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

Was tun?

Zusammenfassung des Vortrags von Frank Rieger

Der globale jährliche Überwachungsetat kann ungefähr mit 50 Mrd. US-Dollar beziffert werden. Diese Zahl beinhaltet den Aufwand sämtlicher Geheimdienste, also nicht nur den der *Five-Eyes*-Staaten, sondern auch den Russlands, Chinas, Israels, Deutschlands etc. Aber selbst wenn man von den staatlichen Schritten, die IT-Sicherheit zu untergraben, absieht, muss festgestellt werden, dass wir schon gegen normale Kriminalität machtlos sind. Gerade einmal die Hälfte der aktuellen Trojaner lassen sich mit der neuesten Anti-Viren-Software erkennen. Das stellt ein fundamentales Versagen der IT-Security dar. Zu lange wurde davon ausgegangen, dass wir im Internet alle Freunde sind.

Was also ist zu tun?

Eines der Probleme ist die Herausbildung von Datenkonzentration bei wenigen Unternehmen. Dabei geht der Trend hin zu Lebensassistenten, die uns den Alltag erleichtern sollen, während sie Werbung platzieren und uns zum Kaufen animieren. Dabei werden immer mehr Daten angehäuft, die wiederum die Grundlage dafür sind, wie wir überwacht werden. Deshalb müssen wir erkennen, dass unser Verhalten in der digitalen Welt selbst ein Aspekt des Problems ist.

Es stellt sich also die Frage: Wie kann es gelingen, den Oligopolen Anreize zu geben, nicht mit den Geheimdiensten zu kooperieren? Zum einen ist das gelungen durch die mediale Aufmerksamkeit, da der natürliche Instinkt der Unternehmen es ihnen verbietet, ihre Nutzerdaten zu teilen. Die sind ja wertvoll. Wenn die Nutzer aber ihr Vertrauen in die Datensicherheit dieser Firmen verlieren, wandern sie womöglich ab, wodurch weniger Daten gesammelt werden würden und folglich weniger Werbung verkauft werden könnte. Wenn wir aber wollen, dass die Oligopole weniger Daten besitzen, dann wäre also ein Ansatz dazu, die Werbeökonomie zu brechen. Das werbefinanzierte Internet entstand ja erst deshalb, weil niemand bereit war, für Internetdienste Geld zu bezahlen. Stattdessen zahlt man jetzt mit seinen Daten. Man könnte sich aber auch vorstellen, dass alle Dienste auch ohne Tracking, aber für Geld zu erhalten wären. Bei den geringen Beträgen, die eine Firma pro Nutzer an Werbeeinnahmen generiert, wäre eine entsprechende geringe Nutzungsgebühr für jeden erschwinglich und den Geheimdiensten wäre die Überwachung bedeutend erschwert.

Privatsphäre ist nämlich ein Mittel, um Machtkonzentrationen entgegenzuwirken, genauso wie Transparenz ein Mittel ist, um zu verhindern, dass Machtkonzentrationen missbraucht werden. Derzeit wird das Prinzip umgekehrt, so dass Privatpersonen immer transparenter und große Entitäten immer intransparenter werden. Man könnte also auch die Internetindustrie wie andere große Industrien dahingehend regulieren. Wie das Beispiel des Rechts auf Vergessen gezeigt hat, funktioniert diese Regulation von Internetunternehmen. Sie wollen Aufwand und Kosten minimieren und halten sich daher an die Regeln.

Anders sieht das jedoch mit Geheimdiensten aus. Sie funktionieren auf der Grundlage von Intransparenz, weshalb die einzige sinnvolle Forderung ist, sie abzuschaffen. Regelmäßig werden Skandale bekannt, die zeigen, dass die Geheimdienste jenseits der Rechtsstaatlichkeit agieren. Sie zeigen die strukturelle Eigenschaft, sich von der Öffentlichkeit nicht in die Karten schauen zu lassen, so dass man sagen muss, dass sie unsere demokratischen Prozesse vorsätzlich unterwandern.

Da die Abschaffung der Geheimdienste relativ unwahrscheinlich ist, müssen politische Forderungen ausgearbeitet werden.

Die Geheimdienstkontrolle muss derzeit als nicht existent angesehen werden. Die Parlamentarische Kontrollkommission ist nicht einmal technisch in der Lage, ihre Arbeit zu machen, denn sie besteht aus einer kleinen Gruppe von Leuten, meist Juristen, die von der Technik keine Ahnung haben. Wir brauchen also eine Organisation/Behörde, in der Experten in hinreichender (also dreistelliger) Anzahl vertreten sind, die die Technik verstehen und die die entsprechenden Zugriffsrechte auf Geheimdienstgeheimnisse erhalten, um deren Bedeutung unabhängig zu beurteilen.

Datenschutzbeauftragte, die dem Innenministerium unterstehen, nützen hier nichts.

Frank Rieger

Frank Rieger ist Technikpublizist, Aktivist und Sachbuchautor in den Bereichen *Datenschutz* und *Grundrechte im digitalen Zeitalter*. Darüber hinaus beschäftigt er sich mit den globalen Verflechtungen und historischen Grundlagen von Geheimdiensten und verdeckten Operationen. Er gründete verschiedene Startup-Unternehmen.

Ein weiterer Punkt wäre es, eine Evidenzpflicht für Geheimdienste einzuführen. Die Dienste müssten also wissenschaftlich belegen, dass die Befugnisse und technischen Mittel, die man ihnen gibt, wirksam sind. Daten zu sammeln zum Selbstzweck des Ringtauschs mit anderen Geheimdiensten ist keine Begründung. Die Befugnisse sollten mit einer zeitlichen Begrenzung auch verfallen können, wenn sich zeigt, dass sie unwirksam waren.

Ein nächster Schritt wäre es, eine Haftung für kommerzielle Software einzuführen, wenn diese Sicherheitslücken aufweist oder wenn Daten aus der Software abfließen. Einerseits würde die Qualität der Programmierung steigen, andererseits würden weniger Daten gesammelt werden, da diese einen potenziellen Haftungsfall auslösen könnten.

Technisch lässt sich vorstellen, dass die Massenüberwachung mittelfristig, z. B. innerhalb der nächsten 5 Jahre, unterbunden wird. Dabei gibt es drei Komponenten: die Metadaten, die Daten, die irgendwo gespeichert werden, und die Inhaltsdaten der Kommunikation. Für alle drei gibt es technische Sicherungsmethoden. Der erste und einfachste Schritt wäre die Transportwegverschlüsselung. Außerdem sollten neue Cryptostandards entwickelt werden, die gut verständlich und für jedermann anwendbar sind. Wenn es also politisch gelingt, dass durch eine Wirksamkeitsbeweispflicht der Geheimdienste einerseits und durch die standardmäßige Verschlüsselung andererseits die Kosten für die Datenauswertung stark steigen, dann kann man die Massenüberwachung politisch beenden.

Der Ansatz, auf geschlossene Systeme wie Apple oder Google etc. zu setzen, ist dabei keine Lösung, auch wenn die Datensicherheit innerhalb dieser Systeme besser funktioniert. Die Datenkonzentration bleibt nämlich auch hier erhalten, und es stellt ein Problem dar, das Vertrauen zu zentralisieren. Eine andere Strategie wäre die Schaffung von sicheren, offenen Systemen und neuen, simplen Cryptostandards, so dass alte, überkomplizierte Standards ausgesondert werden können. Der Staat ist dafür jedoch der falsche Ansprechpartner, da er den Interessen der Sicherheitsbehörden folgt und sich deshalb immer Hintertürchen offen hält. Ein guter Ansatz wäre es, wenn diese Aufgabe von einer Art öffentlich-rechtlicher Einrichtung übernommen werden würde. Wenn man das als langfristiges Projekt von ca. 10-15 Jahren konzipiert, kann man damit auch in der Politik Gehör finden. US-Standards sollten nach heutigem Wissen dabei nicht verwendet werden. Es braucht alternative Projekte auf EU-Ebene oder einen offenen Wettbewerb. Die Informatiker und Informatikerinnen, die man für die Umsetzung braucht, müssen das sichere Programmieren aber erst einmal lernen. Dazu sollte in der Ausbildung einiges verändert werden.

Darüber hinaus müssen wir auf weitere Whistleblower hoffen, sonst wird es schwer, politisch genügend Druck aufzubauen. Dass die Politiker die Probleme nicht verstehen würden, stimmt im Übrigen nicht. Sie verstehen vielleicht die technischen Details nicht, z. B. von Kryptographie, aber über Netzpolitik wie Urheberrecht oder Netzneutralität wissen sie Bescheid. Sie haben schlichtweg eine andere Meinung und andere Ansichten über die Interessen, die sie vertreten sollen. Es fehlt also nicht an Wissen, sondern an der richtigen Ideologie.

FIfF-Konferenz 2014

Gleiche Brüder, gleiche Kappen?

Zusammenfassung des Vortrags von Erich Schmidt-Eenboom

Es scheint fast so, als gäbe es einen neuen Auftrag der US-amerikanischen Geheimdienste, und zwar jeden Staat der Welt, alle wichtigen Akteure aus Militär, Politik, Gesellschaft, Wirtschaft und Wissenschaft zu überwachen. Doch dieser Auftrag besteht nicht erst seit Kurzem und auch nicht seit 9/11, sondern schon seit Juni 1946. Dies war die *Basic*
Nachrichtendienste haben länger

Seit ca. 2009 kann die *National*
fast alles abgreifen, sodass die Liste dessen kürzer wäre, was sie nicht abgreifen kann. Angriffe auf täglich eine Million Ziele und terabyteweise Daten sind das Resultat von 10 Milliarden USD pro Jahr und ca. 100.000 Mitarbeitern. Ergebnisse sind z. B. 122 abgehörte Staatschefs und die *Special Collection Services*, also Abhörstationen von CIA und NSA in ca. 80 US-Botschaften weltweit.

In diesem Vortrag werden grundsätzlich zwei Fragen behandelt: Welche Informationen aus Snowdens Enthüllungen sind tatsächlich neu? Und zweitens: Gibt es Wirtschaftsspionage gegen die Bundesrepublik Deutschland?

Die Frage, was an den Enthüllungen neu ist, kann natürlich nur mit einem Blick in die Geschichte beantwortet werden. Obwohl die Politik aktuell überrascht tut und von nichts gewusst haben will, ist die Liste der bekannten Unterwanderungen durch Geheimdienste doch lang. Schon in der jungen BRD informierte
ns diesen darüber, dass Bundes-
hört würde. Gehlen, Direktor des
ation *Operation Gehlen*, reichte
Adenauers Staatssekretär Hans
Globke weiter. Nur beiläufig sei darauf verwiesen, dass sowohl der Mitarbeiter Gehlens, Gehlen selbst als auch Globke zur Nazizeit hohe Positionen bekleideten.

Die US-Geheimdienste blieben auch danach weiter am Ball. Von 1965-1987 entstanden 13.347 Seiten Aktenmaterial. Von deutschen Melderegistern bis hin zu Siemens wurde das technisch Mögliche getan. Bei Siemens ging es speziell um die Überwachung der Exporte. Die zuvor angesprochene Spionage aus US-Botschaften heraus betraf laut James Bamford schon 1986 die Hälfte der Auslandsvertretungen. Das ging sogar so weit, dass die NSA 1987 den BND bat, in drei Staaten, in denen die USA

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