H 7625

FIfF Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

32. Jahrgang 2015 Einzelpreis: 7 EUR **1/2015 – März 2015**

– Der Fall des Geheimen – Ein Blick unter den eigenen Teppich

ISSN 0938-3476

• CETA, TTIP und TiSA • Cyberpeace-Kampagne • Fairphone bald fair? •

FIfF-Kommunikation

Titelbild: Logo der FIfF-Konferenz 2014, Benjamin Kees, CC BY-ND

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V.

Inhalt

Ausgabe 1/2015

inhaltt

Editorial

Die Enthüllungen von Wikileaks und von Edward Snowden haben unseren Blick auf die Aktivitäten des Militärs und der Geheimdienste gelenkt. Weitere Whistleblower folgten. Heute wissen wir von der massenhaften, weltweiten Ausspähung unserer Kommunikation, von Folter und von der gnadenlosen, zynischen Jagd auf Personen, die für „Terroristen" gehalten werden. Die Entscheidung trifft die Politik – offenbar insbesondere der US-amerikanische Präsident –, ohne rechtsstaatliches Verfahren, ohne die Möglichkeit der Opfer, sich gegen die Vorwürfe zu verteidigen.

Die Ausspähung, die Edward Snowden im Juni 2013 offenlegte, wird als *NSA-Skandal* bezeichnet. Immer deutlicher wird aber, dass dieser Begriff zu kurz greift. Es ist nicht nur die NSA, sondern es sind auch deutsche Behörden, die für die Ausspähung und den damit verbundenen Bruch der Menschen- und Bürgerrechte verantwortlich sind.

Der Fall des Geheimen – Ein Blick unter den eigenen Teppich. Dies war das Ziel unserer *FIfF-Konferenz 2014*, bei der eine Reihe kompetenter und prominenter Referentinnen und Referenten versucht haben, die Beteiligung deutscher Dienste an der Überwachung zu beschreiben und zu verstehen. „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."

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 haben bei unserer FIfF-Konferenz die Thematik aus unterschiedlichen Blickwinkeln beleuchtet und bewertet. Die Zusammenfassungen ihrer Beiträge zur Konferenz, die vom Organisationsteam dokumentiert wurden, bilden den Schwerpunkt dieser Ausgabe der *FIfF-Kommunikation*.

Die Beiträge dokumentieren, wie auch von Deutschland aus bedenkenlos dieser Bruch der Menschenrechte unterstützt und vorangetrieben wird. Ein Untersuchungsausschuss des deutschen Bundestages hat die Aufgabe, die Vorwürfe aufzuklären – wiederholt sieht er sich Widerständen gegenüber, zuletzt als der britische GCHQ damit drohte, seine Erkenntnisse nicht mehr den deutschen Diensten zur Verfügung zu stellen. Die Bundesregierung hat diese Drohung offenbar beeindruckt. Die Menschenrechte werden zur Verhandlungsmasse internationaler Abkommen.

Bei der Tagung haben wir auch unseren *FIfF-Studienpreis 2014* verliehen – für eine Arbeit, die die Automatisierung von Videoüberwachung zum Thema hat, die Funktionsweise und Fähigkeiten eines wahrscheinlichen Überwachungssystems für den öffentlichen Raum entwirft und dieses aus informationstechnischer, soziologischer, psychologischer und rechtlicher Perspektive auf gesellschaftliche Probleme hin untersucht. *Benjamin Kees*, der Autor, stellt die Arbeit kurz vor. Sie ist unter dem Titel *Algorithmisches Panopticon* als Buch erschienen.

Ein Schwerpunkt unserer derzeitigen Arbeit ist die Kampagne *Cyberpeace*. In diesem Rahmen sind mehrere Stellungnahmen des FIfF entstanden, die wir in dieser Ausgabe dokumentieren. Ausführlich haben wir den aktuellen Entwurf des IT-Sicherheitsgesetzes untersucht. *Schutz von Grundrechten nicht in Sicht* – das stellt *Ingo Ruhmann* in seinem Beitrag fest, der unsere Stellungnahme zusammenfasst. „Das neue IT-Sicherheitsgesetz erweist sich … in Sachen Datenschutz als hochgradig defizitär, in Sachen IT-Sicherheit als ungenügend und … als ein Weg in massiv weiter ausufernde Sicherheitsprobleme in der Fläche. Einfach mögliche Lösungsansätze wurden nicht verfolgt, die wenigen positiven Aspekte beim Stand der Sicherheitstechnik und beim Personal sind nur ein schwacher Ausgleich."

Weitere Themen ergänzen die Ausgabe. *Nazir Peroz* diskutiert die IT-Entwicklung an den afghanischen Universitäten. Obwohl angesichts der Bilder von Terroranschlägen und Zerstörung der Eindruck entsteht, dass der Wiederaufbau des Landes immer wieder zurückgeworfen wird, findet in großem Rahmen ziviles Engagement in Afghanistan statt, welches vielerorts Früchte trägt.

Viel diskutiert werden die „Freihandelsabkommen" CETA, TTIP und TiSA. Der Umgang der europäischen Institutionen mit den rund 1,5 Millionen Unterschriften gegen TTIP zeigt, wie stumpf das Schwert der europäischen Bürgerinitiative in der Praxis ist. Dagmar Boedicker setzt sich in ihrem Beitrag mit den Abkommen – insbesondere aus Sicht des Datenschutzes – auseinander. „Wenn Freihandelsabkommen, dann solche, die höhere Standards für den Schutz von Menschen und Natur vereinbaren. Andere braucht die Welt nicht", so ihr Fazit.

Am 28. Dezember 1879 stürzte vor der schottischen Stadt Dundee die erst kurz zuvor errichtete Brücke über den Firth of Tay ein und riss 75 Menschen – Passagiere des Zugs aus Edinburgh

– in den Tod. Diese frühe Katastrophe der Technik – drei Jahrzehnte vor dem Untergang der Titanic – wurde von *Theodor Fontane* in einer Ballade verarbeitet, die wir als SchlussFIfF abdrucken. „*Tand, Tand / Ist das Gebilde von Menschenhand*" – so das Fazit von Fontane. Freilich ist eine Eisenbahnbrücke heute nichts Außergewöhnliches mehr. Doch auch dieses Beispiel sollte uns eine Warnung vor unkritischer Anwendung der Technik sein. Sie zeigt, dass technische Lösungen, die eigentlich zum Nutzen der Menschen hergestellt wurden, immer auch zu Katastrophen führen können.

Stefan Hügel
für die Redaktion

CC BY

Brief an das FIfF

Westliche Zivilisation

Liebe Mitglieder des FIfF, liebe Leserinnen und Leser,

es heißt, Mahatma Gandhi sei einmal gefragt worden, was er von der westlichen Zivilisation halte. Das wäre eine gute Idee, habe er geantwortet.

Gandhi hatte Gründe für diese skeptische Einschätzung; er musste erleben, wie zunächst südafrikanische und später, in Indien, britische Behörden und Sicherheitskräfte damals die Interessen der Regierung gegen die Bevölkerung durchsetzten. Von dem, was sonst im 20. Jahrhundert in Europa geschah, nicht zu reden. Doch heute gelten andere Standards der Menschen- und Bürgerrechte. Heute wäre das undenkbar.

Wirklich undenkbar? Vor kurzem wurde der Bericht des Geheimdienstausschusses des US-Senats veröffentlicht, der dokumentiert, in welchem Umfang der Geheimdienst CIA Verdächtige gefoltert hat. Folter galt Ende des 20. Jahrhunderts als absolut geächtet – niemals kann es legitim sein, Menschen zu foltern, um Informationen oder Geständnisse damit zu erzwingen.

Heute scheint dies anders zu sein. Menschen, die als „Terroristen" verdächtigt werden, werden „verschärften Verhörmethoden" ausgesetzt, vorgeblich um Anschläge zu verhindern. Auch der Bericht, der diese Praxis kritisiert, betont nicht zunächst eine Haltung, die Folter ächtet, sondern fragt zuerst nach der Effektivität solcher Methoden für die Terrorismusbekämpfung. Früher galt in Demokratien der Konsens, dass Folter absolut verboten ist – heute ist sie offenbar erlaubt, wenn sie nur ihren vorgeblichen Zweck des *Kriegs gegen den Terror* erfüllt. Das Folterverbot gerät zum Lippenbekenntnis.

Doch es ist noch schlimmer. Im Mittelalter wurden Menschen verbrannt, weil sie beschuldigt wurden, Ketzer oder Hexen zu sein. Davor stand die Inquisition – zweifelsfrei kein Verfahren, das heutigen menschenrechtlichen Standards genügt hätte.

Heute wird selbst auf dieses Verfahren verzichtet. Menschen werden heute, ohne jedes Verfahren, im Feuer von *Hellfire*-Raketen verbrannt, weil sie für „Terroristen" gehalten werden. Einzelne dieser Menschen mögen tatsächlich gefährlich sein – doch auch sie hatten nach bisher akzeptierten Standards das Recht auf ein faires Verfahren. Es ist alarmierend, dass der unerklärte *Krieg gegen den Terror* offenbar bereits hinter den menschenrechtlichen Standards des Mittelalters zurückbleibt. Zu Beginn seiner Amtszeit versprach US-Präsident und Friedensnobelpreisträger Barack Obama noch, das Gefängnis in Guantánamo zu schließen. Dieses Versprechen hat er nicht gehalten. Doch heute werden Verdächtige nicht mehr inhaftiert, sondern gleich getötet.

Die Empörung darüber in der Bevölkerung, in Europa und in den USA, hält sich in Grenzen. Die Tötung von Menschen durch Drohnen erfährt beachtliche Akzeptanz – *wir müssen doch etwas gegen Terrorismus unternehmen!* Dass hier Menschen teilweise grausam getötet werden, ohne Verfahren und aufgrund unsicherer Eigenschaften, bleibt allzu oft im Hintergrund. Dass die *Signature Strikes* häufig auch Unschuldige treffen, tut ein übriges. Zu recht trauern wir um die Opfer des Terrorismus, nicht nur in Europa. Doch wir sollten auch um die unschuldigen Opfer des *Kriegs gegen den Terror* trauern – weit über 1 Million Menschen, wie eine gerade herausgegebene Studie festgestellt hat.

Bekannt wurde dies zunächst durch Veröffentlichungen und Enthüllungen von Wikileaks und Edward Snowden. Der Film *Citizen Four*, der Snowdens Enthüllungen thematisiert, wurde im Februar mit dem Oscar ausgezeichnet. Auch ich habe mich zunächst darüber gefreut, dass den Berichten über eine Menschenrechtsverletzung, der ein großer Teil der Weltbevölkerung ausgesetzt ist, diese Ehrung zuteil wird – ein neuer Höhepunkt nach vielen Ehrungen, der Snowden in den letzten Monaten erhalten hat.

Denke ich jedoch weiter, kommen mir Zweifel. Bis heute haben die Enthüllungen von Edward Snowden keine substanziellen politischen Konsequenzen nach sich gezogen. Im Gegenteil – die Ausspähung der Bevölkerung wird weitergeführt und sogar noch ausgebaut. So gesehen sind die wiederholten Preise fast schon so etwas wie eine Verhöhnung der Menschen, die Tag für Tag ausgespäht werden, während, statt zu Handeln, immer wieder nur folgenlos darüber berichtet und debattiert wird.

Dennoch schmälert das nicht den großen Verdienst Edward Snowdens und der ihn unterstützenden Journalistinnen und Journalisten – allen voran Laura Poitras und Glenn Greenwald. Doch die Enthüllungen und der Umgang damit zeigen vor allem, dass Menschenrechte gerne hinter politischen „Notwendigkeiten" zurücktreten, wenn es opportun erscheint.

Wir dürfen dabei aber nicht in den Fehler verfallen, mit dem Finger auf die USA zu zeigen. Einiges spricht dafür, dass auch deutsche Dienste und Behörden Ausspähung, Folter und Drohnenmorde unterstützen, von ihnen profitieren oder sie stillschweigend dulden. In unserer *FIfF-Konferenz 2014* haben wir auch die deutsche Beteiligung mit Hilfe von hochkarätigen Referentinnen und Referenzen aufgearbeitet – die Zusammenfassungen ihrer Referate bilden den Schwerpunkt dieses Hefts. Die Schwierigkeiten, denen sich beispielsweise der NSA-Untersuchungsausschuss gegenübersieht, zuletzt nach einer Intervention des britischen GCHQ, dem die Ermittlungen des Untersuchungsausschusses ein Dorn im Auge sind, sind ein beredtes Zeichen für die menschen- und bürgerrechtspolitischen Prioritäten der Bundesregierung.

Während dessen bricht sich in Deutschland eine Mischung aus allgemeiner politischer Unzufriedenheit und dumpfem Nationalismus Bahn: PEGIDA, die „Patriotischen Europäer gegen die Islamisierung des Abendlandes" und ihre regionalen Ableger hatten zeitweise großen Zulauf – inzwischen scheinen ihre wöchentlichen „Spaziergänge" wieder abzuebben. Doch das ist sicher noch nicht das Ende. Die Einstellungen, die PEGIDA zugrunde liegen, sind nicht neu und werden auch nach PEGIDA fortbestehen. Bestätigt werden sie durch Publikationen wie von Thilo Sarrazin und durch Spitzenpolitiker, die Gesprächsangebote an PEGIDA formulieren – wohl in der Hoffnung, Wählerstimmen abzuschöpfen.

Einer, der mit den „besorgten Bürgern" von PEGIDA reden wollte – „privat", wie er beteuerte – war der SPD-Vorsitzende Sigmar Gabriel. Kritiker des transatlantischen Freihandelsabkommens TTIP hält er dagegen für „hysterisch". Damit stellt er sich gegen ca. 1,5 Millionen Teilnehmer an der *Selbstorganisierten Europäischen Bürgerinitiative*, durch die das Quorum einer „richtigen" *Europäischen Bürgerinitiative* weit überschritten wurde. Doch die EU-Kommission hatte diese kurzerhand für unzulässig erklärt – damit wird dieses stumpfe Schwert der Bürgerbeteiligung, das von Einigen schon als Durchbruch europaweiter Demokratie gefeiert wurde, endgültig zum Witz. Es zeigt aber auch, wie kaltschnäuzig mit solchen Bürgerbegehren umgegangen wird, wenn dem andere Interessen entgegenstehen.

Worum es bei TTIP geht, sollte inzwischen deutlich geworden sein. Es geht eben nicht darum, dass wir mit Chlorhühnchen überschwemmt werden, eine angebliche Auswirkung von TTIP, mit der dessen Gegner gerne lächerlich gemacht werden, sondern es geht angesichts des Investitionsschutzabkommens und privater Schiedsgerichte um die Zukunft unseres Rechtsstaats.

Beispiel Datenschutz: Gerne wird von TTIP-Befürwortern vorgetragen, es gehe in dem Abkommen überhaupt nicht darum. Das mag vordergründig stimmen – wenn aber der Datenschutz, ebenso wie Umwelt- oder Verbraucherschutz – als nichttarifäres Handelshemmnis eingestuft wird – von privaten Schiedsgerichten, gegen die kein Rechtsbehelf möglich ist –, kann er leicht ausgehebelt werden.

Möglicherweise hat auch dies PEGIDA Unterstützer zugeführt. Es mag unterschiedliche Motive geben, sich ihr anzuschließen, vielleicht auch die Unzufriedenheit mit politischen Entwicklungen wie Arbeitslosigkeit und Sozialabbau. Doch wer, um gegen Sozialabbau zu demonstrieren, sich einer Initiative „gegen die Islamierung des Abendlandes" anschließt und gleichzeitig behauptet, nichts gegen Muslime zu haben, muss sich fragen lassen, ob er überhaupt weiß, was er da tut – und ob nicht seine gesellschaftspolitischen Maßstäbe ein wenig verrutscht sind.

Zurück zur IT. Für das IT-Sicherheitsgesetz liegt nach langen Jahren der Diskussion nun ein Entwurf vor. Bundesinnenminister Thomas de Maizière hatte erklärt, die „weltweit sicherste" IT in Deutschland zu schaffen. Abgesehen von der Frage, was dies angesichts der Passivität der Bundesregierung bei der Aufarbeitung des geheimdienstlichen Ausspähskandals bedeutet: Es kann nicht ausschließlich um Sicherheit gehen. Das Ziel muss sein, IT-Sicherheit schaffen und sie mit der Wahrung der Bürgerrechte in Einklang zu bringen.

An dem Spannungsfeld zwischen IT-Sicherheit und Vorratsdatenspeicherung entzündete sich so auch gleich eine Debatte, bei der unsere Vorschläge kritisiert wurden. Doch wir bleiben dabei: Wir wenden uns strikt gegen die Vorratsdatenspeicherung, sehen aber die Notwendigkeit, zur Analyse von langfristigen Angriffsbildern IP-Adressdaten zu speichern: zeitlich strikt begrenzt und pseudonymisiert. Das hat nichts mit der anlasslosen Speicherung der Daten von Millionen von Internetnutzern zu tun, nach der immer wieder schnell gerufen wird, wenn ein schreckliches Attentat geschieht.

Das IT-Sicherheitsgesetz ist nur eines der Themen, mit dem wir uns in unserer Kampagne Cyberpeace auseinandersetzen. Durch Aktionen, Veranstaltungen und Veröffentlichungen wollen wir uns weiter gegen die Militarisierung des Internet wenden. Im Zentrum stehen die 14 Forderungen, die in der letzten Ausgabe der FIfF-Kommunikation und auf unserer Kampagnenseite *cyberpeace.fiff.de* nachzulesen sind. Dort finden sich auch aktuelle Hinweise auf unsere Aktionen. Unsere Kampagne nimmt dabei immer mehr Fahrt auf – wir freuen uns, dass wir Thomas Reinhold als Campaigner für die Kampagne gewinnen konnten, der auch schon mehrfach für die *FIfF-Kommunikation* geschrieben hat, dieses Mal unsere regelmäßige Kolumne *Betrifft: Cyberpeace*. Herzlich willkommen!

Auch die Planung unserer FIfF-Konferenz 2015 nimmt Formen an. Sie wird vom 6. bis 8. November 2015 unter dem Leitmotiv *Kommerzialisierung des Sozialen: Markt und Macht im Zeitalter der digitalen Kompletterfassung* in Erlangen stattfinden. Prof. Dr. Felix Freiling und sein Team werden ein Programm zusammenstellen, das die Reise dorthin lohnt.

Mit FIfFigen Grüßen

Stefan Hügel

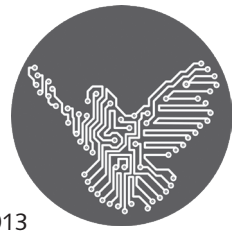
Hallo. Ich bin **Thomas Reinhold**, seit einigen Wochen Campaigner der Cyberpeace-Kampagne des FIfF, und möchte mich an dieser Stelle gern näher vorstellen. Ich bin Diplom-Informatiker mit einem Nebenfachstudium der Psychologie und beschäftige mich seit vielen Jahren mit den Themen Cyberpeace und den Problemen einer Militarisierung des Cyberspace. Seit 2009 bearbeite ich dieses weite Feld als wissenschaftlicher Fellow des Instituts für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH). Um mir die notwendige Flexibilität für eine solche Arbeit zu sichern, habe ich mich 2012 als freiberuflicher Software-Entwickler und Consultant selbstständig gemacht. Erfahrungen in politischen und öffentlichkeitswirksamen Kampagnen konnte ich unter anderem durch mein Engagement in diversen politischen und regionalen Initiativen (u. a. für Amnesty International und Pro-Asyl) sammeln. Darüber hinaus habe ich 2012 im Rahmen einer Projektanstellung im deutschen Büro von Greenpeace gearbeitet. Die Zeit im Elbspeicher hat es mir ermöglicht bei den „Kampagnenprofis" in die Lehre zu gehen und wichtige Kontakte zu knüpfen, die ich nun einbringen kann. Wer sich im Übrigen mehr für meine wissenschaftliche Arbeit interessiert, dem möchte ich die Seite *cyber-peace.org* empfehlen. Dort versuche ich wichtige Ereignisse dieses Themenfelds zu kommentieren und eine Datenbank mit Analysen und Hintergrundinformationen aller relevanten „Cybervorfälle" aufzubauen.

Ich freue mich, dass ich nun den FIfF bei seiner Kampagne unterstützen und mein Wissen einbringen kann und bin gern Ansprechpartner für Ideen, Fragen, Anregungen und Kritik.

Auf bald

Thomas / *thomas.reinhold@fiff.de*

Thomas Reinhold



Betrifft: Cyberpeace

Auswirkungen der Wassenaar-Kontrolle von Cyberwaffen

Seit den Erkenntnissen über *Stuxnet* und angesichts der NSA-Enthüllungen werden international wieder verstärkt die Möglichkeiten für die Kontrolle der Verbreitung von *Cyberwaffen* debattiert. Angesichts der zunehmenden Ausweitung der geheimdienstlichen und militärischen Aktivitäten auf den Cyberspace sind solche Maßnahmen ein wichtiger Bestandteil der politischen Einhegung des Konfliktpotenzials in den Kommunikationsnetzen und der internationalen Vertrauensbildung. Ein erster Schritt in diese Richtung wurde Ende 2013 mit der Erweiterung des *Wassenaar-Abkommens* gegangen, indem unter anderem *intrusion software* in den Katalog, der im Rahmen des Abkommens regulierten kritischen Güter aufgenommen wurde. Das *Wassenaar-Abkommen für Exportkontrollen von konventionellen Waffen und doppelverwendungsfähigen Gütern und Technologien*, dem mittlerweile 41 Mitgliedsstaaten beigetreten sind, wurde 1996 als Nachfolger des aus den Zeiten des kalten Krieges stammenden COCOM-Abkommens verabschiedet. Das Ziel des Übereinkommens ist die Vergrößerung der internationalen Transparenz und der Regulierung des Handels sowie die Eingrenzung der Verbreitung ursprünglich ausschließlich konventioneller Rüstungsgüter. 2009 wurde das Regelwerk um den Bereich der *Dual-Use*-Güter erweitert, als Produkte, die neben zivilen Zwecken auch für die Rüstung eingesetzt werden können. Die Mitgliedsstaaten des Abkommens verpflichten sich, den Export dieser kritischen Güter im Rahmen bestimmter Grenzen zu kontrollieren, Exportanfragen zu prüfen und bei Verdacht auf eine sicherheitspolitisch kritische oder menschenrechtsgefährdende Anwendung abzulehnen. Die Handelsdaten werden zwischen den Mitgliedsstaaten zweimal pro Jahr ausgetauscht.

Mit der neuerlichen Erweiterung von 2013 fällt erstmals Software in diesen Bereich staatlicher Rüstungskontrolle. Der Begriff der *intrusion software* wird spezifiziert als all jene Software, die für das verborgene Agieren entwickelt wurde, in der Lage ist, Daten zu entwenden oder zu modifizieren sowie ein Computersystem in seinen Ausführungsroutinen zu manipulieren oder zur Ausführung fremder Anweisungen zu bewegen. Diese Definition erscheint angesichts der Probleme, den etwas überstrapazierten Begriff der *Cyberwaffe* einzugrenzen, vordergründig sinnvoll gewählt. In erster Linie wird der Funktionsumfang einer Anwendung als hinreichendes Kriterium herangezogen, und weniger die möglichen Schäden oder das konkrete Einsatzumfeld berücksichtigt. Damit fallen jedoch auch Software-Tools unter die Regulierungsanforderungen, die für rein zivile Zwecke wie IT-Sicherheitsüberprüfungen und Penetrations-Test benötigt werden, also ausschließlich friedlichen Zwecken dienen. Die Etablierung von Prüfverfahren für den Export von *Dual-Use*-Gütern ist jedoch eines der wichtigsten Aufgabenfelder des *Wassenaar-Abkommens*, wird in den Handlungs- und Prüfrichtlinien umfassend behandelt und in Form von *Best-Practice*-Richtlinien kontinuierlich weiterentwickelt. Die Umsetzung dieser Maßgaben liegt in der Hoheit und Verantwortung der Mitgliedsstaaten, die jeweils unabhängig entscheiden. Für die Prüfung von Exportanfragen ist in Deutschland das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) beauftragt worden. Die deutschen Kontrollkriterien unterscheiden sich dabei hinsichtlich des Ziellands eines geplanten Exports. Exporte in EU-Mitgliedsstaaten, NATO-Staaten oder Staaten mit einem ähnlichen Status werden grundsätzlich genehmigt, sofern

nicht besondere politische Gründen dagegen sprechen. Exporte in andere Staaten werden grundsätzlich in Frage gestellt und mit Blick auf den potenziellen Käufer, den möglichen offenen und versteckten Einsatzzweck sowie die politische Lage und Stabilität im Zielland geprüft.

Eine Ankündigung der in Frankreich ansässigen Firma *Vupen* von Ende 2014 macht indessen deutlich, dass die Erweiterung des Regelwerks tatsächlich praktische Konsequenzen hat. *Vupen* ist eines der bekanntesten Unternehmen weltweit, die sich auf den Handel mit Schwachstellen und Sicherheitslücken in Software spezialisiert haben, und eigenen Aussagen zufolge ausschließlich staatliche Institutionen beliefern. Das Unternehmen, zu dessen Kunden zwischen 2011 und 2014 auch das BSI im Rahmen eines *Threat protection programs* gehörte, hatte nach der Erweiterung des Abkommens noch verkündet, ihre Aktivitäten den neuen Regularien anzupassen und die friedenspolitischen Ziele zu unterstützten. Mittlerweile hat *Vupen* jedoch beschlossen seinen Stammsitz aus Frankreich zu verlegen, da die „Verzögerungen französischer Behörden nicht länger [für uns] hinnehmbar, weil inkompatibel mit der Geschwindigkeit des Geschäftes [sind]". Die Deutlichkeit, mit der *Vupen*-Geschäftsführer Chaouki Bekrar die aus seiner Sicht störenden Genehmigungen als eine „Überdosis Bürokratie" abtut, deutet darauf hin, dass die französischen Behörden ihre Aufgabe ernst nehmen und die neuen Regularien greifen. Da in Frankreich genauere Kontrollen erst bei Exporten in Länder außerhalb der EU vorgesehen sind, weist dies möglicherweise auch auf den Kundenkreis von *Vupen* hin. Es ist jedoch strittig, ob diese Entwicklung wünschenswert ist.

Es ist für ein Unternehmen, dessen Wirtschaftsgut vor allem aus immateriellen Gütern und technischem Wissen besteht, leichter den Firmensitz zu verlegen, als dies für klassische Rüstungsfirmen mit umfangreichen Fertigungs- und Entwicklungsanlagen der Fall ist. Damit wird das Problem jedoch nur verdrängt und in Regionen ausgelagert, die sich einer effektiven Kontrolle entziehen. Im Fallen von *Vupen* wird der neue Stammsitz wohl in Singapur eingerichtet werden. Singapur ist kein Mitgliedsstaat des *Wassenaar-Abkommens* und *Vupen* unterhält dort bereits Zweigstellen. Neben diesem Effekt wird das Abkommen noch aus weiteren Gründen kritisiert. Zum einen liegt es in der Hoheit und Verantwortung jedes Mitgliedsstaates, die Regelungen und Vereinbarung konkret in nationales Recht umzusetzen und Kontrollziele, Verfahren und Prioritäten zu definieren. Damit fehlt dem Abkommen eine rechtliche Verbindlichkeit, und die unterschiedlichen nationalen Regelungen bilden keine einheitliche Bewertungs- und Rechtsgrundlage. Andere Mitgliedsstaaten haben bei Entscheidungen über Exporte keine Veto-Möglichkeiten und werden stets nur im Nachhinein über erfolgte Exporte informiert. Auch die Formulierung der *intrusion software* lässt offen, ob beispielsweise der Handel mit dem reinen Wissen über Sicherheitslücken unter das *Wassenaar-Abkommen* fällt, wenn es sich bei dem Export nicht um eine konkrete Software handelt, in der ein solches Wissen in Form eines *Exploits* eingebaut ist. Schließlich stehen internationale Abkommen der Rüstungskontrolle stets vor dem Problem der Handelsverschiebungen in den Schwarzmarkt, eine Tendenz die im Falle von immaterieller Software sehr viel einfacher umzusetzen und umso schwerer zu kontrollieren ist.

Zusammen genommen ist festzustellen, dass mit dem *Wassenaar-Abkommen* keine effektive Rüstungs- und Proliferationskontrolle möglich ist. Gleichwohl deuten die Bemühungen in eine richtige Richtung und die Erfahrungen mit dem Unternehmen *Vupen* zeigen, dass eine staatliche Kontrolle in jedem Fall wünschenswerter ist, als ein unkontrollierter Handel mit diesen *Cyberwaffen*.

CC BY

FIfF e. V. – Pressemitteilung

Ganz großes Staatstheater

Die Geister, die ich rief, ich werd sie nicht mehr los

26. November 2014 – In dieser Woche wird im Deutschen Bundestag ein Staatstheater der besonderen Art aufgeführt, das es an Überheblichkeit und Wichtigtuerei mit Goethes *Zauberlehrling* aufnehmen kann. Die Beamten des Bundesnachrichtendienstes (BND) werden unseren Vertretern im Deutschen Bundestag vorführen, wer sich ihrer Ansicht nach in diesem Staat nicht zu verantworten, aber stets etwas zu sagen hat.

Am 28. November 2014 soll nach dem gegenwärtigen Stand im Deutschen Bundestag über die Haushaltsmittel beraten werden, mit denen der BND das Wissen von Kriminellen über geheim gehaltene Software-Schwachstellen – sogenannte *Zero-Day-Exploits* – aufkaufen will. Daraus soll Schadsoftware entwickelt werden, um Computersysteme im Ausland anzugreifen und zu sabotieren. Der BND hat bereits erklärt, „man müsse jetzt auf Augenhöhe mit anderen Diensten operieren". Dass NATO-Rechtsexperten eine staatliche Computersabotage als militärische Aggression mit erheblichen Eskalationsgefahren werten, wird seitens des BND verschwiegen.

Diese Woche soll dem *Focus* zufolge die Bundesanwaltschaft die Untersuchungen zur Überwachung des Handys der Bundeskanzlerin einstellen – mangels Beweisen. Bemerkenswert ist, dass weder die *Deutsche Telekom* noch das Telekommunikationsunternehmen *NetCologne* jene Sicherheitslücken in ihren Computersystemen finden konnten, durch die die NSA Interna aus den Steuerungssystemen beider Unternehmen abgreifen kann. Interessant wird dies durch die aktuellen Veröffentlichungen über den Trojaner *Regin*, der zu 28 % auf Backbones von Telekommunikationsunternehmen aufgetaucht ist und die Funktionalität hat, Aktivitäten und Daten in der infizierten Infrastruktur aufzeichnen und an den GHCQ bzw. an die NSA übermitteln soll. Die Telekom bestreitet laut *Spiegel-Online*, dass sie von *Regin* betroffen war. Dieses Dementi kommt verdächtig schnell. „Eine solche Analyse braucht deutlich mehr Zeit" kommentiert Kai Nothdurft, IT Sicherheitsexperte im FIfF-Vorstand.

Deutsche Behörden und Unternehmen beweisen erneut, dass sie nicht einmal im Ansatz in der Lage sind, die Kommunikations- und IT-Systeme der wichtigsten Personen des politischen Lebens im Lande zu schützen, geschweige denn die der Bürger und Bürgerinnen. Und weil sie ganz offensichtlich nichts von IT-Systemen verstehen, wollen sie nun Wissen über Sicherheitslücken zukaufen – aber nicht, um unseren Staat und die Bürger zu schützen, sondern um selbst zu Cyberangreifern zu werden.

Das wirkt fast schon verzweifelt mutig, ist aber letztendlich gefährlich dumm. Cyberangriffe ziehen häufig Gegenreaktionen nach sich, also weitere Angriffe auf Computersysteme in Deutschland. „Angriffe von anderen Staaten auf dem Qualitätsniveau von *Regin* können gegenwärtig weder Staat noch Unternehmen entdecken, geschweige denn unterbinden", gibt Sylvia Johnigk, ebenfalls Sicherheitsexpertin im FIfF-Vorstand zu bedenken. Sie spricht aus der Praxis, denn sie berät Unternehmen im Bereich Informationssicherheit.

Wir sorgen uns um außenpolitische Krisenherde wie in der Ukraine und die daraus entstehende Gefahr für die Versorgung mit russischem Erdgas. Mit Cyberwaffen in Händen des BND brauchen wir für solche Szenarien gar keine Konflikte im Ausland. Ein wenig Schadsoftware, ein kleiner Cyberangriff eines anderen Staates und die Gegenreaktion des Angegriffenen kann völlig ausreichen, um zum Beispiel die Energieversorgungssysteme hierzulande zusammenbrechen zu lassen.

Zero-Day-Exploits durch den BND aufzukaufen, daraus Cyber-Angriffswaffen zu entwickeln und für Angriffe einsetzen zu wollen ist kriminell und unverantwortlich. Die vom BND geforderten 300 Mio. € für Cyberangriffssysteme sind eine Gefährdung der Sicherheit Deutschlands. Nötig ist stattdessen, dass zum Beispiel das BSI solches Wissen bekannt macht und dafür sorgt, die Sicherheitslöcher in staatlichen und zivilen IT-Systemen zu stopfen. Das Geld sollte in Personal und Infrastruktur fließen, um einen vertrauenswürdigen und transparenten *Cyber-Zivilschutz* zu gewährleisten.

CC BY

FIfF e. V. – Pressemitteilung

Snowden enthüllt: „Deutschland im Cyberkrieg"

Unsere Cyberpeace-Kampagne zeigt Wege aus der Rüstungsspirale

11. Januar 2015 – In der Sendung *Schlachtfeld Internet: Wenn das Netz zur Waffe wird* am 12. Januar 2015 in der ARD erklärt der ehemalige Geheimdienstmitarbeiter Edward Snowden im Interview nicht nur, wie er dem schon in Marsch gesetzten Gefangenentransport entkam. Snowden erklärt auch, wie NSA und andere Geheimdienste das Internet zur Waffe machen. Das weltweite Abhören und Datensammeln der NSA – so Snowden – ist eindeutig die Vorstufe zum Cyberkrieg. Neu ausgewertete Dokumente von Snowden zeigen, dass „Deutschland Drehkreuz des digitalen Krieges ist".

Damit dringt die Debatte um den NSA-Skandal zu ihrem Kern vor: Bisher ging es bei diesem Skandal um die globale Überwachung und die Werkzeuge dafür, wie PRISM und andere. Gerade PRISM überwacht nicht nur, sondern analysiert automatisch die überwachten Kommunikationssysteme auf Schwachstellen und versucht wenn möglich, dort Schadsoftware einzuschleusen. Einbrüche in die Computer von UNO und Belgacom und der EU-Kommission, Trojaner wie *Stuxnet* und *Regin* sind nur einige wenige Beispiele dafür, dass die NSA die am besten ausgerüstete Hackertruppe der Welt ist, sie führt unterschiedslos Cyberkrieg gegen Freund und Feind.

„Cyberkrieg ist alles andere als harmlos", warnt Sylvia Johnigk, IT-Sicherheitsexpertin im FIfF. Cyberkrieg ist in jedem Fall so unkontrollierbar wie der für ein einziges Ziel entwickelte *Stuxnet*-Trojaner. Cyberkrieg gibt jedem politischen Irrläufer Werkzeuge in die Hand, um sinnlose Aktionen zu beginnen, wie den Angriff auf die Sony-Studios. Und Cyberkrieg ist brandgefährlich in seinem Eskalationspotenzial mit Angriffen, die sich schnell zu flächendeckenden Schäden an der zivilen Infrastruktur – Energienetze, Anlagen zur Gefahrstoffproduktion und vieles mehr – ausweiten können.

Das FIfF arbeitet seit Jahrzehnten an der Verhinderung von Überwachung und Cyberkrieg. Mit der aktuellen Cyberpeace-Kampagne setzt das FIfF diese Arbeit fort. Das FIfF hat schon 1997 die *Constant-Web*-Referenz-Datenbank über Sicherheitslücken beschrieben, die vom NSA-Überwachungssystem PRISM heute noch genutzt werden. Der Deutsche Bundestag ließ sich 1994 vom FIfF eine Studie über Cyberkrieg und präventive Rüstungskontrolle erarbeiten. Das FIfF warnt seit den 1980er Jahren vor der Telekommunikationsüberwachung und vor Versuchen, IT-Sicherheitssysteme zu schwächen oder Verschlüsselungssysteme zu verbieten.

„Nichts von alledem, was das FIfF in 30 Jahren analysiert und prognostiziert hat, ist heute Science Fiction", gibt Stefan Hügel, Vorsitzender des FIfF, zu bedenken. Edward Snowden hat der Welt Materialien zur Verfügung gestellt, damit Politik und Öffentlichkeit an offiziellen Dokumenten detailliert nachvollziehen können, dass Massenüberwachung ein Übel ist – das Ziel dieser Überwachung aber sind die Zerstörung ziviler Infrastrukturen und Cyberkrieg.

Die Sendung *Schlachtfeld Internet – Wenn das Netz zur Waffe wird* ist daher eine wichtige Dokumentation, die es zu sehen lohnt. Cyberkrieg ist aber nicht das zwangsläufige Ende dieser Entwicklung. Mit der Cyberpeace-Kampagne des FIfF wollen IT-Experten Lösungen für eine friedliche Nutzung des Internets aufzeigen. Es gibt Wege aus der globalen Überwachungsgesellschaft, Wege aus der Cyber-Rüstungsspirale, und Wege zu mehr IT-Sicherheit.

Referenzen

http://cyberpeace.fiff.de
http://www.ard-digital.de/meldungen/programmtipps/programmtipp-12012015-schlachtfeld-internet

CC BY

FIfF e. V. – Pressemitteilung

Cyberpeace beginnt bei der Wahrung der Privatsphäre im Internet

10. Februar 2015 – Zum zwölften Mal wird heute weltweit der *Safer-Internet-Day* begangen. Die von der Europäischen Kommission ins Leben gerufene Initiative hat das Ziel, die friedliche Entwicklung des Internets zu fördern, um insbesondere für Kinder und Jugendliche einen gefahrlosen Raum zu entwickeln. Unter dem Motto „*Let's create a better internet together*" werden am heutigen Tag weltweit Aktionen gestartet, um die Sensibilität für das Thema *Sicherheit im Internet* zu fördern und „ein aktives Wirken von Institutionen, Organisationen, Verbänden, Unternehmen, Initiativen, Schulen, Privatpersonen auf nationaler, regionaler und lokaler Ebene zu initiieren."

Nicht erst seit den Enthüllungen von Edward Snowden stehen die Gefahren der Überwachungsgesellschaft im Vordergrund unserer Aufklärungsarbeit. Snowdens Dokumente belegen, dass Gefahren im Internet auch von befreundeten Staaten oder den eigenen nationalen Institutionen und deren unkontrolliertem Informationshunger ausgehen können. Immer mehr Informationen aus dem digitalen Leben jedes Einzelnen werden im Namen der Terror-Bekämpfung allumfassend gesammelt und in Datenbanken zusammengeführt. Gesetzliche Grenzen werden von Nachrichtendiensten ignoriert und u. a. durch den Datenaustausch mit „befreundeten Diensten" ausgehebelt. Demokratische Kontrollgremien werden hintergangen. Während politische Aktivisten in Diktaturen Internet-Zensur, Überwachung oder den Zwang zur absoluten Transparenz kritisieren und für Freiheit kämpfen, lassen wir uns diese gerade nehmen. „Gerade für Kinder und Jugendliche ist das Internet elementarer Bestandteil ihres täglichen Lebens" gibt Kai Nothdurft, Vorstandsmitglied im FIfF, zu bedenken. „Ihnen dürfen die Chancen auf eine freie, selbstbestimmte und unbeschwerte Entfaltung ihres Lebens nicht durch die ewige Datenbank aller Jugendsünden verwehrt werden."

Das FIfF informiert seit den 80er Jahren über die Sicherheitsrisiken der Informationstechnologie. Mit der aktuell laufenden *Cyberpeace*-Kampagne sensibilisiert das FIfF für die derzeit größten Sicherheitsrisiken im Internet: den militärischen und geheimdienstlichen Missbrauch, insbesondere die Massenüberwachung und deren Konsequenzen.

Die Kampagne setzt sich für die ausschließlich friedliche Nutzung der IT und den Schutz vor militärischem und politischem Missbrauch ein. Die menschenrechts- und verfassungswidrige Ausspähung der Zivilgesellschaft muss sofort beendet werden. „Wir müssen uns von einer Sicherheitsdoktrin abwenden, die alle Menschen unter Generalverdacht stellt", so Sylvia Johnigk, Sprecherin der *Cyberpeace*-Kampagne. „Cyberpeace beginnt bei der Achtung der Privatsphäre des Menschen und der Menschenwürde als einem elementaren Menschenrecht – auch im Internet."

Das Bundesverfassungsgericht hat den Begehrlichkeiten von Sicherheitsbehörden eine Schranke in Form des neuen Grundrechts auf *Gewährleistung der Integrität und Sicherheit informationstechnischer Systeme* gesetzt. Das Bundeskriminalamt, Microsoft und weitere, die im Beirat des deutschen *Safer-Internet-Day* vertreten sind, sollten sich an diese Schranken erinnern. Der Aufkauf des Staatstrojaners oder strategische Partnerschaften mit der NSA werden dem Ziel eines friedlichen und sicheren Internets nicht dienen. Mit solchen Partnern verliert die Initiative an Aufrichtigkeit und ein eigentlich guter Gedanke bekommt einen faden Beigeschmack.

FIfF e. V. – Pressemitteilung

FIfF kritisiert Entwurf des IT-Sicherheitsgesetzes als mangelhaft und verfassungswidrig

Die Bundesregierung muss endlich für wirksamen Schutz sorgen

12. Februar 2015 – Die Expertinnen und Experten des FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung – haben den am 17. Dezember 2014 vorgelegten Entwurf für das neue IT-Sicherheitsgesetz in einer umfassenden Stellungnahme als mangelhaft und nicht verfassungsgemäß kritisiert. „Trotz zweier positiver Neuerungen – die Festlegung auf den Stand der Technik bei kritischen Infrastrukturen und die Berücksichtigung von Atomanlagen als kritische Infrastruktur – fällt die Bilanz ernüchternd aus", so Stefan Hügel, Sprecher der *cyberpeace*-Kampagne des FIfF und dessen Vorsitzender.

Im besonderen kritisieren die IT-Expertinnen und -Experten die Beschränkung auf den Schutz der IT-Systeme des Bundes. Die Pflicht zum Schutz des *Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, das auch gegenüber Dritten gilt, wird dagegen nicht eingelöst; der Staat reduziert ihn auf seine eigenen IT-Systeme und schafft sich dafür zusätzlich eine Sonderpolizei beim BKA.

Während Anbieterinnen und Anbietern von Diensten im Web durch unveränderte Bestimmungen im Telemediengesetz (TMG) die notwendigen Befugnisse zur Sicherstellung der IT-Sicherheit verwehrt werden, wird Service-Providern durch eine Änderung am Telekommunikationsgesetz (TKG) die umfassende und unbegrenzte Datenerhebung der gesamten Telekommunikation beim Nutzer und deren Auswertung erlaubt. „Wer bösgläubig wäre, müsste in dieser unbegrenzten Datenspeicherung bei jenen Telekommunikations-Unternehmen, die ohnehin im Zentrum des Interesses der Sicherheitsbehörden stehen, die ultimative rechtliche Grundlage für den Datenzugang der Dienste zum Daten-

verkehr von Nutzern sehen", sagte dazu die Sicherheitsexpertin Sylvia Johnigk, ebenfalls Sprecherin der *cyberpeace*-Kampagne und FIfF-Vorstandsmitglied. „Die Datensammlung ist nach unserer Auffassung nicht mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und dem Fernmeldegeheimnis nach Artikel 10 Grundgesetz vereinbar und damit verfassungswidrig."

Damit sorgt die Bundesregierung nach 18 Jahren der Diskussion um den Schutz kritischer Infrastrukturen immer noch nicht für einen wirksamen Schutz der Menschen und der Wirtschaft im digitalen Zeitalter. Aus Sicht des FIfF muss nach dem immer noch nicht aufgearbeiteten Skandal der Ausspähung durch Geheimdienste eine klare und unabhängige Bestandsaufnahme erfolgen. Zusätzlich fordert das FIfF den Gesetzgeber auf:

- für IT-Sicherheit für die Allgemeinheit statt nur für die IT des Bundes zu sorgen,
- Transparenz zu schaffen, indem Sicherheitslücken obligatorisch offen gelegt werden müssen,
- klar definierte, einheitliche Regeln für die Datenerhebung zur Störungserkennung zu schaffen, um das Grundrecht auf informationelle Selbstbestimmung, das Grundrecht auf Gewährleistung der Integrität von IT-Systemen und das Fernmeldegeheimnis effektiv zu schützen,
- eine von Weisungen unabhängige Organisationsstruktur für das BSI zu schaffen, und die Behörde auf den Schutz der IT von Bürgerinnen und Bürgern in der Informationsgesellschaft auszurichten.

„Offenbar ist die Bundesregierung nicht in der Lage oder nicht willens, die Bevölkerung effektiv vor den Bedrohungen aus dem Netz zu schützen – stattdessen trägt sie durch die Geheimdienste, die sie eigentlich kontrollieren sollte, selbst zu der Verschärfung der Situation bei", so erneut Stefan Hügel. „Nachdem aus den Snowden-Enthüllungen keine erkennbaren politischen Konsequenzen gezogen wurden, ist nun der Entwurf des IT-Sicherheitsgesetzes, trotz einzelner Lichtblicke, ein weiterer Schritt in die falsche Richtung."

CC BY

Ingo Ruhmann

Schutz von Grundrechten nicht in Sicht

Zur Stellungnahme des FIfF zum Entwurf des IT-Sicherheitsgesetzes

Egal, ob das Internet kaputt ist oder nicht –, die heutige Lage von Datenschutz und Privatsphäre im Internet und bei der IT-Sicherheit ist ein Zustand von unkontrollierter Ausspähung und Computerattacken im Wilden Westen ohne Recht und Gesetz. Die Bundesregierung ist mit ihrem Ende 2014 beschlossenen Entwurf eines IT-Sicherheitsgesetzes angetreten, dem Recht und dem Schutz bei IT-Systemen zu mehr Geltung zu verhelfen. Was davon zu halten ist, zeigt die Stellungnahme des FIfF zum Gesetzentwurf.

Auch eineinhalb Jahre nach Beginn der von Edward Snowden ermöglichten Enthüllungen werden immer noch neue Fakten bekannt im Skandal um das Ausspähen von Computern durch die NSA und deren Angriffe auf IT-Systeme von Verbündeten ebenso wie von erklärten Gegnern. Der NSA-Skandal hat IT-Verantwortlichen, aber auch der Allgemeinheit unmissverständlich deutlich gemacht, in welchem Umfang IT-Systeme kompromittiert sind. Verschlüsselungssysteme werden ausgehebelt, vertrauliche Kommunikationsinhalte abgefangen, privateste Daten auf den eigenen Computersystemen ausgespäht – selbst, wenn diese Computer nicht mit dem Internet verbunden sind. IT-Sicherheitsprofis wie Bruce Schneier bringen den Kenntnisstand auf ein einfaches Fazit: „Wenn die NSA in Deinen Computer hinein kommen will, dann kommt sie auch hinein."

Privatsphäre und Sicherheit in der digitalen Welt sind in Auflösung begriffen. Wer dies nicht als schicksalhafte Folge des Tuns großer Mächte hinnehmen will, muss aktiv werden. Die *Cyberpeace*-Kampagne des FIfF ist eine Form konstruktiver Gegenwehr. Das zentrale Ziel der Kampagne ist das Ende der unbegrenzten geheimdienstlich-militärischen Ausspähung und Manipulation beliebiger IT-Systeme und der Schutz von Grundrechten. Doch Appelle, Verbote und technische Hilfsmittel allein helfen nicht. Gefordert ist auch die Abwehr konkreter Attacken mit zivilen und rechtstaatlichen Mitteln. Die *Cyberpeace*-Kampagne verfolgt daher auch das Ziel, Computerspionage und -sabotage zu ahnden und die Täter zu verfolgen.

Gerade aus der Sicht von IT-Fachleuten sieht das FIfF die Notwendigkeit, IT-Sicherheit nicht nur technisch zu verbessern, sondern auch den rechtstaatlichen Schutz zu stärken und damit den Schutz von gleich drei derzeit über alle Maßen verletzten Grundrechten zu gewährleisten:

1. das Fernmeldegeheimnis nach Art. 10 GG,
2. das Datenschutz-Grundrecht auf *informationelle Selbstbestimmung*[1] und
3. das IT-Grundrecht auf *Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*[2].

Artikel 1 (3) Grundgesetz bestimmt: „Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht." Es ist also staatliche Aufgabe, den Schutz dieser drei Grundrechte seiner Bürgerinnen und Bürger zu gewährleisten, staatliches Handeln darauf auszurichten und auf den Schutz der Grundrechte auch gegenüber nicht-staatlichem Handeln hinzuwirken.

Vor diesem Hintergrund war es zu begrüßen, dass die Bundesregierung Ende 2014 in einem zweiten Anlauf ein Gesetz zur IT-Sicherheit im Kabinett verabschiedete, das seinen Beitrag dazu leisten will, „dass das Netz sicherer wird und die digitalen Infrastrukturen Deutschlands künftig zu den sichersten weltweit gehören."

Kern des Entwurfes der Bundesregierung ist es[3], Betreiber kritischer Infrastrukturen auf einen Mindeststandard an IT-Sicherheit zu verpflichten und erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Die beim BSI zusammenlaufenden Informationen sollen ausgewertet und zur Verbesserung des Schutzes kritischer Infrastrukturen zur Verfügung gestellt werden. Telekommunikationsunternehmen – so das BMI in seiner Pressemitteilung – werden zudem verpflichtet, ihre Kunden zu warnen, wenn ihnen auffällt, dass der Anschluss des Kunden für Angriffe missbraucht wird.

Doch leider erweist die genaue Lektüre auch dieses Gesetzesvorhabens, dass zwischen verfassungsmäßigen Pflichten und gesetzgeberischem Tun ganz erhebliche Differenzen bestehen. Das FIfF hat Mitte Februar eine detaillierte Stellungnahme zum IT-Sicherheitsgesetz vorgestellt[4], die sich auf vier Themenbereiche konzentriert:

1. die nicht verfassungsgemäßen gesetzlichen Regelungen und Rechtsgrundlagen für IT-Sicherheit,

2. das BSI als zentrale IT-Sicherheitsinstanz,

3. die Sonderrolle für staatliche IT und der defizitäre Schutz für die Allgemeinheit,

4. die unzureichende Umsetzung von Schritten und Maßnahmen, die für IT-Sicherheit nötig sind.

Positionen und Kritik des FIfF werden im Folgenden in geraffter Form dargestellt. Die ausführliche Stellungnahme ist auf den Webseiten der Cyberpeace-Kampagne verfügbar.[5] Es wäre zusätzlich eine eigene Betrachtung, ob die Ansätze und Aufwände für den Schutz kritischer Infrastrukturen ausreichen. Dies kann hier nicht geleistet werden.

1. Rechtsgrundlagen für IT-Sicherheit nicht vorhanden oder nicht verfassungsgemäß

Die Kritik des FIfF setzt dort an, wo es um die rechtlichen Grundlagen geht, IT-Sicherheit mit rechtstaatlichen Mitteln überhaupt zu gewährleisten und der Pflicht des Staates zum Schutz von Grundrechten nachzukommen.

Für das Verständnis der Kritik bedeutsam ist, dass das Internet im deutschen Recht in zwei Bereiche aufgeteilt ist[6]: Das Recht der Telekommunikation (im Telekommunikationsgesetz, TKG) etwa für E-Mails, Chatten und andere direkte Kommunikationsformen einerseits und das Recht der Telemedien (im Telemediengesetz, TMG), in dem alle Webangebote geregelt sind, also die Pflichten der Anbieter von Webseiten, Webshops, Cloud-Speichern oder komplexen webbasierten Softwarediensten. Für beide Bereiche erlauben und verbieten beide Gesetze verschiedene IT-Sicherheitswerkzeuge. Wichtig zum Verständnis ist auch, dass das Bundesverfassungsgericht im Januar 2012 IP-Adressen als personenbezogene Daten bewertete.[7]

Regelung für Webangebote

Für Webangebote – Telemedien – ausdrücklich verboten ist die beliebige Speicherung personenbezogener Daten – also auch IP-Daten – in §12 TMG. Zulässig ist eine Speicherung nur, wenn es gesetzlich explizit erlaubt ist, oder der Nutzer eingewilligt hat, und eine Speicherung und Verarbeitung der Daten zur Kommunikation und zur Abrechnung bei Vertragsverhältnissen nötig ist. In allen anderen Fällen sind alle Daten am Ende der Nutzung umgehend zu löschen. Allein „bei Verwendung von Pseudonymen" ist es zulässig, pseudonyme Nutzungsprofile für „Werbung, Marktforschung oder zur bedarfsgerechten Gestaltung" der Telemedien zu erstellen. Verstöße gegen diese Regelung können als Ordnungswidrigkeit geahndet werden.

Für Zwecke der IT-Sicherheit erlaubt das Gesetz damit nur, IP-Nummern von Nutzern eines Webangebotes solange zu verarbeiten, wie die aktuelle Nutzung andauert. Da die IT-Sicherheit als Zweck im Gesetz nicht vorgesehen ist, greift das generelle Speicherungsverbot und damit die Pflicht zur Löschung der IP-Daten nach Nutzungsende oder zumindest deren Pseudonymisierung, wenn auch fraglich ist, ob das zu einer „bedarfsgerechten Gestaltung" zählt. Unzweifelhaft gesetzwidrig ist es, vollständige IP-Adressen für irgendeinen Zweck dauerhaft zu speichern.

Bei Webangeboten dürfen damit IP-Daten von IT-Sicherheitswerkzeugen durch ein *Intrusion Detection System* genutzt werden. Es gibt aber bei Webangeboten keine Rechtsgrundlage für den Einsatz von IT-Sicherheitswerkzeugen für mehrschrittige Analysen und erst recht nicht für die Verfolgung von Angreifern und die Beweissicherung nach einem Fall von Cybersabotage, sondern das Verbot der entsprechenden Datenspeicherung und -verarbeitung. Der Bundesregierung ist die Problematik spätestens seit 2006 bekannt, als dem Bundesjustizministerium genau diese Speicherung von IP-Daten rechtskräftig untersagt wurde[8].

Für eine rechtstaatliche Verfolgung von Cyberattacken ist es aus Sicht des FIfF also notwendig, für IT-Sicherheitswerkzeuge eine grundrechtskonforme Rechtsgrundlage zu schaffen – also eine, die datenschutzkonform ist und möglichst wenig Daten erfordert. Aus Sicht des FIfF ist es dabei auch völlig unbegründet, Unterschiede in der Rechtslage und der IT-Sicherheit zwischen der Telekommunikation und den Telemedien zu machen.

Der Gesetzentwurf der Bundesregierung sah in einer Vorversion aus dem Sommer 2014 hierzu eine Regelung vor, die nach berechtigter Kritik wieder gestrichen wurde. In dieser Vorversion plante die Bundesregierung, einfach eine ähnliche Regelung aus dem Telekommunikationsrecht – §100 TKG – zu übertragen. Das FIfF sieht schon in den heutigen, aus der Zeit der analogen Telefonie stammenden Befugnissen zur Datensammlung nach §100 TKG eine deutlich überzogene Regelung. Der §100 TKG erlaubt heute ohne jede Einschränkung, jede Form von Daten

zur Störungserkennung aus Telefonaten und Datenverkehren zu sammeln, zu analysieren und sich sogar auf Kommunikationsverbindungen aufzuschalten.

Regelung in der Telekommunikation

Die Bundesregierung verabschiedete nun in ihrem Entwurf des IT-Sicherheitsgesetzes für den Telekommunikationssektor eine noch sehr viel weiter reichende Regelung. Danach sollen Telekommunikationsanbieter nicht nur jedes beliebige Datum zur Störungserkennung speichern und analysieren dürfen, sondern obendrein auch Daten über

> *„Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können."*

Der für analoge Technik 1996 formulierte §100 TKG hatte ursprünglich das Ziel, strafbare Eingriffe in Fernmeldesysteme für die Öffentlichkeit zu ermitteln und den Telekommunikationsunternehmen die Befugnis zu geben, dafür Messungen vorzunehmen. Die geplante Änderung des neuen Gesetzes will dies nun ausweiten auf

- die Verfügbarkeit unspezifischer „Informations- und Kommunikationsdienste" sowie
- auf die unbegrenzte Datensammlung zum Schutz vor einem „unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer" – also von beliebigen Telekommunikationskunden.

Es geht also nicht mehr um die Verfolgung von Gesetzesverstößen – im Kern Betrugshandlungen an TK-Systemen – durch Manipulationen. Hier sollen Telekommunikationsunternehmen dazu befugt werden, als Helfershelfer der Strafverfolgung unbegrenzt Daten über ihre Kunden zu sammeln und auszuwerten, um zu erkennen, ob es unerlaubte „Zugriffe" auf die IT-Systeme der Kunden geben könnte. Eine solche unspezifische Datensammlung zu Zwecken der IT-Sicherheit wäre ein nahezu unbegrenzter Eingriff in das Fernmeldegeheimnis. Im starken Gegensatz zu den Vorgaben des Bundesverfassungsgerichts für Eingriffe in Grundrechte ist diese geplante Vorschrift

1. nicht an die Angabe eines Anlasses (sondern unspezifisch eine „Störung") gebunden,
2. ohne einen genügend spezifischen Zweck (nur Erkennung eines „unerlaubten Zugriffs"),
3. ohne spezifische Kriterien und
4. ohne Vorgaben zu Speicherdauer und zur Datennutzung.

Obendrein soll durch einen geplanten neuen §109a TKG jeder Diensteanbieter bei „Störungen, die von Datenverarbeitungssystemen der Nutzer ausgehen", diese Nutzer

> *„soweit ihm diese bereits bekannt sind, unverzüglich darüber … benachrichtigen. Soweit technisch möglich und zumutbar, hat er die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können".*

Das geht nur durch die Durchsuchung von Datenkommunikation zur Kenntnisnahme, Identifikation und Benachrichtigung von Telekommunikationskunden ohne die geringsten Vorgaben für eine Eingrenzung auf Kriterien, Speicherdauer oder Analyseform für diese Daten.

Diese Vorschriften an Beispielen durchzuspielen, macht das Ausmaß der Idee erkennbar. Danach dürfte jeder Telekommunikations-Provider die Kommunikationsdaten von Kunden unbegrenzt durchsuchen und speichern, um beispielweise

- „unerlaubte Zugriffe" einer Smartphone-App auf eigene Daten zu erkennen,
- die von einigen Providern nicht erlaubte und als „Störung" unterbundene Nutzung von Skype auf Smartphones zu erkennen und zu verhindern,
- natürlich auch „unerlaubte Zugriffe" z. B. auf urheberrechtlich geschütztes Material zu verfolgen.

Rufen wir uns in Erinnerung, welche Zugriffe auf IT-Systeme „unerlaubt" sind oder was als „Störung" gilt, dann ist man schnell bei einer Ahnung von nahezu unbegrenzter Überwachung des Datenverkehrs ohne jede Einschränkung und damit der faktischen Aushebelung des Fernmeldegeheimnisses. Eine solche dauerhafte Durchsuchung von Telekommunikationsverkehren zur Ermittlung von „Störungen" – nicht einmal „Gefährdungen" – ohne jede Einschränkung entspricht nicht einmal im Ansatz den Anforderungen an Grundrechtseingriffe. Dies macht deutlich, dass die im IT-Sicherheitsgesetz vorgesehene Ausweitung an §100 TKG und die Nutzung der gewonnen Daten für die im geplanten §109a TKG genannten Zwecke aus Sicht des FIfF eindeutig unvereinbar ist mit Art. 10 GG. Es ist mit Sicherheit davon auszugehen, dass sie einer Verfassungsklage nicht standhalten werden.

Zusammenfassend zur Frage der Rechtsgrundlagen soll es im IT-Sicherheitsgesetz für die im TMG geregelten Webservices weiterhin keine Rechtsgrundlage für IT-Sicherheitswerkzeuge geben, im TKG dagegen eine klar verfassungswidrige uferlose Datensammlung, die einem Gang nach Karlsruhe nicht standhalten wird. Im Ergebnis des Gesetzes, das für mehr IT-Sicherheit sorgen sollte, entstünde so ein Rechtsvakuum, das der IT-Sicherheit absolut jede Rechtsgrundlage entzieht und damit zugleich jede Basis für Investitionen in mehr Ressourcen – von einer datenschutzkonformen Lösung einmal ganz abgesehen.

Verfassungskonformer Gegenvorschlag

Der Gegenvorschlag des FIfF zielt darauf ab, die Verarbeitung von IP-Daten zu Zwecken der IT-Sicherheit in allen Bereichen einheitlich und so datensparsam wie möglich zu gestalten. Da ohne die Auswertung von IP-Daten keine Identifikation und

Rückverfolgung von Cyberangreifern möglich ist, die notwendige schnelle Reaktion auf Angriffe eine längere Datenspeicherung unnötig macht und obendrein die große Menge der protokollierbaren Daten die Analyse eher behindert, schlägt das FIfF als Verfahrensprinzip vor, Verdachtsfälle sofort kriterienbasiert zu ermitteln und alle unnötigen Daten zu löschen oder in Zweifelsfällen zumindest zu pseudonymisieren. Für die eingehende Analyse von Cybersicherheitsvorfällen muss dem FIfF-Vorschlag gemäß ein auditierbares Verfahren eingesetzt werden, mit dem nachvollziehbar ist, welche Daten genutzt, und dass nicht benötigte Daten gelöscht wurden. Mit diesem Prinzip ist in einem gerichtsfesten Verfahren die minimal zur Verfolgung notwendige Menge an Daten benannt, bei zugleich weitestgehender Löschung von Daten.

Dass sich das FIfF für eine derart minimierte Sammlung von IP-Daten ausspricht, führte zur Kritik des AK Vorratsdatenspeicherung, der jede Form der IP-Datenspeicherung bei Telemedien ablehnt, die bei Telekommunikationsdaten allerdings nicht weiter erwähnt. Unterstützung für den Vorschlag des FIfF kam indes vom Schleswig-Holsteinischen Landesdatenschutzbeauftragten Thilo Weichert, der in einer Stellungnahme[9] ebenfalls darauf hinweist, dass eine Verfolgung von Cyberangreifern eine IP-Datenspeicherung erfordert und sich daher „hundertprozentig hinter den FIfF-Vorschlag" stellte[10].

Das FIfF bleibt bei seiner Forderung einer einheitlichen Rechtsgrundlage für die IT-Sicherheit, die sowohl das Grundrecht auf *informationelle Selbstbestimmung* wie auch das Grundrecht auf *Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* umsetzt und zugleich das Fernmeldegeheimnis wahrt und nicht weiter aushöhlt.

2. Rolle des BSI

Das FIfF hat die Gründung des BSI 1989 kritisch kommentiert. Wir haben dabei zwar die Notwendigkeit einer solchen Behörde betont, aber zugleich deren Doppelaufgabe für staatliche Stellen einerseits und Bürgerinnen und Bürger andererseits problematisiert.[11]

Diese Doppelaufgabe hat dem BSI in den letzten Monaten erhebliches Misstrauen auf Seiten der deutschen Wirtschaft eingebracht, nachdem durch die von Edward Snowden zugänglich gemachten Dokumente auch bekannt wurde, dass der BSI-Präsident anlässlich einer USA-Reise die NSA zu einem Arbeitstreffen besucht hatte[12]. Dies wurde von den Wirtschaftsverbänden überaus kritisch gesehen, wenngleich das BSI die Berichte dementierte[13].

Das FIfF teilt viele dieser Bedenken der Wirtschaft und sieht einige akut anstehende Aufgaben besser bei anderen IT-Sicherheitsexperten aufgehoben. Entscheidend für das FIfF ist jedoch, dass staatliche Stellen sehr wohl eine unabhängige Kontrollfunktion ausüben können, wenn sie in geeigneter Weise unabhängig organisiert sind. Genauso, wie die Datenschutzbeauftragten frei von der Einflussnahme der von ihnen kontrollierten Stellen sein müssen, so muss auch das BSI nach Ansicht des FIfF in Zukunft weisungsungebunden und unabhängig von anderen staatlichen Stellen organisiert sein, um den Verfassungsauftrag der *Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* erfüllen zu können.

Das IT-Sicherheitsgesetz will das BSI zwar personell und finanziell aufstocken, was keine ganz schlechte Idee ist, aber weiter in seiner bisherigen Rolle belassen, die vorrangig dem Schutz staatlicher IT-Infrastrukturen dient. Der vom Bundesverfassungsgericht formulierte Verfassungsauftrag wird so jedenfalls nicht umgesetzt.

3. Die Sonderrolle für staatliche IT und der defizitäre Schutz für die Allgemeinheit

In der detaillierten Betrachtung der Rechtslage im ersten Abschnitt blieb ein Detail unberücksichtigt: Die rechtliche Sonderstellung in Sachen IT-Sicherheit, die sich der Bund für seine IT-Systeme ab 2007 eingeräumt hat und die jetzt weiter gestärkt werden soll.

Im ersten Abschnitt wurde kurz erwähnt, dass es dem Bundesjustizministerium 2006 untersagt wurde, IP-Daten zu speichern. Der Bundesregierung war die Gefahr für die IT-Sicherheit – ausweislich ihrer Antwort auf eine Kleine Anfrage[14] – unmittelbar bewusst; sie reagierte binnen Jahresfrist. In der Novelle des BSI-Gesetzes erhielt das BSI 2007 in §5 BSIG die Befugnis, in jedem Anwendungsbereich des Internets für Zwecke der IT-Sicherheit IP-Daten bei IT-Systemen des Bundes zu erheben und auszuwerten. Als einzige Stelle darf daher das BSI – das auch kein Telekommunikationsunternehmen ist, denen ansonsten allein eine Datensammlung gemäß §100 TKG erlaubt ist – IT-Sicherheitswerkzeuge für die IT des Bundes umfassend einsetzen.

Diese Ausnahmereglung für staatliche IT-Systeme wird nun im neuen Gesetzentwurf weiter getrieben. Das BSI erhält nicht nur die Rolle der zentralen Sammelstelle für IT-Sicherheitsvorfälle bei Betreibern kritischer Infrastrukturen, obendrein schafft sich die Bundesregierung eine Sonderpolizei für Cyberattacken beim BKA. Mit der im Gesetzentwurf formulierten Begründung, dass die Strafverfolgung und „die örtliche Zuständigkeit oftmals dem Zufall überlassen" bleiben, soll das BKA bei Computerstrafdelikten gegen die IT des Bundes und kritischer Infrastrukturen ermitteln. Das Argument des „Zufalls" meint offensichtlich – deutlicher gesagt, dass die für IT-Kriminalität zufällig zuständigen Strafverfolgungsbehörden der Republik nicht mit hinreichenden Kompetenzen und Ressourcen ausgestattet sind, um Angriffe auf die IT des Bundes mit der nötigen Sachkunde zu verfolgen.

Bürgerinnen und Bürger, die Wirtschaft, aber auch die Behörden der Länder und Kommunen werden mit den Problemen der Sicherheit ihrer IT-Systeme also nicht nur bei den rechtlichen Grundlagen allein gelassen, sondern auch bei der Strafverfolgung, die in der Fläche nach Meinung der Bundesregierung von so geringer Qualität ist, dass nur ein eigenes zentrales Sonderdezernat helfen kann. Die Bundesregierung beziffert laut Gesetzentwurf den Aufwand für diese Aufgabe beim BKA auf „48 und bis zu maximal 78 Planstellen mit jährlichen Personalkosten in Höhe von jährlich zwischen rund 3,226 und bis zu maximal 5,310 Millionen Euro".

Während gerade Sicherheitspolitiker nicht müde werden zu betonen, das Internet sei kein „rechtsfreier Raum", zieht sich die Bundesregierung bei den Rechtsgrundlagen und bei der Straf-

verfolgung von der Aufgabe eines Schutzes der Allgemeinheit zurück. Für die Allgemeinheit macht die Bundesregierung das Internet damit erst zum rechtlosen Raum, für den zwar Gesetze formuliert sind, aber die Strafverfolgung kaum Handlungsmöglichkeiten hat – in wichtigen Bereichen für die Allgemeinheit sind nicht einmal die Verfolgung von Tätern und die Beweissicherung über die zielgerichtete Speicherung von IP-Daten zulässig.

4. Maßnahmen für die IT-Sicherheit unzureichend

Aus der Sicht von IT-Fachleuten im FIfF ist das IT-Sicherheitsgesetz eine höchst unpassende Konstruktion. Wer IT-Sicherheit verbessern will, muss zwangsläufig das allgemeine Sicherheitsniveau erhöhen und Einfallstore und Hintertüren beseitigen. Alles andere wird Kosmetik bleiben.

Das FIfF hat daher Ergänzungsvorschläge für das IT-Sicherheitsgesetz gemacht, die aus Sicht der Praxis vordringlich sind. Die wichtigsten sind:

- **Umgang mit IT-Sicherheitslücken.** Wie alle IT-Sicherheitsexperten hält auch das FIfF den Austausch über IT-Sicherheitslücken für einen der wichtigsten Wege zur Verbesserung der Sicherheitslage. Das FIfF fordert, dass das BSI seine Kenntnisse zeitnah und umfassend publizieren muss und nicht selbst darüber entscheidet, ob es dies tut. Das FIfF fordert weiter, dass zur Aufdeckung von Sicherheitsproblemen durch interne Whistleblower und zur Realisierung einer Produkthaftung ein gestuftes Meldeverfahren etabliert wird, bei dem eine vertrauenswürdige Stelle Hinweise sammelt und an die Hersteller oder Anwender weiterleitet, die die Sicherheitsrisiken zu verantworten und zu beseitigen haben. Werden bekannt gewordene Sicherheitslücken nicht nach einer angemessenen Frist geschlossen, wird der Weg möglich, geltende Produkthaftungsregelungen auch im IT-Bereich gegen die Verursacher von Sicherheitsrisiken anzuwenden.

- **Zuverlässigkeit zentraler IT-Sicherheitsmechanismen.** Wenn die Dokumente von Edward Snowden eines gezeigt haben, dann, in welchem Ausmaß zentrale Sicherheitsmechanismen der IT-Sicherheit kompromittiert sind. Schon bevor der SSL-*Heartbleed-Bug* überhaupt programmiert wurde, war NSA-Dokumenten zu entnehmen, dass die SSL-Verschlüsselung erfolgreich angegriffen wurde. VPN-Verbindungen sind durch Hintertüren und Implementationsdefizite verwundbar. Das FIfF fordert, solche und andere zentrale IT-Sicherheitskomponenten jetzt und auf Dauer periodisch auf ihre Zuverlässigkeit oder Kompromittierung hin durch unabhängige Stellen zu untersuchen und die Ergebnisse zu veröffentlichen.

- **Schutz des Fernmeldegeheimnisses.** Zu den zielgerichtet in das Strafrecht formulierten Absonderlichkeiten des deutschen Rechts gehört, dass kein Geheimdienstmitarbeiter dafür belangt werden kann, das Fernmeldegeheimnis durch Abhören gebrochen zu haben. Strafbar machen sich beim Abhören nach §206 StGB nur Mitarbeiter von Telekommunikationsunternehmen. Das FIfF fordert angesichts des NSA-Skandals, die Strafbarkeit von Abhörhandlungen genauso zu regeln wie den Bruch des Postgeheimnisses, bei dem es für jedermann strafbar ist, verschlossene Sendungen zu öffnen und zu lesen.

5. Gibt es gar nichts Positives?

Bei aller Kritik und Verbesserungsvorschlägen ist die Frage natürlich richtig, welche genuin positiven Aspekte das Gesetz aus Sicht des FIfF enthält. Diese sind schnell genannt.

Die Verpflichtung von Betreibern kritischer Infrastrukturen auf bessere IT-Sicherheit ist sicherlich eine gute Idee. Kerntechnische Anlagen, die bisher aus der Debatte heraus gehalten wurden, auch zu kritischen Infrastrukturen zu zählen, ist eine positive Überraschung. Das Gesetz regelt hierzu aber nur genau das als Maßstab, was das Bundesdatenschutzgesetz ohnehin seit Jahren vorschreibt: Den Stand der Technik.

Der aktuelle Stand der Technik ist aber keine echte Perspektive in der IT-Sicherheit. Schon seit über drei Jahren arbeiten das DIN und die ISO an neuen Sicherheits-Standards für Energienetze, die zur Grundlage für Zertifizierungen werden und zu EU-weiten Standards führen sollen. Auch die EU hat mehrfach angekündigt, in Sachen IT-Sicherheit regulativ tätig zu werden[15], das EU-Parlament hat Ergänzungen angemahnt[16]. Es ist zu vermuten, dass die EU die IT-Sicherheit umfassender regeln wird und auf Deutschland Nachbesserungsbedarf zukommt. Hier hätte die Bundesregierung auch aus den Interessen der Industrie heraus weiter gehende Maßstäbe setzen können. Aktiv gestalten, statt bei der IT-Sicherheit nur zu reagieren, wäre für Deutschland der bessere Ansatz.

Grundsätzlich positiv zu sehen sind auch die zusätzlichen Ressourcen für die IT-Sicherheit. Dass aber nicht nur das BSI 133 zusätzlichen Planstellen erhält und damit von derzeit ca. 600 Stellen auf dann über 730 Stellen anwächst, sondern laut IT-Sicherheitsgesetz für das Bundesamt für Verfassungsschutz 55 neue Planstellen und das BKA bis zu 79 zusätzliche Planstellen vorgesehen sind – in Summe also 134 Stellen –, ist nicht nachzuvollziehen. Die neuen Stellen für Verfassungsschutz und BKA wären besser beim BSI aufgehoben, hätten den Stellenzuwachs dort glatt verdoppelt, und könnten im BSI die Sachkompetenz zur Bekämpfung von IT-Sicherheitsproblemen für die Allgemeinheit bündeln und verstärken, statt die nachrichtendienstliche Ausforschung voran zu treiben. Das BSI hat seit seiner Entstehung schon die Aufgabe, Polizeibehörden mit Sachkunde zu unterstützen und könnte dies bei Cyberangriffen mit mehr Personal besser leisten.

6. Fazit

Das neue IT-Sicherheitsgesetz erweist sich – so die detaillierte Analyse des FIfF – in Sachen Datenschutz als hochgradig defizitär, in Sachen IT-Sicherheit als ungenügend und – insbesondere auch durch die Reduktion der Sicherheitsperspektive auf IT-Systeme des Bundes – als ein Weg in massiv weiter ausufernde Sicherheitsprobleme in der Fläche. Einfach mögliche Lösungsansätze wurden nicht verfolgt, die wenigen positiven Aspekte beim Stand der Sicherheitstechnik und beim Personal sind nur ein schwacher Ausgleich.

Sicher ist nur, dass dieses Gesetz für Juristen neue Arbeit bringen und IT-Sicherheitsexperten nicht entlasten wird. Die Sicherheit in der IT und der Schutz der Grundrechte werden mit diesem Gesetz nicht im Ansatz verbessert.

Anmerkungen

1 *BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83 u. a. – Volkszählung –, BVerfGE 65, 1*
2 *Bundesverfassungsgericht vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274 ; http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html*
3 *Pressemitteilung des Bundesinnenministeriums vom 17.12.2104 zum dort ebenfalls publizierten Gesetzentwurf: http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/12/bundeskabinett-beschlie%C3%9Ft-it-sicherheitsgesetz.html*
4 *http://cyberpeace.fiff.de/Kampagne/ITSicherheitsgesStellungn*
5 *FIfF-Stellungnahme zum IT-Sicherheitsgesetz; http://cyberpeace.fiff.de/Uploads/Uploads/FIfF_Stellungnahme_IT-Sicherheitsgesetz.pdf*
6 *Im Detail dazu: Ingo Ruhmann: IT-Sicherheit und das geplante IT-Sicherheitsgesetz; in: telepolis, 11.04.2013; http://www.heise.de/tp/artikel/38/38891/1.html*
7 *Beschluss des Ersten Senats vom 24. Januar 2012 - 1 BvR 1299/05 - http://www.bverfg.de/entscheidungen/rs20120124_1bvr129905.html*
8 *Endgültiger Beschluss des Amtsgericht Mitte zu Berlin mit Androhung von Zwangsgeld gegen das BMJ vom 10.01.2008, 5 C 314/06, http://www.daten-speicherung.de/data/Beschluss_AG-Mitte_2008-01-10.pdf*
9 *ULD-Stellungnahme zum IT-Sicherheitsgesetz-Entwurf; https://www.datenschutzzentrum.de/artikel/877-ULD-Stellungnahme-zum-IT-Sicherheitsgesetz-Entwurf.html*
10 *IT-Sicherheitsgesetz: Streit um Nutzung von IP-Adressdaten; in: Heise Newsticker, 17.02.2015, http://www.heise.de/newsticker/meldung/IT-Sicherheitsgesetz-Streit-um-Nutzung-von-IP-Adressdaten-2552632.html*
11 *Ute Bernhardt; Ingo Ruhmann: ZSI: Die Bundesregierung will den Bock zum Gärtner machen; in: Computerwoche, Nr. 52, 22. Dez. 1989, S. 6-8 und: dies.: Mutationen einer Geheimdienststelle; in: Computerwoche, Nr. 12, 23. März 1990, S. 44-47*
12 *René Pfister, Laura Poitras, Marcel Rosenbach, Jörg Schindler, Holger Stark: Der fleißige Partner; in: Spiegel Online, 22.07.2013, http://www.spiegel.de/spiegel/print/d-104058608.html*
13 *BSI-Pressemitteilung: Keine Unterstützung ausländischer Nachrichtendienste, Bonn, 26.07.2013, https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Keine_Unterstuetzung_auslaendischer_Nachrichtendienste_26072013.html*
14 *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Petra Pau, Sevim Dagdelen, weiterer Abgeordneter und der Fraktion DIE LINKE: Speicherung der IP-Adressen von Besucherinnen und Besuchern der Website des Bundeskriminalamtes, 7.11.2007, Bt.-Drs. 16/6938, Antworten zu den Fragen 11 und 13*
15 *Kommissionsvorschlag für eine Richtlinie zur Netz- und Informationssicherheit (NIS) vom 7.02.2013, http://europa.eu/rapid/press-release_IP-13-94_de.htm*
16 *Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zum Thema „Cyberangriffe in der EU“, 10.07.2014; http://edz.bib.uni-mannheim.de/edz/doku/wsa/2014/ces-2014-1488-de.pdf*

FIfF e. V. – Pressemitteilung

FIfF fordert wirksame EU-Gesetzgebung für verantwortungsvolle Rohstoffbeschaffung von Unternehmen

Europäische Unternehmen profitieren vom Handel mit Konfliktrohstoffen

3. Dezember 2014 – Seit Jahrzehnten spielt der Handel mit Mineralien, Edelsteinen und anderen Rohstoffen eine zentrale Rolle bei der Finanzierung bewaffneter Konflikte weltweit. Konfliktparteien in Ländern wie Afghanistan oder Zentralafrikanische Republik werden mit Erlösen aus dem internationalen Rohstoffhandel finanziert. Europäische Firmen importieren eine große Menge an Rohstoffen für Handys oder Laptops aus eben diesen Konfliktgebieten, ohne dass Unternehmen offenlegen müssen, ob und inwiefern sie mit dem Kauf dieser Rohstoffe zur Finanzierung von Kriegen und Menschenrechtsverletzungen beitragen.

Die Europäische Kommission hat im März 2014 einen Verordnungsentwurf vorgelegt, der verhindern soll, dass „Erträge aus dem Handel mit Mineralien zur Finanzierung bewaffneter Konflikte verwendet werden“. Dass die EU diesbezügliche Regelungen vorsieht, ist zu begrüßen, denn ihr Einfluss ist groß: Fast ein Viertel des globalen Handels mit Zinn, Tantal, Wolfram und Gold entfällt auf die EU, letztes Jahr wurden 240 Millionen Handys und 100 Millionen Laptops in die EU importiert, die alle diese Rohstoffe enthalten.

„Der derzeit vorliegende Entwurf ist viel zu schwach. Er bezieht sich einerseits ausschließlich auf Direktimporteure der unter die Verordnung fallenden Mineralien, zum anderen handelt es sich nur um ein Modell der freiwilligen Selbstverpflichtung. Doch am 4. Dezember 2014 gibt es die Möglichkeit, diesen Entwurf zu stärken“ erklärt Sebastian Jekutsch, Sprecher der Arbeitsgruppe *Faire Computer* des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung. Morgen findet eine öffentliche Anhörung des Ausschusses für internationalen Handel zum Thema Konfliktmineralien in Brüssel statt. Das FIfF fordert, dass der Parlamentsausschuss Führungsqualitäten zeigt und den Entwurf stärkt:

„Zurzeit sind die Unternehmen nicht verpflichtet sicherzustellen, dass die Erlöse aus dem Handel mit diesen Mineralien nicht in die falschen Hände geraten. Doch Unternehmen kommen ihrer Sorgfaltspflicht beim Bezug von Rohstoffen aus Konfliktgebieten nur dann nach, wenn sie gesetzlich dazu gezwungen werden. Verpflichtende Regeln sind daher unbedingt notwendig“, so Sebastian Jekutsch. „Zudem müssen auch Unternehmen Verantwortung übernehmen, deren Endprodukte diese Rohstoffe

enthalten, nicht nur die Rohstoffimporteure." Jekutsch fordert daher die politischen Entscheidungsträger in der EU zu einer wirksamen EU-Gesetzgebung auf, damit Unternehmen zu einer verantwortungsvollen Rohstoffbeschaffung verpflichtet werden.

Die USA ist im Vergleich zur EU in diesem Bereich Vorreiter. Zwar ist es zu begrüßen, dass die EU nicht nur den Handel in Zentralafrika regulieren will, dennoch ist das *Dodd-Frank-Gesetz Absatz 1502* ein Meilenstein: Alle in den USA an der Börse notierten Unternehmen müssen veröffentlichen, ob diese Rohstoffe aus der Demokratischen Republik Kongo oder ihren Nachbarstaaten stammen und überprüfen lassen, ob die in ihren Produkten enthaltenen Mineralien einen Beitrag zur Finanzierung bewaffneter Gruppen in Zentralafrika leisten.

CC BY

Sebastian Jekutsch

Betrifft: Faire Computer

Fair wie in Faires Gold.

An die Zustände und gelegentlichen Skandale haben wir uns gewöhnt. Man könnte fast von Langeweile sprechen. Alles, was wir schon vor einem Jahr diskutierten, ist immer noch in Diskussion. Neues ist nicht hinzugekommen. Bei der Fairness in der Elektronikindustrie reden wir über klitzekleine Fortschritte in den immer gleichen Problemfeldern.

Zum Beispiel Konfliktmineralien: Das EU-Parlament hat im Dezember zwar über eine geplante EU-Regulierung diskutiert und den Stellungnahmen einiger Interessenvertreter aus Wirtschaft, Zivilgesellschaft, der OECD und – das ist neu! – der eigentlich Betroffenen (in diesem Fall aus der D.R. Kongo) zugehört ... und dann alles erst einmal wieder zu den Akten gelegt. Der Kommissions-Rapporteur sieht kaum Änderungsnotwendigkeiten an dem schwachen Kommissionsvorschlag. Die Bundesregierung findet es toll so, das FIfF fordert hingegen wirksame Gesetze und nicht die geplante *freiwillige Selbstverpflichtung*. Gleichzeitig streiten sich NGOs aus dem Pro- und Contra-Lager, Bischöfe aus aller Welt, Investoren, Kongolesen und Wissenschaftler darüber, ob das US-amerikanische Vorbildgesetz *Dodd-Frank-Act Sect. 1502* nun gute oder schlechte Wirkungen hat. Dabei geht es gar nicht um Fairness für die ArbeiterInnen, auch nicht um Handelsgebote, sondern nur darum, wie sehr Firmen darauf achten, dass ihre Rohstoffgeschäfte mit bestimmten Metallen nicht Milizen und Rebellen in Bürgerkriegsregionen zu Gute kommen. Die Geschäftsleute befreien sich unterdessen per Betrug und Schmuggel von all diesem Nervkram aus dem reichen Norden.

Zum Beispiel Samsung: In den seit einem Jahr laufenden Gesprächen zwischen dem Konzern, der ihm gewogenen Entschädigungsbehörde, der Opfervertretergruppe SHARPS, einzelnen anderen Opferfamilien, Anwälten und Politikern um 1. das Schuldeingeständnis für Vergiftungen in ihrer Halbleiter- und LCD-Herstellung und 2. die Entschädigung der Opfer der dort eingesetzten Chemikalien hat Samsung nun einen Kompromissvorschlag zu 2. vorgelegt (und gleichzeitig 1. strikt abgelehnt), der grob sagt: Uns ist das Schicksal unserer ArbeiterInnen wichtig, deshalb zahlen wir allen Opfern Entschädigung, vorausgesetzt es sind keine Leiharbeiter, sie haben bestimmte Krebsarten, sie waren eine Mindestzeit beschäftigt und haben sich rechtzeitig bei der Behörde untersuchen lassen, kurzum: nur ein kleiner Teil der Betroffenen darf hoffen. Unterdessen kommen die ersten Kinder der vergifteten Arbeiterinnen krank zur Welt.

Zum Beispiel Apple: Am Vorabend der *Apple Watch*, die mit immer mehr Miniaturisierung auch immer speziellere Chemikalien und Rohstoffe benötigen wird, hat der Konzern turnusgemäß seinen Zuliefererbericht veröffentlicht und eine durchaus beeindruckende Menge von Aktivitäten zur Verbesserung der Arbeitssituation in den globalen Fertigungshallen vorgelegt. Bei Lichte betrachtet steigt aber die Anzahl an Trainingsprogrammen, Audits und Rohstoffinitiativen auch nur linear mit den beeindruckenden Umsatz- und Gewinnsteigerungen dieser Firma. Ihr bislang größter Auftragnehmer Foxconn, der in China einen ungewohnten Rüffel des Kommunistischen Gewerkschaftsbundes wegen der vielen Überstunden bekam, hat einen teilweisen Einstellungsstopp erlassen, auch weil Apple nun zunehmend Konkurrent *Pegatron* beauftragt, was laut *China Labor Watch* allein aus Kostengründen geschehen sei, denn dort werde geringerer Lohn gezahlt. Die BBC hat sich bei Pegatron umgeschaut und in einem viel beachteten TV-Beitrag reichlich faule Stellen an Apple hergezeigt: miese Trainings, viele Überstunden, autoritäre Vorgesetzte in den Zulieferbetrieben, zudem illegal abgebautes Zinn aus Indonesien in den Geräten.

Alles alte Hüte, wie gesagt. Auch nicht neu, aber zunehmend diskutiert werden Formen von Zwangsarbeit in der Elektroindustrie. Um einen Job zu bekommen, zahlen nämlich Arbeitslose aus armen Ländern hohe Vermittlungsgebühren, wodurch sie sich verschulden und somit in einer Art Schuldknechtschaft während der ersten Arbeitsmonate im wesentlichen diese Schulden abbezahlen. Sie sind in dem Job gefangen, und wenn sie ihn verlieren sollten, können sie in aller Regel nicht wieder nach Hause, weil das Geld dafür fehlt. In der *FIfF-Kommunikation* hatten wir schon über Vietnamesen in Tschechien berichtet, die ein ähnliches Schicksal teilen. Aktuell wird dies in der Elektroindustrie in Malaysia viel thematisiert. Hewlett-Packard fordert nun Direktanstellung von Gastarbeitern. Das Industriekonsortium EICC möchte zu hohe Vermittlungsgebühren unterbinden. Apple zwingt Zulieferer, eventuelle Gebühren komplett zurückzuzahlen. Die USA drohen, Malaysia auf eine Sanktionsliste zu setzen. Zwangsarbeit könnte also das nächste große Fairness-Thema in der Elektroindustrie werden. Es gibt auch schon einige Gesetze. In der EU und Deutschland fehlen die meines Wissens aber noch.

Immerhin: Der deutsche IT-Branchenverband BITKOM engagiert sich für eine sozial-ökologische IT-Beschaffung der Behörden. Welchen Beweises bedarf es noch, dass Nachhaltigkeit auch ein Geschäft sein kann? *TCO Development*, die mit dem einzigen Fairness-Siegel der Branche, wird beispielhaft erwähnt in den neuen Vergaberichtlinien.

Das MakeITfair-Projekt wurde unterdessen offiziell beendet

Und was machen die Vorbildprojekte in Sachen Faire Computer? *NagerIT* ist ziemlich präsent in Zeitungen und Märkten, verkauft auch stetig, veröffentlicht aber wenig Neues über ihre Computermaus oder ihre detailliert dokumentierte Lieferkette. Alle *Fairphones* sind inzwischen verkauft, und im Laufe des Jahres wird es das nächste Modell geben, über dessen Fairness man noch nichts sagen kann, auf dessen Design das Unternehmen dank Wechsel des Partners (wieder aus China, Auditbericht steht noch aus) aber nun mehr Einfluss hat. *Shiftphones* behauptet zwar weiter, fairer zu sein als andere, hat aber noch keinen Nachweis geliefert. Derweil öffnet Posteo in ihrer Berliner Zentrale eine Art ersten Fair-IT-Shop. Trotz des fehlenden Angebots eine tolle Sache.

Auch bei diesen Projekten also eine gewisse Stagnation. Ich finde, es ist ein Punkt erreicht, an dem die Gesetzgeber am Zuge sind, denn der Markt alleine bewegt sich nicht genügend. Wir wollen nicht auf den nächsten Skandal warten, sondern ihn verhindern.

Sebastian Jekutsch ist Sprecher der AG Faire Computer des FIfF. Wer sich für die Quellen oder das Thema allgemein interessiert, kann gerne Kontakt aufnehmen per *sj@fiff.de*.

Sebastian Jekutsch

Fairphone bald fair?

Fairphone *[1] ist ein kleines Unternehmen, das mit dem Ziel, ein möglichst faires Smartphone anzubieten, viel Beachtung bekommen hat. Es konnte zwar nur enttäuschend wenig Verbesserungen gegenüber konventionellen Geräten umsetzen [2], hat aber immerhin die Startup-Phase überlebt und ist in der Entwicklungsphase des neuen Modells, das im Laufe des Jahres erscheinen soll. Im Vorfeld hat sich das Unternehmen von seinem bisherigen Kontraktfertiger der* Fairphone*s getrennt [3]. Warum dies nötig war, erklären wir im Vergleich mit der nachhaltigen Computermaus von* Nager IT.

3

Abbildung 1; „This Phone would be even fairer if ...", ein Vorschlag für ein Fairphone Case Design [30]

Der Grund, den Kontraktfertiger zu wechseln, ist der Wunsch, mehr Einfluss auf das Gerätedesign zu bekommen [4]. *Fairphone* wechselt nun von einem Lizenzmodell zu einem selbstbestimmten Entwurf. In der Fachsprache heißt das: Sie wechseln von einem ODM (*Original Design Manufacturer*) zu einem EMS (*Electronics-Manufacturing-Services)* Anbieter [5]. Damit werden sie mehr Einfluss auf die Auswahl der Geräteteile und auf das Gerätedesign bekommen und damit sozialverträglichere Rohstoffquellen und Geräteproduktion ermöglichen. Mit einem EMS-Partner könnte *Fairphone* besser bestimmen, woher z. B. das vielleicht bald konfliktfreie Wolfram im Vibrationsalarm [6] oder das Gold in der Leiterplatine [7] kommt.

Das *Fairphone* war bisher nämlich ein konventionelles Gerät mit ein paar *Interventions* [8]. Es wurde im wesentlichen etwas verkauft, was auf ähnliche Weise vom alten Kontraktfertiger auch direkt angeboten wurde, allerdings nicht auf dem europäischen Markt. *Fairphone* konnte beeinflussen, welche Lötpaste (mit Rohstoff Zinn) und welcher Elektrolytkondensator (mit Rohstoff Tantal) eingesetzt wurde, offensichtlich auch, wie das Gehäuse aussieht, aber das elektrische Design dürfte wiederverwendet worden sein.

Nun tritt *Fairphone* in die Fußstapfen der konventionellen Großen. Apple, HP, Dell und wie sie alle heißen, folgen ebenfalls dem EMS-Modell, nachdem sie vor vielen Jahren das andere Extrem, das Modell OBM (*Original Brand Manufacturer*) aufgaben. Die zur Auswahl stehenden EMS-Anbieter haben so illustre Namen wie Flextronics, Jabil Circuit und ... Foxconn, weltweit berüchtigt nach der Häufung von Angestelltenselbstmorden in 2010 [9].

Die Teile- und Zuliefererliste

Fairphone berichtet öffentlich lediglich über Fairness in der Endmontage. Es gibt einen Fertigungs-Auditbericht dazu [10]. Es fehlen aber Informationen zu den vorgelagerten Stufen, Ausnahme ist die teilweise geklärte Tantal- und Zinnherkunft. Über die vergangenen Monate hat *Fairphone* eine immer umfangreichere Teile- und Zuliefererliste veröffentlicht [11]. Sie ist allerdings nicht vollständig, so fehlt beispielsweise der schon oben

erwähnte Vibrationsalarm. Die aktuelle Version umfasst aber immerhin 80 Positionen. Wie diese Informationen zustande kamen, ist leider nicht bekannt. Zum Vergleich:

- *Hewlett-Packard* veröffentlicht keine Teileliste ihrer Produkte. Sie fassen aber Zulieferinformationen in Produktkategorien wie Notebooks, Storage, Printer, etc. zusammen. Es gibt also a) diese Zuliefererliste [12], die die einzelnen Endfertigungsfabriken und die Firmennamen einiger Teilehersteller auflistet, b) eine jährliche Zusammenfassung von Audit-Ergebnissen bei meist direkten Zulieferern [13] und c) die Liste einiger Metallhütten [14] – HP hatte als erste Firma damit schon vor Jahren begonnen –, ergänzend dazu der pflichtgemäße Bericht gemäß US-amerikanischem *Dodd-Frank-1502 (DF-1502)* [15], einer Regulierung zu sogenannten Konfliktmineralien.

- *Apple* veröffentlicht ebenfalls keine Teileliste ihrer Produkte, verrät aber a) ebenfalls anhand von Produktkategorien die Endfertigungsfabriken und – auf einen Haufen geworfen – sogar die meisten Komponentenlieferanten [16], womit sie HP übertreffen. Jährlich veröffentlicht Apple b) Erkenntnisse aus ihren Audits in ihrem *Supplier Report* [19], zudem hat Apple ausführliche Berichte über einige Foxconn-Werke [18] veröffentlichen lassen. Auch Apple hat inzwischen c) eine Liste der Metallhütten [19] und natürlich ebenfalls den gesetzlichen DF-1502-Bericht [20].

- Von *Samsung* ist weder eine Teile- noch eine Zuliefererliste öffentlich. Sie publizieren ein paar Ergebnisse ihrer Audits bei den Betrieben [21] und vage Zahlen über Metallhütten [22], über die sie allerdings als koreanische Firma auch nicht DF-1502-berichtspflichtig sind, genauso wie die niederländischen *Fairphone* übrigens.

Ich möchte an dieser Stelle betonen, dass diese Analyse nur die Transparenz in der Zulieferung betrifft, und dass die in diesem Punkt herausragende Firma Apple mitnichten faire Geschäftspraktiken unterhält [23].

Abbildung 2: Fairphone Zulieferer: Dunkelgrau sind die Länder aus denen die Teile des Fairphone kommen, soweit überhaupt bekannt. Leider werden nicht die Produktionsländer angezeigt, sondern in den meisten Fälle die Länder der Firmenzentralen, was eine ziemlich nutzlose Information ist. [11]

Fairphone geht also bei den Zuliefererinformationen über die Arbeit von Samsung, nicht aber von HP und Apple, hinaus. Teilelisten sind bei Apple, HP und Samsung nicht zu bekommen, werden aber kostenpflichtig bei z. B. IHS oder Chipworks und eher als Nebeneffekt bei z. B. iFixit angeboten [24].

Die Lieferkette fehlt

Die Zuliefererliste von *Fairphone* ist keine sogenannte *Lieferkette*, also keine Aufstellung, welche Geräteteile von wem wo hergestellt und zusammengebaut wurden. Es werden zwar einige Teile veröffentlicht, aber nicht die Fertigungsfabriken der Hersteller – lediglich deren Firmensitz, der aber irrelevant ist – und auch nicht, welche Teile aus welchen Teilen bestehen ... bis runter zu den Quellen der Rohstoffe. Zugegebenermaßen: So etwas kennen wir nur aus der Lebensmittelbranche, und dort ist es auch nicht öffentlich.

Es gibt mit der Computermaus von *Nager IT* [25] dennoch ein Vorbildprojekt in Sachen Lieferkettendokumentation (siehe Abbildung 3).

Deren öffentliche Lieferkette [26] zeigt zum einen den *Baum* der Zusammenstellung des Produkts von (oben) dem Vertrieb bis (unten) den Rohstoffen, wobei noch nicht alle Beziehungen bekannt sind. Zum anderen zeigt es per Farben an, ob der Hersteller/Fertigungsbetrieb bekannt ist und wie die Arbeitsbedingungen sind.

Wenn man etwas Ähnliches für *Fairphone* aufstellen wollte, käme man in etwa zu einem Bild wie in Abbildung 4 dargestellt.

Erstellt wurde das Bild mit dem Supply Chain Editor von *Lebensland* [27], einem vom FIfF unterstützen Softwareprojekt. Erläuterung der Grafik: Pro Kategorie werden jeweils nur zwei exemplarische Teile dargestellt; es gilt eh für alle das Gleiche. Und mit der Ausnahme von Tantal in Kondensatoren und Zinn in der Lötpaste und den Leiterplatinen wurden die vielen Rohstoffe unten und oben lediglich angedeutet und nicht mit Kanten verbunden. Die Farben entsprechen nicht ganz denen der *Nager-IT*-Lieferkette und bedeuten: Grün = gute Arbeitsbedingungen, Grau-Blau = verbesserungswürdige Arbeitsbedingungen, aber Teilerfolg erzielt, Orange = Hersteller bekannt, aber Arbeitsbedingungen unbekannt, Rot = weder Hersteller/Hütten/Minen noch Arbeitsbedingungen bekannt.

Das Bild musste ich leider selbst malen. *Fairphone* hat sich meines Wissens nie die Mühe gemacht. Hat das Unternehmen mit *Fair* im Namen überhaupt je versucht, die Herkunft der Teile und Rohstoffe und die dort vorzufindenden Arbeitsbedingungen zu klären?

Fair oder Fairer?

Der wesentliche Unterschied zwischen *Nager IT* und *Fairphone* bezüglich der Lieferkettendokumentation ist die Menge der „grünen" Zulieferungen. Der Grund ist einfach: *Nager IT* folgt einem EDM-Modell, fast schon einem OBM und nicht einem ODM, d.h. das Mausdesign ist in der Hand des Herstellers und damit die Möglichkeit, faire Alternativen auszuwählen. Nur so konnten die grünen Stellen in der Lieferkette entstehen. Die Facebook-Seite von *Nager IT* [28] und ihr Newsletter sind voller Geschichten über die Recherche von Herkunft und Arbeitsbedingungen und der Auswahl fairerer Alternativen.

Ein weiterer wichtiger Unterschied zwischen den beiden Projekten ist zu bedenken: Während *Nager IT* die fairste mögliche

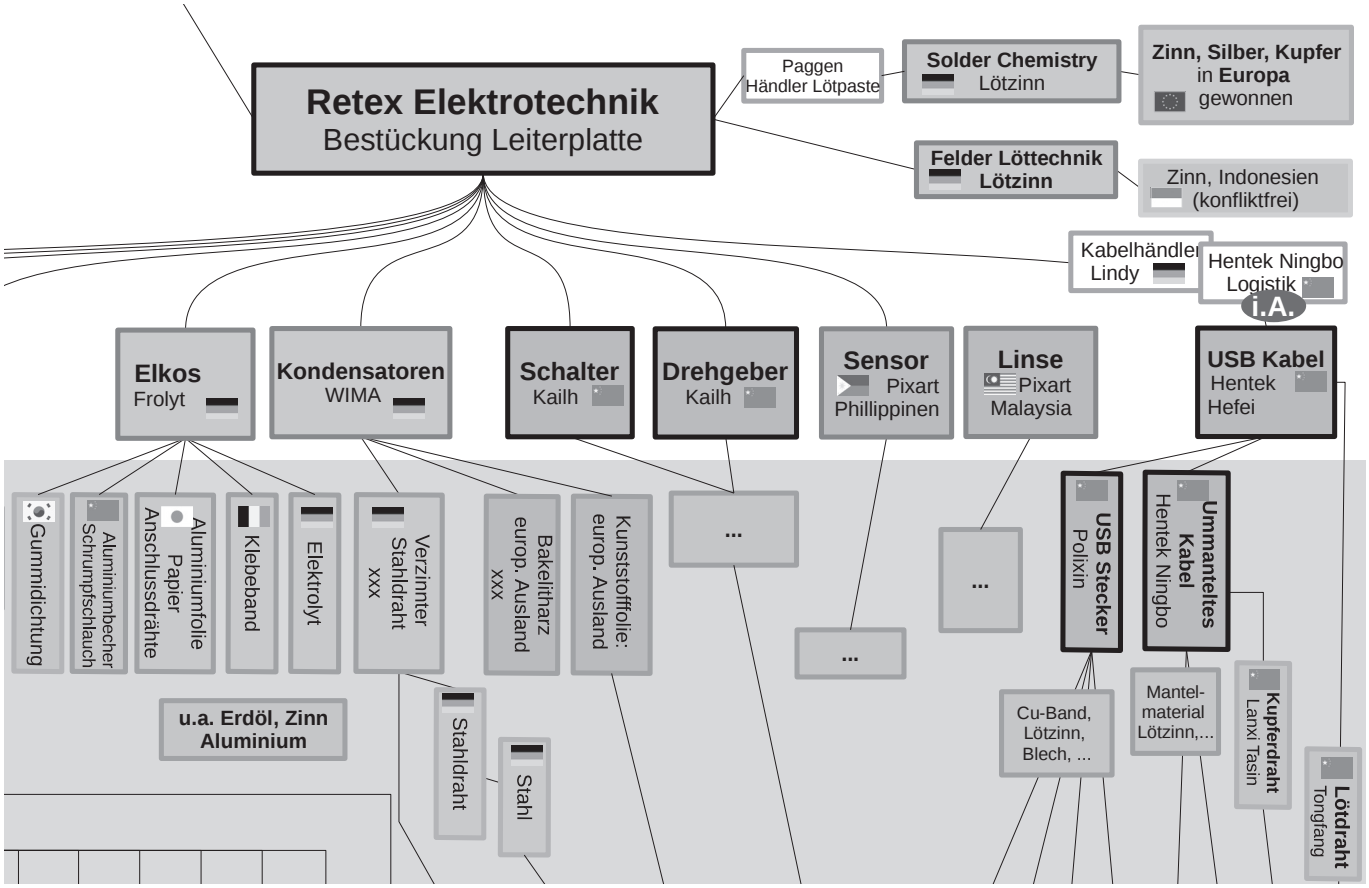


Abbildung 3: Ausschnitt aus der Lieferkette von Nager IT [20]

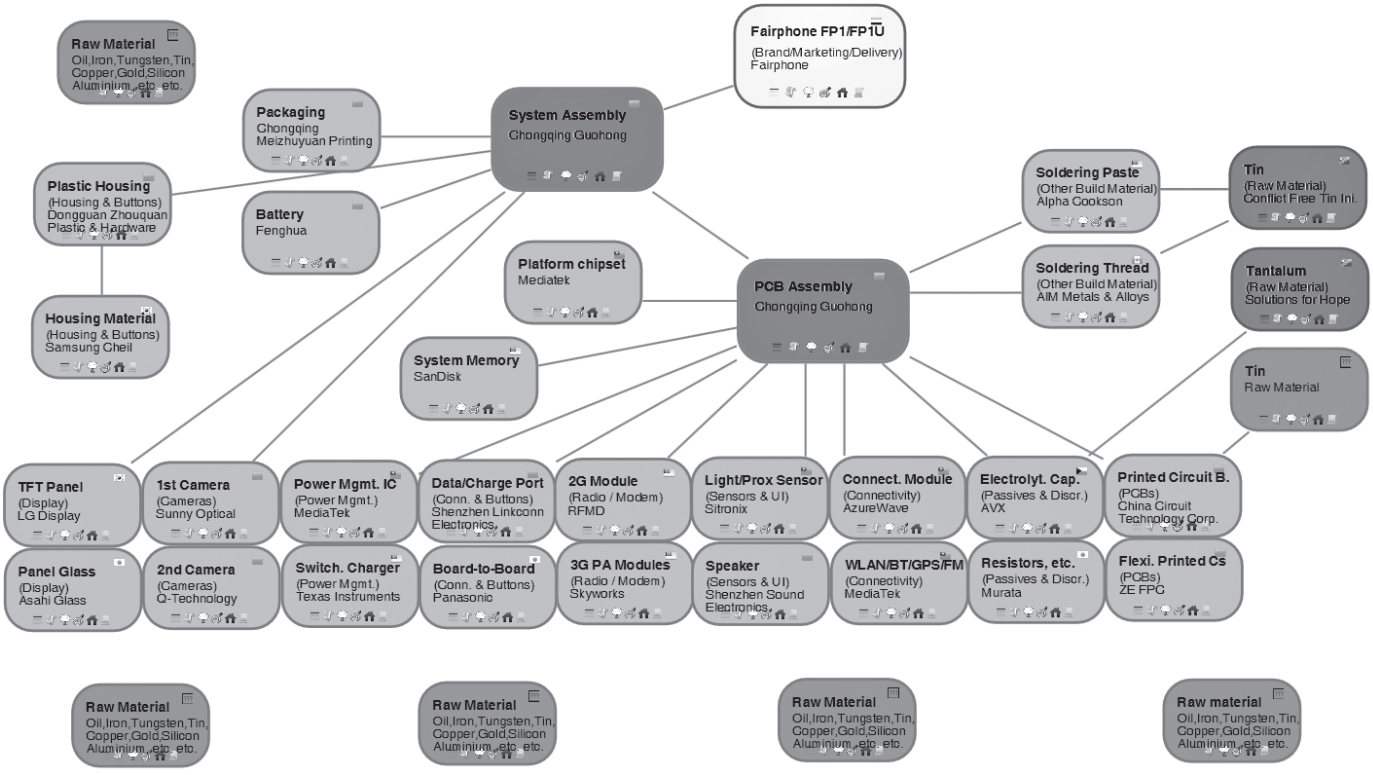


Abbildung 4: Versuch einer Nachbildung der Lieferkette des Fairphone

Alternative auswählt, möchte *Fairphone* dort etwas verändern (und hoffentlich verbessern), wo die Bedingungen bekanntermaßen schlecht sind.

Abbildung 5: Zwei unterschiedliche Ansätze von Fairness. Folie aus dem FIfF-Vortrag "Wanted! Faire Computer". Man kann uns übrigens einladen zu solchen Vorträgen, einfach eine Mail an fairit@fiff.de schicken.

Mit diesem Ansatz wird bei *Fairphone* stets mehr im grau-blauen Bereich bleiben als beim grünen *Nager IT*. Da müssen sich die Konsumenten also selbst überlegen, welche Form von Fairness ihnen wichtiger ist: die absolute Fairness von *Nager IT* oder die eher entwicklungs-orientierte Fairness von *Fairphone*. Andererseits: wer muss sich schon entscheiden zwischen einer Maus und einem Handy?

Es bleibt interessant zu beobachten, wie sich die Projekte *Nager IT* und *Fairphone* entwickeln und wieweit sie es schaffen, trotz geringem Budget und kleiner Auflage Dinge in Sachen Fairness zu schaffen, die Konzerne wie Logitech oder Samsung aus der Werbekasse bezahlen und aufgrund ihrer Marktmacht viel leichter umsetzen könnten. Aber die wollen nicht.

Dieser Text ist eine aktualisierte und redigierte Version von [29].

Referenzen

[1] http://www.fairphone.com/

[2] Sebastian Jekutsch: „Fairphone: Zu viel versprochen. Eine Bilanz", Blog Faire Computer , Jan. 2014, http://blog.faire-computer.de/fairphone-zu-viel-versprochen-eine-bilanz/

[3] Bas van Abel: „Our next steps with Guohong, the manufacturer of the first Fairphone", Fairphone Blog, Nov. 2014, http://www.fairphone.com/2014/11/25/our-next-steps-with-guohong-manufacturer-of-first-fairphone/

[4] Bas van Abel: „Next chapter in Fairphone's strategy: Outlook for 2015", Fairphone Blog, Nov. 2014, http://www.fairphone.com/2014/11/04/next-chapter-in-fairphones-strategy-outlook-for-2015/

[5] Annelie Evermann: „The ICT sector in the spotlight. Leverage of public procurement decisions on working conditions in the supply chain", Electronics Watch, Okt. 2014, http://electronicswatch.org/the-ict-sector-in-the-spotlight_723519.pdf

[6] Laura Gerritsen: „Research trip: Visiting tin, tantalum and tungsten mines", Fairphone Blog, Okt. 2014, http://www.fairphone.com/2014/10/02/research-trip-visiting-tin-tantalum-and-tungsten-mines/

[7] Laura Gerritsen: „The search for responsibly sourced gold for the Fairphone", Fairphone Blog, März 2015, http://www.fairphone.com/2015/03/11/the-search-for-responsibly-sourced-gold-for-the-fairphone/

[8] Fairphone B.V.: „The Cost Breakdown of the First Fairphone", Sept. 2013, http://www.fairphone.com/wp-content/uploads/2013/09/Fairphone_Cost_Breakdown_and_Key_Sept2013.pdf

[9] Sebastian Jekutsch: „Helden bei Foxconn", Blog Faire Computer, Juni 2014, http://blog.faire-computer.de/helden-bei-foxconn/

[10] TAOS: „A'Hong – Chongqing Guohong Technology Development Co. Ltd., Summary Audit Report", in Fairphone B.V.: „Made with Care: Social Assessment Program", Dez. 2013, https://www.fairphone.com/wp-content/uploads/2013/12/Fairphone-Made-with-Care-Social-Assessment-Program.pdf

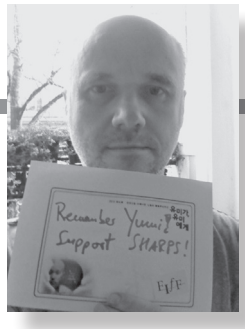
[11] Fairphone B.V.: „List of suppliers for First Edition Fairphone (FP1 & FP1U)", Juli 2014, http://www.fairphone.com/wp-content/uploads/2014/07/Fairphone-List-of-Suppliers_July2014.pdf

[12] Hewlett-Packard Development Company L.P.: „HP 2013 Living Progress Report: HP suppliers", 2013, http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=c03728062

[13] Hewlett-Packard Development Company L.P.: „HP 2013 Living Progress Report: Audit findings", 2014, www8.hp.com/us/en/hp-information/global-citizenship/society/auditresults.html

[14] Hewlett-Packard Development Company L.P.: „HP 2013 Living Progress Report: HP list of smelters", 2013, http://h20195.www2.hp.com/v2/getpdf.aspx/c03722457.pdf

[15] U.S. Securities and Exchange Commission: HEWLETT PACKARD CO (Filer) CIK: 0000047217, Filing Detail, Form SD, http://www.sec.gov/Archives/edgar/data/47217/000110465914042006/a14-13437_1sd.htm



Sebastian Jekutsch

Sebastian Jekutsch ist Autor im *blog.faire-computer.de* und aktiv in der AG Faire Computer des FIfF e. V. Er lebt in Hamburg und arbeitet bei einem Hafenbetrieb in der Softwarequalitätssicherung. Kontakt: *sj@fiff.de*

[16] Apple Inc.: „A detailed list of our suppliers and final assembly facilities“, Feb 2015, https://www.apple.com/supplier-responsibility/our-suppliers/
[17] Apple Inc.: „Supplier Responsibility: 2014 Progress Report“, Feb. 2015, https://www.apple.com/supplier-responsibility/pdf/Apple_SR_2014_Progress_Report.pdf
[18] Fair Labor Association (FLA): „Foxconn Investigation Report“, März 2012, http://www.fairlabor.org/report/foxconn-investigation-report. FLA: „Second Foxconn Verification Status Report“, Mai 2013, http://www.fairlabor.org/report/2013-foxconn-remediation-verification. FLA:“Final Foxconn Verification Status Report“, Dez. 2013, http://www.fairlabor.org/report/final-foxconn-verification-status-report
[19] Apple Inc.: „Quarterly Smelter List“, Feb. 2015, https://www.apple.com/supplier-responsibility/pdf/Apple_Smelter_List_2015.pdf
[20] U.S. Securities and Exchange Commission: APPLE INC (Filer) CIK: 0000320193, Filing Detail, Form SD, http://www.sec.gov/Archives/edgar/data/320193/000119312514217311/d729300dsd.htm
[21] Samsung Electronics: „2014 Samsung Electronics Sustainability Report: Supplier Compliance“, 2014, http://www.samsung.com/us/aboutsamsung/sustainability/sustainabilityreports/download/2014/7_Material_Issues_Supplier_Compliance.pdf
[22] Samsung Electronics: „Sustainability: Conflict Materials, Mineral Sourcing“, http://www.samsung.com/us/aboutsamsung/sustainability/suppliers/conflictminerals/
[23] Sebastian Jekutsch: „Kaufempfehlung Apple“, Blog Faire Computer, März 2014, http://blog.faire-computer.de/kaufempfehlung-apple/
[24] IHS siehe https://technology.ihs.com/teardowns, Chipworks siehe http://www.chipworks.com/en/technical-competitive-analysis/teardown-reports, iFixit siehe https://www.ifixit.com/Teardown
[25] https://www.nager-it.de/
[26] Nager IT: Lieferkette, Jan. 2015, https://www.nager-it.de/static/pdf/lieferkette.pdf
[27] Lebensland: „Supply Chain Editor“, Nov. 2014, http://lebensland.de/Wordpress/blog/2014/11/06/lieferketten-editor/
[28] Nager IT, Facebook, https://de-de.facebook.com/pages/nager-it/250437861762129
[29] Sebastian Jekutsch: „Fairphone bald fair?“, Blog Faire Computer Dez. 2014, http://blog.faire-computer.de/fairphone-bald-fair/
[30] Fairphone Design-a-Day Idea #3, http://designaday.fairphone-open.com/community-3/

Das FIfF verleiht 2015 wieder den

FIfF-Studienpreis

für herausragende Abschlussarbeiten aus dem Bereich Informatik und Gesellschaft.

Wir wollen damit Studierende sowie Wissenschaftlerinnen und Wissenschaftler in der Qualifikationsphase zur fundierten und differenzierten Auseinandersetzung mit den gesellschaftlichen Auswirkungen der Informatik ermutigen.

Das FIfF möchte mit der Einrichtung dieses Studienpreises herausragende Leistungen des wissenschaftlichen Nachwuchses in diesem Bereich würdigen und die Aufmerksamkeit der Öffentlichkeit auf das Thema der Arbeit sowie die besonderen Leistungen der Autorinnen und Autoren lenken.

Wir laden dazu ein, geeignete Arbeiten bis 31. Mai 2015 einzureichen.

Das Preisgeld beträgt:

1. Preis: 333 €
2. Preis: 222 €
3. Preis: 111 €

Es können Qualifikationsarbeiten (Bachelor-, Master-, Diplomarbeiten oder Dissertationen) eingereicht werden, die in den letzten zwei Jahren vor Nominierungsschluss abgeschlossen wurden. Die Ausschreibung bezieht sich zwar schwerpunktartig auf Abschlussarbeiten in Informatik, jedoch wird auch zur Einreichung thematisch einschlägiger Arbeiten anderer Fachgebiete ausdrücklich eingeladen.

FIfF-Geschäftsstelle
– Studienpreis 2015 –
Goetheplatz 4, 28203 Bremen
oder (vorzugsweise) per E-Mail an *studienpreis@fiff.de*.
Weitere Details unter *http://www.fiff.de/studienpreis.*

Der Preis wird in einer Feierstunde im Rahmen der 31. FIfF-Konferenz 2015 verliehen, die vom 6. bis 8. November an der Friedrich-Alexander-Universität in Erlangen stattfindet.

Nazir Peroz

IT-Entwicklung an den afghanischen Universitäten

Engagement im Bereich IT für die höhere Bildung in Afghanistan

Afghanistan ist ein Land, das in den vergangenen zwei Jahrzehnten stark unter den Auswirkungen von Krieg und Bürgerkrieg zu leiden hatte. Immer noch dominieren heute Bilder und Nachrichten von Terroranschlägen und Zerstörung die Berichterstattung in den Medien, und es entsteht der Eindruck, dass der Wiederaufbau des Landes immer wieder zurückgeworfen wird. Dennoch findet in großem Rahmen ziviles Engagement in Afghanistan statt, welches vielerorts Früchte trägt.

Das Zentrum für internationale und interkulturelle Kommunikation (ZiiK) der Technischen Universität Berlin (TU Berlin) ist bereits seit 2001[1] am Aufbau akademischer Strukturen im Bereich Informationstechnologie (IT) aktiv. Mit Finanzierung des Auswärtigen Amts und gefördert durch den DAAD wurden im Rahmen dieser Projekte z. B. fünf IT-Center an großen Universitäten Afghanistans errichtet sowie eine Vielzahl von Informatikern (Bachelor, Master, PhD) und IT-Fachkräften (IT-Administratoren, Webmaster, IT-Dozenten etc.) sowohl vor Ort in Afghanistan als auch an der TU Berlin ausgebildet.

Strategisches Ziel aller Aktivitäten des ZiiK in Afghanistan ist der Aufbau eines sicheren und nachhaltigen IT-Versorgungssystems im Bereich höhere Bildung im ganzen Land. So wurden bereits IT-Strukturen an den Universitäten Kabul, Herat, Balkh, Nangarhar, Qandahar, Khost und Kunar sowie an der Politechnischen Universität Kabul, der Erziehungswissenschaftlichen Universität Kabul sowie in der IT-Abteilung des Ministeriums für höhere Bildung (MoHE) geschaffen.

Die inhaltlichen Schwerpunkte des ZiiK der TU Berlin liegen im Aufbau von IT-Infrastruktur und IT-Ausbildung, in der Modernisierung der Verwaltungsstrukturen sowie in der IT-Sicherheit. Im Einzelnen wurden seit 2002 bis heute hierzu folgende Maßnahmen durchgeführt:

1. Analyse und Evaluation der Situation vor Ort
2. Entwicklung und Erweiterung einer nationalen IT-Strategie
3. Aufbau von IT-Infrastruktur
4. Bedarfsorientierte IT-Aus- und Weiterbildung
5. Ernennung von IT-Verantwortlichen und Multiplikatoren
6. Jährliche IT-Konferenz in Kabul

Abbildung 1: Analyse der Situation 2002, Fotos ZiiK

1. Analyse und Evaluation der Situation vor Ort

Im Rahmen der ersten DAAD-Delegation im März 2002 wurde die Situation der akademischen Strukturen der Universität Kabul analysiert. Im September 2002 reiste ein sechsköpfiges Informatiker-Team von der TU Berlin nach Kabul, um die Situation der IT-Strukturen vor Ort zu evaluieren und einen Vorschlag zum Aufbau der afghanischen Hochschulen im Bereich IT/Computer Science zu erarbeiten. In den Jahren 2004, 2005, 2010 und 2012 wurden ähnliche Analysen an den Universitäten Herat, Balkh, Nangarhar und Qandahar durchgeführt.

2. Entwicklung und Erweiterung der nationalen IT-Strategie

Auf Grundlage der Analyseergebnisse von 2002 hat das Team des ZiiK eine nationale IT-Strategie für den Bereich höhere Bildung in Afghanistan entwickelt. Diese wurde 2003 in Berlin im Rahmen einer internationalen IT-Konferenz vorgestellt, an der auch die Minister für höhere Bildung, Bildung und Kommunikation aus Afghanistan sowie acht Präsidenten afghanischer Universitäten teilnahmen. Die Konferenz hatte das Ziel, die Kooperation der afghanischen Hochschulen miteinander und mit internationalen Partnerländern bezüglich des IT-Einsatzes für Prozesse in Lehre, Forschung und Verwaltung zu fördern.

Abbildung 2: Planungsteam des ZiiK

Die Strategie von 2003 wurde in den Jahren 2005 und 2008 in Zusammenarbeit mit der IT-Abteilung des MoHE erweitert und jeweils im Rahmen der IT-Konferenzen vorgestellt. Auf Initiative des afghanischen Ministers für Höhere Bildung erarbeitete das ZiiK zusammen mit den Teilnehmern eines Alumni-Programms

für Computer-Science-Dozenten aus verschiedenen afghanischen Universitäten einen aktualisierten IT-Strategieplan und legte dem MoHE im September 2012 einen Vorschlag vor.

3. Aufbau von IT-Infrastruktur

Mit der Errichtung des IT-Centers an der Universität Kabul (ITCK) hat das Team des ZiiK im Jahr 2003 ein sichtbares und greifbares Beispiel für den Aufbau einer nachhaltigen und sicheren IT-Versorgung für den universitären Betrieb geschaffen.

Nach dem Vorbild des ITCK wurden später weitere IT-Center an den Universitäten Herat (ITCH), Nangarhar (ITCN), Balkh (ITCB) und Qandahar (ITCQ) errichtet. Zu diesen IT-Centern gehören jeweils PC-Pools mit ca. 50 bis 90 PCs, Serverräume, Administratoren- und Tutorenbüros sowie Konferenzräume und PC-Werkstätten.

Abbildung 3: IT-Center der Universität Kabul, März 2003

Abbildung 4: Feierliche Eröffnung des IT-Centers der Universität Qandahar, Februar 2014

Neben den zentralen IT-Centern wurden an der Deutsch-Abteilung und an den Fakultäten für Wirtschaft und Computer Science der Universität Kabul, an der Deutsch-Abteilung und der Fakultät Computer Science der Universität Herat sowie an der Universität Balkh und in der IT-Abteilung des MoHE bedarfsorientiert PC-Pools errichtet. Die Fakultäten Computer Science an den Universitäten Kabul und Herat erhielten je eine Fachbibliothek. Aus Gründen der Sicherheit, der Nachhaltigkeit und auch, um Lizenzkosten zu sparen, wurde fast ausschließlich Open-Source-Software eingesetzt. Seit 2007 ermöglichen PC-Werkstätten an den Universitäten Kabul, Herat und Balkh eine zeitnahe Reparatur sowie ein umweltbewusstes Recycling von wiederverwendbarer PC-Hardware.

4. Bedarfsorientierte IT-Aus- und Weiterbildung

Ziel der Aus- und Weiterbildungsprogramme des ZiiK war und ist es einerseits, Hochschulangehörigen IT-Grundkenntnisse zu vermitteln. Darüber hinaus wurden junge Studierende und Dozenten als qualifiziertes und akademisches Personal für die Lehre im Bereich Computer Science und für den Betrieb der IT-Center aus- und weitergebildet.

Allein bis heute wurden so mehr als 7.000 Dozenten, Angestellte und Studierende mit den Grundlagen der IT vertraut gemacht. Die Universitäten Kabul, Herat, Nangarhar, Balkh, Qandahar und die IT-Abteilung des MoHE verfügen inzwischen über qualifiziertes Personal (IT-Techniker, IT-Administratoren, IT-Webmaster) und bilden selbst weitere Studierende als Multiplikatoren aus. Für die Weiterbildung der IT-Administratoren steht ein Team aus ZiiK-Mitarbeitern online bereit, um bei komplizierten technischen Fragen weiterzuhelfen.

Abbildung 5: IT-Ausbildung

Abbildung 6: Teilnehmer der 3. Generation des Computer-Science-Masterprogramms an der TU Berlin

Für die akademische Ausbildung sorgen die Fakultäten für Computer Science an den Universitäten Kabul, Herat, Balkh und Nangarhar und an der Politechnischen Universität Kabul. Zu diesem Zweck hat das Team des ZiiK der TU Berlin ein IT-Curriculum entwickelt. Teil dieses IT-Curriculums ist eine Bachelor-Ausbildung in Computer Science, die vor Ort an den afghanischen Universitäten durchgeführt wird.

Um den afghanischen Wissenschaftlern zum Anschluss an die internationale *scientific community* zu verhelfen, wurde ein spezielles Masterprogramm für afghanische Dozenten für den Bereich Computer Science an der TU Berlin entwickelt und umgesetzt. Ziel dieses Programms ist es, bedarfsorientiertes Wissen zu vermitteln und die Teilnehmer zu Multiplikatoren auszubilden und sie damit in die Lage zu versetzen, an ihren Heimatuniversitäten IT-Strukturen aufzubauen.

Die ersten beiden Durchgänge dieses Masterprogramms für Computer Science wurden in den Jahren 2010 und 2013 an der TU Berlin abgeschlossen. Seitdem verfügt die Universität Kabul über 14 Masterabsolventen, die Universität Herat über 11, die Politechnische Universität Kabul über 5, die Universität Nangarhar über 5, die Universität Balkh und die Universität Qandahar über jeweils 3. Derzeit studieren weitere 25 Masterstudierende von neun afghanischen Universitäten an der TU Berlin.

5. Ernennung von IT-Verantwortlichen und Koordinierung der Projekte

Auf Initiative des ZiiK wurde 2004 eine IT-Abteilung am MoHE zur Koordinierung der nationalen und internationalen IT-Projekte gegründet. Auf Grundlage dieses Modells wurden ähnliche Strukturen an den Universitäten Kabul, Herat, Balkh, Nangarhar und Qandahar geschaffen. Hierzu wurde von Beginn an Personal wie IT-Manager, IT-Administratoren, IT-Techniker, Tutoren etc. zunächst an der TU Berlin und später in Afghanistan unter Leitung des ZiiK-Teams der TU Berlin ausgebildet. Dieses Personal sorgt für den Betrieb der IT-Center und der PC-Pools an den Universitäten und am MoHE.

Die Verantwortung für das ITCK wurde im Sinne eines *Afghan Ownership* im Jahr 2012 an die Leitung der Universität Kabul übergeben.

Ferner wurde ein IT-Board gegründet, das im Jahr 2012 offiziell vom MoHE berufen wurde. Es ist allen IT-Strukturen übergeordnet und hat die Aufgabe, eine Bedarfsplanung durchzuführen und nachhaltige IT-Strukturen aufzubauen.

Zudem wurde im Rahmen der 7. IT-Konferenz im Jahr 2011 eine Gesellschaft für IT nach dem Vorbild der deutschen Gesellschaft für Informatik gegründet.

6. Jährliche IT-Konferenz in Kabul

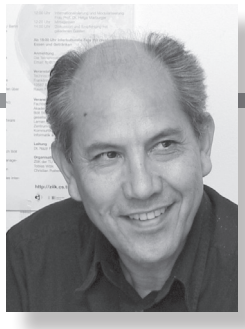
Das ZiiK organisierte 2014 in Zusammenarbeit mit dem MoHE in Kabul die zehnte in der Reihe von jährlichen Konferenzen zum Thema IT in der höheren Bildung in Afghanistan. Die jüngste Veranstaltung beschäftigte sich mit der „Entwicklung der IT an den afghanischen Hochschulen“ und fand vom 16. bis 18. Dezember 2014 in Kabul statt.

Abb. 7: IT-Konferenz in Kabul

Unter den Gästen der Konferenz waren Vertreter afghanischer Ministerien, des Parlaments, internationaler Botschaften in Kabul sowie Präsidenten von staatlichen und privaten afghanischen Universitäten, IT-Berater der afghanischen Universitäten, Informatik-Masterabsolventen der TU Berlin, weitere Informatik-Dozenten, Studierende und Experten auf dem Gebiet der IT/Computer Science sowie internationale Gäste wie Vertreter der Weltbank, von staatlichen Behörden, NGOs und anderen Universitäten. Insgesamt nahmen an der Konferenz mehr als 150 Personen teil.

Der Höhepunkt des zweiten Tages war die Videobotschaft von S.E. Dr. Ashraf Ghani, Präsident der Islamischen Republik Afghanistan, der den Stellenwert der Förderung von IT-Experten und Fachkräften in und für Afghanistan im Allgemeinen und das Engagement Deutschlands in diesem Zusammenhang im Besonderen hervorhob.

Auf der Konferenz wurden durch viele Redebeiträge und Vorträge die noch bestehenden Defizite und Schwierigkeiten in diesem Bereich in Afghanistan deutlich. Trotz der erfolgreichen Umsetzung vieler IT-Projekte an den Universitäten fehlt es immer noch oft an einer stabilen Stromversorgung, entsprechend



Nazir Peroz

Dr. **Nazir Peroz** ist Leiter des Zentrums für internationale und interkulturelle Kommunikation (ZiiK) der TU Berlin. Er leitet die Arbeitsgruppe „Informatik und Entwicklungsländer“ an der Fakultät für Elektrotechnik und Informatik.
Mehr Infos unter: http://ziik.tu-berlin.de

ausgestatteten Gebäuden für die Nutzung von IT, IT-Center, ausreichender Internetbandbreite, PC-Pools für Universitätsangehörige und Ausstattung für die Hochschulverwaltungen. Ferner gibt es an vielen Universitäten noch keine Computer-Science-Fakultäten.

7. Ausblick

Mit dem bisherigen Engagement in Afghanistan im Bereich IT/Computer Science hat das ZiiK der TU Berlin erfolgreich Basis-Strukturen für eine solide und nachhaltige IT-Versorgung geschaffen.

Durch die rasante Ausbreitung der IT in allen Bereichen des privaten und öffentlichen Lebens in Afghanistan entsteht ein großer Bedarf an neuen Berufen wie z. B. Informatikern, Systemelektronikern, Softwareentwicklern, IT-Projektmanagern, Webdesignern, System- und Netzwerkadministratoren, IT-Beratern, Datenbankentwicklern, Dozenten und Lehrern.

Um die geschaffenen Strukturen weiter auszubauen und den wachsenden Bedarf an IT-Expertise in Afghanistan zu decken, sollen daher vor allem Sonderprogramme für IT-Aus- und Weiterbildungen für Mitarbeiter der Universitätsverwaltungen und andere Hochschulangehörige durchgeführt sowie die Modernisierung der Verwaltung und die Gründung von IT-Abteilungen vorangetrieben und IT-Beauftragte an den Hochschulen ernannt werden.

Vor diesem Hintergrund und auf Basis des nationalen Strategieplans[2] des MoHE wird das ZiiK seine Aktivitäten 2015 weiter fortsetzen und sich auch im Rahmen der beginnenden Transformationsdekade durch gezielte Maßnahmen darauf konzentrieren, den Aufbau einer sicheren, integrierten und funktionierenden IT-Versorgung im Bereich höhere Bildung weiterhin nachhaltig voranzubringen.

Zu den Maßnahmen der kommenden Dekade zählen neben der Weiterführung der akademischen Ausbildung in Form von Master- und PhD-Programmen ebenso ein Ausbildungsprogramm für IT-Fachpersonal für die vom ZiiK der TU Berlin errichteten IT-Center an den Universitäten Kabul, Herat, Balkh, Nangarhar und Qandahar. Weitere zentrale Projekte, in denen sich das ZiiK engagiert, sind der Aufbau eines stabilen und sicheren Hochschulnetzes (Afghanistan Research and Education Network, AfgREN), die IT-gestützte Modernisierung der Verwaltung (Higher Education Management Information System, HEMIS) und die Entwicklung von IT-Curricula sowie die Beratung bei allen Fragen der IT-Sicherheit.

Anmerkungen

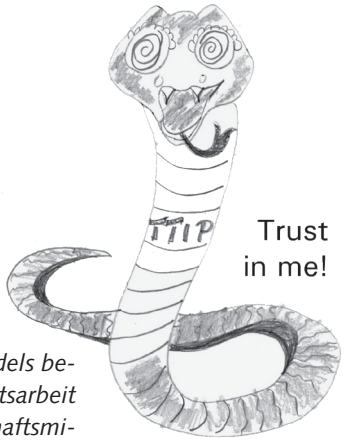
1 *Nazir Peroz: IT Structures for Higher Education in Afghanistan, Project Overview 2001-2014, ZiiK-Report, November 2014*

2 *Measures for the implementation of the National IT Strategy Plan for Higher Education in Afghanistan, November 2012*

Dagmar Boedicker

Die Büchse der Pandora

CETA, TTIP, TiSA



Bis jetzt dreht sich die öffentliche Kritik an TTIP und TiSA[1] *vor allem um die Schiedsgerichte und den Investorenschutz (ISDS)*[2] *sowie die Folgen des Abkommens für unsere Lebensmittelsicherheit und den Naturschutz. Das lenkt von anderen wichtigen Themen ab, wie der öffentlichen Beschaffung, der Kultur und dem Datenschutz. – Es sind aber Schwerpunkte für uns als FIfF e. V., deshalb möchte ich sie kurz beleuchten.*
Ich bitte um Nachsicht, wenn das keine leichte Lektüre ist. Transparenz auf dem Gebiet des Freihandels bedeutet entweder Hunderte oder Tausende von Seiten, meist in englischer Sprache, oder Öffentlichkeitsarbeit in Gestalt trivialer Frage-und-Antwort-Listen. Oder, wie mir ein Mitarbeiter des bayerischen Wirtschaftsministeriums erklärte: Sie müssen eben Vertrauen in unsere Bürokratie und in Ihre Abgeordneten haben.

Datenschutz

Eine Analyse der Generaldirektion für Außenpolitik[3] fasst wesentliche Kritikpunkte der Zivilgesellschaft an TTIP so zusammen:

1. Die Lobby mächtiger IKT-Konzerne wird den profitträchtigen Datenhandel nicht einschränken lassen.
2. ACTA[4] könnte *durch die Hintertür* wieder einziehen.

Laut dieser Analyse verteidigt die EU-Kommission (EK) das Abkommen, indem sie sich zum ersten Punkt auf die geltende Regelung des Datenschutzes zwischen USA und EU durch Verträge wie *Safe Harbor* beruft. Safe Harbor ist ein Abkommen zur Übermittlung von Daten zwischen der EU und den USA, bei dem die Unternehmen in den USA selbst erklären können, dass ihre Verarbeitung der Daten mit europäischen Standards vergleichbar ist. Ob das stimmt, wird in der Regel nicht geprüft. Safe Harbor wurde nach den Snowden-Enthüllungen von vielen Datenschützern, von der G29[5] und sogar der letzten Justiz-Kommissarin Viviane Reding in Frage gestellt. Das Europäische Parlament forderte seine Aussetzung.[6]

Zum zweiten Punkt bestreitet die Kommission, dass ACTA-Regelungen in TTIP eingehen können. Nachdem der Entwurf eines Dokuments durchgesickert war, musste die EK zugeben, dass es doch eine Verbindung zwischen ACTA und einer Auflage für Internet-Service-Anbieter gegeben habe. Sie sei später aber entfallen.

Karel de Gucht, EU-Handelskommissar und Verhandlungsbeauftragter in der letzten EK, der es gegenüber dem Europäischen Parlament (EP) und der Öffentlichkeit mit der Wahrheit nicht immer so genau genommen hat[7], behauptete, dass Datenschutz nicht Inhalt der Verhandlungen sei.[8]

Die EU-Kommission hat im Juli 2013 von den Mitgliedstaaten das Mandat erhalten, mit den USA über TTIP zu verhandeln – auf ausdrücklichen Wunsch Deutschlands.[9] Nichtregierungs-Organisationen und Abgeordnete im europäischen und in nationalen Parlamenten mussten beharrlich gegen die Geheimhaltung der zugehörigen Dokumente protestieren, bis die Kommission nach ersten Lecks schließlich Unterlagen veröffentlichte. Ein weiteres Mandat an die EK zum Freihandelsabkommen TiSA datiert vom März 2013, auch darüber wurde bisher wenig veröffentlich. Inzwischen gibt es ein Leck: von *Associated Whistleblowers Press (AWP).* Die darin veröffentlichten Informationen stehen im Widerspruch zur wiederholten Behauptung der EK, über Datenschutz werde nicht verhandelt (siehe Kasten zu TiSA).[10]

Was können TTIP/TiSA beim Datenschutz anrichten?

Die Regierungen der Mitgliedstaaten und die Kommission möchten den Eindruck erwecken, dass Datenschutz und der Schutz der Privatsphäre gar nicht berührt sind.[15] Selbst Gutgläubige, die das für TTIP ernst nehmen wollen, müssen zu grübeln beginnen, wenn es um TiSA geht. Ein internationaler Handel mit Dienstleistungen lässt sich wohl kaum auf den anonymen Friseurbesuch reduzieren. Es geht beispielsweise um Finanzdienstleistungen, um den Handel mit geistigem Eigentum, Lizenzen, um IKT und die Cloud, Logistik, Reisen, ... Ohne Vernetzung und Datenaustausch geht bei Google, Apple und Co. nun mal nichts.

Jan Philipp Albrecht, ständiger Berichterstatter des EP-Innen- und Justizausschusses (LIBE)[16] für TTIP, schrieb:[17]

> *„Auf amerikanischer Seite wird dagegen alles versucht, um den europäischen Datenschutz zu unterlaufen. Dafür werden sogar neue Lobbyverbände gegründet - zum Beispiel die von der US-Großkanzlei Hogan Lovells koordinierte ‚Coalition for Privacy and Free Trade'. Sie werben seit mehr als einem Jahr für ‚Interoperabilität' zwischen den europäischen und den amerikanischen Regeln zum Datenschutz. Damit ist eine gegenseitige Anerkennung der jeweiligen Regeln auf beiden Seiten des Atlantiks gemeint."*

und:

> *„Es ist daher zu befürchten, dass TTIP am Ende zumindest in abgeschwächter Form Regelungen enthalten wird, die unsere Datenschutzstandards unterlaufen. [...] Falls das TTIP-Abkommen beschlossen werden sollte, bevor die EU-Datenschutzreform in Kraft tritt, können sich Unternehmen aus den USA unter Umständen auf die berüchtigten Klauseln zum Investorenschutz berufen und gegen die neuen und schärferen europäischen Datenschutzregeln vor intransparenten Schiedsgerichten klagen."*[18]

TiSA

Das *Trade in Services Agreement (TiSA)* ist das geplante Nachfolgeabkommen zu *GATS (General Agreement on Trade in Services)* der WTO. Im GATS waren Dienstleistungen aufgeführt, auf deren Liberalisierung sich die Vertragspartner geeinigt hatten (Positivliste).[11] TiSA listet dagegen alle Dienstleistungen in einer Negativliste, deren Liberalisierung ein Staat beschränken oder ausschließen darf. Was bedeutet: alle in dieser Liste nicht aufgeführten Dienstleistungen sind zu liberalisieren.

Gemäß einem Briefing vom 17. Dezember 2014 von Professor Jane Kelsey, Faculty of Law, University of Auckland, New Zealand und Dr. Burcu Kilic, Public Citizen, Washington D.C., USA., haben die USA folgende Ziele: [12]

- kommerzielle Interessen der US-amerikanischen Dienstleistungs-Industrie, besonders des IKT-Sektors, mit grenzüberschreitenden Angeboten fördern. Allgemein: Schutz der US-Position im Wettbewerb und der technischen und IPR[13]-Monopole;
- Datenbestände zum Nutzen von Regierung, transnationalen Konzernen (TNKs) und Dritten konsolidieren, sowohl für kommerzielle Zwecke als auch für die nationale Sicherheit;
- Regulierung durch Regierungen vermeiden oder minimieren, die globale Dienstleistungs-Unternehmen in ihren Aktivitäten und Gewinnen beeinträchtigt;
- ungehinderten Datenverkehr über die Grenzen garantieren.

Die Verhandlungen über TiSA begannen im März 2013 und sind – wie die über TTIP – geheim. Der Vorschlag der USA über E-Commerce, Technologietransfer, grenzüberschreitenden Datenverkehr und Netzneutralität wurde laut Kelsey/Kilic am 25. April 2014 eingereicht. Für fünf Jahre nach In-Kraft-Treten des Abkommens oder nach einem Scheitern der Verhandlungen sollen die Dokumente geheim bleiben.

50 Staaten verhandeln über TiSA.[14] Die Volksrepublik China, Indien und Russland sind nicht dabei – warum wohl? Ich vermute, dass sie sich nicht über den Tisch ziehen lassen möchten und das auch nicht nötig haben.

In seinem Entwurf einer Stellungnahme fordert der LIBE-Ausschuss[19] Transparenz bei den Verhandlungen und ruft den Handelsausschuss des EP auf, Vorschläge in seine Resolution zu übernehmen wie:

- eine Menschenrechtsklausel in alle Handelsabkommen mit Drittstaaten, damit die Grundrechte-Standards der EU ausnahmslos garantiert sind;
- die Warnung, dass angesichts der EP-Resolution vom März 2014 über das NSA-Überwachungsprogramm die Zustimmung des Parlaments zu TTIP gefährdet sei, wenn solche anlasslosen Überwachungsaktivitäten nicht vollständig beendet und eine angemessene Regelung für den Schutz der Privatsphäre von europäischen Bürgerinnen und Bürgern gefunden würde;
- einen Verweis auf Art. XIV des GATS[20] und seine Datenschutz-Regelungen;
- die Forderung, in TTIP eine Klausel über europäischen Datenschutz ohne Ausnahme oder Konsistenzforderungen mit einzelnen TTIP-Abschnitten einzubringen;
- eine Erinnerung an die geltenden Regelungen zur Übermittlung an Drittstaaten und an die Möglichkeit, die Übertragung personenbezogener Daten in Drittstaaten zu untersagen, wenn diese die EU-Standards nicht angemessen erfüllen;
- eine Erinnerung daran, dass rechtliche Entscheidungen über Grundrechts-Konflikte nur von regulären Gerichten getroffen werden dürfen und Regelungen zu ISDS die Demokratie gefährden und den Rechtsweg verlegen können;[21]
- große Besorgnis über den TiSA-Entwurf, *„durch den sämtliche Vorschriften und Schutzbestimmungen der EU für die Übermittlung personenbezogener Daten an Drittländer vollkommen untergraben würden"*.

Im Vorschlag der USA über E-Commerce (und in den strittigen Freihandelsabkommen) spielen *forced localization*[22] und *geographic indicators (GI)* eine wichtige Rolle. Ralf Bendrath erklärt die *Lokalisierung* in einem Artikel für *Eurozine* als Angriff der USA auf die Drittstaaten-Regelungen im europäischen Datenschutz:

> *„From the US side, the debate is now being used to attack European rules and limitations for the transfer of personal data to third countries. They throw terms like ‚Schengen network', ‚cloud computing' and the third country rules of the EU Data Protection Directive into the same category, which they term ‚localization'."* [23]

Nach Bendraths Einschätzung handelt es sich dabei um ein Ablenkungsmanöver, mit dem die Regelung ausgehebelt werden soll, die für die Übermittlung von Daten in Drittstaaten ein angemessenes Datenschutzniveau fordert. Routing und Datenverarbeitung seien aber zu trennen.

Europäische Werte

Auch die Artikel-29-Gruppe (G29) hat eine Erklärung[24] verabschiedet, die das Grundrecht auf Datenschutz bekräftigt und ausschließt, dass personenbezogene Daten einschließlich Metadaten als Ware behandelt werden dürfen. Die Autoren berufen sich auf europäische Werte wie Meinungsfreiheit, Nicht-Diskriminierung und Datenschutz, die miteinander und mit den Sicherheitserfordernissen in Einklang gebracht werden müssen. Sie verlangen die Unterordnung der kommerziellen und technischen Möglichkeiten oder Überwachungswünsche unter die sozial, ethisch, rechtlich und vernünftig akzeptablen Standards für die Menschen. Diese Datenschutz-Anforderungen müsse die digitale Wirtschaft erfüllen, um vertrauenswürdig zu sein.

Zur Überwachung aus Gründen der Sicherheit stellt die G29 fest, dass die geheime, massive und unterschiedslose Überwachung weder mit EU-Recht vereinbar noch ethisch akzeptabel ist. Die Datenschützer lehnen eine Vorratsdatenspeicherung ab, sofern sie nicht verhältnismäßig und mit wirkungsvollen Sicherungen auf das erforderliche Maß begrenzt ist. Mehrfach weisen sie in der Stellungnahme darauf hin, dass ihre Kritik sich auf private wie staatliche Akteure bezieht, und verlangen, dass das europäische Datenschutzniveau nicht verwässert werden darf durch *„bilaterale oder internationale Abkommen, auch nicht solche über den Handel mit Waren oder Dienstleistungen mit Drittstaaten."*[25]

Öffentliche Beschaffung von sozial und ökologisch verträglicher IT

Die Zustände bei der Produktion von IT-Geräten sind katastrophal, sowohl bei Rohstoffgewinnung und Arbeitsbedingungen als auch bei Entsorgung und Recycling. Seit Jahren fordern nationale und internationale Organisationen wie *Good Electronics, China Labor Watch, Germanwatch, WEED*[26], die FIfF-*AG Faire Computer* und viele andere, dass sich das ändert. Wir Verbraucher sind weniger kritisch, weil wir Computer weder essen noch sie uns (bisher) direkt auf der Haut sitzen. Wir sind bequem. – Leider gibt es auch kaum faire Alternativen. Außerdem sind die Produktionsbedingungen globalisiert, kompliziert und intransparent, was es den Herstellern erleichtert, sich aus der Verantwortung zu stehlen.

Dagmar Boedicker

Dagmar Boedicker ist Journalistin und technische Redakteurin und hat Politikwissenschaft studiert. Sie ist seit langem Mitglied des FIfF, war Vorstandsmitglied und stellvertretende Vorsitzende, und ist Redakteurin der *FIfF-Kommunikation*.

Was tun, wenn individuelle und industrielle Käufer wenig Bereitschaft zur Verantwortung zeigen? Als Wähler und Finanziers können wir immerhin den Hebel der öffentlichen Beschaffung nutzen. Noch! Es gibt rechtliche Grundlagen für die öffentliche Vergabe von Beschaffungsaufträgen, und sie bestehen nicht nur aus Anforderungen an Preise und die diskriminierungsfreie internationale Vergabe. Kommunen, Bund und Länder können soziale und Umweltstandards anlegen.

Was können TTIP/TiSA anrichten?

Ein wesentliches Element von Freihandelsabkommen ist es, den *„Bruch der legitimen Erwartungen von Investoren"*[27] zu verhindern, der als indirekte Enteignung betrachtet wird. – Bisherige Auflagen für die öffentliche Beschaffung würden gemäß TTIP zwar voraussichtlich gültig bleiben. Eine Verbesserung der Kriterien könnte sich aber als nachträgliche Verschlechterung der Investitionsaussichten beurteilen lassen: KO-Kriterium, wenn ein Freihandelsabkommen mit entsprechendem Investorenschutz in Kraft wäre –, und damit KO-Kriterium für Forderungen nach einer sozialverträglicheren und ökologischeren öffentlichen Beschaffung, wenn Entscheidungen vor internationalen Schiedsgerichten landen.

Einen Ausblick liefert CETA[28].

> *„Das CETA-Kapitel über das staatliche Auftragswesen (Government Procurement) erfasst den Einkauf von Waren, Dienstleistungen und Bauleistungen durch Beschaffungsstellen der EU, des Bundes, der Bundesländer und der Gemeinden. […] Im handelspolitischen Ausschuss des EU-Rats bekannten sich Kommissionsvertreter zu dem Ziel, einen integrierten Beschaffungsmarkt im Sinne eines* ‚Buy Transatlantic' *zu etablieren."*[29]

Thomas Fritz kommt für *Campact* zur Einschätzung, dass auf der Basis von CETA einige Klauseln

> *„… ermöglichen könnten, die Auftragsvergabe zumindest an ökologische Kriterien zu koppeln. […] Sozialstandards wie die Einhaltung von Tarifverträgen fehlen jedoch. […] Laut Artikel IX.6 dürfen Beschaffungsstellen technische Spezifizierungen vorschreiben, die u. a. dem Schutz natürlicher Ressourcen oder der Umwelt dienen. Sozialstandards aber fehlen auch hier."*[30]

Campacts Zusammenfassung:

> *„Erhält TTIP ähnliche Vergaberegeln wie CETA, entsteht ein vertiefter transatlantischer Beschaffungsmarkt, der öffentliche Aufträge privaten Unternehmen beiderseits des Atlantiks leichter zugänglich macht. Durch die Fixierung von Schwellenwerten, ab denen transatlantisch ausgeschrieben werden muss, verliert die öffentliche Hand Spielräume für eine autonome Einkaufspolitik. Sozial-ökologische Reformen des Beschaffungswesens wie Vergabe und Tariftreuegesetze könnten mit TTIP-Regeln in Konflikt geraten."*[31]

Umweltschützer auf der ganzen Welt lehnen TTIP und CETA ab, sie kommen zum Ergebnis, dass sie die TNK dieser Welt in die Lage versetzen werden, auf Menschen und Natur in den Vertragsstaaten, aber auch in anderen Ländern, einen inakzeptablen Druck auszuüben. Auch die internationalen Verteidiger der Bürgerrechte sehen keinen Nutzen in den Abkommen sondern vielmehr eine Bedrohung der Demokratie.

CETA

Die EK hat das Verhandlungs-Mandat auch erhalten für das *Canada-European Union Comprehensive Economic and Trade Agreement*, das Freihandels-Abkommen zwischen Kanada und der EU. Die Verhandlungen waren geheim. Der konsolidierte Text[32] wurde am 26. September 2014 von der EK veröffentlicht. Zur Zeit findet die *Rechtsförmlichkeitsprüfung* statt, im Juli 2016 vermutlich das Zustimmungsverfahren im EP. Eine Ratifizierung durch die EU ist Ende 2018 zu erwarten.[33] Das Abkommen gilt als vergleichbar mit TTIP und wird häufig als *Blaupause* für TTIP bezeichnet. Es regelt die weitgehende Liberalisierung beispielsweise von Dienstleistungen (auch Finanz-Dienstleistungen), die Öffnung des IKT-Markts und der öffentlichen Beschaffung. Für internationale Ausschreibungen soll der Schwellenwert auf 200.000 Euro[34] gesenkt werden, die USA fordern einen Schwellenwert von 20.000.[35]

Kultur

Kultur bereichert, inspiriert, verbindet oder wirkt kontrovers. Die Kunst ist frei. Wir haben aber gelernt: Handeln lässt sich nicht nur mit dem, was normale Menschen als Güter oder Waren betrachten. In den Augen derjenigen, die die Welt als Markt wahrnehmen, gehören dazu auch *commodities,* deren warenförmige Gestalt uns nicht auf Anhieb auffällt: Vorlesungen, Fernsehprogramme, Kinofilme, Bücher oder Zeitungen, geistiges Eigentum. ACTA hat uns das deutlich vor Augen geführt. Nach gehörigem zivilgesellschaftlichen Druck lehnte das Europäische Parlament ACTA ab.

Für diejenigen, die die Welt als Markt betrachten, ist Kultur vor allem *content.* Handelbar beispielsweise im E-Commerce, und dafür sollen Regelungen gelten, die die Diskriminierung ausländischer Anbieter untersagen *(Non-Discriminatory Treatment).* CETA nimmt die *Kulturwirtschaft* Kanadas von den Regelungen zur Nicht-Diskriminierung aus, für die EU sind aber nur *audiovisuelle Dienste* ausgenommen:

> *„For the EU, the Section on Establishment of Investments and Section on Non-Discriminatory Treatment do not apply to measures with respect to Audiovisual services. For Canada, the Section on Establishment of Investments and Section on Non-Discriminatory Treatment do not apply to measures with respect to cultural industries."* (Artikel X.1, 3.)[36]

Was können TTIP/TiSA in unserer Kultur anrichten?

Wenn wir davon ausgehen, dass CETA eine Blaupause für TTIP und TiSA darstellt, wäre europäische Kultur also weitgehend Freiwild auf dem Markt. Gegen protektionistische Maßnahmen

der Mitgliedstaaten könnten Konzerne mit dem Argument vorgehen, dass sie Investitionen behindern und/oder diskriminierend wirken.

Ein **Rechtsgutachten**[37] kommt zu dem Schluss, dass nationale Parlamente über *CETA* (und vergleichbare Freihandelsabkommen) mit entscheiden:

> *„Das CETA umfasst eine Vielzahl von Regelungsbereichen: Niederlassungsfreiheit, Zuwanderung, Bildungsanerkennung, Datenschutz, Urheberrecht, Finanzdienstleistungen, Investitionsschutz. Es ist deshalb zu prüfen, ob der EU für die Regelung der jeweiligen Sachbereiche im CETA eine Kompetenz zukommt. Wenn der Union für Teile des Abkommens die Verbandskompetenz fehlt, müsste ein sog. ‚gemischtes Abkommen' geschlossen werden, an dem auch die Mitgliedstaaten als Vertragsparteien beteiligt und nach ihren jeweiligen nationalen Vorgaben in den Ratifikationsprozess einbezogen werden."*[38]

Was die Zuständigkeit im Bereich der Kultur betrifft, gilt für Deutschland:

> *„Die Vorgaben für die Verwaltungsverfahren der Länder (Art. 84 GG) und die Tatsache, dass […] die Zustimmung der Länder dann notwendig ist, wenn – wie hier bspw. durch die Eingriffe in die Kultur- und Rundfunkhoheit der Länder – durch das Abkommen ausschließliche Länderkompetenzen berührt werden, führen dazu, dass das CETA ohne eine Zustimmung des Bundesrates nicht zustande kommen darf.*[39]

Zusammenfassung

Wie das Europäische Parlament ACTA abgelehnt hat, so wird es auch beim Abschluss von CETA, TTIP, TiSA eine entscheidende Rolle spielen. Auch die nationalen Parlamente haben voraussichtlich ein Mitspracherecht, weil es sich um *gemischte* Abkommen handelt. Das sind Abkommen mit gemischter Zuständigkeit zwischen der EU, ihren Mitgliedstaaten und/oder deren nationalen Institutionen, in einem föderal organisierten Land wie Deutschland beispielsweise dem Bundesrat. Damit würden sich wahrscheinlich in Teilbereichen Nachverhandlungen durchsetzen lassen.

Fischer-Lescano/Horst beurteilen die Vereinbarkeit von CETA mit europäischem und deutschem Recht skeptisch, es ist wahrscheinlich, dass auch TTIP/TiSA nicht unserem Recht entsprechen. Verträge zwischen Nationen oder supranationalen Organisationen wie der EU sind aber nachträglich schwer aus der Welt zu schaffen. Grundsätzlich ist es höchst fraglich, ob diese Abkommen für uns als Bürgerinnen und Bürger Vorteile bringen.[40] Wohlstandsversprechen über TTIP sind bei genauer Betrachtung übertrieben[41], die jährlich erwartete Höhe liegt unterhalb des statistischen Irrtums. Versprechungen von mehr Arbeitsplätzen sind zweifelhaft.[42] Die Nachteile niedrigerer Preise haben sich herumgesprochen (Geiz ist *nicht* geil!), und wir sollten uns fragen, ob Wachstum das ist, was dieser Planet braucht, auch nur verkraften kann. Braucht er nicht vielmehr Nachhaltigkeit? Verteilungsgerechtigkeit? Den Abbau von Barrieren gegenüber Importen aus den Ländern, deren nationale Wirtschaften wir mit unseren Exporten schädigen …? Wer braucht eine Ausweitung des Handels beispielsweise mit Finanzdienstleistungen oder Lebensmitteln im globalen Maßstab?

Sinn und Zweck von Freihandelsabkommen ist die Wirtschaftsförderung, Deutschland und die EU haben bereits Hunderte abgeschlossen. Solange diese Abkommen nicht für die Verbesserung und Angleichung von Arbeits- und Umweltstandards sorgen, nützen sie eben *nicht* allen, es sind gerade die Unterschiede, die sie attraktiv für Unternehmen machen. Die Vorteile sind in den letzten Jahrzehnten vorwiegend großen, internationalen Konzernen zu Gute gekommen, kleine und mittlere Unternehmen profitieren weniger. BDI-Präsident Ulrich Grillo hat TTIP auf dem Weltwirtschaftsforum in Davos als *kostenloses Konjunkturprogramm* bezeichnet;[43] kostenlos ist es aber nur für TNK, weil sie große Teile ihrer Kosten erfolgreich externalisiert haben: zu Lasten der Umwelt, der Beschäftigten und der Steuerzahler.

Wenn wir also keinen Nutzen in diesen Freihandelsabkommen sehen, sollten wir kaum geduldig abwarten, ob unsere Vertreter ihnen zustimmen möchten, nur weil große Konzerne und das Kapital sie für sinnvoll halten. Wenn Freihandelsabkommen, dann solche, die höhere Standards für den Schutz von Menschen und Natur vereinbaren. Andere braucht die Welt nicht.

Anmerkungen

1 *Trade in Services Agreement (TiSA)*
2 *Investor-to-State Dispute Settlement (ISDS)*
3 *Autoren: Marika Armanovica/Roberto Bendini, DG Expo, SQM 03 Y 54, Rue Wiertz 60, B-1047 Brussels; http://www.europarl.europa.eu/RegData/etudes/IDAN/2014/536404/EXPO_IDA(2014)536404_EN.pdf, S. 16 (abgerufen 6.1.15)*
4 *Anti-Counterfeiting Trade Agreement*
5 *unabhängige Arbeitsgruppe der europäischen Datenschutzbeauftragten auf Basis des Artikel 29 der Datenschutz-Richtlinie 95/46/EC*
6 *am 12. März 2014*
7 *Das zeigt sich beim Vergleich seiner Angaben zu Inhalten der Verhandlungsrunden mit den nachträglich veröffentlichten Berichten der EK.*
8 *http://europa.eu/rapid/press-release_SPEECH-13-720_en.htm?locale=en (abgerufen 1.2.15)*
9 *Dieter Janecek MdB, Sprecher für Wirtschaftspolitik der Fraktion Bündnis 90/Die Grünen, auf einer Tagung der Evangelischen Akademie Tutzing am 7.7.2015 (wie auch andere Referenten)*
10 *TiSA leak, veröffentlicht am 17.12.2014 von Associated Whistleblowers press (AWP) https://data.awp.is/filtrala/2014/12/17/19.html (abgerufen 14.1.15)*
11 *Vortrag von Prof. Dr. Christoph Scherrer, Leiter Fachgebiet Globalisierung und Politik, Universität Kassel, am 7.2.2015 in der Evangelischen Akademie Tutzing*
12 *Associated Whistleblowers Press*
13 *Intellectual Property Rights (geistige Eigentumsrechte)*
14 *SZ vom 18.12.2014, S. 24*
15 *http://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/stellungnahme-zu-grundrechten-und-transparenz-bei-ttip-vorgelegt.html (abgerufen 28.1.15)*
16 *zuständig für Grundrechte-Einschätzungen*
17 *am 21.5.2014*

18 *http://www.boell.de/de/2014/05/07/datenschutz-ist-nicht-verhandelbar (abgerufen 28.1.15)*
19 *vom 6.1.2015, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-546.558+01+DOC+PDF+V0//DE (abgerufen 1.2.15)*
20 *General Agreement on Trade in Services der WTO*
21 *„Denn die Union weist die Aufgabe der Rechtsprechung den mitgliedstaatlichen Gerichten (sofern sie Unionsrecht anwenden) und dem EuGH zu." www.mehr-demokratie.de/fileadmin/pdf/CETA-Rechtsgutachten.pdf, S. 9 (abgerufen 28.1.15)*
22 *ich würde das als Lokalisierungspflicht übersetzen*
23 *Trading away privacy. TTIP, TiSA and European data protection. http://www.eurozine.com/articles/2014-12-19-bendrath-en.html (abgerufen 6.1.15)*
24 *am 25.11.2014: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp227_en.pdf (abgerufen 1.2.15)*
25 *„13. The European level of protection of personal data should not be eroded, wholly or in part, by bilateral or international agreements, including agreements on trade in goods or services with third countries." wp227_en.pdf, S. 4*
26 *Weltwirtschaft, Ökologie & Entwicklung – WEED e. V.*
27 *blog.campact.de/wp-content/uploads/2014/09/Campact_TTIP_vor_Ort.pdf, S. 10 (abgerufen 28.1.15)*
28 *Comprehensive Economic and Trade Agreement, Handelsabkommen zwischen der EU und Kanada*
29 *Campact_TTIP_vor_Ort.pdf, S. 15*
30 *Campact_TTIP_vor_Ort.pdf, S. 16*
31 *Campact_TTIP_vor_Ort.pdf, S. 17*
32 *tradoc_152806CETA.pdf, http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/ceta-aecg/text-texte/10.aspx?lang=eng (abgerufen 23.1.15)*
33 *Vortrag von Dr. Bernd Diekmann, Leiter Referat USA, Kanada, Mexiko, Bundesministerium für Wirtschaft und Energie, am 7.2.2015 in der Evangelischen Akademie Tutzing*
34 *eigentlich IWF-Sonderziehungsrechte (mit Währungsmix aus Dollar, Euro, Pfund und Yen)*
35 *Vortrag von Prof. Dr. Christoph Scherrer, Leiter Fachgebiet Globalisierung und Politik, Universität Kassel, am 7.2.2015 in der Evangelischen Akademie Tutzing*
36 *tradoc_152806CETA.pdf, S. 147*
37 *CETA-Rechtsgutachten vom Oktober 2014 von Prof. Dr. Andreas Fischer-Lescano, LL.M. (EUI), und Johan Horst, LL.M. (Georgetown), Zentrum für europäische Rechtspolitik (ZERP) an der Universität Bremen, www.eesc.europa.eu/resources/docs/04-gutachten_ceta_171014_final-fischer-lescano.pdf (abgerufen 23.1.15)*
38 *CETA-Rechtsgutachten. S. 5*
39 *CETA-Rechtsgutachten, S. 33*
40 *Kopper, Christopher: Die Entwicklung des europäischen Binnenmarktes und die Einheitliche Europäische Akte von 1986. In: Themenportal Europäische Geschichte (2011): „Der Cecchini-Bericht suggerierte eine exakte Prognostizierbarkeit der wirtschaftlichen Wohlfahrtseffekte, die sich in der Retrospektive als unangemessen erwies. Ökonomen kamen in empirischen ex-post-Untersuchungen in einer kurzfristigen Betrachtung zu erheblich niedrigeren Wachstumsraten von 0,5 bis 1,5 Prozent, die durch den Binnenmarkt induziert wurden." http://www.europa.clio-online.de/2011/Article=497 (abgerufen 23.1.15)*
41 *Selbst das wirtschaftsfreundliche IFO-Institut prognostiziert für die Mitgliedstaaten über die nächsten 15 Jahre (!) nur ein potenzielles Wachstum des Einkommens pro Kopf von 2,12%: „The long-run level of real per capita income would change by 2.12% in the EU, by 2.68% in the US, and by -0.03% in the rest of the world relative to the status quo." cesifo1_wp5150.pdf (abstract), http://www.cesifo-group.de/ifoHome/infoservice/News/2015/01/news-20150119-cesifo-wp-5150.html (abgerufen 23.1.15)*
42 *1,8 Millionen europäische Arbeitsplätze hatte schon der Cecchini-Bericht für die Vollendung des Binnenmarkts versprochen. /www.europa-union.de/fileadmin/files_ebd/PDF-Dateien/EBD-EUD-Studie-Vital-endg.pdf (abgerufen 23.1.15)*
43 *Deutschlandfunk, 21.1.15*

Dagmar Boedicker

Aus der Regionalgruppe München

Sylvia und Kai auf der Security Conference der Piraten

Am 24. und 25. Januar veranstaltete die Piratenpartei eine Konferenz in München, bei der es um internationale Sicherheitspolitik, kritische Infrastrukturen sowie die Mythen und Fakten des Terrorismus ging. Für Journalistinnen und Journalisten gab es am Sonntag außerdem einen ganztägigen Workshop, in dem sie erfuhren, wie sie sich und ihre Quellen schützen können.

Das Programm: Security Politics since Snowden

Weil ich zu spät von der Konferenz erfahren hatte, habe ich den ersten Teil des Programms verpasst, mit Stefan Körner, Dr. Mark Daniel Jaeger und Dr. Rob Imre. Zum Vortrag von Yvonne Hofstetter kam ich dann gerade rechtzeitig, um ein einigermaßen deprimierendes Fazit über *Key technologies for security measures* zu hören. Angelika Beer und Peter Matthiesen referierten anschließend über *Terrorist threats and the fight against them in the century of digital revolution* und *The comprehensive approach*, zwei kurze Vorträge, die am Sonntag fortgesetzt wurden. Diese Fortsetzung habe ich nicht gehört, denn der folgende Vortrag von Stephane Koch, *From attribution to appropriation, the brave new world of manipulation,* war so anregend, dass ich den Sonntag dann für seinen Workshop reserviert habe. Vorher gab es am Samstagnachmittag aber noch einen Vortrag über Gas-Infrastruktur und Versorgungssicherheit in Deutschland und Europa, und dann das FIfF-Highlight, Sylvias und Kais Vortrag zum *Cyberpeace*.

Am Sonntag setzten Angelika Beer und Peter Matthiesen ihre Referate fort, außerdem trug Enno Lenze zur *Current Situation in Iraq* vor, und Peter Finkelgruen zu *Conflict dynamics in the Middle East.* Was mir sehr gut an der Konferenz-Planung gefallen hat, war ausreichend Zeit für Diskussionen, bei denen auch deutlich wurde, wie vielfältig das Publikum war: ein breites Spektrum, das von der Friedensbewegung zu Beschäftigten in der IT-Sicherheit reichte.

Cyperpeace – a campaign for a peaceful internet

Sylvia und Kai beteten nicht etwa einfach die Forderungen der Kampagne (http://cyberpeace.fiff.de/Kampagne/Home) herunter. Sie setzten Schwerpunkte bei den Forderungen Abrüstung, demokratische Kontrolle und regierungsunabhängige Cybersicherheits-Zentren und erläuterten ausführlich die Motivation des FIfF e. V. für die Kampagne. Vielleicht wäre eine etwas kürzere Fassung gut gewesen, um mehr Zeit für die Diskussion zu lassen, aber es gab einige Fragen und Beiträge, beispielsweise zur Vernetzung des FIfF mit anderen (internationalen) Organisationen. Außerdem hatten Sylvia und Kai in der anschließenden Podiumsdiskussion Gelegenheit, ihr Fachwissen zu zeigen und die Kompetenz des FIfF zu diesem Thema herauszustreichen.

Yvonne Hofstetter *Key Technologies*

Hofstetters Vortrag zu Schlüsseltechnologien und staatlicher Sicherheitsvorsorge skizzierte ein trauriges Bild. Deutschland und die Europäische Union sind Welten entfernt von Hofstetters Forderung, der Staat müsse das Internet als systemrelevante Infrastruktur grundrechtssicher garantieren und dabei der Menschenwürde als Grundkonzept der europäischen Verträge folgen. *Das* sei das Supergrundrecht! Die staatliche Verpflichtung in Europa kollidiere mit technischer Unfähigkeit, weil Europa seine technischen Fähigkeiten verloren habe, unter anderem wegen fehlendem Risikokapital. Bei der Sicherheits-Technik seien wir von den überlegenen USA abhängig, deren andere Rechtskultur betrachte aber den europäischen Grundrechtsschutz als Handelsbarriere. Sicherheitspolitik müsse den Primat vor Industriepolitik erhalten. Hofstetters Frage: Wie vernünftig ist es, wenn man nicht mehr in der Lage zur Verteidigung ist?

Quellenschutz und Sicherheit für Journalisten

Stephane Kochs Workshop am Sonntag war fantastisch, und eigentlich hab ich mich ein bisschen geärgert, weil wir eine so kleine Gruppe waren. Wissen die Journalisten in München etwa alle schon alles über Informations-Sicherheit? Das kann ich mir nicht vorstellen. Es hätte ihnen bestimmt nicht geschadet zu hören, was Koch über *Anonymous Communications, Data Security And Protection Of Sources for Journalists and NGOs* zu sagen, zeigen und erklären hatte.

Es war eine gut besuchte und hochinteressante Konferenz der Piraten. Die Vorträge gibts zum Nachhören und -sehen unter: *http://pirate-secon.org/index.php?id=12*.

vor*gänge* **– Zeitschrift für Bürgerrechte und Gesellschaftpolitik**

Geheimdienstliche Kommunikationsüberwachung außer Kontrolle

Am 6. Juni 2013 veröffentlichte die britische Zeitung *The Guardian* erstmals vertrauliche Informationen über ein US-amerikanisches Überwachungsprogramm, mit dem die Verbindungsdaten aller Telefonate gespeichert werden, die innerhalb, von und mit den Vereinigten Staaten geführt werden. Die Zeitung berief sich dabei auf eine ihr vorliegende Überwachungsanordnung, nach der die Firma *Verizon* (einer der größten Telefonanbieter der USA) diese Daten täglich an den Geheimdienst *National Security Agency* (NSA) zu übermitteln habe. Wenige Tage später veröffentlichten der Guardian und die *Washington Post* Informationen über einen direkten Zugang der NSA auf die Kundenserver großer amerikanischer Internetanbieter (Programm PRISM). Die NSA kann demnach auf die Kontaktdaten, Dokumente, E-Mails und Fotos aller Kunden dieser Anbieter zugreifen. Betroffen sind u. a. die Firmen Apple, Facebook, Google, Microsoft und Skype.

Mit diesen Veröffentlichungen begann das, was in den Medien mittlerweile als NSA-Überwachungsskandal bezeichnet wird. Schnell wurde bekannt, dass die Informationen aus der selben Quelle stammen, einer Sammlung geheimer Unterlagen der NSA, die Edward Snowden einigen Journalisten zugespielt hatte. Seitdem reißen die Enthüllungen aus den „Snowden-Dokumenten" kaum noch ab. Nahezu wöchentlich werden neue Details veröffentlicht, die verdeutlichen, wie umfassend, flächendeckend und perfide die geheimdienstliche Überwachungspraxis der NSA und ihrer Partnerdienste ist. Sie greifen die weltweiten Kommunikationsdaten auf den transatlantischen Glasfaserkabeln ab, lassen ganze Länder flächendeckend abhören und speichern die Inhalte aller dort stattfindenden Telefonate; sie kompromittieren technische Sicherheitsstandards beim Mobilfunk und der Verschlüsselung von Daten; sie fangen von Kunden bestellte IT-Geräte auf dem Versandweg ab und manipulie-

ren diese … Es besteht kein Zweifel, dass der NSA-Skandal die Maßstäbe dafür, in welchem Umfang staatliche Überwachungsaktivitäten heute denkbar und möglich sind und praktiziert werden, weit verschoben hat.

Die NSA-Überwachungsaffäre bildet den Ausgangspunkt für diese Ausgabe der **vor***gänge*. Alle Beiträge des Schwerpunkts beziehen sich mehr oder weniger intensiv auf die damit verbundenen Erkenntnisse. Dennoch ist dies kein Schwerpunkt zur Überwachung durch die NSA, zeigen wir nicht mit dem Finger auf Amerika. Wir richten den Blick vielmehr auf die Arbeit der deutschen Geheimdienste, allen voran den BND. Warum das? Zum einen arbeitete und arbeitet die NSA mit zahlreichen europäischen Geheimdiensten – allen voran natürlich dem britischen Government Communications Headquarter (GCHQ), aber auch dem Bundesnachrichtendienst (BND) – eng zusammen. Darüber hinaus sehen wir auch bei den hiesigen Geheimdiensten, besonders im Bereich der Telekommunikation (TK), eine Tendenz zur grenzenlosen Überwachung, erhebliche Rechtslücken und unzureichende Kontrollmechanismen. Bevor sich Deutschland auf internationaler Ebene glaubhaft für eine menschen- und grundrechtsorientierte Beschränkung der Überwachungsaktivitäten einsetzen kann, sind aus unserer Sicht noch zahlreiche Hausaufgaben zu erledigen. Diese zu benennen, ist Anliegen und Anspruch des aktuellen **vor***gänge*-Schwerpunkts.

aus dem Editorial der **vor***gänge Nr. 206/207 (Heft 2-3/2014) von Claudia Krieg und Sven Lüders*

Linus Neumann

Politische Lösungen für eine sichere Zukunft der Kommunikation

In ihren bisherigen Versuchen, die NSA-Spähaffäre aufzuklären, betreibt die Bundesregierung viel Heimlichtuerei: Zu den technischen Details der amerikanisch/britischen Abhörprogramme könne man nichts sagen; und sofern die Techniken doch bekannt sind (weil deutsche Behörden sie auch nutzen) will man aus Sicherheitsgründen keine Details verraten. Dabei ist die Telekommunikationsüberwachung der beste Beleg dafür, wie sich konspirative Überwachungstechnologien einer transparenten Kontrolle entziehen und tendenziell verselbständigen. Geheime Sicherheitstechnologien sind ein Sicherheitsrisiko, denn ihre Geheimhaltung macht sie selbst anfällig für Angriffe Dritter, die Lücken in den Überwachungssystemen ausnutzen können.

Linus Neumann skizziert in seinem Essay, woher eigentlich die Sicherheitslücken kommen, die Geheimdienste wie Kriminelle für ihre Angriffe auf vertrauliche Telekommunikationen nutzen. Für eine echte Sicherheit sei deshalb ein Wandel der Sicherheitskultur notwendig, der nicht die Geheimhaltung, sondern die öffentliche Kontrolle der zugrundeliegenden Technologien (und Verfahren) zum Leitbild macht. Neben den ganzen politischen wie rechtlichen Gründen für die öffentliche Kontrolle der Staatsgewalt sprechen nach seiner Auffassung auch technische Aspekte dafür, Sicherheit als Aufgabe der Öffentlichkeit zu verstehen und in deren Obhut zu stellen.

Mit der Massenüberwachung durch Geheimdienste und dem Bekanntwerden immer neuer, schwerwiegender IT-Sicherheitslücken steigt der Druck auf die Bundesregierung, wirksame Schutzmaßnahmen für sichere Kommunikation und Nutzung von Computern durch Bürger/innen und Wirtschaft zu ergreifen.

Dazu ist nötig zu verstehen, wie Sicherheitslücken zustande kommen und wie sie verhindert werden können. Aus diesem Verständnis heraus können die notwendigen politischen Weichenstellungen folgen, die weiter unten vorgestellt werden.

Wie entstehen Sicherheitslücken und welche Typen gibt es?

Der einfache Bug

Die große Mehrheit von Sicherheitslücken in heutigen Software-und Kommunikationssystemen entsteht durch simple Programmierfehler („Bugs“). Die komplexe Logik der Programme bildet sich in Millionen von Zeilen Programmcode ab, die von großen Teams geschrieben werden. Sie alle zu lesen und ihre gegenseitigen Abhängigkeiten und Referenzierungen vollständig zu durchdringen, ist Einzelpersonen kaum möglich. Einzelne Programmteile („Routinen“) der Software verlassen sich auf das korrekte Funktionieren anderer, bestimmte Vorbedingungen werden angenommen, aber an anderer Stelle nicht sichergestellt. So entstehen Bedingungen, die ein/e Angreifer/in durch vom Programm unerwartetes Verhalten auslösen, und so seine Integrität unterwandern kann. Häufig ist der notwendige „Fix“, also die Reparatur des Programms, nur das Löschen oder Hinzufügen einer einzelnen Zeile, wie der inzwischen berühmt gewordenen Zeile „goto fail;“ in *Apples* Implementierung der SSL-Verschlüsselung, die das gesamte Sicherheitsmodell in sich zusammenbrechen ließ.

Backdoors und „Bugdoors“

Oft werden in Programme, Anwendungen und Apps auch absichtliche Hintertüren eingebaut, die den Entwickler/innen oder staatlichen Stellen eine Möglichkeit des Fernzugriffs (also die Umgehung aller Sicherheitsmaßnahmen) bieten sollen. Da immer auch mit dem Entdecken solcher Backdoors gerechnet werden muss, werden diese oft so gestaltet, dass ihre absichtliche Platzierung glaubhaft abzustreiten ist. Äußerlich ähneln sie daher nicht selten versehentlichen Bugs (Programmierfehlern), was den schönen Begriff der „Bugdoor“ geprägt hat.

Absichtliche Design-Schwächen

Insbesondere in Kommunikationssystemen werden Angriffsflächen jedoch häufig schon spezifiziert (geplant), bevor überhaupt eine Zeile Programmcode geschrieben ist: Selbstverständlich ist jeder Telefonanbieter in der Lage, alle Telefonate aller Kund/innen abzuhören und selbstverständlich sind alle E-Mail-Anbieter in der Lage, alle E-Mails aller Kund/innen zu lesen. Das gilt natürlich ebenso für die Sicherheitsbehörden, mit denen der Anbieter kooperiert, wie für staatliche Stellen oder kriminelle Angreifer/innen, die den Anbieter unterwandern. Da die Massenüberwachung möglich ist, findet sie auch statt.

Doch das muss nicht so sein: Kommunikationssysteme, die ihre Nutzer/innen auch vor dem Zugriff durch den Mail- oder Telekommunikationsanbieter schützen, sind zwar möglich, aber ihre Verbreitung von keiner Regierung dieser Welt wirklich gewünscht. Zu groß ist die Sorge, allen Menschen ein nicht überwachbares Kommunikationsmittel zur Verfügung zu stellen und die eigenen und freundschaftlich verbundenen Geheimdienste in ihrer Überwachung zu beschränken.

Das System De-Mail, als „sichere Alternative zur E-Mail" beworben, ist hierfür das beste Beispiel: Nicht nur bietet es keine sichere Verschlüsselung, es wurde zudem unter Beteiligung der selben US-amerikanischen Firma entwickelt, die auch an der Entwicklung des Staatstrojaners beteiligt ist und in den USA einer der größten Zulieferer der NSA ist: der *Computer Sciences Corporation*, kurz CSC.

Sichere Kommunikation braucht politische Lösungen

Um eine verlässliche und sichere Kommunikation zu ermöglichen, müssen alle drei Arten von Sicherheitslücken eingedämmt werden: unabsichtliche Bugs, absichtliche Backdoors und schon im Design eingeplante Schwächen. Hierzu gibt es mehrere Ansätze, die eine Politik, die IT-Sicherheit und sichere Kommunikation fördern will, umsetzen sollte:

1) Open-Source-Software fördern

Das Finden von Bugs und Backdoors ist eine sehr mühselige Arbeit, die enorm erleichtert wird, wenn nicht erst das fertige Programm geprüft, sondern sein zugrundeliegender Programm-Quelltext gelesen werden kann. Nur bei einer Software, deren vollständiger Quelltext offen liegt, besteht überhaupt die Basis für ein Vertrauen in deren Integrität. Denn wie wir alle wissen, ist Vertrauen gut, aber Kontrolle besser. Genau diese öffentliche Kontrolle verweigern jedoch die meisten kommerziellen Anbieter, da sie das Abfließen ihrer Entwicklungen an die Konkurrenz fürchten: Wer den Quelltext hat, kann die Software weiterentwickeln, verbessern oder verändern. Das wäre zwar im Interesse der Allgemeinheit, nicht jedoch im Interesse des Anbieters.

Hier gilt es, einerseits kommerzielle Anreize zur Open-Source-Entwicklung zu bieten, andererseits entsprechende Bedingungen für die Anbieter von sicherheitsrelevanter Software zu setzen: Auch heute noch operieren sie größtenteils frei von jeglicher Haftung für ihr intransparentes Produkt, und somit ohne Anreiz zur nennenswerten Qualitätssicherung.

2) Den Schwarzmarkt trockenlegen

Wer mit seiner Fähigkeit zum Finden von Sicherheitslücken den Lebensunterhalt bestreiten möchte, dem bieten sich heute zwei Möglichkeiten:

Ein solides mittelständisches Auskommen hat, wer als Dienstleister/in Sicherheitsprüfungen bei Dienstanbietern und Software-Schmieden durchführt und sich im Anschluss an seine Untersuchung den bürokratischen und firmenpolitischen Diskussionen um die Behebung der entdeckten Probleme stellt.

Wer ethisch flexibler ist, dem winken auf dem Schwarzmarkt sechsstellige Beträge für das Finden von großen Sicherheitslücken in weit verbreiteter Software. Die fürstliche Entlohnung entschädigt für die Gewissensbisse, weil die entdeckte Lücke künftig nicht geschlossen, sondern von Kriminellen und/oder Geheimdiensten ausgenutzt wird. Letztere sind dabei die treibende Kraft hinter den hohen Preisen auf diesem moralisch verwerflichen Markt.

Hier gilt es, einen Riegel vorzuschieben: Die staatliche Subventionierung des Schwarzmarkts muss unterbunden und alle staatlichen Stellen müssen verpflichtet werden, beim Bekanntwerden von Sicherheitslücken kompromisslos auf ihre Beseitigung hinzuarbeiten – und nicht auf ihre Ausnutzung.

3) Eine offene Sicherheitskultur pflegen

Natürlich werden Sicherheitslücken nicht nur wegen kommerzieller Anreize entdeckt. Eine weltweite Community begeisterter Hacker, Nerds und Sicherheitsforscher/innen sucht, findet und

Linus Neumann

Linus Neumann ist Diplompsychologe und arbeitet bei einem Unternehmen zur IT-Sicherheit in Berlin. Er ist Mitglied des Chaos Computer Clubs und vertritt diesen als Sachverständiger. Darüber hinaus gehört er seit 2010 zur Redaktion von *netzpolitik.org* und erstellt gemeinsam mit Tim Pritlove den wöchentlichen Podcast *Logbuch: Netzpolitik.*

beseitigt Sicherheitslücken ohne direkte monetäre Kompensation. Namentliche Erwähnungen in „Security Bulletins“, die Nutzer/innen auf Lücken und erhältliche Updates hinweisen, sind oft der einzige Dank, der ihnen für ihre Dienste an der Gemeinschaft zuteil wird.

Immer beliebter wird daher das Ausloben von „Kopfgeld“ („Bug Bountys“) auf Sicherheitslücken in kritischer Open-Source-Software: Wer einen Fehler definierter Schwere findet, wird dafür entlohnt. Vom entstehenden Wettkampf der Forschenden profitiert die Allgemeinheit. Um dies zu stärken, könnte das Bundesamt für Sicherheit in der Informationstechnik (BSI) sich an der Finanzierung dieser „Bug Bountys“ beteiligen und so Open-Source-Software sicherer machen.

4) Eine unabhängige Sicherheitspolitik ermöglichen

Mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) verfügt die Bundesregierung über eine Institution, die aktuell viele Möglichkeiten ungenutzt lässt, auf den überfälligen Paradigmenwechsel in der IT-Sicherheit hinzuwirken. Dem Verantwortungsbereich des Innenministeriums unterliegend, kann das BSI in seinen Empfehlungen, Spezifizierungen und Zertifizierungen nie wirklich frei agieren. Das mit einer staatlichen Abhörschnittstelle versehene und zusammen mit einem NSA-Dienstleister entwickelte De-Mail-System ist mit Fug und Recht zur Blamage für das BSI geworden.

Solange das BSI dem Innenminister untersteht, ist trotz aller Lippenbekenntnisse nicht damit zu rechnen, dass dort künftig Spezifikationen ohne absichtliche Design-Schwächen entwickelt werden. Ein starkes, unabhängiges BSI mit unzweideutigem Sicherheitsauftrag – und zwar auch gegen staatliche Angreifer – ist der einzige Weg, das notwendige Vertrauen im Bereich der IT-Sicherheit aufzubauen und Sicherheitsversprechen auch halten zu können.

2008 formulierte das Bundesverfassungsgericht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, das so genannte Computergrundrecht. Bisher haben staatliche Stellen nur halbherzige und unglaubwürdige Schritte zu seiner Sicherung unternommen. Das schockierende Ausmaß der Snowden-Enthüllungen ist eine direkte Folge der bisherigen Politik und ein weiteres Warnsignal an die Bundesregierung, die Sicherheit der Bürgerinnen und Bürger in Sachen Computernutzung und Kommunikation nicht unnötig der vermeintlichen Sicherheit des Staates zu opfern.

CC BY SA

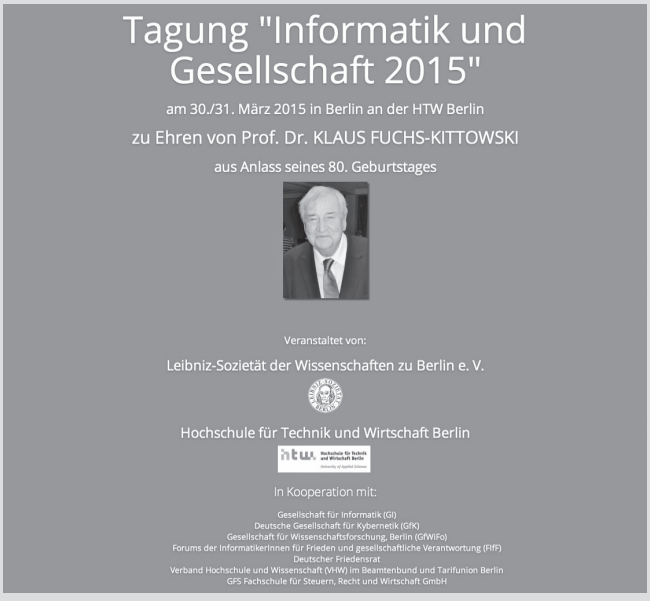
Dieser Artikel wurde zuerst bei der Heinrich-Böll-Stiftung und in **vor***gänge* – Zeitschrift für Bürgerrechte und Gesellschaftspolitik – *veröffentlicht. Der Nachdruck erfolgt mit freundlicher Genehmigung des Autors.*

FIfF e.V.

Wir gratulieren Klaus Fuchs-Kittowski zu seinem 80. Geburtstag.

Aus diesem Anlass fand am 30./31. März 2015 in Berlin die Tagung *Informatik und Gesellschaft 2015* statt, die von der Leibniz-Sozietät der Wissenschaften zu Berlin und der Hochschule für Technik und Wirtschaft Berlin veranstaltet wurde; das FIfF war einer der Kooperationspartner. An zwei Tagen wurden die Themen

- Information, Informatik, Gesellschaft
- Big Data und Datenschutz
- Industriearbeit 4.0
- Umwelt (-informatik) und Gesellschaft
- IKT – Arbeit und Gesellschaft
- Wissenschaftstheorie/-geschichte und Ethik
- Datenschutz und Datenausspähung
- Information und Big Data
- Methodologie der Informationssystemgestaltung
- Softwareentwicklung und der soziale Aspekt



behandelt und diskutiert. Ein Tagungsband ist in Vorbereitung.

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.

FIfF-Konferenz 2014

Begrüßung und Auftakt

Zusammenfassung des Vortrags von Hans-Jörg Kreowski

Dies ist die 30. Jahrestagung des FIfF, daher kann man auch kurz ein paar Reminiszenzen formulieren. Vor 30 Jahren hat die Berliner Regionalgruppe des FIfF hier wichtige Arbeit geleistet, hierbei ist sie aus der „Friedensinitiative Informatik" der TU Berlin hervorgegangen.

Die Friedensinitiative erstellte damals z. B. eine Broschüre und organisierte eine diesbezügliche Veranstaltung mit dem Thema „Informatik – zwischen Krieg und Krieg". Denn die Informatik hat ihre Wurzeln im 2. Weltkrieg und es bestand damals die Gefahr eines 3. Weltkrieges – diesmal mithilfe der Informationstechnologie. Die wesentliche Beteiligung der Informatik gilt leider auch für alle aktuellen und zukünftigen Kriege.

Es gab damals auch einen Hochschulfriedenstag, an dem keine normale Lehre, sondern Diskussionen, Filme und Vorträge statt-

fanden. Der Kanzler der TU wollte diesen Friedenstag jedoch verbieten, denn man könne ja unter dem Thema „Frieden“ keine ganze Universität vereinigen. Doch gerade Berlin stand unter dem Viermächte-Status, demnach war ausschließlich friedliche Forschung erlaubt, sodass der Kanzler sein Entscheidung zurücknehmen musste und der Tag stattfinden konnte. Daran sollte man sich beim Kampf um die Zivilklausel erinnern.

Die erste Vorsitzende des FIfF, Christiane Floyd, arbeitete auch an der TU. Kürzlich beschrieb sie im Vorwort zum neuen FIfF-Sammelband die Themen, die uns vor 30 Jahren wichtig waren:

- Rüstung und Informatik,
- Auswirkungen der Informatik auf die Arbeitswelt,
- Datenschutz.

Man sieht auch gleich, dass diese Bereiche nach wie vor relevant sind, wenn nicht sogar essentiell wichtiger, wie bei dem Beispiel der Kriegsroboter bzw. Killerdrohnen. Die Auswirkungen der Informatik sind nun natürlich nicht mehr auf die Arbeitswelt beschränkt, sondern erstrecken sich auf alle Lebensbereiche. Das ist ja keineswegs immer schlecht, aber mit großer Nutzung eröffnen sich eben auch neue Missbrauchsmöglichkeiten der Technik.

Der dritte Bereich, *Datenschutz*, ist ja mittlerweile überhaupt nicht mehr ausreichend benannt. Passender wäre vielleicht *Datensammelwut und Überwachungswahn in extremem Ausmaße*. Wir sehen uns ja der drohenden Abschaffung unserer Grundrechte gegenüber, von der informationellen Selbstbestimmung über das Telekommunikationsgeheimnis bis hin zur Privatsphäre sind alle allgemein und grundsätzlich beeinträchtigt, gerade von den Diensten.

Natürlich waren Programme wie Echelon bekannt, mit denen weltweit Daten ausgespäht werden sollten, aber jetzt hat die Situation ganz neue Größenordnungen erreicht. Dass britische und amerikanische Geheimdienste diesbezüglich zentrale Akteure sind, ist ja spätestens seit den Enthüllungen von Edward Snowden bzw. dem NSA-Skandal bekannt, doch auf dieser Konferenz soll gerade beleuchtet werden, wie die deutschen Dienste sich in dieser Sache verhalten, denn ihre Rolle ist mitnichten zu vernachlässigen.

Man muss auch die Zusammenhänge erwähnen; im Rahmen der Morde des Nationalsozialistischen Untergrundes (NSU) spielten die Dienste auch eine sehr dubiose Rolle. Es ist auch bekannt, dass deutsche Geheimdienste Informationen, die sie von hiesigen Flüchtlingen und Asylsuchenden bekommen, an die US-Amerikaner weitergeben, die auf dieser Grundlage illegale Drohnenmorde in anderen Ländern durchführen.

Die deutschen Dienste haben auch geholfen, großflächig Daten in Deutschland auszuleiten und an fremde Dienste weiterzugeben. Nun entschuldigt sich der Präsident des BND, dass in den entsprechenden Abhörprogrammen die „Deutschenfilter“ nicht funktioniert haben, dabei sollte man doch annehmen, dass Grundrechte für alle Menschen gelten, nicht nur für Deutsche.

Dem Eindruck nach „handeln die deutschen Geheimdienste verfassungswidrig, und verfassungswidrige Einrichtungen gehören verboten“. Mindestens aber muss die aktuelle demokratische „Kontrolle“ in eine echte Kontrolle verwandelt werden. Es kann nicht angehen, dass der parlamentarische NSA-Untersuchungsausschuss zum Teil vollständig geschwärzte Dokumente bekommt oder andere Dokumente überhaupt nicht. Teilweise können Zeugen nicht aussagen, aber genau zu diesem Thema werden wir in den nächsten zwei Tagen mehr hören.

Jedenfalls sollten gerade die InformatikerInnen ob dieser Entwicklungen sehr betroffen sein – allein schon als Bürger eines demokratischen Landes, aber auch, weil wir InformatikerInnen mit unserer Arbeit auch die technischen Grundlagen für die angesprochene Datensammelwut und den Überwachungswahn liefern.

Wir InformatikerInnen müssen also auch die Verantwortung übernehmen. Verantwortung ist hier im Sinne des Philosophen Hans Jonas und seiner Ethik für die technologische Zivilisation gemeint: „Handele so, dass die Wirkungen deiner Handlungen verträglich sind mit der Permanenz echten menschlichen Lebens auf Erden.“ Wenn man dazu auch ein demokratisches Gemeinwesen zählt, laufen das Handeln der Geheimdienste und die Untätigkeit der Regierung in diesem Zusammenhang einem solchen Verantwortungsverständnis entgegen. Zählt man noch die wachsenden Möglichkeiten von „Cyber“kriegen dazu, zeigt sich, dass die Zivilisation zunehmend in ihren Grundlagen gefährdet ist.

Abschließend soll noch auf die (Wieder-) Eröffnung der Technischen Universität Berlin vor fast 70 Jahren verwiesen werden. Auf dieser Eröffnung hat General Nares, Kommandant der Britischen Truppen in Berlin, viele interessante Sachen gesagt, insbesondere aber auch folgendes: „Science and technology can and must be devoted to advancing the peace and civilisation of man. This can only be so if they are used with responsibility. Responsibility is a cornerstone of democracy.“

Hans-Jörg Kreowski

Prof. Dr. **Hans-Jörg Kreowski** ist Leiter der Forschungsgruppe *Theoretische Informatik* an der Universität Bremen. Von 2003 bis 2009 war er Vorsitzender des FIfF.

Warnen, Täuschen, Tarnen

Zusammenfassung des Vortrags von Wolfgang Coy

Die Konzeption und Gründung von Geheimdiensten ist ein Phänomen der Industriezeit/Neuzeit, allgemein also der modernen Gesellschaft. Die deutschen Dienste wurden seit Hitlerdeutschland zu Staaten im Staate. Der Anfang war u. a. die Geheime Staatspolizei (Gestapo), dann kamen Ministerium für Staatssicherheit (Stasi/MfS), Bundesnachrichtendienst (BND), Verfassungsschutz (VS) und Militärischer Abschirmdienst (MAD). Die deutschen Geheimdienste wurden nach dem Krieg in beiden Regierungen zielstrebig ausgebaut, wobei das Ziel seit jeher Spionage, Überwachung und Sabotage war.

Ursprünglich entstand der BND aus dem militärischen Aufklärungsdienst *Fremde Heere Ost* der Nationalsozialisten. Nach dem Krieg wurden *Fremde Heere Ost* durch ihren Leiter Reinhard Gehlen (Generalmajor im Dritten Reich) zur *Organisation Gehlen* umfirmiert und den US-Amerikanern als Geheimdienst schmackhaft gemacht. Diese akzeptierten und 1956 entstand aus diesem Gebilde offiziell der BND. Die Verstrickungen mit anderen Naziverbrechern wurden nie aufgearbeitet. Hans Josef Globke, hochrangiger Nazijurist und Mitverfasser der Nürnberger Rassegesetze, später Kanzleramtschef unter Adenauer, stand dem BND nahe und wurde von ihm unterstützt. Globke wurde nur deshalb nicht bei den Nürnberger Prozessen erwähnt, weil Israel von der Bundesrepublik nur so eine schnelle „Wiedergutmachung" in Aussicht gestellt wurde.

Als charakteristische Aktivität hatte der BND z. B. die Operation *Gladio* mit aufgebaut. Gladio war eine europaweite geheime *stay-behind*-Organisation der NATO, die im Falle einer Invasion der Mächte des Warschauer Vertrages einen Guerillakrieg hätte führen sollen. Dafür wurden versteckte Lager mit Waffen und Munition angelegt, auch in Deutschland. Der BND war zudem auch in Anschläge verwickelt, mit Sicherheit in das Massaker von Bologna und höchstwahrscheinlich auch in den Oktoberfestanschlag in München.

Die Stasi war ähnlich radikal. Die dokumentierte Geisteshaltung der führenden Köpfe war „Hinrichten, auch ohne Gerichtsurteil". Doch die Stasi prägte geheime Strukturen auch in anderer Weise, sie hatte letztlich Modellcharakter für die Errichtung eines Überwachungsstaates. Aber was auch deutlich wurde: Widerstand ist möglich und erfolgreich. Das können und sollten wir mit anderen Diensten auch so machen.

Es gibt viele Beispiele für deren generelle Arbeitsweise wie staatliche Hinrichtungen, Aktionen der Dienste oder auch unterlassene Hilfeleistung.

Es sollen hier nur kurz exemplarisch drei Beispiele angeführt werden: Erstens der Mord am V-Mann Ulrich Schmücker im Jahre 1974. Der Verfassungsschutz hätte eingreifen können. Nach 591 Verhandlungstagen voller Beweismittelunterdrückung, Täuschung, Manipulation, illegaler Überwachung der Verteidigung und in der Folge Verurteilungen Unschuldiger zu lebenslangen Haftstrafen, lautete die offizielle Beurteilung „Extremfall rechtswidriger staatlicher Praxis". Letztendlich wurde der Vorfall auch nach 15 Jahren nicht richtig aufgeklärt und der Prozess schließlich eingestellt.

Zweites Beispiel ist Werner Teske, ein Hauptmann des Ministeriums für Staatssicherheit (MfS), der am DDR-System zu zweifeln begann und mit dem Gedanken spielte, sich in die BRD abzusetzen. Dafür wurde er von der Stasi 1981 im Geheimen hingerichtet, was selbst nach DDR-Gesetzen illegal war. Offiziell sollte es ein Unfalltod gewesen sein, wobei seine Frau und Tochter neue Identitäten bekamen, aus Berlin vertrieben und zum Schweigen gebracht wurden.

Um zuletzt ein nicht-deutsches Beispiel und zudem einen Informatiker als Opfer anzuführen, sei noch auf den mysteriösen „Selbstmord" Alan Turings 1954 in Großbritannien und die diesbezüglichen „Verwirrungen" verwiesen.

Dabei sind die Geheimdienste auch Sprungbrett für andere Karrierewege. Die Verflechtung der Dienste mit der Gesellschaft kann an den Beispielen George H. W. Bush (vormals Director of Central Intelligence DCI, dann Präsident der USA), Joseph Aloisius Ratzinger (vormals Präfekt der Kongregation für die Glaubenslehre, sprich Inquisition, dann Papst) oder Vladimir Putin (erst KGB-Offizier, dann Präsident Russlands) veranschaulicht werden.

Wolfgang Coy

Wolfgang Coy ist Informatiker und gestaltete den Fachbereich *Informatik und Gesellschaft* in Deutschland wesentlich mit. Er leitete die Forschungsgruppe *Informatik in Bildung und Gesellschaft* an der Humboldt-Universität zu Berlin und arbeitet aktuell im Interdisziplinären Labor *Bild – Wissen – Gestaltung*. Er ist im Beirat des FIfF.

Der Volljurist und Leiter des Ressorts für Innenpolitik der Süddeutschen Zeitung, Heribert Prantl, bewertet die aktuelle Situation bezüglich der Machenschaften der Geheimdienste mit folgenden Worten: „Der Wesensgehalt des GG Art. 10 ist schon lange ausgehöhlt". Die Kritik an der V-Leute-Praxis wird auch von Clemens Binninger (CDU) bis Hans-Christian Ströbele (B90/Grüne) geteilt, wobei die Beurteilung „dringend reformbedürftig" lautet. Die regelmäßige Shredder-Praxis der Dienste rundet das so erzeugte Bild ab.

Und was geschieht heute? Orte wie das *Utah-Data-Center* oder Projekte wie *Stuxnet* symbolisieren eine tiefgreifende Infrastrukturschwächung gesellschaftlicher Relevanz; dabei dient sich die Informatik als „Dienst der Dienste" an.

Somit: Schande über diejenigen InformatikerInnen, die dort mitarbeiten. Scham ist zwar ein revolutionäres Gefühl – wie Marx es ausdrückte –, aber es genügt nicht, es ist noch kein Handeln.

Leider muss man immer wieder daran erinnern: Es geht aktuell nicht um Sabotage des Einzelnen – es geht um Wirtschaftsspionage und mehr. Um dieser Entwicklung Einhalt zu gebieten, ist es dringend geboten, die Unterstützung von Whistleblowern auszubauen. Wir brauchen einen effektiven „Hinweisgeberschutz", damit Informatiker und alle anderen, Grundrechtsverstöße melden und wir uns somit wehren können.

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

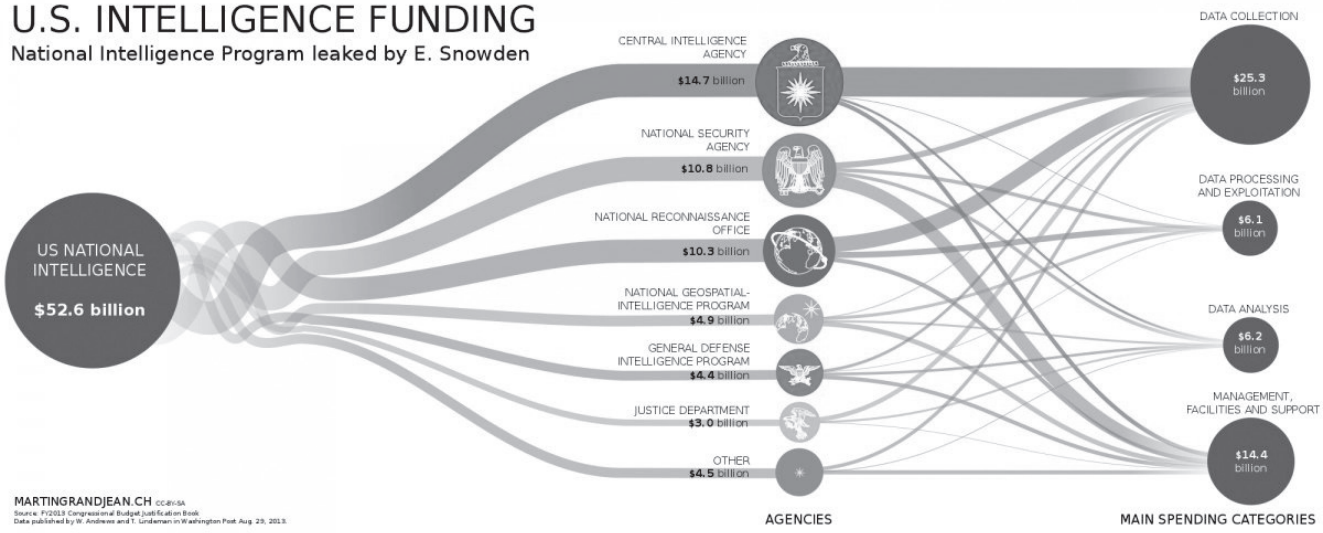
Die Veröffentlichungen zu Snowden in einem Vortrag auch nur zu nennen, würde vier Stunden dauern. Mit Sicherheit könnte man eine ganze Vorlesungsreihe zu diesem Thema aufbauen. An dieser Stelle soll es darum gehen, was grundsätzlich ans Licht gekommen ist, welche Reaktionen es darauf gab, und welche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



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-

griffsmöglichkeiten in den Flugverkehr, der auf korrekte Daten der Bodenstellen angewiesen ist.

Dass Provider statt des kürzesten den billigsten Weg für Daten wählen, erlaubt es staatlichen Stellen, ihren Machtbereich durch Subventionen auszuweiten, sodass mehr Verkehr durch ihr Zugriffsgebiet läuft. Weniger implizit ist die Installation von über 50.000 fernsteuerbaren Implantaten in Stellen anderer Staaten, von denen auf einer NSA-Folie berichtet wird. Gar an Allmachtsphantasien stößt das Programm TREASUREMAP, mit dem Endgeräte im Internet in Echtzeit inklusive verknüpfter Informationen visualisiert werden.

Doch auch auf andere Staaten wurde der Blick gelenkt. *Lawful Interception*, das Abgreifen der Daten direkt bei den Betreibern, geschieht ohne deren Wissen – da sie sonst Hinweise an das Opfer geben könnten –, und vor allem sind diese Systeme frei konfigurierbar. Durch die breite Einführung in den verschiedenen Ländern ergibt sich als Unterschied, egal ob Monarchie, Faschismus oder parlamentarische Demokratie, nur noch die Konfigurationsdatei. Die Grundlagen sind schon vorhanden und somit wurde vor der Gefahr einer intensiveren Nutzung unter anderen politischen Rahmenbedingungen gewarnt.

Anbieter von Überwachungstechnologie werben damit, erst einmal alles zu speichern und später die genaueren Kriterien der Durchmusterung zu setzen. Sie spezialisieren sich darauf, auch in rechtlich eingeschränkten Umgebungen kreative Dienstleistungen zu finden, wie es bei der Kurzumleitung in ein Rechenzentrum hinter der Grenze geschieht, um Abhörbefugnisse für Auslandskommunikation zu erreichen.

Angesichts der Souveränitätsverletzungen persönlicher und staatlicher Art muss jedoch die aus den Snowden-Dokumenten fokussierte Sicht auf die Beschafferebene geweitet werden hin zu der Fragestellung, warum und für wen all dies getan wird. Die NSA arbeitet nicht zum Selbstzweck, sondern für eine lange Liste von Kunden wie staatliche und militärische Stellen. Als gängiges Verwendungsmittel wurde an das Kompromat erinnert, ein Begriff des MfS, der definierbar ist als „Sachverhalt aus dem Leben einer Person, der im Widerspruch zu gesellschaftlichen […] Normen und Anschauungen steht, bei seinem Bekanntwerden zu rechtlichen oder disziplinarischen Sanktionen, zu Presigeverlusten, zur öffentlichen Bloßstellung, zur Gefährdung des Rufes im Bekannten- und Umgangskreis […] führen würde". Neben klassischen Gehemdienstmethoden des geschaffenen Problems für eine Zielperson inklusive Rettung, um an einen geschuldeten Gefallen anknüpfen zu können, sei der psychologische Trick *Greymailing* genannt. Statt einer harten Erpressung führt die Andeutung einer Erpressung, von der bezeugt wird, sie nicht zu wollen, zu viel besseren Resultaten.

Durch Daten werden Menschen verwundbar und einteilbar. Wir handeln fahrlässig mit Daten, die wir über uns und andere ins Netz geben. Könnte schon von Datenverbrechen und Beihilfe gesprochen werden? Zugriff auf Cloud-Services findet statt, und wenn Personen in Facebooks Datenbanken als Targets geführt werden, braucht nicht viel uminterpretiert zu werden im Angesicht der Drohnenmorde. Dass Ministerin Aigner damals Facebook verbieten wollte, lässt sich durchaus nachvollziehen, auch wenn Auslöser nur der Fall eines Psychotherapeuten war, dessen Telefonbuchdaten sein Telefon verließen und dessen Patienten gegenseitig als Freunde vorgeschlagen wurden. Sicherheit ist vielseitig, und somit verstehen wir unter einer informatischen IT-Sicherheit etwas anderes als Staatssicherheit. Und für einen Geheimdienst wie die NSA hat sie die Bedeutung, dass nur er selbst Zugriff hat.

Kryptologie funktioniert nicht im luftleeren Raum, sondern vielmehr in unsicheren Umgebungen. Verfahren werden geschwächt und umgangen, Schlüssel erbeutet. Der Markt für Schwachstellen, in dem nun auch die Dienste mitspielen, und die Verzögerung von Fehlerbehebungen aufgrund von PR-Abwägungen werfen kein gutes Licht auf den Stand der Technik. Den Aussagen von Industrie und Behörden kann kein Vertrauen entgegengebracht werden. Am Beispiel *RSA Security* wird dies besonders deutlich; im Austausch gegen 10 Mio. Dollar erreichte die NSA, dass Schwachstellen in Produkte eingebaut wurden. Auch Microsoft schließt den Einbau von *Back Doors* nicht aus, und beim Stichwort *Trusted Computing* müssen wir uns fragen, wem zu vertrauen ist. Freie Software bietet in vielerlei Hinsicht Vorteile. Die Einschränkung von Kryptotechnologie bringt eine Einschränkung der digitalen Souveränität. Um nachprüfen zu können, ob der Code unterwandert wurde, stand die Forderung nach einer offenen Kryptoanalyse im Raum, die durch Festangestellte einer gut aufgestellten Institution durchgeführt wird.

Informationen zur Überwachungstechnologie und deren Anbietern lässt sich im *Bugged-Planet-Wiki* finden, einer Gegenkartographie der Überwachungserkenntnisse, die durch Andy Müller-Maguhn betrieben wird.

Andy Müller-Maguhn

Andy Müller-Maguhn ist Bürgerrechtsaktivist im digitalen Bereich. Er arbeitete als *at-large director* bei der *Internet Corporation for Assigned Names and Numbers* (ICANN) und bekleidete Positionen in verschiedenen NGOs wie der *European Digital Rights* (EDRi) oder dem *Chaos Computer Club* (CCC). Aktuell beschäftigt er sich mit Unternehmen, die Überwachungssoftware verkaufen.

Vom Elend der parlamentarischen Kontrolle der Geheimdienste

Zusammenfassung des Vortrags von Wolfgang Nešković

Parlamentarische Kontrolle der Geheimdienste ist ein Placebo, ein Witz. Würde man parlamentarische Kontrolle so ineffektiv wie möglich institutionalisieren wollen, würde man sie genau so gestalten, wie sie zur Zeit geschieht.

Snowden ist für eine Änderung dieses Zustandes ein Hoffnungsträger. Seine Veröffentlichungen führten zu einem Bewusstsein, dass was vorher noch als abenteuerlich und abwegig galt, heute Konsens unter Verfassungsrechtlern ist.

Verfassungsrechtlicher Kontext

In einem Aufruf formulierten im Jahr 2014 fünf Nobelpreisträger und 560 Schriftsteller zwei Kernsätze, worum es geht:

> *„Ein Mensch unter Beobachtung ist niemals frei und eine Gesellschaft unter ständiger Beobachtung ist niemals eine Demokratie."*

Verfassungsrechtlich übersetzt, geht es um Artikel 1 des Grundgesetzes: *Die Würde des Menschen ist unantastbar*. Der Hintergrund dieses ersten und wichtigsten Grundgesetzes ist, dass der Staat für die Menschen da ist und nicht die Menschen für den Staat. Das Individuum – der Mensch – ist praktisch das Zentrum allen staatlichen Handelns und nicht der Staat. Alle Grundrechte in ihrer institutionellen Funktion sind Abwehrrechte gegen einen unvernünftigen Staat, der Machtmissbrauch betreibt. Die Grundrechte sind demnach institutionelles Misstrauen gegen den Staat, die wir nicht bräuchten, wenn wir ihm vertrauen würden.

Die Mütter und Väter des Grundgesetzes waren sogar so misstrauisch gegenüber ihren Nachfahren, dass bestimmte Grundsätze der Verfassung mit der *Ewigkeitsklausel* für unantastbar erklärt wurden. Artikel eins ist demnach nur abschaffbar, wenn das Grundgesetz insgesamt abgeschafft wird.

Am Beispiel der Vorratsdatenspeicherung wird deutlich, dass das notwendige Verständnis des Grundgesetzes gerade an dieser zentralen Stelle umgekehrt wird: Der Staat institutionalisiert das Misstrauen gegen seine Bürger, indem Daten ohne konkreten Anlass auf Vorrat gesammelt werden.

Gesetze der Geheimdienste

Die 251 Seiten Gesetze der Geheimdienste wurden dem Parlamentarischen Kontrollgremium von der Verwaltung des Bundestages vorgelegt. In meinem gesamten juristischen Leben habe ich nie Gesetze gelesen, die so unlesbar sind und bei denen erkennbar ist, dass die Lobbyisten, die hinter den Gesetzen stehen, den Gesetzgebern unmittelbar die Hand geführt haben. Sie widersprechen ganz eindeutig dem Grundsatz der Normenklarheit. Nur fällt das keinem auf, weil alle denken: „Versteh ich nicht", oder „So sind eben juristische Texte …" Dies führt auch dazu, dass kein Bundestagsabgeordneter und insbesondere kein Abgeordneter des Parlamentarischen Kontrollgremiums sich je damit intensiv beschäftigt hat. Wünschenswert wäre eine parlamentarische Bildungspflicht mit finanziellen Sanktionen bei Nichteinhaltung. Abgeordnete sollten sich beispielsweise den Vortrag von Bäcker ansehen – am besten verpflichtend dreimal die Woche.

Warum gibt es parlamentarische Kontrolle der Geheimdienste?

Normalerweise müssen Eingriffe der öffentlichen Hand einer effizienten gerichtlichen Kontrolle unterzogen werden. Die naheliegendste Erklärung, warum im Fall der Geheimdienste eine parlamentarische Kontrolle stattfindet, ist jedoch der Grundsatz der Gewaltenteilung. Weil es hier aber um den Fall des Geheimen geht, kommt noch ein zusätzlicher Gesichtspunkt zum Tragen. Das *Geheime* wird von der normalen Gerichtskontrolle ausgeschlossen – das Parlament nimmt die Rolle der Gerichte ein. Ein Beispiel dieser Justiz-ersetzenden Wirkung ist der Einsatz der G10-Kommission, wenn es um das Fernmelde- und Postgeheimnis geht.

Seit kurzem gibt es einen Artikel, der sich mit der parlamentarische Kontrolle auseinandersetzt. Dadurch hat sie nun auch Verfassungsrang und muss demnach effizient durchführbar sein. Das ist sie jedoch nicht.

Strukturelle Ohnmacht der parlamentarischen Kontrolle

Um etwas kontrollieren zu können, muss man den Gegenstand der Kontrolle kennen. Man muss wissen, was die Dienste tun.

Wie ist dies umgesetzt? Im Gesetz steht, die Regierung hat umfassend über die allgemeine Tätigkeit der Geheimdienste und über Vorgänge von besonderer Bedeutung zu berichten. Außerdem besteht eine Verpflichtung, dass Mitarbeiter auf Anfrage des Gremiums vortragen müssen.

Das Gremium tagt etwa alle drei bis vier Wochen für nur maximal drei Stunden, da Menschen mit wenig Zeit und oft nur aus Prestigegründen im Gremium sitzen. Einerseits kann die all-

gemeine Tätigkeit der 10.000 Mitarbeiter und Mitarbeiterinnen der drei Geheimdienste so unmöglich begutachtet werden. Andererseit müsste man, um rechtlich einwandfrei beurteilen zu können, welche Vorgänge von besonderer Bedeutung sind, über alle Aktivitäten Bescheid wissen. Faktisch ist das Gremium also der Willkür der Geheimdienste darüber ausgesetzt, was dem Kontrollgremium mitgeteilt wird und was nicht. Die gesetzlichen Berichtsverpflichtungen sind demnach nichts anderes als leere Versprechungen – Märchenstunde für die Abgeordneten. Obendrein hat niemand im Gremium einen Vertreter, bis 2009 gab es nicht einmal Mitarbeiter. Wünschenswert wären mindestens fünf, davon drei Juristen und zwei Informatiker, am besten beides, weil sonst technische Informationen – z. B. über *Deutschenfilter* – gar nicht sinnvoll eingeschätzt werden können.

Verbesserungsvorschläge

In einem Gesetzesentwurf schlägt Nešković eine Reihe von Verbesserungen für die Effektivität der parlamentarischen Kontrolle vor:

In Regelbeispielen soll beschrieben sein, in welchen Fällen die Dienste das Gremium zwingend unterrichten müssen. Etwa: Jede neue Dienstanweisung und jede Datenübermittlung ins Ausland muss dem Gremium automatisch mitgeteilt werden, ohne dass nachgefragt werden muss.

Um an weitere Informationen zu kommen, braucht es einen Whistleblower-Schutz. Alle Mitarbeiter und Mitarbeiterinnen der Dienste sollen unter bestimmten Voraussetzungen Eingaben an das Gremium machen können.

Juristisch präziser ausgedrückt besteht die Arbeit des Kontrollgremiums eigentlich in der Kontrolle der Aufsichtstätigkeit der Regierung über die Geheimdienste. Diese wiederum findet maßgeblich durch das Bundeskanzleramt in informeller Runde in der sogenannten *Präsidentenrunde* und der *Nachrichtendienstlichen Lage* statt. Bei diesen Besprechungen zu Einzelfällen und Strategien müsste das Parlamentarische Kontrollgremium Zugang bekommen.

Das Parlamentarische Kontrollgremium kann zwar Mitarbeiter und Mitarbeiterinnen der Dienste anhören. Da im Gesetz zwar steht, dass sie dann die Wahrheit sagen müssen, aber nicht, dass sie den *Zeugenstatus* haben, bedeutet dies formal, dass sie ohne Konsequenz, ohne Strafbarkeit lügen können. Selbst Disziplinarmaßnahmen würden vom Dienst selbst ausgeführt werden, woran der Dienst wohl kein ernsthaftes Interesse haben kann. Gegen die Forderung nach einem Zeugenstatus wehren sich die Dienste mit Händen und Füßen, weil sie wissen, was das im Einzelfall bedeuten kann. Dies muss unbedingt geändert werden.

Eine weitere, besonders für die NSA-Affäre entscheidende gesetzliche Beschränkung der Zugriffe auf Informationen der Geheimdienste durch das Kontrollgremium liegt darin begründet, dass das Kontrollgremium nur auf die Informationen zugreifen darf, für welche die deutschen Geheimdienste die Verfügungsberechtigungen haben. Das schließt nur die Daten ein, die sie selbst generiert haben. Alle Daten von den sogenannten Partnerdiensten unterliegen nicht der Kontrolle des Gremiums. Zusätzlich betrifft das auch selbst erhobene Daten, die mit den von anderen Diensten erhaltenen Daten vernetzt und verbunden werden. Beim BND kann insgesamt davon ausgegangen werden, dass dies für etwa 80-90 % der Daten zutrifft. Das ist verfassungsrechtlich nicht haltbar, weil es in einer Demokratie keine kontrollfreien Räume geben darf. Ein BND-Mitarbeiter darf grundsätzlich nicht mehr wissen als ein Abgeordneter.

Das kann juristische Begründung werden: Wir haben das Demokratieprinzip, und dieses lebt von der demokratischen Legitimierung der Handlungsträger im öffentlich-rechtlichen Bereich. Die Abgeordneten haben eigentlich die oberste Legitimation (durch die Repräsentation) und eine weitere durch das gesamte Parlament. Ein BND-Mitarbeiter ist in der Legitimationskette ganz weit hinten angesiedelt, darf aber kritikwürdigerweise mehr wissen als jemand vom Kontrollgremium. Diese Bestimmung ist verfassungswidrig, aber es gibt bisher keine Möglichkeit, vor dem Bundesverfassungsgericht zu klagen, da formale Kriterien nicht erfüllt sind.

Der Kontrollgegenstand für das Parlamentarische Kontrollgremium ist also aus rechtlichen Gründen ein unbekanntes Wesen, so dass die Kontrollaufgabe nicht ausgeführt werden kann. Es können Dienstemitarbeiter angehört werden, mit dem sicheren Wissen, dass sie gefahrlos lügen können; es können Zugriffe auf alle Daten und Schriftstücke angefordert werden und sogar überraschende Besuche stattfinden. Diese Rechte sind jedoch allesamt keine Rechte des einzelnen Abgeordneten, sondern Gremiumsrechte, die nach dem Mehrheitsprinzip entschieden werden. Da auch das Gremium nach Parteiproporz zusammengesetzt ist, hat die Mehrheit kaum ein Interesse, die eigenen Leute „in die Pfanne zu hauen". Zusätzlich zur strukturellen Ohnmacht leidet das Gremium auch aus diesem Grunde an Antriebsarmut.

Benötigt wird und verfassungsrechtlich geboten ist eine gesetzliche Regelung, dass jedes Gremiumsmitglied Kontrollbefugnisse hat. Wenn im Grundgesetz „Kontrolle" steht, dann muss sie auch effizient stattfinden können. Da sie dies faktisch nicht kann, ist diese Regelung verfassungswidrig.

Eine einfache, naheliegende, aber bisher nie geäußerte Forderung: Das Gremium falsch oder irreführend oder rechtswidrig nicht zu informieren, muss ein Straftatbestand werden! Es müssten Richter eingesetzt werden, weil Rechtskontrolle ihre berufliche Sozialisation ist, das Kontrollgremium wird nie eine Chance haben Kontrolle auszuüben, so lange darin nur PolitikerInnen sitzen. Viele Dinge müssen verändert werden – unveränderlich sind sie mit Sicherheit nicht.

Wolfgang Nešković

Wolfgang Nešković ist fraktionsloser Politiker und ehemaliger Richter am Bundesgerichtshof. Er war langjähriges Mitglied des Deutschen Bundestages und dort auch lange Mitglied des Parlamentarischen Kontrollgremiums (PKG).

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 Intelligence Directive*, doch 28 Nachrichtendienste haben länger als 50 Jahre dieses Ziel verfehlt.

Seit ca. 2009 kann die *National Security Agency* (NSA) jedoch 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 Enhüllungen 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 ein Mitarbeiter Reinhard Gehlens diesen darüber, dass Bundeskanzler Konrad Adenauer abgehört würde. Gehlen, Direktor des BND und der Vorläuferorganisation *Operation Gehlen*, reichte die Informationen dann an 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

keine diplomatischen Vertretungen besaßen, mit Hilfe von US-Technik an deutschen Standorten aktiv zu werden. In der Konsequenz war den deutschen Stellen die Technik der NSA schon länger bekannt, weil sie diese selbst – wenn auch stellvertretend – verwendet hatten. Im Jahre 1993 dann forderte der Geheimdienstkoordinator im Kanzleramt, Bernd Schmidbauer, eine nachrichtdienstliche Rundumverteidigung, weil die angelsächsischen Freunde im deutschen Wirtschaftsraum spionierten.

Seit 1942 gab es zusätzlich die *Five Eyes* genannte weltweite Zusammenarbeit der Geheimdienste der USA, Großbritanniens, Kanadas, Australiens und Neuseelands. Gemeinsam spähen sie politische, wirtschaftliche und auch gesellschaftliche Akteure aus. Dies führte im November 2002 zu der Forderung des Europäischen Parlaments, dass man umgehend mit den USA Verhandlungen aufnehmen müsse, um die Datensicherheit der EU-Bürger und den Schutz vor Wirtschaftsspionage (*competetive* intelligence) zu gewährleisten. Diese ernsthaften Bestrebungen versandeten jedoch mit den Eindrücken und Auswirkungen der Anschläge vom 11. September.

Die Enthüllungen

Interessanterweise kann man zwischen den Snowden-Veröffentlichungen und Artikeln der Fachzeitschrift *Intelligence online* aus den Jahren 2000 bis 2012 viele Parallelen erkennen. Die Fachpresse berichtete regelmäßig über die technologischen Fortschritte der NSA für deren alltäglichen Gebrauch. Dazu gehört, verschlüsselten Verkehr automatisiert zu extrahieren oder Internettelefonie (VoIP) in über 40 Sprachen mit Hilfe von künstlicher Intelligenz zu analysieren.

Diese Fähigkeiten werden auch gegen Deutschland verwendet. Das wissen wir deshalb, weil das Auswärtige Amt (AA) eine Liste mit Firmen vorhält, die hoheitliche Aufgaben für die USA übernehmen. Derartige Aktivitäten sind nämlich in Deutschland detailliert bis hin zum Aufgabenbereich meldepflichtig. Zudem finden sich in der Fachpresse auch Ausschreibungen für bestimmte Positionen, bspw. im Jahre 2013 vom Internetprovider Level3 für einen *Analytiker für soziale Netzwerke*, Standort Stuttgart-Vaihingen, also am Sitz des EUCOM und des AFRICOM.

Somit mutet es seltsam an, dass der Präsident des Verfassungsschutzes im November 2013 die USA gebeten hatte, ihm eine Liste der US-Kontraktoren zukommen zu lassen, obwohl er diese auch direkt vom Auswärtigen Amt hätte bekommen können.

Doch auch auf der anderen Seite gibt es bemerkenswerte Verhältnisse. Die NSA gibt ca. 70 % ihres Budgets für private Kontraktoren aus. So entsteht ein nachrichtendienstlich-wirtschaftlicher Komplex, der wiederum großen Einfluss auf die Politik ausübt. Zur Verdeutlichung dieser Machtsituation kann man sich vor Augen halten, dass im Jahr 2013 ca. 1,4 Mio. Menschen in den USA berechtigt auf Geheimmaterialien zugreifen konnten, 700.000 davon waren Angestellte der Privatwirtschaft – und Snowden war einer davon. Hoffentlich finden sich darunter noch andere mutige Menschen, die den Schritt zum Whistleblower wagen.

Weitere Zeugen

Doch nicht nur das Auswärtige Amt ist über derartige Machenschaften informiert. Dazu ein Beispiel des Bundesfinanzministeriums: Im Jahre 2007 erfuhr der damalige Bundesfinanzminister Peer Steinbrück, dass sich viele deutsche Banken aus der Finanzierung von Irangeschäften zurückgezogen hätten, aber die BAF (eine Deutsche-Bank-Tochter) und die Deutsche Genossenschaftszentralbank in die Bresche gesprungen waren. Steinbrück wurde nämlich von einem Staatssekretär des US-amerikanischen Schatzministeriums darauf hingewiesen, dass die US-Amerikaner auch den BND darüber in Kenntnis gesetzt hatten. Man wusste also genau, dass die Transaktionen deutscher Geldinstitute voll im Visier der US-Geheimdienste stehen.

Phantomschmerz Wirtschaftsspionage?

Zwar gab es viele Klagen deutscher Unternehmen über eine mögliche Wirtschaftsspionage, doch in Snowdens Dokumenten finden sich zwar generelle Programme wie *Trackfin*, mit denen europäische Banküberweisungen abgefischt werden, aber keine dezidierten Hinweise auf Wirtschaftsspionage gegen deutsche Unternehmen.

So behauptete der Präsident des Bundesverfassungsschutzes Hans-Georg Maaßen im Handelsblatt, dass es keine von den US-Amerikanern betriebene Wirtschaftsspionage in Deutschland gäbe.

In den Wikileaks-Dokumenten finden sich jedoch allerlei gegenteilige Informationen. Als Stichwort sei der interessierten Person das *Bundesamt für Ausfuhr* oder kurz *Bafa* ans Herz gelegt. Dazu treten 101 Geheimdokumente zutage, die eine klare Sprache über Wirtschaftsspionage der US-Amerikaner in Deutschland sprechen. Das Vorgehen ist fast immer das gleiche: Der US-amerikanische Botschafter in Berlin bekommt eine Weisung vom US-Außenministerium mit Hinweisen auf unerwünschte/dubiose Rüstungsexporte aus der Bundesrepublik. Er wird dann im Auswärtigen Amt in einem sogenannten Non-Paper vorstellig. Diese Non-Paper existieren natürlich offziell nicht und können somit auch nicht durch parlamentarische Kontrollen oder Untersuchungsschüsse überprüft werden. Der Inhalt dieser Non-Paper wird vom Auswärtigen Amt geprüft und dann mit dem Bundesamt für Ausfuhr, dem BND und dem betreffenden Unternehmen koordiniert. Es folgt die Antwort an das US-Außenministerium, natürlich wieder via Non-Paper.

Dafür kann man viele Beispiele anführen, z. B. Dual-Use-Güter der Firma *Deckel-Maho-Gildemeister* (DMG), die Fräsmaschinen für Geschützrohre oder nukleare Zentrifugen nach Karachi, Pakistan, verkaufen wollte. Dieser Export wurde durch die Intervention der US-Amerikaner gestoppt.

Ein anderes Beispiel waren die geplanten Exporte der Firma *Alexander Wiegand GmbH*, die 200 Druckmessumformer nach Schweden liefern wollte. Allerdings klärten die US-Geheimdienste auf, dass Schweden nur Durchgangsland gewesen wäre und der Iran das eigentliche Zielland hätte sein sollen.

Der BND ist also bei der Aufklärung illegaler oder fragwürdiger deutscher Exporte ausgesprochen schwach aufgestellt. Sar-

kastisch könnte man somit anmerken, dass die US-Nachrichtendienste eigentlich die Exportkontrolle deutscher Unternehmen übernehmen, was aus Sicht der Friedensbewegung doch sicher ein sinnvoller und positiver Aspekt ist. Das ist natürlich nur die eine Seite der Medaille, denn viele Interventionen richten sich natürlich gegen legale Exporte, die den US-Amerikanern einfach nicht passen.

In einem Falle ging es um den Export von Scharfschützengewehren in den Iran, der eigentlich legal gewesen wäre, weil es sich nicht um automatische Waffen handelte, doch die USA haben trotzdem interveniert. Kleinere Firmen reagieren bei solchen Eingriffen meist sehr sensibel. Nur in einem Fall hat sich ein großes Unternehmen nicht an die Hinweise der US-Dienste gehalten: Mercedes sollte den Export von Schwerlast-LKW abbrechen, doch sie konnten es sich leisten, die Anfragen des Auswärtigen Amtes einfach zu ignorieren.

Das gravierendste Beispiel war jedoch eine Kooperation von Eon und Intershell, die Erdgasverflüssigungsanlagen an den Iran verkaufen wollten. In diesem Fall ging der US-Botschafter einfach direkt zur Bundeskanzlerin, die dann den Dokumenten nach versprach, „informell" Druck auszuüben, und das mit großem Erfolg: das Geschäft kam nicht zustande.

Noch mehr Zeugen

Der BND legte im Sommer 1991 eine Studie auf, um die neue Ausrichtung der US-Geheimdienste nach dem Ende des Kalten Krieges zu untersuchen. Schon der Titel dieser Studie ist unmissverständlich: „Verstärkung der wirtschaflichen Wettbewerbsfähigkeit der USA durch Nachrichtendienste." Darin findet sich folgende Zusammenfassung: In den USA besteht Einigkeit darüber, dass die amerikanischen Nachrichtendienste in Zukunft durch verstärkte Wirtschaftsaufklärung zur Verbesserung der Wettbewerbsfähigkeit der heimischen Industrie beitragen sollen. Weiter heißt es, die Vorgänge um die libysche Chemiefabrik in Rakta sowie die Überwachung des gegen den Irak verhängten Wirtschaftsembargos haben gezeigt, dass die *Intelligence Community*, insbesondere die NSA, sehr wohl über Möglichkeiten verfügt, *Competitive Intelligence* zu betreiben. Der BND formulierte daher die Befürchtung, dass die Amerikaner unter dem Deckmantel der Bekämpfung des illegalen Technologietransfers und des Drogenhandels Informationen über legale Geschäfte ausländischer Wettbewerber sammeln und sie politisch zwischen staatlichen Nachrichtendiensten und privaten Sicherheitsfirmen umsetzen. Dabei sitzen in den Sicherheitsfirmen überwiegend ehemalige Geheimdienstmitarbeiter mit ihren Beziehungen, sodass die staatlich erbeuteten Wirschafts- und Konkurrenzspionagedaten Eingang in die Wirtschaftspolitik der USA finden.

Der Bundesnachrichtendienst (BND)

Wenden wir uns nun dem Bundesnachrichtendienst mit Schwerpunkt technische Aufklärung zu. Der Vorläufer des BND – *Organisation Gehlen* (die *Org*) – wurde 1949 von der CIA übernommen. Weil die CIA aber hauptsächlich menschliche Spionage betrieb, waren die technischen Gegebenheiten weniger relevant. Es wurden in der Folge nur 3 % des Budgets von 1,2 Mio. D-Mark für *Signals Intelligence* (SIGINT) verwendet, das ist ausgesprochen wenig.

Während der Berlin-Blockade 1948 hatte die Organisation Gehlen als einziger westlicher Geheimdienst einen Überblick über die Bedrohungslage für die *Rosinenbomber*. Deswegen wurde sie für die US-Amerikaner interessant. Ab 1956, der Gründung des BND aus der Organisation Gehlen, kam es zum Aufbau einer Kette von Abhörstationen (z. B. das *Ionosphäreninstitut*). In den 1970er und 1980er Jahren folgten massive finanzielle Investitionen für die Optimierung der Inlandsstationen zur Aufklärung, wobei schon ab Anfang der 1960er Jahre Anlagen am Schwarzen Meer, in der Türkei, in Taiwan und auch beim Schah in Persien/Iran in Betrieb genommen wurden, oft auch als Joint Ventures.

Ab ca. 1982 war laut BND-Bericht die technische Aufklärung dann zur tragenden Säule geworden. 50 % des Budgets wurde für die technische Beschaffung verwendet. Ein geheimer Jahresbericht über die fernmeldetechnische Aufklärung aus dem Jahre 1984 besagte, dass 650.000 militärische Meldungen abgefangen worden sind, aber nur 119.000 davon vom BND in Eigenregie. 145.000 bekam er über den Austausch mit Großbritannien und den USA, 95.000 wiederum in Zusammenarbeit mit Österreich, Südafrika, Israel und der Schweiz. Ein weiterer *Datenverbund* aus USA, Taiwan und Großbritannien erspähte nochmals 286.000 Meldungen.

Erich Schmidt-Eenboom

Erich Schmidt-Eenboom ist Journalist, Publizist und Leiter des *Forschungsinstituts für Friedenspolitik e. V.* Er publizierte kritisch über den Bundesnachrichtendienst (BND) und wurde längere Zeit auch von diesem überwacht.

Der Jahresbericht bezeugte zudem, dass der BND auch diplomatische Verkehre ausspäht, was sich in 304.000 diesbezüglichen Meldungen niederschlug. Weiterhin sind auch die sogenannten „Gelbstrichmeldungen" interessant, die anzeigen, dass der Schutz kryptographisch gesicherter Meldungen ausgehebelt werden konnte. Das machte der BND aber nicht allein, sondern er kooperierte mit dem Schweizer Unternehmen Crypto AG, das neutral und unabhängig wirken sollte, aber vollständig von Siemens und dem BND kontrolliert worden ist.

An dieser Stelle kann man die starke Prognose wagen, dass es wohl keine deutsche Verschlüsselung geben wird, die nicht BND-kompromittiert ist.

Althergebrachte Arbeitsweisen

Im Übrigen gab es nie Druck zur Kooperation aus den USA oder aus Großbritannien. Immer hat der BND sich angeboten und „gebaggert", um in den Verbund der Amerikaner und der Briten aufgenommen zu werden. Nach Jahrzehnten rückte der BND endlich in den vorderen Bereich der *Third parties*, und im Jahre 1988 durfte er sogar als Juniorpartner in die US-Abhörbasen Bad Aibling und Gablingen einziehen. Später wurden diese Stützpunkte ganz vom BND übernommen, was ihn in der Folge an die technologische Weltspitze katapultierte.

Aber auch die Spionageausrichtung des BND ist schon seit langem ebenso gegen westliche Partnermächte gerichtet. Bereits in den 1960er Jahren formulierte der schon erwähnte Reinhard Gehlen, dass angesichts der wachsenden Konkurrenz zwischen westlichen Industrienationen genau dort ein völlig neuer Aufklärungsschwerpunkt liegen müsse. Folglich rangierten in den 1980er Jahren sowohl die USA als auch Großbritannien mit Priorität 2 (von 6) in der BND-Zielausrichtung fast ganz oben, insbesondere in Hinsicht auf ihre Außen-, Nuklear- und Europapolitik.

Die Überraschung der Politk, dass der BND nun auch die existierende Infrastruktur anzapft, ist tatsächlich nichts wesentlich Neues. Schon im Jahre 1953 wurde das erste (Ost-)Seekabel durch die Organisation Gehlen angezapft. In den 1970er Jahren dann wurde ein Großteil des Mittelmeerverkehrs direkt abgegriffen, denn dieser landete an der spanischen Mittelmeerküste und wurde dann über eine Richtfunkstrecke nach Portugal und dann wieder per Kabel nach Großbritannien, West-Afrika und in die USA weiterverteilt. In dieser Funkstrecke hatte der BND die Station *Eismeer* installiert und dadurch Vollzugriff. Diese *Operation Delikatesse* existierte nach dem Kalten Krieg bis zum Jahre 1992 und wurde dann unter großem Widerstand des BND stark reduziert an die spanischen Dienste übergeben. Aktuell werden ca. 200 Seekabel direkt vom BND überwacht.

Die Kritik an der Kooperation mit den US-Partnerdiensten greift ebenfalls zu kurz, denn seit 1985 ist auch die Volksrepublik China direkter Kooperationspartner, z. B. bei Abhöranlagen im Pamir. Das muss man im Hinterkopf haben, wenn in öffentlichen Reden vor der (Wirtschafts-)Spionage durch die Chinesen gewarnt wird. Der Deal ist immer der gleiche: der BND liefert die Technik (Siemens sowie Rohde & Schwarz), die Chinesen hören ab, und beide teilen sich die Erkenntnisse.

Der britische Geheimdienst: *Government Communications Headquarters* (GCHQ)

Der britische Geheimdienst GCHQ hat lange Zeit in der öffentlichen Berichterstattung ein Schattendasein gefristet, was direkt mit dem Konzept der *DA-Notice (Defence Advisory Notice)* oder *Defence Notice (D-Notice)* im britischen Presserecht zu tun hat. Die Regierung kann bezüglich bestimmter Themen aus Gründen der „nationalen Sicherheit" auf den *Official Secrets Act* verweisen und Berichte darüber auf diese Weise unterdrücken.

Die britischen Geheimdienste haben ein Budget von ca. 2,3 Mrd. Euro, wobei ein Großteil davon direkt dem GCHQ und seinen 6.000 Mitarbeitern zugute kommt. Es gibt Spekulationen über weitere finanzielle Hilfen durch die US-Amerikaner, auf jeden Fall bekommt der GCHQ aber sehr viele technische Geschenke von ihnen, sodass man schon von einer Filiale der NSA sprechen kann.

Lange Zeit war Großbritannien stolz auf die Investitionen in die Verzahnung von Geheimdiensten und Privatwirtschaft nach dem Modell der USA, doch aktuell will man davon nichts mehr wissen. Grund dafür sind die enhüllten GCHQ-Ausspähungen des G20-Gipfels, vieler Überseeglasfaserkabel oder des Internetproviders Belgacom, Versorger diverser EU-Institutionen.

Bislang gibt es in Großbritannien jedoch nur Kritik vom Guardian, die restliche Medienlandschaft betreibt eine gnadenlose Rechtfertigungsoffensive. Der GCHQ sagt natürlich von sich selbst, er führe keine Massenüberwachung durch, glaubwürdig sind solche Behauptungen jedoch nicht. Doch die Strategie geht noch tiefer: Die britische Regierung vertritt öffentlich die Position, verschlüsselnde US-Firmen seien Komplizen der Terroristen und der organisierten Kriminalität, doch diese Empörung ist nur vorgespielt, damit z. B. der *Islamische Staat* und andere die Systeme auch nutzen. Der Zugriff erfolgt dann durch die Hintertür in Kooperation mit den Firmen.

Abschluss

Leider gibt es auch keinen Grund für Optimismus, denn alle Geheimdienste setzen aktuell darauf, dass im Jahre 2015 und danach andere Medienthemen von der hier besprochenen Problematik ablenken und nur noch die Fachwelt – wie vorher auch – kritisch darüber reflektiert.

Man muss sich immer vor Augen halten, dass Nachrichtendienste niemals nur Sammler sind, sondern immer auch Jäger. Der BND liefert z. B. Grundlagen für illegale Entführungen, Folterflüge und Drohnenmorde, die *Operation Mustang* unterstützte beispielsweise die Regierung Nepals gegen die Maoisten, was zu Verhaftungen und (Selbst-) Morden führte, die Afghanen wurden u. a. durch die Lieferung von Handytracking-Technik unterstützt, und auch die NSA bekam diese Daten; die PKK wurde für gezielte Tötungen ausgeforscht und so weiter und so fort. Der BND tut all dies oft nicht direkt, sondern über Umwege, eben im Geheimen.

Wir Deutsche dürfen derartige Aktionen nicht nur nicht selber machen, sondern wir dürfen auch nicht mitmachen, sonst sind

wir eben Komplizen. Das betrifft auch Siemens China, die Überwachungstechnik via Abu Dhabi in den Iran verkaufen wollten. Nur weil die Briten darauf hinwiesen, stoppte die Bundesregierung den Deal widerwillig. Viele Nachrichtendienste von Diktaturen (von Sudan bis Oman) hätte ihre Fähigkeiten ohne Deutschland und die mitwissenden deutschen Regierungen überhaupt nicht. Unser Vorteil in Deutschland – im Gegensatz zum angelsächsischen Raum – ist die Risikoaversion des BND, denn er lässt sich alles vom Bundeskanzleramt absegnen. Zumindest in Deutschland existiert also kein „tiefer Staat", die Dienste sind nicht außer Kontrolle. Natürlich erschafft das Wissen des Bundeskanzleramtes noch lange keine Rechtsgrundlage und umreißt das politische Problem.

Dass wir nun durch Snowden eine derartige Aufmerksamkeit haben, ist der Masse und Unabstreitbarkeit der Dokumente zu verdanken, denn viele Einzelheiten waren der Fachwelt schon bekannt. Die öffentliche Diskussion ist also der eigentliche Verdienst Snowdens.

Wenn diese Geheimstrukturen gebrochen werden sollen, müssen viele Personengruppen am gleichen Strang ziehen. Medien müssen sich weniger auf Skandale und „große" Persönlichkeiten, als auf tiefergehende Berichterstattung konzentrieren; Auslandsjournalisten dürfen nicht mehr direkt dem BND zuarbeiten, wie es leider aktuell oft der Fall ist; und nicht zuletzt könnte auch die Technikergemeinde massiv Gegenaufklärung betreiben.

FIfF-Konferenz 2014

Das trojanische Pferd *Terrorismus*

Zusammenfassung des Vortrags von Anne Roth

Angesichts der Errichtung des *Islamischen Staates* im Nordwesten des Iraks und Syriens ist das Thema Terrorismus wieder näher in die Berichterstattung gerückt. Als wohlbekannter Propagandabegriff wird er immer wieder benutzt, um Grundrechte zu verändern. Dabei ist meist unklar, was mit dem Begriff *Terrorismus* tatsächlich gemeint ist.

Die Bundeszentrale für politische Bildung bezeichnet Terrorismus als Mittel der unterdrückten Klasse, die herrschende Schicht unter Druck zu setzen. Wer gerade als Terrorist bezeichnet wird, dies variiert meist je nach Dekade und auch nach politischem Interesse der Regierenden. Per dieser Definition handelt es sich meist um Minoritätengruppen, die eine Überreaktion der Herrschenden verursachen möchten. So galt die damalige *Rote-Armee-Fraktion* in den 70ern als gewaltbereit, und sie konnte aufgrund der Schwere der Anschläge die Sympathie der Bevölkerung nicht auf sich ziehen. Somit zeigt sich an den unterschiedlichen Vereinigungen (ETA, Hamas), dass sie mittels Anschlägen und medienwirksamen Taten politische Ordnungen verändern und einen strukturellen Wandel hervorrufen möchten. Inwiefern sie jedoch als Freiheitskämpfer, Revolutionäre, Opfer oder Terroristen bezeichnet werden, hängt davon ab, wer die Definitionsmacht besitzt und sie auch ausführen kann.

Der 11. September als Blaupause

Interessant ist dabei ebenfalls, dass terroristische Aktivitäten erst seit dem 11. September 2001 als Straftatbestand gelten. Nach Ansicht der UN handelte es sich beim 11. September um Terro-

rismus, da unschuldige Menschen getötet wurden, aus dem einfachen Grund, zur falschen Zeit am falschen Ort zu sein. Brigitte Zypries, die damalige Justizministerin, bezeichnet 9/11 nicht als Terrorakt, da die Vereinigten Staaten nicht in ihrem Bestand gefährdet wurden. Verwirrung gibt es auch über die statistische Erfassung der Fälle. EU-weit wurden bisher 7 Tote durch Terroranschläge registriert, doch ist unklar, ob diese Anschläge terroristisch oder politisch einzuordnen sind. Auch die Heraushebung einzelner Personenmerkmale wird dabei immer wieder herangezogen, um Kausalketten schlüssig manipulieren zu können. So spielen Religionszugehörigkeit und Nationalität meist eine größere Rolle als Veganismus, linke politische Einstellung oder Aktivismus im Anti-Atom-Bereich. Seit den Anschlägen des 11. September wird daher Terrorismus meist der Gruppe der muslimischen Männer zugeschrieben, obwohl gerade auf dem europäischen Kontinent dieser Begriff viel weiter gefasst werden müsste. Ob Frankreich,

Anne Roth

Anne Roth ist Politologin, Netzaktivistin und Bloggerin. Ihre Beschreibungen der persönlich erlebten (zweifelhaften) Überwachung und der (später aufgehobenen) Verhaftung ihres Partners sowie ihre Arbeiten zu Terrorismus und den Ämtern für Verfassungsschutz sorgten für Aufsehen. Sie arbeitete für das *Tactical Technology Collective* und ist Referentin im NSA-Untersuchungsausschuss.

Irland oder Spanien, sie alle haben mit Separationsbewegungen zu kämpfen. Wird jedoch über Terrorismus gesprochen, werden zumindest in unserer deutschen Medienkultur diese Bewegungen kaum beachtet. 1871 wurde im Reichsstrafgesetzbuch §129 die Definition für Terrorismus festgelegt: dabei handelt es sich um die Teilnahme an einer Verbindung, um Verwaltung oder Gesetzesdurchsetzungen zu verhindern oder zu entkräften. Erst später wurde eingeführt, dass auch die Werbung für solch eine Teilnahme verboten ist. Während der RAF-Zeiten wurde dann außerdem das Einschüchtern und Angreifen von Grundstrukturen hinzugefügt.

Leider hat sich in der Vergangenheit immer wieder gezeigt, dass diese Definition nicht ausreichend ist, sodass bisherige Verfahren in 95 % der Fälle wieder eingestellt wurden. Die Betroffenen wissen meist nicht, dass sie in das Visier der Ermittler geraten sind. Es kann somit festgestellt werden, dass Terrorismus eine Art Konjunkturbegriff ist, der immer wieder zur Verschärfung von Sicherheitsgesetzen herangezogen wird. Als gefährlich eingestufte Gruppen wechseln daher ständig, mal sind es linksextreme Gruppen, dann die organisierte Kriminalität oder Hooligans.

Gleichzeitig verwendet die politische Öffentlichkeit diese Bezeichnungen sehr ungenau. Eine Wand der Bedrohung wird nahezu täglich gezeichnet und Hass, eine durchaus unpolitische Regung, wird geschürt. Geschichtlich verankerte Begriffe, die mit der eigenen Identität zusammenhängen könnten, werden allerdings aus Selbstschutz und Überdrüssigkeit nicht mehr verwendet. So werden Nazis nicht mehr als Nazis bezeichnet, sondern als Hooligans.

Trojaner werden dann eingesetzt, wenn die vermeintliche Terrorgefahr eingedämmt werden muss, wozu jedoch auch Sicherheitsgesetze verschärft werden. Diese Begründung hilft dann eben, noch schärfere Verfahrensweisen anzuwenden. Die Definitionen, die diese Verfahrensweisen legitimieren, sind jedoch äußerst schwammig, und Fehlurteile sind vorprogrammiert: wer Terrorist ist, wird definiert. Dass die Überwachung der Kommunikation der eigentliche Terror ist, wird als übertrieben, naiv und übersensibel abgetan. Dies ändert jedoch nichts an der Tatsache, dass Menschen bereits heute am Telefon wieder genauestens überlegen, was sie sagen.

FIfF-Konferenz 2014

Skandal! Reform? Weitermachen! Eine Analyse der Geschichte des Verfassungsschutzes mit Hilfe von Text Mining

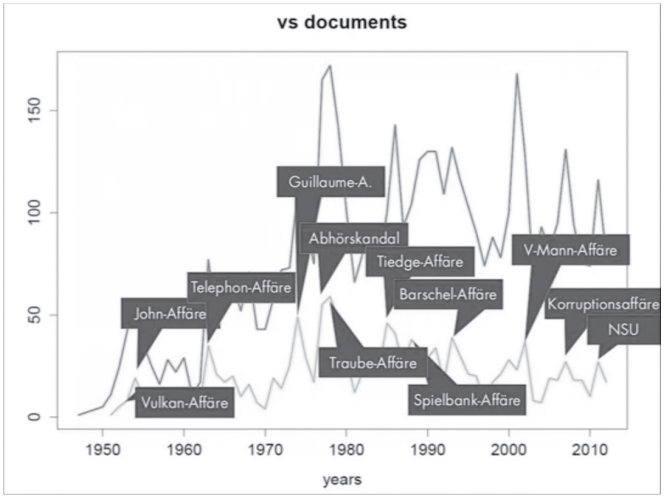
Zusammenfassung des Vortrags von Gregor Wiedemann

Das Terrornetzwerk NSU *(Nationalsozialistischer Untergrund)*, das jahrelang aus dem Untergrund heraus raubte und mordete, hat sich im Jahr 2011 selbst enttarnt. Der Verfassungschutz hatte es angeblich nicht entdeckt, obwohl er laut Recherchen von Untersuchungsauschüssen und Journalistinnen und Journalisten vielen Fällen erheblich nahe gekommen sein muss. Als Frühwarnsystem, das das Bundesamt für Verfassungsschutz laut seines Auftrags sein soll, hat es mehrmals kläglich versagt. Dies ist der Ausgangspunkt der Forschung von Gregor Wiedemann.

1950 gestatteten die Westalliierten der Bundesrepublik neben der Gründung des BKA auch die Einrichtung eines Inlandsgeheimdienstes. Die seitdem stattgefundende Berichterstattung über den Verfassungsschutz nahm Wiedemann mit strukturentdeckenden Verfahren und Textanalyse, sogenanntem Text-Mining, unter die Lupe. Text-Mining nutzt computerbasierte Methoden für eine semantische Analyse von Text, die automatisch oder halbautomatisch unter Ausnutzung von statistischem oder linguistischem Wissen Strukturen in sehr großen Textmengen entdecken.

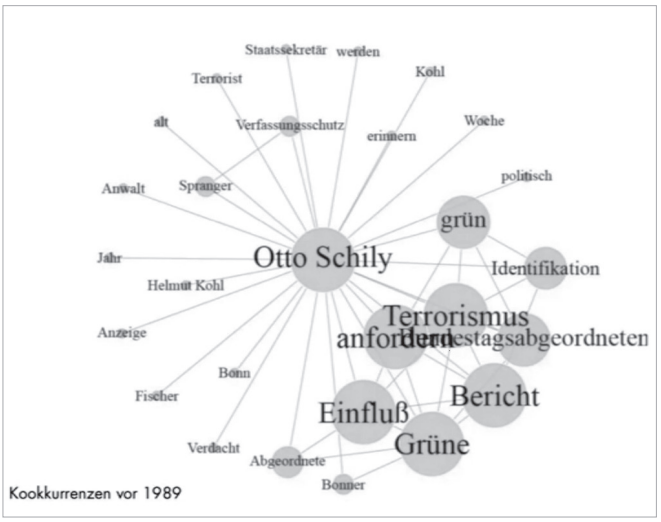
Wiedemann analysierte auf diese Weise 5.078 Artikel von *Der Spiegel* und *Die Zeit* von 1950 bis 2011, die sich in irgendeiner Form mit dem Verfassungsschutz beschäftigen.

Die Verteilung der Artikel über die Zeit zeigt eine ansteigende Kurve mit vielen Spitzen. Die Berichterstattung nimmt also zu



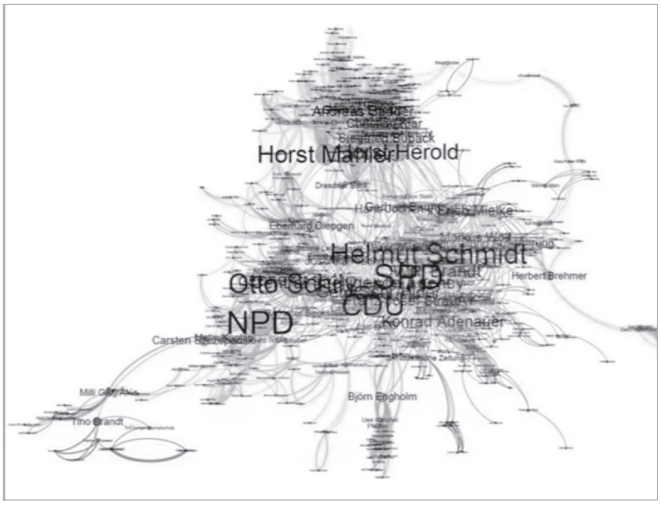
und schwankt sehr stark im Abstand von etwa fünf bis sechs Jahren. Interessant zu untersuchen sind die Ausschläge der Kurve. Sucht man in den Texten nach den Teilworten *skandal*, *affäre* und *panne* und trägt die Anzahl der Artikel, in denen sie vorkommen, über die Zeit ab, kann man eine massive Korrelation zur ersten Kurve feststellen. In den Spitzen geht es also in vielen Fällen um irgendwelche Affären oder Skandale. Visualisiert man die Anzahl einzelner Begriffe wie *NSU-Affäre*, *V-Mann-Affäre* oder *Abhörskandal* pro Jahr in einer sogenannten *Heatmap*, so können diese Begriffe als Bezeichnungen für die Ausschläge genutzt werden.

Nun kann versucht werden, Themen- und Bedeutungsstrukturen aus den Daten herauszuziehen. Mit *Topic-Modellen* – probabilistischen Modellen, die Themen innerhalb einer Textkollektion als Verteilung über dem Vokabular modellieren – erhält man Cluster von Zeitungsartikeln, die zu einem Thema gehören. Mit der *Kookkurrenzanalyse* findet man Begriffskombinationen, die in den Texten überzufällig häufig vorkommen. Beide Methoden lassen Aussagen über Bedeutungsstrukturen oder Bedeutung und Semantik zu – die Ergebnisse können als Graphen visualisiert werden.



Hintereinander angewendet lässt etwa der Graph zum Begriff *Telephon-Affäre* Begriffs-Cluster erkennen, die dann zum ersten Mal dazu führen könnten, sich die betreffenden Dokumente anzusehen, um herauszufinden, worum genau es dabei ging. Die letztendlichen Zusammenhänge ergeben sich zwar nicht aus dem Graphen, jedoch gibt er schon vorher Anhaltspunkte, in welche Richtung die jeweiligen Vorfälle gehen.

Auf diese Weise ergaben sich automatisiert unter anderem Begriffs-Cluster zur Telephonaffäre, Lauschaffäre Traube, das Celler Loch, die Spielbankenaffäre oder die V-Mann-Affäre. Die Cluster können statt nach Themen auch nach Namen von Personen gefiltert werden, um die sich die verschiedenen Affären dann anordnen.



Ein weiterer Schritt ist die Erstellung eines Kookkurrenzgraphen über Personen- und Organisationsnamen über alle Artikel. Hierbei ergeben sich verschiedene Cluster um verschiedene Kontexte, wie etwa um die RAF oder den Spionagezusammenhang zwischen DDR-MfS und den Deutschen Spitzenpolitikern von CDU und SPD, oder ein Cluster um das NPD-Spektrum und den NSU-Skandal.

Reform

Untersucht man den gesamten Textkorpus auf den Begriff *Reform* hin, findet man viele Artikel und Zitate, die auf Probleme und den Reformbedarf hinweisen. Deutlich wird, dass die betreffenden Textstellen über den gesamten Zeitraum verteilt sind. Das deutet darauf hin, dass die Probleme des Verfassungsschutzes so alt sind wie der Verfassungsschutz selbst.

Mit überwachtem maschinellem Lernen lassen sich nach einem manuellen Training anhand von Beispielsätzen Textstellen finden, die Aussagen über Reformforderungen oder erfolgreiche Reformen treffen. Trägt man die Anzahl der Artikel, in denen diese Reformforderungen oder -ergebnisse vorkommen, gegen die Zeit ab, so lässt sich einerseits erkennen, dass sich auch die Reformforderungen über den gesamten Zeitverlauf des Bestehens des Verfassungsschutzes erstrecken, und andererseits, dass auch hier eine sehr starke Korrelation zur Kurve mit Artikeln über die Skandale erkennbar ist.

Gregor Wiedemann

Gregor Wiedemann ist Politologe und Mitarbeiter im Projekt *Postdemokratie und Neoliberalismus* der Universität Leipzig. Darüber hinaus beschäftigt er sich mit dem Versagen des Verfassungsschutzes um die NSU-Affäre. Er ist außerdem Mitbegründer des Vereins *Engagierte Wissenschaft*, in dem sich Nachwuchswissenschaftler kritisch mit gegenwärtigen Herrschaftsdiskursen und -praktiken auseinandersetzen.

Fazit

Text-Mining kann helfen, sehr große Textmengen effizient zu explorieren und sie daraufhin semantisch zu erschließen. Die Verfahren der Informationsextraktion und Strukturerkennung finden allerdings nur große, statistisch signifikante Auffälligkeiten in den Daten, also etwa große Skandale, die in der Öffentlichkeit bearbeitet worden sind. Kleinere Zusammenhänge und solche, die sich nicht oder kaum in den Medien widergespiegelt haben, werden übersehen. Problematisch werden die Methoden auch, wenn mit ihnen versucht wird, Rückschlüsse auf Einzelfälle zu ziehen, indem ohne Bedacht von der Makrosicht in die Mikrosicht gesprungen wird.

Mit dieser Methode konnte Wiedemann zeigen, dass in den Zeitungsartikeln ewige Wiederholungen der Verfassungsschutzskandale und Reformbemühungen zu entdecken sind, danach jedoch nicht ernsthaft etwas unternommen und verändert wurde. Skandal! Reform? Weitermachen!

FIfF-Konferenz 2014

NSA, IT-Sicherheit und die Folgen

Zusammenfassung der Vorträge und Diskussion von Hans-Christian Ströbele, Ingo Ruhmann und Ute Bernhardt

Ruhmann

Das FIfF wurde 1984 gegründet mit dem Thema *Rüstung und Informatik*, vor diesem Hintergrund sollte somit auch der militärische Aspekt des NSA-Skandals diskutiert werden.

Betrachtet man z. B. *XKeyScore*, so zeigen Snowdens Materialien, dass es dabei neben der Ausspähung und Datensammlung ebenso um *Digital Network Intelligence* (DNI) geht, also um *Information Warfare*. Das aber bedeutet, dass nicht mehr nur die umfassende Überwachung durch die NSA thematisiert werden muss, sondern auch deren aktive Manipulation und Sabotage von IT-Systemen. In diesem Zusammenhang ist das *Office of Tailored Access Operations* (TAO) zu nennen. Dessen ca. 900 spezialisierte Hacker entwickeln automatisierte Systeme zur Infiltration von IT-Systeme oder treten selbst in Aktion, wenn dies scheitert. Sie agieren entweder via Internet oder durch die Manipulation von Hardware, während der Produktion und vor deren Auslieferung oder, im Falle eines *Airgaps* (wenn ein IT-System keine Verbindung zum Internet hat), mittels Agenten vor Ort. Das ist jedoch keineswegs etwas Neues, sondern gängige Praxis aus Zeiten des Kalten Krieges. Bereits 1989 wurde über Schadsoftware und Computersabotage berichtet. Auch über die von den Geheimdiensten erstellten Schwachstellendatenbanken, die jetzt einen Teil von XKeyScore darstellen, hat das FIfF bereits 1997 informiert. Damals noch nicht bekannt war allerdings das Ausmaß dieser Manipulationsaktivitäten. Hierbei zeigt sich, dass die Verbreitung von staatlicher Schadsoftware in etwa das gleiche Niveau erreicht hat wie das nichtstaatlicher Viren, Trojaner etc. Ein Blick in den Budgetentwurf der NSA von 2013 beziffert die beantragten Ressourcen für die Internetüberwachung, die Entschlüsselung und die Entwicklung von Angriffswerkzeugen, wie z. B. einem Programm zur Verbreitung von Schadsoftware, auf insgesamt 12 Mrd. US-Dollar. Damit stellt die NSA die am besten finanzierte Hackertruppe der Welt dar. Der größte Anteil dieser Ressourcen in Höhe von 10 Mrd. US-Dollar wurde dabei für die Entwicklung von Angriffstechnologie zum Brechen von Verschlüsselung ausgegeben.

Während der *Heartbleed-Bug* die Aufmerksamkeit auf sich zog, trat der Umstand in den Hintergrund, dass die NSA bereits vor dessen Programmierung „durch spezielle Zugänge zu Unternehmen und [die] Manipulation von Softwarelösungen" die Fähigkeit besaß, sowohl die aktuelle SSL-Verschlüsselung zu umgehen als auch die älteren gesammelten SSL-verschlüsselten Daten zu dechiffrieren. Das bedeutet aber nichts anderes, als dass das ganze Zertifizierungsprinzip hinterfragt und überdacht werden muss, da es offensichtlich kompromittiert ist.

Dass die von Snowden ausgelöste Debatte um den Datenschutz nur ein Teil der weit größeren Thematik *Cyberwar* ist, erschließt sich aus der Aufgabenbeschreibung der NSA, die sie zu weit mehr als einem nur mit Spionage betrauten Geheimdienst macht. Die NSA ist demnach eine Verteidigungs- und Kampfunterstützungseinrichtung des US-Verteidigungsministeriums. Sie ist also nicht nur ein Geheimdienst, sondern auch die bedeutendste Kampftruppe im Bereich des Informationskriegs. Dieser beinhaltet Medienmanipulation inklusive gezielter Falschinformation und Propaganda sowie die Sabotage, aber auch die Bombardierung von Medieneinrichtungen und Kommunikationssystemen. Als *Cyberwarfare* wird all das bezeichnet, was auf Netzen abläuft. Da der NSA-Direktor gleichzeitig der Kommandeur des *US Cyber Commands* ist, steht er den *information operations units* der US-Streitkräfte vor (von denen die NSA wiederum das größte Kontingent stellt), deren Arbeit allein dem tagtäglichen Krieg im und um den informationstechnischen Bereich gilt. Diese militärischen Operationen richten sich

dabei nicht nur gegen sogenannte Feinde, sondern auch gegen die „Freunde“ und „Verbündeten“ der USA wie Regierungsstellen in Deutschland oder Institutionen wie die Vereinten Nationen oder die Europäische Kommission. Dabei legitimiert die NSA als staatliche Institution ihre Kriegshandlungen durch gesetzliche Befugnisse. Betrachtet man nun die Strategie der Medienbeeinflussung als Bestandteil des Informationskrieges, dann zeigt sich in Verbindung mit der aktuellen Definition des US-Verteidigungsministeriums für *information operations* (den Methoden zur Umsetzung des Informationskrieges), dass sie sich gegen die Willensbildung von Feinden und potenziellen Feinden richten, wobei die Methode der psychologischen Kriegsführung um das Mittel der Computerdisruption erweitert wird.

Diese Definition bedeutet, dass sich der US-Cyberkrieg als eine uneingeschränkte, fortwährende Auseinandersetzung mit Staaten, NGOs, Privatpersonen und Medien darstellt. Dem CERT der Bundeswehr ist dieser Umstand durchaus bekannt, nennt es doch als potenzielle Bedrohung unter anderem nicht nur die feindlichen Nachrichtendienste, sondern auch die befreundeten. Dies führt zu der Feststellung, dass die größte Bedrohung im Netz und für IT-Systeme von der NSA und den mit ihr kollaborierenden Diensten ausgeht, dass die IT-Sicherheitssysteme weitreichend kompromittiert sind und es daher keine Gewissheit über deren Wirksamkeit gibt, dass es die USA sind, die die „Rechtsfreiheit“ des Internets zum uneingeschränkten Cyberkrieg gegen Freund und Feind missbrauchen, und dass deshalb die Datenschutzfrage in diesem Kontext nur ein Teil der Debatte über den „Cyberkrieg unter Freunden“ sein kann. Die Diskussion über Datenschutz und IT-Sicherheit „nach Snowden“ hat also noch gar nicht begonnen!

Bernhardt

Das FIfF entstand vor 30 Jahren aus der Debatte um die Zuverlässigkeit von (militärischen) IT-Systemen. Vor 20 Jahren schon bezeichnete das FIfF das Fernmeldegeheimnis als „strategisches Grundrecht“: Das Fernmeldegeheimnis ist der zentrale Punkt für die Kontrolle der Informationsgesellschaft. Entscheidend ist daher der Schutz von Grundrechten für die IT-Welt. Es gibt seit 1983 das Grundrecht auf informelle Selbstbestimmung und seit 2007 das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Ersteres hat sich in Form von Institutionen, z. B. zum Datenschutz in unserer Gesellschaft, etabliert, während letzteres noch nicht institutionell repräsentiert ist. Das bedeutet aber, dass unsere Gesellschaft auf Grundrechten beruht, die von ihrem eigenen Staatsapparat weder garantiert noch eingehalten werden können. Polemisch gesprochen, ist das Telekommunikationsgeheimnis faktisch abgeschafft, der Datenschutz wurde aufgegeben, und die Integrität von IT-Systemen ist gründlich kompromittiert. Was bedeutet aber diese Diskrepanz zwischen dem Grundgesetz und dem ihm zum Teil entgegengesetzten Verhalten einzelner Staatsorgane für unser Staatsverständnis und unsere Staatsform? Welche technischen und gesellschaftlichen Kosten bringt es mit sich, wenn die IT-Systeme einer Gesellschaft, die in bedeutendem Maße von einer IT-Infrastruktur abhängt, kompromittiert sind und wenn die politische Entscheidungsfindung durch information warfare manipuliert wird? Die Geheimdienste haben ihre Rolle erweitert – von einer Kraft der Exekutive hin zu einem politischen Akteur, der seine Mittel nutzt, um die demokratische Debatte zu steuern.

Ströbele

Als langjähriges Mitglied des Parlamentarischen Kontrollgremiums und des NSA-Untersuchungsausschusses spricht Hans-Christian Ströbele über die Arbeit des NSA-Untersuchungsausschusses.

Da die US-Behörden keine Reaktion auf die Anfrage des Untersuchungsausschusses zeigen, konzentriert sich dieser hauptsächlich darauf, herauszufinden, inwieweit auch deutsche Geheimdienste, allen voran der BND, in die verdachtslose und massenhafte Überwachung der Bevölkerung verwickelt sind. Deutschland hat die vorbildlichste Datenschutzgesetzgebung in ganz Europa, auch was die Beschränkungen der Geheimdienste angeht. Im Untersuchungsausschuss wird nun ermittelt, wie der BND z. B. die strategische Satellitenüberwachung in Bad Aibling so filtert, dass der Datenschutz für Grundrechtsträger gewährleistet ist. Es besteht der Verdacht, dass die Geheimdienste in der Weise zusammenarbeiten, dass die einzelnen nationalen Dienste jeweils die Daten von fremden Staatsbürgern sammeln und dann gegen die Daten der eigenen Mitbürger austauschen, die sie nach den nationalen Datenschutzbestimmungen nicht selber erfassen dürfen.

Die methodische Frage, wie mit den technischen Möglichkeiten der Überwachung umgegangen werden soll, die sich aus der stetig wachsenden Ausbreitung und Verknüpfung der IT-Systeme ergeben, entfachte nach dem 11. September 2001 in der NSA selbst einen Konflikt darüber, ob zu einer anlasslosen, umfassenden Vorratsdatenspeicherung übergegangen werden sollte oder ob der Schutz der Bürgerrechte nur einen verdachtsbegründeten, gezielten Einsatz erlaubt. Das mündete in dem Ausscheiden des damaligen für die Datensammlung und Filterung verantwortlichen Direktors Binney, der als Whistleblower den Auslöser für die öffentliche Debatte lieferte und dem NSA-Untersuchungsausschuss bereits als Zeuge zur Verfügung stand. Zwischen der Offenlegung Binneys und den Snowden-Veröffentlichungen hat die NSA die Vorratsdatenspeicherung auf globale Größe ausgebaut. Dabei ist es gar nicht notwendig, die Datenleitungen z. B. in Deutschland direkt zu überwachen, das hat die NSA auch immer bestritten, sondern die Architektur der Netzinfrastruktur vereinfacht die Überwachung. Da der Datenstrom über zentrale Knotenpunkte fließt, genügt es, wenn diese Schnittstellen kompromittiert sind. Der Untersuchungsausschuss soll auch klären, wie genau die Massendatenüberwachung abläuft. Alle Fragen klären solche Ausschüsse nie, aber wesentliche Fragen können

doch beantwortet werden, und so konnte bereits mit der Hilfe des ehmaligen Präsidenten des Bundesverfassungsgerichts, eines weiteren Verfassungsrichters und anderer Rechtsverständiger festgestellt werden, dass die Überwachungsaktivitäten des BND verfassungswidrig sind. Die Reaktion müsste natürlich sein, dass diese Aktivitäten sofort eingestellt werden, was die Bundesregierung nicht durchsetzt und stattdessen eigene Gutachten vorlegt. Eine weitere Erkenntnis ist, dass es wahr ist, dass der BND in Deutschland Daten abschöpft und an die NSA weitergibt, was vorher stets bestritten wurde. Die NSA ihrerseits behauptet ebenso, sich an deutsches Recht zu halten – und hat trotzdem die Kanzlerin abgehört. Es ist also offensichtlich, dass die Vertreter der NSA systematisch lügen. Da kann der Untersuchungsausschuss somit nicht ansetzen. Da der BND aber Daten weitergibt, muss nun ermittelt werden, ob es dem BND überhaupt möglich ist, die Daten von Deutschen aus diesen auszufiltern. Laut Aussage eines Zeugen ist das technisch gar nicht möglich. Die Aktenprüfung umfasst jetzt ungefähr schon 1000 Leitzordner mit 500-800 Seiten Aktenkopien, die zu großen Teilen geschwärzt sind, wofür angeblich 100 Mitarbeiter des Kanzleramtes abgestellt wurden. Wenn der BND aber Deutsche abhören würde, müsste der G10-Ausschuss jede dieser Abhörmaßnamen prüfen und genehmigen, was eine Massenüberwachung unmöglich macht. Betrachtet man die Zeugenbefragung, so kann man sagen, dass sich die öffentlichen Sitzungen in Maßen von den nichtöffentlichen unterscheiden, da die Aussagegrenzen bei letzteren schwächer sind. Bei diesen nichtöffentlichen erfährt der Ausschuss etwas mehr. Bezüglich der Diskussion über die Bespitzelung der Welthungerhilfe in Afghanistan unterlief dem BND-Juristen in der Befragung ein Fauxpas. Er rechtfertigte die Überwachung damit, dass es sich bei den NGO-Mitarbeitern um „Funktionsträger“ handelte und nicht um „Grundrechtsträger“. Auf Nachfrage, was denn einen „Funktionsträger“ ausmachte, erkannte er den Unsinn seiner Aussage und gab zu, dass er sich da vielleicht vertan hätte.

Interessant in diesem Zusammenhang ist jedoch, dass sich der BND mit derartigen Überwachungsoperationen (und von der G10-Kommission abgesegnet) in seiner Arbeit an die weiter oben von Hr. Ruhmann aufgezeigte US-Auffassung angepasst hat, Cyberwar gegen Feinde und potenzielle Feinde zu führen.

Da die Mitglieder des Untersuchungsgremiums nicht das technische Expertenwissen besitzen, um Urteile z. B. über die Tauglichkeit von Filtern zu fällen, lassen sie sich von Sachverständigen, z. B. auch vom Chaos Computer Club, beraten, da diese keinen staatlichen Verpflichtungen unterworfen sind.

Im Übrigen scheut sich der Ausschuss nicht davor, etwaige Falschaussagen der Zeugen als Lügen zu protokollieren.

Warum aber gibt es keinen Aufschrei, bei diesen Zuständen? Jeder könnte aufschreien und jeder sollte aufschreien, das wäre dringend nötig! Leider sieht es aber so aus, dass das Interesse an den Snowden-Veröffentlichungen stark zurückgeht.

Was kann aber nun jeder selbst tun? Man kann z. B. so etwas wie Lavabit, Posteo oder GnuPG und eine dezentrale Internetstruktur nutzen. Wann immer US-Firmen z. B. für die Kommunikation genutzt werden, so werden diese Daten in den USA zentriert; sie sind dort sehr einfach auswertbar. Wenn mehr Menschen ihre Kommunikation verschlüsseln, wird für die Geheimdienste die Überwachung unendlich viel mühsamer, bis es sich schließlich nicht mehr lohnt. Darüber hinaus ist ein Gesetzentwurf zum Whistleblowerschutz eingebracht worden, und die Bundesregierung soll auf Grundlage der EU-Grundrechtecharta ein Vertragsverletzungsverfahren gegen Großbritannien anstreben.

Hans-Christian Ströbele, Ingo Ruhmann und Ute Bernhardt

Hans-Christian Ströbele ist ein erfahrener Politiker, langjähriger Parlamentarier für Bündnis 90/Die Grünen und Rechtsanwalt. Er ist Mitglied des Deutschen Bundestages und beschäftigt sich mit Sicherheits-, Rechts- und Entwicklungspolitik. Er arbeitet im Parlamentarischen Kontrollgremium (PKG) und im NSA-Untersuchungsausschuss.

Ingo Ruhmann ist Informatiker und arbeitet im Bereich Technikfolgenabschätzung, Forschungspolitik, IT-Sicherheit, Information Warfare, *Cyberwar*, Geschichte der Geheimdienste und Datenschutz. Er ist Lehrbeauftragter im Studiengang *Security Management* der Fachhochschule Brandenburg. Er ist Mitglied des FIfF und war Vorstandsmitglied von 1991 bis 1998.

Ute Bernhardt ist Informatikerin und beschäftigt sich seit Jahren mit Forschungspolitik, Datenschutz und IT-Sicherheit, dem Verhältnis von Wissenschaft und Frieden sowie der Beziehung von Informatik und Militär. Sie hat Lehraufträge an der Fachhochschule Bonn-Rhein-Sieg und der FernUni Hagen. Sie ist Mitglied des FIfF und war FIfF-Vorstandsmitglied von 1991 bis 1998.

Datenschutzkontrolle bei Sicherheitsbehörden

Zusammenfassung des Vortrags von Peter Schaar

Zuständigkeit

Die Datenschutzkontrolle bei Sicherheitsbehörden ist ein Spezialfall der Datenschutzkontrolle bei Behörden. Im Gegensatz zum Rest der Welt und größtenteils auch Europas, ist es in Deutschland selbstverständlich, dass es auch in Sicherheitsbehörden Datenschutzbeauftragte gibt. Zwar besteht keine Kontrollbefugnis der Geheimdienste durch Datenschutzbehörden, doch da es vielfältige Verknüpfungen der geheimdienstlichen Datenverarbeitung und der Datenverarbeitung von Unternehmen gibt und sich diese Überwachung für einen Großteil der Menschen massiv auswirkt, besteht eine unabhängige Datenschutzkontrolle hinsichtlich der Telekommunikationsunternehmen und des Ausleitens ihrer Daten durch Geheimdienste. Die Datenschutzbehörden des Bundes und der Länder sind also grundsätzlich auch für Geheimdienste zuständig.

1983 stellte das Bundesverfassungsgericht im Zusammenhang mit dem Volkszählungsurteil fest, dass die Unabhängigkeit der Datenschutzbeauftragten für einen effektiven Rechtsschutz unverzichtbar ist. Gemeint war hier der Rechtsschutz bei staatlichen Maßnahmen wie etwa der Volkszählung. Bei der Ermittlung und Überwachung durch Sicherheitsbehörden, insbesondere die im Geheimen stattfindende, funktioniert der normale Rechtsschutz nicht. Durch Artikel 10 Grundgesetz ist er sogar formell ausgenommen. Bei G10-Maßnahmen tritt an Stelle der richterlichen Kontrolle die Kontrolle durch parlamentarische Gremien.

Die G10-Vorschriften entstanden auf Iniatitive und Druck der damaligen Westalliierten, die so sicherstellen wollten, weiterhin strategische Fernmeldekontrolle ausüben zu können, also die Kontrolle grenzüberschreitenden Fernmeldeverkehrs.

Die Datenverarbeitung bei G10-Maßnahmen bildet demnach einen Ausnahmebereich, für den nicht Datenschutzbehörden, sondern die G10-Kommission zuständig ist, die streng geheim tagt. Überall, wo die G10-Kommission zuständig ist, sind die Datenschutzbeaufragten per Gesetz blind.

Nach 9/11 erhielten die Geheimdienste zusätzliche Befugnisse, so dass diese Regelung nicht mehr „nur" Telekommunikationsmaßnahmen betraf, sondern auch beispielsweise den Zugriff auf Daten von Reiseagenturen und Banktransaktionen durch Geheimdienste.

Die G10-Kommission tagt streng geheim und hört nur die Nachrichtendienste und die Vertreter der Bundesregierung an, aber z. B. keine Anwälte des öffentlichen Interesses. Amtshilfe, die Schaar als Bundesdatenschutzbeauftragter mehrfach angeboten hatte, wurde abgelehnt.

Unabhängigkeit

Die Stellung der Datenschutzbehörden ist nach dem Volkszählungsurteil eine grundrechtssichernde. Sie müssen daher unabhängig sein.

Die exklusive Auswahl der ersten Bundesdatenschutzbeauftragten ab 1977, die somit weisungsabhängig waren, genügte diesem Anspruch nicht. Sie werden seit 1990 durch das Parlament gewählt, jedoch nach wie vor auf Vorschlag der Bundesregierung.

Da die Behörde jedoch an Ministerien angegliedert ist, unter der Dienstaufsicht des Bundesinnenministers steht und der Rechtsaufsicht der Bundesregierung unterliegt, kann nach wie vor von Unabhängigkeit nicht die Rede sein. Die mangelnde Unabhängigkeit ergibt sich weiterhin verwaltungstechnisch aus dem vom BSI vergebenen Budget und der Priorisierung des Finanzministeriums. Während z. B. hunderte neue Stellen für Sicherheitsbehörden geschaffen wurden, entstand nicht eine einzige für den Datenschutz. Obendrein kann der Datenschutzbeauftragte seine Mitarbeiter und Mitarbeiterinnen nur aus einem Pool von Menschen wählen, der vom BMI nach einer Vorauswahl zusammengestellt wurde. Die Kriterien für diese Auswahl sind umstritten. Qualifikation wird hier beispielsweise geringer gewichtet als die Erfahrung in irgendwelchen Gremien.

Peter Schaar

Peter Schaar ist Vorsitzender der *Europäischen Akademie für Informationsfreiheit und Datenschutz* (EAID). Er war zuvor seit 2003 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit.

Wirksamkeit

Das verfassungsrechtliche Gebot einer grundrechtssichernden Stellung kann aus drei Gründen faktisch nicht mit Leben gefüllt werden: Erstens wegen der rechtlichen Stellung, zweitens, wenn die Aufgabe vom Leiter oder der Leiterin nicht ausgefüllt wird, und drittens, wenn die tatsächlichen Mittel für die Erfüllung der Aufgabe nicht ausreichen.

Nach der Einleitung eines Gesetzgebungsverfahrens 2014 soll die Bundesdatenschutzbehörde nun oberste Bundesbehörde werden, die Dienstaufsicht durch das BMI soll entfallen. Diese Entwicklung ist eigentlich sehr begrüßenswert, der Pferdefuß dabei ist jedoch, dass dies nur theoretisch mehr Autonomie bedeutet, die jedoch praktisch nicht ausübbar ist. Mit dem Mehr an Selbstverantwortung gehen nicht genügend neue MitarbeiterInnen einher, was real weniger Prüfmöglichkeiten bedeutet.

Eine weitere Einschränkung der Wirksamkeit ist, dass die Behörde keine Sanktionen verhängen kann. Einziges Mittel ist die formalisierte Kritik in Form einer „Beanstandung", auf die jedoch nur mit einer öffentlichen Rechtfertigung reagiert werden muss.

Auch der Zugriff auf relevante Daten ist beschränkt. Wenn beispielsweise eine Telekommunikationsfirma die Datenanfrage verweigert, muss die Bundesnetzagentur angerufen werden, die dann über den Zugriff entscheidet. Wenn es um Sicherheitsbehörden geht, entscheidet sie meist dagegen.

Während das BKA Daten aus Ländern einsehen darf, ist dies dem Bundesdatenschutzbeauftragten nicht gestattet, weil dieser nur für den Bund zuständig ist. Die Landesdatenschutzbeauftragten wiederum müssen das BKA fragen. Generell ist zu beobachten, dass verschiedene Behörden unterschiedliche Zugriffsmöglichkeiten bekommen. So können Sicherheitsbehörden automatisierte Zugriffsmechanismen nutzen, während Datenschutzbehörden Papierprotokolle prüfen müssen.

Das Thema der NSA-Aktivitäten war 2013 so politisch aufgeladen, dass der Bundesinnenminister sogar Antworten zu Fragen verweigerte, die ganz eindeutig in den Aufgabenbereich des Bundesdatenschutzbeauftragten fielen. Auf eine formelle Beanstandung dessen gab es als Reaktion nur einen bösen Brief vom Staatssekretär des Bundesinnenministers, dem jetzigen Geheimdienstkoordinator.

Durch die Bundesdatenschutzbehörde kann nur Datenverarbeitung geprüft werden, die ihr bekannt ist. Kapazitäten für eine eigenständige, z. B. systematische, rasterfahndungsartige Suche, etwa nach Nachrichtendienstgebäuden sind jedoch nicht vorhanden, und Informationen, die die Behörde für eine Untersuchung benötigen würde, werden häufig nicht vorgelegt. So musste die Datenschutzbeauftragte des BND feststellen, dass für eine Vielzahl der vom BND angelegten Dateien die verbindlich vom Gesetz vorgesehenen Dateianordnungen, die dem BDS zur Prüfung der Rechtmäßigkeit hätten vorgelegt werden müssen, nicht bestanden.

Fazit

Die Geheimdienstkontrolle muss dringend verbessert werden. Schaar bemängelte 2013 in einem Bericht für den Deutschen Bundestag die bestehenden Kontrolllücken. Er forderte eine verbesserte Koordination der Kontrollorgane und effektive Prüfmöglichkeiten durch diese. Diese Forderungen haben den damaligen Bundesinnenminister „not amused", der darauf hin im Bundestag äußerte, wir bräuchten keine „Superaufsichtsbehörde".

Wenn schon den Forderungen nach der Überprüfung der Notwendigkeit von Nachrichtendiensten nicht nachgekommen wird, muss sich wenigstens für eine ernstzunehmende Geheimdienstkontrolle dringend etwas ändern. Für die Genehmigung von Maßnahmen dürfen nicht mehr nur die Nachrichtendienste und Regierungsvertreter aus Ministerien und Bundeskanzleramt angehört werden, sondern auch Vertreter öffentlichen Interesses sowie Datenschutzbeauftragte.

FIfF-Konferenz 2014

Der NSA-Ausschuss

Zusammenfassung des Vortrags von Patrick Sensburg

Als der NSA-Untersuchungsausschuss eingesetzt wurde, prognostizierten viele dem Vorsitzenden Patrick Sensburg sofort, dass dabei nichts herauskommen würde. Die Mitglieder seien nicht vom Fach, würden also nichts verstehen und obendrein weder von den ausländischen noch den deutschen Diensten Informationen bekommen.

Auch aus der Bevölkerung hört er teilweise den Satz „Ich habe nichts zu verheimlichen", und von kleinen und mittelständischen Unternehmen „Wir sind doch nicht interessant für die". Sensburg sieht das anders. Er ist überzeugt, dass es in sehr weiten Bereichen um Wirtschaftsspionage geht und dass der Ausschuss Aufklärung schaffen wird.

„Wartet erst mal ab, was wir dann alles rausbekommen …"

Die Ausschussarbeit fing sehr langsam an – in den ersten Wochen kamen die öffentlich gewordenen Informationen noch nicht vom Ausschuss, sondern von der Presse. Nachdem die Zeugenvernehmung von Snowden „nicht mehr ausschließlich im Fokus war", wurden Themenblöcke gebildet, um die Fragestellungen Schritt für Schritt abarbeiten zu können:

1. Wie arbeiten deutsche Dienste – und machen sie alles rechtmäßig?

2. Was haben die *Five Eyes* über uns ausspioniert?

3. Was lernen wir daraus, welche Empfehlungen kann der NSA-Untersuchungsausschuss geben?

Erster Schritt

Der erste Schritt bestand darin, die Aktivitäten der deutschen Dienste zu betrachten. Es wurde vermutet, aus den Akten, welche Verfassungsschutz und BND betreffen, auch etwas über die Aktivitäten der ausländischen Dienste, der *Five Eyes*, zu erfahren. Aus rechtlichen Gründen müssen diese Akten dem Ausschuss von der Bundesregierung zur Verfügung gestellt werden. Direkt bei den ausländischen Diensten Anfragen zu stellen, erschien nicht erfolgversprechend.

Zeugen

Eine weitere Informationsquelle sind die Zeugenvernehmungen. Beispielsweise zeigte die Datenschutzbeauftragte des BND Fehler auf. Sie sagte aus, dass Dateianordnungen nicht ordnungsgemäß beantragt und diese Dateien trotzdem genutzt wurden. Sie ist sich außerdem uneinig mit dem BND-Präsidenten, nach welchem Recht Signale abgegriffen werden dürfen und dass sehr wohl Grundrechte betroffen sind. Da die Zeugen „richtig aussagen müssen" und es ansonsten eine Straftat wäre, ist es auch Pflicht des Ausschusses, darauf zu achten und zu beobachten, ob die Zeugen in Zukunft dienstlichen Nachteilen im BND ausgesetzt werden. Erfreulich ist, dass die Bundesregierung nicht nur Zeugen aus Abteilungsebene und aufwärts für die öffentlichen Sitzungen zur Verfügung stellt, sondern auch aus der operationellen Ebene.

Von einzelnen Zeugen kann oft nicht viel erwartet werden. Erst die Gesamtschau auf die Aussagen und die sich ergebenden Widersprüche bringen die wichtigen Informationen zu Tage. Das braucht jedoch Zeit.

Unter den über 70 geladenen Gästen sind nicht nur Mitarbeiter der Dienste. Ein ganz wesentlicher Bereich ist auch die Zusammenarbeit von Firmen mit Geheimdiensten. Es wurden mehrere Chefs von kooperierenden Unternehmen als Zeugen geladen. Deutsche Firmen haben die Pflicht zu kommen, aber auch ausländische Firmen wie Facebook und Google haben schon Willen zur Kooperation ausgedrückt.

Schwärzungen und Gegenwind

Es war abzusehen, dass die Arbeit des Ausschusses einem gewissen Druck und Schwierigkeiten ausgesetzt ist, da der Konflikt zwischen Regierung und Parlament offensichtlich wird und der Ausschuss auch von der Presse unter Beschuss genommen wird – er wird z. B. als „Staatswohlgefährder" bezeichnet. Wenn dann aber ein Dokument mit dem Namen des Geheimdienst-Tools in der Überschrift komplett geschwärzt ist, mit der Begründung, das habe nichts mit der Ausschussarbeit zu tun, „dann fällt uns allen der Unterkiefer runter". Eigentlich müsste jede einzelne dieser Schwärzungen von der Regierung gerechtfertigt werden. Aus Sicht von Sensburg muss nicht darüber diskutiert werden, da der Ausschuss den rechtlichen Anspruch schlichtweg hat. Wenn die Bundesregierung das auch nach erneutem Durchlesen des Urteils anders sieht, müsste dieser Konflikt gerichtlich geklärt werden. Das würde jedoch nur Zeit kosten. Sensburg hat die Hoffnung, dass die Bundesregierung das verstanden hat, dass die bisherigen Schwärzungen nicht in Ordnung waren und dass dann nur noch über einen kleinen Teil der Schwärzungen diskutiert werden muss. Eine Forderung ist außerdem, nicht von irrelevanten Aktenbergen arbeitsunfähig gemacht zu werden, sondern die wesentlichen Akten zur Verfügung gestellt zu bekommen.

Zeitplanung

Anfang dieses Jahres sollten die *Five-Eyes*-Staaten thematisiert werden. Es ist nicht klug, nur auf die amerikanischen Dienste zu schauen. Es scheint erfolgversprechender, auch den GCHQ zu betrachten, da dieser ein Geheimdienst eines EU-Mitgliedslandes ist und der Rechtssprechung des Europäischen Parlaments zur Vorratsdatenspeicherung unterliegt. Die Briten brauchen aber „noch ein bisschen Motivationsunterstützung", um sich zu öffnen. Sensburgs Ziel ist es, bis Ende 2016 den Abschlussbericht zu veröffentlichen, damit die aktuelle Bundesregierung dann unter Druck gesetzt werden kann, diese Empfehlungen noch vor Ablauf dieser Legislaturperiode umzusetzen, da das Thema sonst zum Wahlkampfthema wird.

Patrick Sensburg

Patrick Sensburg ist Bundestagsabgeordneter für die CDU, er war vormals Professor an der Fachhochschule des Bundes für öffentliche Verwaltung im Fachbereich Kriminalpolizei/BKA. Er ist Vorsitzender des NSA-Untersuchungsausschusses des Bundestages..

Handlungsempfehlungen

Über die Ergebnisse und Handlungsempfehlungen kann noch nicht viel ausgesagt werden. Sensburg vermutet, dass das Thema BND-Gesetz „eines sein könnte, über das man noch mal nachdenken muss." Auch über die Trennung von G10 und Datenschutzbeauftragtem muss nachgedacht werden. Da, wo Eingriffe massiv sind, muss auch die Kontrolle stärker werden. Es muss überlegt werden, wie die parlamentarische Kontrolle verbessert werden kann. Es kann nicht sein, dass jedem Sachbearbeiter der Dienste konstant bei seiner Arbeit über die Schulter geschaut wird, aber wir müssen ein System haben, wo wir systemische Fehler auch erkennen und nicht in den Kontrollgremien abnicken. Es werden in Deutschland, als einem von wenigen Ländern, große Anstrengungen zur Aufklärung unternommen. Der Aufwand, der sich durch das Schwärzen der Akten für den Ausschuss aber auch für die *Clearingstellen* der Bundesregierung ergibt, sollte jedoch minimiert werden. Es kann nicht Aufgabe des Ausschusses sein, „detailliert über Entschwärzungen zu diskutieren".

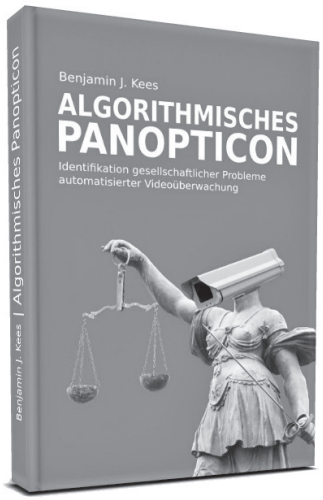
Die Vorschläge sollten aus Sicht des BND nicht als vollkommen ablehnenswert betrachtet werden. Die großen Anstrengungen lohnen sich für Deutschland nämlich auch aus wirtschaftlicher Sicht. Wir haben zur Zeit eine große Chance, den Standort Deutschland für die IT-Branche wieder attraktiver zu machen. Ein kluger Umgang mit Daten und Datenschutz ist dafür sehr interessant.

Patrick Sensburg ist sich sicher, dass es nicht nur um Betroffenheit der Bürgerinnen und Bürger bezüglich Datensicherheit, Datenschutz und Bürgerrechte geht, sondern „es geht zum größten Teil ganz klar um Wirtschaftsspionage." Der größte Teil findet aus klar definierten Machtinteressen und wirtschaftspolitischen Interessen statt – weniger, um etwa Anschläge zu verhindern.

Benjamin Kees

FIfF-Studienpreis 2014

Automatisierte Videoüberwachung – schädlich, gesetzeswidrig und als Buch



Algorithmen erfassen, analysieren und beurteilen jede Regung im öffentlichen Raum einer Großstadt. Was wie Science-Fiction klingt, wird von Wissenschaft und Forschung längst mit Hochdruck für einen baldigen Einsatz vorangetrieben. Angestrebt wird eine möglichst umfassend automatisierte Überwachung, die nicht nur die Aufgabe der OperateurInnen übernimmt, sondern alle Möglichkeiten digitaler Datenerhebung und Informationsverarbeitung ausreizt. Dabei wird jedoch konsequent ignoriert, wie wichtig es für einen mit den Grundrechten vereinbaren Einsatz ist, die erhofften Vorteile gegen mögliche Risiken abzuwägen.

In meiner Diplomararbeit „Identifikation gesellschaftlicher Probleme automatisierter Videoüberwachung", die auf der FIfFKon 2014 mit dem FIfF-Studienpreis ausgezeichnet wurde, werden anhand aktueller wissenschaftlicher Publikationen die Funktionsweise und Fähigkeiten eines wahrscheinlichen Überwachungssystems für den öffentlichen Raum entworfen und dieses aus informationstechnischer, soziologischer, psychologischer und rechtlicher Perspektive auf gesellschaftliche Probleme hin untersucht. Wie in der FIfF-Kommunikation 2/2014 bereits näher ausgeführt, werden in der Arbeit die Unvereinbarkeit der Überwachungsaufgabe mit Grundprinzipien des Datenschutzes hergeleitet, Einfallstore für automatisierte Diskriminierung aufgezeigt, die Rolle der Operateure („Es schaut ja noch mal jemand drauf!") als vermeintliche Legitimation umfangreicher Automatisierung als Feigenblatt entlarvt und die Auswirkungen auf Individuen und Gesellschaft beschrieben. Außerdem wurden Schlussfolgerungen für die Verantwortung der Informatik und die Methodiken der Technikfolgeabschätzung gezogen.

Nach dem Prinzip der Verhältnismäßigkeit beim Eingriff in Grundrechte, die mit Überwachung im öffentlich zugänglichen Raum einhergeht, müssen Notwendigkeit und Tauglichkeit einer Überwachungsmaßnahme abgewogen werden gegen die Schwere des Grundrechtseingriffes. Die Arbeit konzentriert sich auf die Waagschale möglicher negativer Auswirkungen. Was in der anderen liegt, nämlich die Tauglichkeit für einen Sicherheitsgewinn, kann nur am Rande behandelt werden, wird aber grundsätzlich angezweifelt. Um abzuschätzen, ob ein Computer z. B. in der Lage sein kann, anhand von Videomaterial vor einem bevorstehenden terroristischen Anschlag zu warnen, stelle man sich die Frage: „Wie läuft eigentlich ein Terrorist?" Außerdem wissen wir ja nun, dass Sicherheit und Terrorabwehr nur immer wieder als Vorwand angeführt werden. In den Vorträgen der

FIfF-Konferenz wurde deutlich, dass vor allem für einen Machtgewinn und aus wirtschaftlichen Interessen derartig viele Bereiche überwacht werden.

Um festzustellen, dass computergestützte Auswertung von Videobildern unrechtmäßig ist, muss man jedoch gar nicht so weit gehen, düstere Zukunftsszenarien vernetzter, flächendeckender Überwachung zu entwerfen. Schon ganz einfache Ansätze automatisierter Überwachung sind rechtswidrig. Das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Programm MuViT, das mehrere Projekte des BMBF zu Mustererkennung und Videotracking im Rahmen von Videoüberwachung rechtlich und ethisch begleitete, schlussfolgerte jüngst, dass die momentane Rechtsgrundlage nicht für eine automatisierte Auswertung von Videoüberwachungsbildern ausreicht, so dass ihr Einsatz dem Staat versagt bleibt, bis die Rechtslage an die geänderten Erfordernisse angepasst wird. In der Handreichung des MuViT-Projekts werden lediglich sehr sanfte Szenarien automatisierter Videoüberwachung betrachtet, bei denen Videobilder nicht gespeichert und Informationen auch nicht mit anderen Systemen oder Institutionen ausgetauscht werden. Etwa ein Systems, das Gewalt und für den Drogenhandel typische Bewegungsabläufe auf einem Marktplatz automatisiert erkennt und menschliche OperateurInnen darauf aufmerksam machen soll. Bereits dieses System wird nach dem geltenden Gesetz eindeutig als unzulässig bewertet. Deutlich wird daran, dass von der EU und Deutschland geförderte Forschungsprojekte, die zum Teil vollkommen andere Dimensionen der Überwachung vorbereiten gänzlicher Unfug sind. Ergebnisse einer solchen Forschung können ausschließlich für den Export genutzt werden oder führen durch Begehrlichkeiten dazu, dass Gesetze angepasst und Grundrechte weiter geschwächt werden.

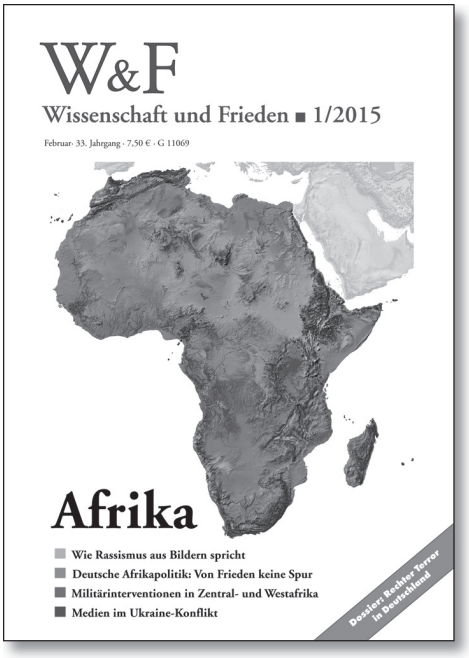
Die Diplomarbeit erscheint in diesen Tagen in überarbeiteter und auch für NichttechnikerInnen verständlicher Form unter dem Titel „Algorithmisches Panopticon“ als Buch im Verlagshaus Monsenstein und Vannerdat in der Edition MV-Wissenschaft. (ISBN 978-3-95645-533-9, www.Algoropticon.de)

Wissenschaft & Frieden 1/2015 „Afrika“

und Dossier: „Rechter Terror in Deutschland“

Afrika schafft es in der Regel nur in die Nachrichten, wenn Konflikte besonders gewaltförmig eskalieren. Dabei wiederholt sich immer wieder das gleiche Muster: Konflikte werden jahrelang ignoriert, bis sie sich so zuspitzen, dass sie nicht mehr ignoriert werden können und »die Weltgemeinschaft« auf den Plan rufen. Der medialen Erregung folgt eine eilige militärische Antwort, das Thema ist aber bald wieder vergessen, wenn es nicht zu einer noch stärkeren Eskalation der Gewalt kommt. Für die Ursachen der Konflikte interessiert man sich nicht. Abgesehen von Kriegen und Katastrophen kommt Afrika in unserer Öffentlichkeit nur als der Kontinent vor, aus dem die Flüchtlinge kommen, die man in Europa nicht haben will. W&F schaut im Schwerpunkt dieser Ausgabe genauer auf einige Länder Afrikas und auf die Rolle Deutschlands. Außerhalb des Schwerpunktes informieren Artikel über die Einschränkung des Informationsrechts des Bundestages aufgrund eines Urteils des Bundesverfassungsgerichtes, die 100-jährige Geschichte der Internationalen Frauenliga für Frieden und Freiheit und die Funktionsweise der deutschen (und US-) Medien im Ukrainekonflikt.

Mit dem rechten Terror in Deutschland befasst sich das Dossier, das dieser Ausgabe beiliegt. In München läuft der Prozess zu den rassistischen Morden des »Nationalsozialistischen Untergrunds«, in den Untersuchungsausschüssen mehrerer Bundesländer kommt zur Sprache, dass V-Leute der Nachrichtendienste massiv in den neonazistischen Strukturen der 1990er Jahre mitmischten, die Pegida-und HoGeSa-Bewegungen verzeichneten in den letzten Wochen hohe Teilnehmerzahlen, Hetze und Gewalt gegen Flüchtlinge und MigrantInnen nehmen zu. Bei der Festlegung des Themas vor einem Jahr konnte die Redaktion nicht ahnen, dass der »Rechte Terror in Deutschland« bei Erscheinen dieses W&F beiliegenden Dossiers so aktuell sein würde.



Wissenschaft & Frieden, 1-2015, **Afrika**, € 7,50 plus Porto.

W&F erscheint vierteljährlich. Jahresabo 30 €, ermäßigt 20 €, Ausland 35 €, ermäßigt 25 €, Förderabo 60 €. W&F erscheint auch in digitaler Form – als PDF und ePub. Das Abo kostet für Bezieher der Printausgabe zusätzlich 5 € jährlich – als elektronisches Abo ohne Printausgabe 20 € jährlich.

Bezug: W&F, Beringstr. 14, 53115 Bonn,
E-Mail: *buero-bonn@wissenschaft-und-frieden.de*,
www.wissenschaft-und-frieden.de

FIfF e.V.

Im FIfF haben sich rund 700 engagierte Frauen und Männer aus Lehre, Forschung, Entwicklung und Anwendung der Informatik und Informationstechnik zusammengeschlossen, die sich nicht nur für die technischen Aspekte, sondern auch für die gesellschaftlichen Auswirkungen und Bezüge des Fachgebietes verantwortlich fühlen. Wir wollen, dass Informationstechnik im Dienst einer lebenswerten Welt steht. Das FIfF bietet ein Forum für eine kritische und lebendige Auseinandersetzung – offen für alle, die daran mitarbeiten wollen oder auch einfach nur informiert bleiben wollen.

Vierteljährlich erhalten Mitglieder die Fachzeitschrift FIfF-Kommunikation mit Artikeln zu aktuellen Themen, problematischen Entwicklungen und innovativen Konzepten für eine verträgliche Informationstechnik. In vielen Städten gibt es regionale AnsprechpartnerInnen oder Regionalgruppen, die dezentral Themen bearbeiten und Veranstaltungen durchführen. Jährlich findet an wechselndem Ort eine Fachtagung statt, zu der TeilnehmerInnen und ReferentInnen aus dem ganzen Bundesgebiet und darüber hinaus anreisen. Darüber hinaus beteiligt sich das FIfF regelmäßig an weiteren Veranstaltungen, Publikationen, vermittelt bei Presse- oder Vortragsanfragen ExpertInnen, führt Studien durch und gibt Stellungnahmen ab etc. Das FIfF kooperiert mit zahlreichen Initiativen und Organisationen im In- und Ausland.

FIfF-Mailinglisten

FIfF-Mailingliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/fiff-L
Beiträge an: *fiff-L@lists.fiff.de*

FIfF-Mitgliederliste
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/mitglieder
Beiträge an: *mitglieder@lists.fiff.de*

Mailingliste Videoüberwachung:
An- und Abmeldungen an:
http://lists.fiff.de/mailman/listinfo/cctv-L
Beiträge an: *cctv-L@lists.fiff.de*

FIfF online

Das ganze FIfF
www.fiff.de
Twitter FIfF e.V. – *@FIfF_de*

Cyberpeace
cyberpeace.fiff.de
Twitter Cyberpeace – *@FIfF_AK_RUIN*

Faire Computer
blog.faire-computer.de
Twitter Faire Computer – *@FaireComputer*

Newsletter (im Mitglieder-Wiki)
https://wiki.fiff.de/wiki/NewsLetter

FIfF-Beirat

Michael Ahlmann (Bremen); **Peter Bittner** (Bad Homburg); **Dagmar Boedicker** (München); Dr. **Phillip W. Brunst** (Köln); Prof. Dr. **Wolfgang Coy** (Berlin); Prof. Dr. **Wolfgang Däubler** (Bremen); Prof. Dr. **Leonie Dreschler-Fischer** (Hamburg); Prof. Dr. **Christiane Floyd** (Hamburg); Prof. Dr. **Klaus Fuchs-Kittowski** (Berlin); Prof. Dr. **Michael Grütz** (Konstanz); Prof. Dr. **Thomas Herrmann** (Bochum); Prof. Dr. **Wolfgang Hesse** (Marburg); Prof. Dr. **Eva Hornecker** (Weimar); **Werner Hülsmann** (Konstanz); **Ulrich Klotz** (Frankfurt); Prof. Dr. **Klaus Köhler** (München); Prof. Dr. **Herbert Kubicek** (Bremen); Dr. **Constanze Kurz** (Berlin); Prof. Dr. **Klaus-Peter Löhr** (Berlin); **Werner Mühlmann** (Oppung); Prof. Dr. **Frieder Nake** (Bremen); Prof. Dr. **Rolf Oberliesen** (Bremen); Prof. Dr. **Arno Rolf** (Hamburg); Prof. Dr. **Alexander Rossnagel** (Kassel); Prof. Dr. **Gerhard Sagerer** (Bielefeld); Prof. Dr. **Gabriele Schade** (Erfurt); Prof. Dr. **Dirk Siefkes** (Berlin); **Ralf E. Streibl** (Bremen); Prof. Dr. **Marie-Theres Tinnefeld** (München); Dr. **Gerhard Wohland** (Waldorfhäslach)

FIfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Prof. Dr. **Dietrich Meyer-Ebrecht** (stellv. Vorsitzender) – Aachen
Sylvia Johnigk – München
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Kai Nothdurft – München
Rainer Rehak – Berlin
Jens Rinne – Mannheim
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
Ingrid Schlagheck – Bremen
Prof. Dr. **Werner Winzerling** – Fulda
Prof. Dr. **Eberhard Zehendner** – Jena

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen
Sara Stadler – Bremen
Thomas Reinhold (Campaigning) – Lübeck

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1 100 Stück
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck, Sara Stadler
Schwerpunktredaktion	Rainer Rehak, Benjamin Kees
V.i.S.d.P.	Stefan Hügel
FIfF-Überall	Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an *hubert.biskup@gmx.de.* Ansprechpartner für die jeweiligen Regionalgruppen finden Sie im Internet auf unserer Webseite *http://www.fiff.de/regional*
Retrospektive	Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de*
Layout	Berthold Schroeder
Titelbild	Logo der FIfF-Konferenz 2014, Benjamin Kees
Druck	Meiners Druck, Bremen

Die FIfF-Kommunikation ist die Zeitschrift des „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V." (FIfF). Die Beiträge sollen die Diskussionen unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige AutorInnen-Meinung wieder.

Nachdruckgenehmigung wird nach Rücksprache mit der Redaktion in der Regel gern erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

Wichtiger Hinweis: Wir bitten alle Mitglieder und Abonnenten, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

Aktuelle Ankündigungen

(mehr Termine unter *www.fiff.de*)

Verleihung der BigBrotherAwards 2015
17. April, Hechelei in Bielefeld

31. FIfF-Konferenz 2015
6. bis 8. November, Friedrich-Alexander-Universität in Erlangen
„Kommerzialisierung des Sozialen: Markt und Macht im Zeitalter der digitalen Kompletterfassung"

FIfF-Vorstandssitzung
27. Juni, Bremen

FIfF-Kommunikation
2/2015 »Datenschutz«
Eberhard Zehendner, Stefan Hügel
Redaktionsschluss: 1. Mai 2015

3/2015 »Rüstung und Informatik/Cyberpeace«
Dietrich Meyer-Ebrecht, Hans-Jörg Kreowski u.a.
Redaktionsschluss: 7. August 2015

4/2015 »Cybercrime«
Eberhard Zehendner
Redaktionsschluss: 6. November 2015

1/2016 »31. FIfF-Konferenz 2015«
Stefan Hügel u.a.
Redaktionsschluss: 5. Februar 2016

W&F – Wissenschaft & Frieden
1/15 – Afrika (mit Dossier 77: Rechter Terror in Deutschland)
2/15 – Technikkonflikte (mit Dossier 78: Zivilklauseln)
3/15 – Friedensverhandlungen (mit Dossier 79: Kriegführung im Cyberspace)

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik
#206/207 (2-3/14) – Geheimdienstliche Kommunikationsüberwachung außer Kontrolle?
#208 (4/14) – Europäische Abschottungstendenzen
#209 (1/15) – Verbot der Suizidbeihilfe
#210 (2/15) – Cybersicherheit

DANA – Datenschutz-Nachrichten
3/14 – Datenschutz im Reiseverkehr
4/14 – Big Data
1/15 – Mobilität/Telematik
2/15 – Flüchtlinge und Datenschutz

Das FIfF-Büro

Geschäftsstelle FIfF e. V.
Ingrid Schlagheck (Geschäftsführung) und Sara Stadler
Goetheplatz 4, D-28203 Bremen
Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56
E-Mail: fiff@fiff.de
Die Bürozeiten finden Sie unter *www.fiff.de*

neue Bankverbindung
Bank für Sozialwirtschaft (BFS) Köln
Spendenkonto:
IBAN: DE79 3702 0500 0001 3828 03
BIC: BFSWDE33XXX

Kontakt zur Redaktion der FIfF-Kommunikation:
redaktion@fiff.de

Schluss FIfF

Theodor Fontane

Die Brück‘ am Tay

(28. Dezember 1879)

When shall we three meet again?
– Macbeth

»Wann treffen wir drei wieder zusamm?«
»Um die siebente Stund‘, am Brückendamm.«
»Am Mittelpfeiler.«
»Ich lösche die Flamm.«
»Ich mit«

»Ich komme vom Norden her.«
»Und ich vom Süden.«
»Und ich vom Meer.«

»Hei, das gibt einen Ringelreihn,
Und die Brücke muß in den Grund hinein.«

»Und der Zug, der in die Brücke tritt
Um die siebente Stund’?«
»Ei, der muß mit.«
»Muß mit«

»Tand, Tand
Ist das Gebilde von Menschenhand!«

Auf der *Norderseite*, das Brückenhaus –
Alle Fenster sehen nach Süden aus,
Und die Brücknersleut’ ohne Rast und Ruh
Und in Bangen sehen nach Süden zu,
Sehen und warten, ob nicht ein Licht
Übers Wasser hin »Ich komme« spricht,
»Ich komme, trotz Nacht und Sturmesflug,
Ich, der Edinburger Zug.«

Und der Brückner jetzt: »Ich seh’ einen Schein
Am anderen Ufer. Das muß er sein.
Nun, Mutter, weg mit dem bangen Traum,
Unser Johnie kommt und will seinen Baum,
Und was noch am Baume von Lichtern ist,
Zünd’ alles an wie zum heiligen Christ,
Der will heuer *zweimal* mit uns sein, —
Und in elf Minuten ist er herein.«

Und es war der Zug. Am *Süder*turm
Keucht er vorbei jetzt gegen den Sturm,
Und Johnie spricht: »Die Brücke noch!
Aber was tut es, wir zwingen es doch.
Ein fester Kessel, ein doppelter Dampf,
Die bleiben Sieger in solchem Kampf.
Und wie’s auch rast und ringt und rennt,
Wir kriegen es unter, das Element.

Und unser Stolz ist unsre Brück’;
Ich lache, denk’ ich an früher zurück,
An all den Jammer und all die Not
Mit dem elend alten Schifferboot;
Wie manche liebe Christfestnacht
Hab’ ich im Fährhaus zugebracht
Und sah unsrer Fenster lichten Schein
Und zählte und konnte nicht drüben sein.«

Auf der Norderseite, das Brückenhaus –
Alle Fenster sehen nach Süden aus,
Und die Brücknersleut’ ohne Rast und Ruh
Und in Bangen sehen nach Süden zu;
Denn wütender wurde der Winde Spiel,
Und jetzt, als ob Feuer vom Himmel fiel’,
Erglüht es in niederschießender Pracht
Überm Wasser unten… Und wieder ist Nacht.

»Wann treffen wir drei wieder zusamm?«
»Um Mitternacht, am Bergeskamm,«
»Auf dem hohen Moor, am Erlenstamm.«

»Ich komme.«
»Ich mit«
»Ich nenn’ euch die Zahl.«
»Und ich die Namen.«

»Und ich die Qual.«
»Hei!
Wie Splitter brach das Gebälk entzwei.«

»Tand, Tand
Ist das Gebilde von Menschenhand.«

Geeignete Texte für den SchlussFIfF bitte mit Quellenangabe an *redaktion@fiff.de* senden.