen (PRISM, MARINA, MAINWAY, PINWALE, NUCLEON). Die Betrachtung der *Tailored Access Operations* in dieser unvollständigen Liste macht deutlich, dass auch sie nicht nur Auswirkung auf handverlesene Personenziele haben. Denn durch den Fingerabdruck, den unsere Systeme unaufgefordert anderen mitteilen, sind einerseits automatische Angriffe praktikabel, andererseits bedeutet die Kompromittierung des TK-Anbieters Belgacom neben Zugriff auf Finanztransaktionsdaten per SWIFT und Infrastruktur des Europäischen Parlaments auch Ein-