H 7625

FIfF-Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

31. Jahrgang 2014 Einzelpreis: 7 EUR

3/2014 – September 2014

Gender

und Informatik

ISSN 0938-3476

• Gustav-Heinemann-Forum • Ethik und Data-Loss-Prevention • Kraft der Metadaten •

FIfF Kommunikation

Titelbild: UNIVAC Model 120 – Foto: Department of Interior, Bureau of Mines, 1961
Rails Girls Leipzig Workshops 2013 – Foto: Natalie Sontopski (links)

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V.

Inhalt

Ausgabe 3/2014

inhaltt

Editorial

Gender – seit Jahrzehnten gehört dieses Thema zum festen Kanon politischer Debatten. Obwohl diese Debatten zweifellos zu Fortschritten geführt haben, gibt es nach wie vor Bereiche, in denen weiter an der Erfüllung des Grundgesetzauftrags gearbeitet werden muss: *Männer und Frauen sind gleichberechtigt. Der Staat fördert die tatsächliche Durchsetzung der Gleichberechtigung von Frauen und Männern und wirkt auf die Beseitigung bestehender Nachteile hin* (Art. 3 (2) GG).

Gleichzeitig stehen wir heftigen, zum Teil mit auffälliger Aggressivität geführten Diskussionen gegenüber. Viele Betroffene beteiligten sich am *#Aufschrei* gegen Sexismus im Alltag, ausgezeichnet mit dem Grimme-Preis, und an den Diskussionen über seinen Anlass, den Berichten über Übergriffe eines hochrangigen Politikers gegenüber einer Journalistin. In den USA sorgte ein Vorfall für Aufsehen, bei dem ein Frau, die sich auf einer Konferenz Belästigungen ausgesetzt sah, ein Bild der Belästiger twitterte, mit einem entsprechenden Kommentar – was sie anschließend die Arbeitsstelle kostete.

Der Schwerpunkt dieser Ausgabe, der von *Britta Schinzel* und *Sara Stadler* zusammengestellt wurde, nimmt sich dieses Themas an. „*Insbesondere Feministinnen sind in der Netzwelt prominentes Ziel unter anderem sexistischer und homophober Angriffe, und die Technik, die uns alltäglich umgibt, spiegelt nicht selten das sexistische Designparadigma wider, dass sich Frauen nur dann an einen Computer trauen, wenn er pink ist*“, stellen sie einleitend fest. Sie beleuchten die Rolle von Gender in der Informatik in verschiedenen Bereichen und aus unterschiedlichen Perspektiven. „*Zu den identifizierten Ausschließungen und Angriffen werden dabei jeweils Gegenstrategien vorgetragen, aber es bleibt viel zu tun.*“

Weltweite Ausspähung der Bevölkerung – Rechtliche Bewertung und Handlungsoptionen, so lautete der Titel des diesjährigen *Gustav-Heinemann-Forums*, das von der *Humanistischen Union* in Rastatt durchgeführt wurde. Eines der Panels, das sich mit technischen Möglichkeiten, Bedrohungen und demokratischer Beherrschbarkeit auseinandersetzte, wurde mit starker Beteiligung des FIfF organisiert – gleichzeitig ein Element unserer *Cyberpeace*-Kampagne, bei der ebenfalls die Humanistische Union unser Partner ist.

Kompromittierung von Geräten und Infrastruktur, der heimliche Einbau von Überwachungstechnik in IT-Produkte und Desinformation und Propaganda sind Instrumente der geheimdienstlichen Ausspähung, so *Sylvia Johnigk* in ihrem Beitrag zur Tagung und zu dieser *FIfF-Kommunikation*. *Dietrich Meyer-Ebrecht* weist auf die unterschiedlichen Faktoren der Ausspähung hin: Innen- und Außenpolitik, Gesellschaft und Psychologie. „*Letztlich hat die Gesellschaft den Schlüssel für eine Veränderung in der Hand. Loslösen müssen wir uns von der verführerischen Annehmlichkeit des scheinbaren Umsonst von Internetdienstleistungen und -werkzeugen*“, stellt er fest. „*Selbst tätig zu werden, andere dazu zu ermutigen, zu unterstützen – das hat mindestens zwei Effekte über den konkreten Nutzen hinaus: Wir erfahren Technik und ihre Mechanismen, wir holen die Technik ein Stück heraus aus ihrer Abstraktheit. Und uns wird bewusst, dass wir uns ein Stück Freiheit zurückerobern. Denn ‚beobachtet werden macht unfrei', sagt uns Glenn Greenwald.*“

Ethische Überlegungen zum Einsatz von Data- Loss-Prevention-Tools in Unternehmen stellt *Klaus Haller* in seinem Beitrag an, und trifft damit auf grundsätzliche Probleme von Maßnahmen der IT-Sicherheit. IT-Sicherheit, die Sicherheit vor Cyberangriffen, dem unberechtigten Eindringen in unsere Computersysteme, ist das Ziel, das wir durch eine Reihe von Maßnahmen erreichen wollen. Doch die konsequente Anwendung von Maßnahmen der IT-Sicherheit hätte sehr wahrscheinlich auch die Enthüllungen von Edward Snowden verhindert, wie *Bob Toxen* in der diesjährigen Mai-Ausgabe der *Communications of the ACM* feststellt. Es gibt hier offensichtlich ein ethisches Dilemma, das nicht leicht aufzulösen ist.

Nur sehr langsam setzt sich die Erkenntnis durch, wie gefährlich das Sammeln von Metadaten der Kommunikation für die Menschenrechte ist. Allzu häufig wird immer noch abgewiegelt, wenn Überwachung „nur“ anhand dieser Metadaten, und nicht anhand der Kommunikationsinhalte erfolgt – ob bewusst oder unbewusst, eine Täuschung der Öffentlichkeit. *Joachim Jakobs* weist in seinem Beitrag erneut auf die Bedeutung dieser Bewegungsdaten für die Ausspähung der Kommunikation hin und gibt einen Überblick über die dafür heute bestehenden technischen Möglichkeiten: *Die Kraft der Metadaten*.

Am 7.-9. November 2014 wird unsere diesjährige Jahrestagung in Berlin stattfinden: *Der Fall des Geheimen – ein Blick unter den eigenen Teppich*. „*Wir wollen die Rolle Deutschlands und insbesondere der deutschen Geheimdienste im Kontext der älteren und aktuellen Erkenntnisse bearbeiten. Wie kommt es, dass Deutschland nach wie vor oft als ‚Datenschutzmekka' und ‚Demokratievorzeigestaat' bezeichnet wird, obwohl sich gerade hier einer der Dreh- und Angelpunkte der flächendeckenden Überwachung Europas, der globalen Drohnenmord-Koordination, der geheimen Folterflüge und generell der allgemeinen Kriegslogistik innerhalb Europas befindet?*“ Wir erwarten eine Reihe hochkarätiger Referenten, die politische, rechtliche, wirtschaftliche, historische und philosophische Aspekte der Thematik abdecken werden.

Unsere Kolumnen runden die Ausgabe ab. *Sebastian Jekutschs* Kolumne *Betrifft: Faire Computer* wird in dieser Ausgabe durch einen Beitrag von *Michael Leben* ergänzt, in dem er sich mit der *Krebserkrankung auf Samsungs Karriereleiter* auseinandersetzt. *Ute Bernhardt* und *Ingo Ruhmann* stellen in der Kolumne *Betrifft:*

Cyberpeace fest, dass Deutschland zum digitalen *failed state* geworden ist und beschreiben die Konsequenzen, wenn der Staat das Gewaltmonopol aufkündigt. *Klaus-Peter Löhr*, Beiratsmitglied des FIfF, fordert in seiner Kolumne *Wehrt Euch!*, das Briefgeheimnis im Netz durch Verschlüsselung technisch zu sichern.

Wir wünschen unseren Leserinnen und Lesern eine interessante und anregende Lektüre – und viele neue Erkenntnisse und Einsichten.

Stefan Hügel
für die Redaktion

Brief an das FIfF

Verantwortung

Liebe Mitglieder des FIfF, liebe Leserinnen und Leser,

in diesen Tagen jährt sich zum hundertsten Mal der Beginn des Ersten Weltkriegs, der „Urkatastrophe" des 20. Jahrhunderts. Als aus Anlass der Ermordung des österreichischen Thronfolgers Erzherzog Franz Ferdinand und seiner Frau in Sarajevo Regierungen und Militärs „Verantwortung übernahmen" – so würden sie es heute wohl nennen –, übergaben sie damit 17 Millionen Menschen dem Tod.

Auch heute stehen wir wieder einer Reihe von Konfliktherden gegenüber, und immer lauter wird der Ruf, Deutschland müsste an der Seite seiner Bündnispartner „Verantwortung übernehmen" – also militärisch eingreifen. Sei es der Konflikt in der Ukraine oder in Gaza oder im Irak – gerade bei Letzterem gibt es inzwischen auch Stimmen aus der Opposition, die fordern, dem Kampf gegen die islamistische Organisation IS durch Waffenlieferungen zu begegnen. Angesichts mancher Nachrichten über Gräueltaten ist man geneigt zuzustimmen – und erinnert sich doch im nächsten Moment wieder an frühere Konflikte, als die Öffentlichkeit getäuscht wurde, um Militäroperationen zu rechtfertigen: Der angebliche „Hufeisenplan" der Serben im Kosovo, mit dem der damalige Bundesverteidigungsminister Rudolf Scharping argumentierte, und die Berichte über Massenvernichtungswaffen im Irak vor dem UN-Sicherheitsrat durch den damaligen US-Außenminister Colin Powell – die er später öffentlich bedauerte. Was ist richtig, was ist falsch?

Gleichzeitig wird immer häufiger gefordert, generell „Verantwortung zu übernehmen", vom Bundespräsidenten, vom Bundesaußenminster, von der Bundesverteidigungsministerin, von Politikerinnen und Politiker aller Couleur – schon erhebt ein Akronym die Forderung zur Doktrin: *R2P*, ‚resposibility to protect'. Neuerdings hören wir diese Forderungen auch aus den Reihen der Linken, von den einmal als pazifistische Partei gegründeten Grünen schon lange. Es heißt lediglich, das Parlament müsse in solche Entscheidungen einbezogen werden. Eine richtige Forderung, zweifellos – am Ergebnis hat dies in der Vergangenheit freilich wenig geändert. Immerhin wäre zu hoffen, dass die damit verbundenen Debatten mehr Transparenz in die Entscheidungen bringen, und die Täuschung der Öffentlichkeit zumindest erschweren. Doch auch hier gilt: Das erste Opfer des Kriegs ist die Wahrheit.

Es besteht schon länger der Eindruck, die Deutschen sollen auf die Normalität solcher Operationen eingestimmt werden, darauf, dass Militär und Waffen geeignete Mittel sind, um in Krisengebieten Frieden zu schaffen. Sicherlich gibt es Entwicklungen, bei denen Diskussionen nicht mehr weiter helfen. Dennoch muss es bei einer zurückhaltenden Politik bleiben. Nur eine Politik, die sich an friedlichen Lösungen orientiert, und Konflikte im Vorfeld mit diplomatischen Mitteln zu verhindern sucht, ist verantwortungsvolle Politik. Nicht zuletzt: Diejenigen, die die Verantwortung „übernehmen", sind nur selten diejenigen, die sie hinterher tragen, die auf den Schlachtfeldern der modernen Kriege Gesundheit und Leben verlieren – auf beiden Seiten, Militär oder Zivilisten.

„Ausspähen unter Freunden – das geht gar nicht." So reagierte die Bundeskanzlerin und ihr Regierungssprecher auf Nachrichten über die nachrichtendienstliche Ausspähung durch US-amerikanische Geheimdienste. Der Bundesnachrichtendienst war offenbar weniger zimperlich und überwachte hochrangige US-amerikanische Politikerinnen und Politiker – und den NATO-Staat Türkei. Es fällt schwer zu glauben, dass zumindest die Bundeskanzlerin darüber nicht informiert war. Auch dies wirft grundsätzliche Fragen der Glaubwürdigkeit von Regierungshandeln auf.

Gleichzeitig gehen die Sicherheitsbehörden auf ihre Weise mit dem Geheimdienstskandal um. Anstatt über eine Reduzierung der menschenrechtsverletzenden Ausspähpraxis nachzudenken, werden neue Forderungen erhoben: Der Bundesnachrichtendienst möchte soziale Netzwerke nun in Echtzeit überwachen. Hier bewies Bundesjustizminister Heiko Maas politischen Instinkt, als er solchen Begehrlichkeiten zunächst einmal eine Absage erteilte. Doch wir können wohl jetzt schon voraussagen, dass sich solche Forderungen wiederholen – bis sie eines Tages umgesetzt werden.

Auch beim – überfälligen – IT-Sicherheitsgesetz sind die Geheimdienste im Spiel. Bundesinnenminister Thomas de Maizière will die „weltweit sicherste" IT in Deutschland etablieren – darunter macht er es wohl nicht. Sieht man sich die aktuellen Entwürfe an, so soll offenbar vor allem der Verfassungsschutz durch neue Stellen vom Sicherheitsgesetz profitieren. Der Verfassungsschutz als Garant der IT-Sicherheit? Nun ja …

Doch wenigstens die Demokratisierung der – meist zu Unrecht – viel gescholtenen Europäischen Union schreitet voran, oder? Der Kommissionspräsident wird von der Bevölkerung gewählt.

(Oder richtiger: Nach langen Diskussionen wird tatsächlich derjenige – Jean-Claude Juncker – als Kommissionspräsident nominiert, der von der relativen Mehrheitspartei zuvor als Spitzenkandidat benannt worden war.) Ein Durchbruch der Demokratie, so wird parteiübergreifend gejubelt.

Doch halt:

> *„Wir beschließen etwas, stellen das dann in den Raum und warten einige Zeit ab, was passiert. Wenn es dann kein großes Geschrei gibt und keine Aufstände, weil die meisten gar nicht begreifen, was da beschlossen wurde, dann machen wir weiter – Schritt für Schritt, bis es kein Zurück mehr gibt."*

Dieses Zitat wird eben jenem Jean-Claude Juncker zugeschrieben. Nun soll man nicht alles, was irgendjemand irgendwann einmal gesagt haben soll, auf die Goldwaage legen. Doch Hoffnung auf echte Demokratisierung machen solche Zitate nicht. Dass Juncker gerade vor einem Jahr nach einem Geheimdienstskandal in Luxemburg – der sogenannten Bombenleger-Affäre *(Affär Bommeleeër)* – sein Amt als Premierminister abgeben musste, passt wohl ins Bild …

Mit FIfFigen Grüßen

Stefan Hügel

Klaus-Peter Löhr

Beiratskolumne

Wehrt Euch!

Seit dem ersten Snowden-Schock ist ein Jahr vergangen. Seitdem haben uns immer neue Enthüllungen in Atem gehalten. Die Empörung war groß, und die langfristigen Folgen sind noch nicht abzusehen. Die Bürger sehen ihre Privatsphäre durch unkontrollierbare Ausspähung bedroht und haben das Gefühl, dass die Politik sie im Stich lässt.

Den meisten Menschen ist allerdings nicht bewusst, dass sie sich an einer Stelle durchaus gegen die Bedrohung wehren können: jeder ist in der Lage, den Inhalt von E-Mails durch Verschlüsselung zuverlässig auch gegen potente Angreifer zu schützen. Würden alle Bürger ihre E-Mails gewohnheitsmäßig verschlüsseln, wäre das Briefgeheimnis im Netz nicht nur theoretisch garantiert, sondern auch technisch gesichert.

Warum geschieht das nicht? Weil wir beim heutigen Stand der Technik nicht erwarten können, dass Erika Mustermann sich der Mühsal der E-Mail-Verschlüsselung unterzieht. Von wenigen Ausnahmen abgesehen ist die einschlägige Software nicht benutzerfreundlich. Als Informatiker haben wir daher die wichtige Aufgabe, in Forschung und Entwicklung das bisher Versäumte nachzuholen. Als Staatsbürger sollten wir aber nicht einfach auf den großen technischen Wurf warten, sondern fragen, wie wir uns der konkreten Utopie einer *flächendeckenden E-Mail-Verschlüsselung* bereits heute annähern können: es gilt, die vorhandenen Möglichkeiten konsequent zu nutzen und evolutionär zu verbessern.

Wer heute E-Mail verschlüsseln will, hat die Wahl zwischen S/MIME und PGP. Beide bieten die gleiche kryptographische Sicherheit. Hier ist nicht der Ort, das Pro und Contra der beiden Ansätze im Detail zu diskutieren. Meine eigene Position ist: im Hinblick auf das Ziel der flächendeckenden Verschlüsselung für jedermann ist S/MIME die bessere Wahl: der S/MIME-Standard wird von jedem Mail-Programm unterstützt, und mit einer gut gestalteten Web-Schnittstelle sind Schlüsselerzeugung und Zertifikatserwerb kinderleicht. (Die Verwaltung und Benutzung des Schlüsselbunds gestaltet sich allerdings je nach Hersteller unterschiedlich – von trivial bis umständlich.)

Ein Plädoyer für S/MIME ist aber letztlich nur dann vertretbar, wenn es gelingt, Zertifizierungsstellen zu schaffen, die 1. einfach, 2. kostenlos, 3. vertrauenswürdig sind; kritisch ist weniger Punkt 2 als vielmehr Punkt 3: es bedarf einer *Offenen Zertifizierungsstelle*, der aufgrund ihrer Konstruktion jeder Bürger vertrauen kann (wie man dem Wahllokal vertraut). Dies wäre eine noble Aufgabe beispielsweise für eine staatsbürgerlich engagierte Stiftung.

Um aber schließlich auf die Verantwortung der Politik zurückzukommen: hier zeigt sich eine Möglichkeit, wie etwas von dem Vertrauen, das die Regierung durch ihr Verhalten in der Snowden-Affäre verloren hat, wiedergewonnen werden könnte. Der Innenminister könnte die Gründung einer Zertifizierungs-Stiftung betreiben und damit zeigen, dass er konkret etwas zum Schutz unserer Privatsphäre tut. Wehren müssen wir uns schon selbst, aber die Politik sollte uns wenigstens nach Kräften dabei unterstützen.

Der Beitrag erscheint auch in Digitale Welt – das Magazin für die Informationsgesellschaft 3/2014

Klaus-Peter Löhr

Prof. (a.D.) Dr.-Ing. **Klaus-Peter Löhr,** Fachbereich Mathematik und Informatik, Freie Universität Berlin; Fellow der Gesellschaft für Informatik; Mitglied im Beirat des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung.

FIfF-Konferenz (Fiffkon) 2014

Der Fall des Geheimen

ein Blick unter den eigenen Teppich

7.-9. November 2014 in Berlin (Technische Universität)

Wir wollen die Rolle Deutschlands und insbesondere der deutschen Geheimdienste im Kontext der älteren und aktuellen Erkenntnisse (J. Radack, E. Snowden bis J. Foschepoth) bearbeiten. Wie kommt es, dass Deutschland nach wie vor oft als „Datenschutzmekka" und „Demokratievorzeigestaat" bezeichnet wird, obwohl sich gerade hier einer der Dreh- und Angelpunkte der flächendeckenden Überwachung Europas, der globalen Drohnenmord-Koordination, der geheimen Folterflüge und generell der allgemeinen Kriegslogistik innerhalb Europas befindet. Inwiefern ist die Rolle Deutschlands also keine widerwillig helfende, ja fast opferhafte, sondern ganz im Gegenteil eine aktive, tragende und führende im sich immer weiter offenbarenden antidemokratischen Zustand der Welt?

Um die Gesamtsituation beschreiben und verstehen zu können, ist es hilfreich zu wissen, wie diese Systeme gebaut sind, nach welchen normativen Weltauffassungen sie konzipiert werden und in welchen Kontexten sie verwendet werden, doch das allein genügt nicht: Mit historischem Blick auf die deutschen Geheimdienste und ihre technisch-organisatorische Entwicklung, mit aktuellen Analysen der gegenwärtigen Lage und Betrachtungen geheimdienstlicher Verflechtungen, mit Aufdeckung ihres technischen Apparats und Bewertung ihrer rechtlichen Einhegung wollen wir helfen, Licht ins Dunkel und verstehbare Ordnung ins geheime Chaos zu bringen. Die Zusammenarbeit von Geheimdiensten, deutschen Telekommunikationsunternehmen und Informatikern bedürfen einer besonderen Aufmerksamkeit, weil die oben beschriebene Entwicklung – zumindest auch – auf das Werk dieser größtenteils kooperierenden Technikergemeinde zurückzuführen ist.

Dabei sind die zum Verständnis nötigen kritisch-technischen Kompetenzen u. a. im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung oder im Chaos Computer Club zu finden, doch für eine aktuelle und perspektivische Einschätzung der Lage sind politische, rechtliche, wirtschaftliche, historische und philosophische Aspekte ebenso essenziell, weswegen die eingeladenen Vortragenden diese Vielfalt abdecken sollen.

Ute Bernhardt ist Informatikerin und beschäftigt sich seit Jahren kritisch mit der Geschichte der Geheimdienste, dem Verhältnis von Wissenschaft und Frieden sowie der folgenreichen Beziehung von Informatik und Militär. Sie hat Lehraufträge an der Fachhochschule Bonn-Rhein-Sieg und der FernUni Hagen.

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

Hans-Jörg Kreowski ist Informatiker und leitet die Forschungsgruppe *Theoretische Informatik* der Universität Bremen. Darüber hinaus arbeitet er auf dem Gebiet *Informatik und Gesellschaft* und ist Herausgeber mehrerer Bücher zu diesem Thema.

Constanze Kurz ist Informatikerin im Bereich *Informatik und Gesellschaft* und Aktivistin. Sie schreibt regelmäßig für große deutsche Zeitungen (z. B. FAZ), ist des Öfteren Sachverständige im Deutschen Bundestag und zudem erfolgreiche Sachbuchautorin, u. a. zu den Themen Datenschutz oder gesellschaftliche Auswirkungen von Automatisierung.

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 hielt Positionen in verschiedenen NGOs wie der European Digital Rights Institution (EDRi) oder dem Chaos Computer Club (CCC). Aktuell beschäftigt er sich mit Unternehmen, die Überwachungssoftware verkaufen.

Linus Neumann ist Aktivist und Autor im Bereich digitale Gesellschaft. Er ist einer der Sprecher des *Chaos Computer Clubs* (CCC), für den er bereits mehrmals in Ausschüssen des Deutschen Bundestags als Sachverständiger für IT-Sicherheit auftrat.

Wolfgang Nešković ist fraktionsloser Politiker (vormals SPD, dann Bündnis 90/Die Grünen und zuletzt Die Linke) und war Richter am Bundesgerichtshof. Er war langjähriges Mitglied des Deutschen Bundestages und dort auch lange Mitglied des Parlamentarischen Kontrollgremiums (PKG).

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.

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 dem Ämtern für Verfassungsschutz sorgten für Aufsehen. Sie arbeitet für das *Tactical Technology Collective* und ist Referentin im NSA-Untersuchungsausschuss.

Ingo Ruhmann ist Informatiker und arbeitet u. a. zu Technikfolgenabschätzung, Forschungspolitik, IT-Sicherheit, Information Warfare, „Cyberwar", der Geschichte der Geheimdienste und Datenschutz. Er ist Lehrbeauftrager im Studiengang *Security Management* der Fachhochschule Brandenburg.

Peter Schaar ist Vorsitzender der *Europäischen Akademie für Informationsfreiheit und Datenschutz* (EAID). Er war zuvor Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, wobei er sich auch zu BKA-Gesetzen und Geheimdienstbefugnissen äußerte.

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

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.

Hans-Christian Ströbele ist erfahrener Politiker und Rechtsanwalt. Er ist Mitglied des Bundestages und beschäftigt sich u. a. mit Sicherheits-, Rechts- und Entwicklungspolitik. Er ist Mitglied des Parlamentarischen Kontrollgremiums (PKG) und des NSA-Untersuchungsausschusses.

Gregor Wiedemann ist Politologie 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.

Das **Nö-Theater** ist ein politisches Theaterensemble aus Köln, das in ihrem Stück *V wie Verfassungsschutz* die jüngeren Geschehnisse rund um den Verfassungsschutz sehr gut recherchiert und eindrucksvoll künstlerisch verarbeitet präsentiert.

Das Programm der Konferenz, weitere Details und andere Hinweise sind hier zu finden: *http://www.fiffkon.de.*

Einladung zur Mitgliederversammlung 2014

des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF e. V.)

Wir laden fristgerecht und satzungsgemäß zur ordentlichen Mitgliederversammlung 2014 ein.

Sie findet am Sonntag, den 9. November 2014, von 11:00 bis 13:00 Uhr
an der Technischen Universität Berlin, Straße des 17. Juni 135, 10623 Berlin, statt.

Vorläufige Tagesordnung

1. Begrüßung, Feststellung der Beschlussfähigkeit und Festlegung der Protokollführung
2. Beschlussfassung über die Tagesordnung, Geschäftsordnung und Wahlordnung
3. Bericht des Vorstands einschließlich Kassenbericht
4. Bericht der Kassenprüfer
5. Diskussion der Berichte
6. Entlastung des Vorstands
7. Neuwahl der Kassenprüfer
8. Diskussion über Ziele und Arbeit des FIfF, aktuelle Themen, Verabschiedung von Stellungnahmen, Berichte aus den Regionalgruppen
9. Anträge an die Mitgliederversammlung
   Anträge müssen schriftlich bis drei Wochen vor der Mitgliederversammlung bei der FIfF-Geschäftsstelle eingegangen sein
10. Verschiedenes

gez. Stefan Hügel
für den Vorstand und die Geschäftsstelle des FIfF

Ute Bernhardt und Ingo Ruhmann

Betrifft: Cyberpeace

„Neuland“ und Anarchie – Wenn der Staat das Gewaltmonopol aufkündigt

„Internet ist das größte Anarchismusexperiment aller Zeiten.“ So erklären die Google-Manager *Eric Schmidt* und *Jared Cohen* den Erfolg des Netzes. So lange Betrügereien und Schäden noch relativ begrenzt schienen, war der Nutzen größer als alle Probleme. Unter fröhlicher Anarchie im Internet mag man sich vorstellen, dass sich alle Beteiligten einig werden können, die paar üblichen Störer im Zaum zu halten. Anarchie setzt ein Gleichgewicht individueller Harmlosigkeit voraus.

Heute operiert im Internet allerdings eine Hackertruppe mit Milliardenbudget, Supercomputern und Zehntausenden von Mitarbeitern – die Hacker des Militärgeheimdienstes NSA, dessen Partnerdienste und Auftragnehmer. Die Konkurrenz in Ost und West ist dabei keineswegs weniger ehrgeizig und clever oder gar verschlafen, nur deutlich ärmer. Die NSA hat Millionen von Computern gehackt und infiziert. Die ihr zuzurechnenden Schadprogramme haben sich in den zurückliegenden Jahren in ebenso viele Computer eingenistet wie die übelsten Produkte herkömmlicher *Cyber-Krimineller*. Ziel der NSA ist es, diese Angriffserfolge zu übertreffen in ihrem unterschiedslosen Cyberkrieg gegen Freund und Feind.

Staatliche Stellen sind beim Schutz vor solchen Angriffen keine Hilfe. *Sascha Lobo* hat zwar Unrecht damit, dass das Internet kaputt sei. Richtig liegt er aber damit, dass staatliche Stellen den Angriffen auf die IT-Systeme von Wirtschaft, Verwaltung und Privatpersonen nichts entgegensetzen. Deutschland ist für Lobo ein digitaler *failed state*.

Solche staatliche Untätigkeit ist nicht neu. Wer das Log seines Routers beobachtet, muss keine zwei Minuten warten, bevor die ersten digitalen Einbrecher versuchen, die Firewall zu überwinden. Jeden Tag sortieren Spam-Filter und Virenscanner Schadcode aus. All diese unerwünschten Besucher und Zusendungen sind strafbare Computerspionage und -sabotage. Nur wer schon einmal daran gedacht hat, diese seit 1989 unter Strafe stehenden Angriffe auf das eigene Computersystem der Strafverfolgung zu überantworten, wird nicht den Eindruck gewinnen, dass die Verfolgung dieser Gesetze gegen Computerspionage, -sabotage und daraus folgender Gefahren hierzulande ernsthaft betrieben würde. Die in gut 20 Jahren ergangenen Verurteilungen lassen sich auch ohne Hilfsmittel schnell im Kopf addieren.

Der Naturzustand der Gewaltausübung von jedem gegen jeden endet nur dann, so Thomas Hobbes 1651 im *Leviathan*, wenn die Einhaltung von Gesetzen durch eine übergeordnete Instanz verfolgt und die Nichtbeachtung bestraft wird. Max Weber hat es 1915 auf den Begriff des *staatlichen Gewaltmonopols* gebracht, wenn Staatsbürgerinnen und -bürger auf eigene Gewaltausübung verzichten, weil der Staat mit Strafverfolgung und Justiz über ein funktionierendes System für die Ahndung von Regelabweichungen verfügt.

Doch ist dies keine einseitige Sache: Wo der Staat bei Regelverstößen untätig bleibt, endet sein Gewaltmonopol. Bisher war solche Untätigkeit an konkrete Orte gebunden. *No-go-areas* ist eine Bezeichnung für kleine Gebiete, *failed states* eine solche für Staatsgebiete, in denen durch die Staatsmacht kein Recht durchsetzbar ist.

Im Internet, das wissen wir dank *Edward Snowden* genauer, werden Rechtsbrüche nicht nur nicht verfolgt. Mit der NSA haben staatliche Stellen den Cyber-Kriminellen und Cyber-Terroristen den Rang abgelaufen. Dass die NSA weiter Datenspionage betreiben kann und Sabotage verübt an Millionen Computersystemen – vielfach an kritischen Infrastrukturen –, ist konsequent fortgeführte Realität der letzten 25 Jahre. Die NSA erklärt von sich selbst schon lange, Cyberkrieg zu führen. Wir wissen jetzt auch genauer, gegen wen: Uns alle, egal, ob Freund oder Feind. Die Sicherheit der Infrastruktur Internet, über die wir unsere Bankgeschäfte, Bestellungen, den Arzt- und Apothekenbesuch und vieles mehr abwickeln, ist zerbröselt, die Fiktion des „Supergrundrechts Sicherheit“ mausetot.

Welche anderen Schlussfolgerung soll man ziehen,

- wenn das Bundesverfassungsgericht 2008 mit dem *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* die Exekutive zu Maßnahmen zum Schutz der IT-Systeme seiner BürgerInnen verpflichtet, aber seither die Kooperation der Dienste mit den NSA-Hackern nicht ab- sondern eher zunimmt?

- wenn im *Nationalen Cyber-Abwehrzentrum* 10 Personen arbeiten, was nicht einmal ausreicht, rund um die Uhr ein Lagezentrum aufrecht zu erhalten, geschweige denn, Gefahren zu identifizieren, zu isolieren und Gegenmaßnahmen zu treffen?

- wenn das ganze *Bundesamt für die Sicherheit in der IT* (BSI), die Entwicklung von Ver- und Entschlüsselungssystemen für die Bundesverwaltung ebenso wie die Zertifizierung von IT-Systemen und dann auch deren Schutz seinen Jahresberichten zufolge mit weniger als 600 Mitarbeitern leistet, während das *Kommando Strategische Aufklärung* der Bundeswehr – das mit Funkaufklärern, Datenauswertern und eigener Hackertruppe ähnlich aufgestellt ist, wie die NSA – noch über etwa 6.000 Soldaten gebietet?

- wenn der BND 300 Millionen Euro dafür beantragt, Cybergefahren aus dem Ausland zu erkennen, während den Pressemeldungen zufolge pro Jahr für die IT-Sicherheitsforschung zur zukünftigen Verhinderung solcher Attacken gerade einmal 30 Millionen Euro bereit gestellt werden und das BSI in die aktuelle Entwicklung sicherer Systeme ganze 10 Millionen Euro steckt?

Die Faktenlage könnte deutlicher nicht sein: Deutschland wendet heute und in Zukunft für die militärisch-geheimdienstliche Aufklärung zehnmal mehr Geld und Personal auf als für den Schutz vor Cyberattacken auf Privatpersonen und Wirtschaft. Zwar beklagen sich politische Entscheidungsträger über das Internet als „rechtsfreien Raum". Sie haben sich ansonsten darauf konzentriert, einige mehr oder weniger brauchbare Gesetze zu erlassen, für deren Anwendung jedoch möglichst wenig Geld und Personal aufzuwenden.

Im Internet ist die Zeit von Anarchie und relativer Harmlosigkeit vorbei. Staatliche Stellen mit fast unbegrenzten Mitteln haben dem Rest der Welt den Cyberkrieg erklärt. Andere Stellen in anderen Ländern eifern dem angestrengt nach. Der deutsche Staat hat seinen Internet-Bewohnern das Gewaltmonopol faktisch aufgekündigt; er lässt Bürgerinnen und Bürgern schutzlos.

Die Folgen sind genau wie es das Lehrbuch erwarten lässt: In geschlossenen Runden erklären Wirtschaftsvertreter dem BSI offen ihr Misstrauen. Wer kann, nimmt seinen Schutz in die eigenen Hände. Und erhält dafür noch Ende Januar 2014 Rechtsbeistand ausgerechnet in der seriösen Zeit und ausgerechnet von einem akademischen Rat der Juristischen Fakultät zu Köln. Danach sei es rechtlich durchaus zulässig, den Abhörposten auf dem Dach der US-Botschaft in Berlin unter Beschuss zu nehmen, und sich mit Waffengewalt gegen die rechtswidrige Überwachung zur Wehr zu setzen. Denn wer Notwehr übt, hat „*bei der Wahl seiner Verteidigungsmittel nicht zimperlich zu sein. Sie verpflichtet lediglich dazu, das relativ mildeste Mittel anzuwenden, sofern der Verteidiger über mehrere geeignete Verteidigungsmittel verfügt. Verhältnismäßig aber braucht die Notwehrhandlung nicht zu sein.*" Und die Systemfrage liefert der Autor gleich mit: Ein Staat, der sich beim Angriff „*auf Rechtsgüter seiner Bürger sehenden Auges handlungsunwillig zeigt, [stellt] die Staatsgewalt selbst in Frage*". Ganz offensichtlich hat unser Staat selbst mit dieser einfachen Begründung für seine Existenz ein Problem in der digitalen Welt.

Die staatliche Ordnung versagt – es lebe der Naturzustand digitaler Gewalt jeder gegen jeden. Der nächste Schritt ist auch klar zu erkennen: jeder *failed state* hat seine Piraten, Milizen, Mafias und andere Profiteure des Machtvakuums. Geht es nach dem abgelösten NSA-Direktor *Keith Alexander*, sollen sich auch im Internet neue Profiteure niederlassen. Er will sein Wissen um Hackerangriffe zum Patent und dabei möglichst viel Geld mit dem Schutz vor Angriffen machen.

So entsteht eine Bevölkerung eines *failed state*, die paradoxerweise zugleich rundum überwacht und von aller Ordnung verlassen ist. Kaum je haben es die Bewohner eines *failed state* geschafft, sich gegen die sie terrorisierenden Banden zu organisieren und diese zu vertreiben. Doch was in der realen Welt gilt, gilt so nicht im Internet: Im digitalen Raum werden Konflikte nicht mit Waffen und Gewalt ausgetragen, sondern mit besserem Wissen, raffinierterer Technik – und einem gemeinsamen Ziel.

Es ist daher keineswegs sicher, dass das Internet an der Überwachung zugrunde geht. Wenn die Idee des freien Internets stirbt, dann an der Atomisierung und Interessenlosigkeit seiner „Bewohner". Wer einen *failed state* diagnostiziert, sollte sicher nicht darauf warten, dass gerade dieser Nicht-Staat etwas tut. Cyberpeace ist dann keine Utopie, wenn wir nicht darauf warten, dass sich der heutige Zustand von allein bessert. Wer die Anarchie des Internets oder zumindest ein ziviles Internet erhalten will, muss diese „Anarchisten" organisieren gegen Cyberkrieg und Cyberkrieger. Organisierte Anarchisten sind vielleicht eine eigenartige Vorstellung. Aber sie ist die beste, die es derzeit gibt.

Autorenhinweise siehe Seite 69

Sebastian Jekutsch

Betrifft: Faire Computer

Fair wie in Faire Orangen.

Am Anfang eine Enttäuschung: Spätestens am 2. Juni 2014 mussten alle US-börsennotierten Unternehmen gemäß *Dodd-Frank-Act 1502* erstmals veröffentlichen, ob sie in ihren Produkten Zinn, Tantal, Wolfram oder Gold einsetzen und wenn ja, ob dies aus der D.R. Kongo oder den Nachbarländern kommen könnte und wenn ja, was sie tun, um zu vermeiden, dass das Geld für diese Rohstoffe an eine der Bürgerkriegsparteien geht und sie somit den Konflikt indirekt anheizen. Noch konnte man sich herausreden, nicht genügend Informationen von den Zulieferern bekommen zu haben, um sich ein Urteil zu bilden. Das haben die meisten auch getan, so dass zusammenfassend gilt: Kein einziges Unternehmen konnte ausschließen, Konfliktmineralien in seinen Geräten zu haben. Die IT-Branche ist im Vergleich etwa zur Automobilwirtschaft durchaus transparent und offensiv der Herausforderung entgegengetreten. Intel etwa macht nun damit Werbung, konfliktfreie Prozessoren zu haben, mit eigenem Logo und großem Werbeaufwand. Viele haben jedoch nur Absichtserklärungen abgegeben. Die US-amerikanische Organisation *Enough Project,* die durch ihre intensive Lobbyarbeit dieses Gesetz erst möglich gemacht hat, sieht zwar große Fortschritte, die von anderen jedoch bezweifelt werden. So bleibt für den Käufer der Aktien und der Produkte vieles weiterhin im Dunkeln. Obschon: So wissen wir nun immerhin, dass HP und IBM Gold aus Nordkorea beziehen.

Bekanntermaßen ist das *Fairphone* vorgeprescht, ein Smartphone anzubieten, welches konfliktfreie Rohstoffe enthält. Das ist inzwischen wohl bei vielen Herstellern der Fall, allerdings kaufen viele schlicht nicht mehr im Kongo ein, was gemäß US-Ge-

setz automatisch Konfliktfreiheit bedeutet. Fairphone bezieht deswegen explizit aus dem Kongo, so ähnlich wie sie explizit in China herstellen lassen, trotz aller Schwierigkeiten und vergleichsweiser Unfairness. In eben diesem Betrieb wurden nun Wahlen für ein Gremium durchgeführt, das über die Verwendung des gut 90.000 Euro umfassenden *Workers Welfare Fund* abstimmt. Die erste Verbesserung wurde schon unternommen: Jeder bekam einen Bonus, und die Kantine bietet nun auch Obst an. Mit dem seit längerem gestarteten Verkauf der zweiten Charge von Fairphones wird sich das Kapital auf mehr als 220.000 Euro erhöhen. Diese verkaufen sich aber eher schleppend; kein Wunder, wenn man ein schon vor einem halben Jahr technisch veraltetes Gerät unverändert nochmal anbietet und das nächste schon angekündigt hat.

Auch *Nager-IT* lässt teilweise in China herstellen, konkret: Das USB-Kabel kommt dorther. Der Hersteller bekommt nun kalte Füße, weil Nager-IT mit dem regierungskritischen *China Labor Bulletin* zusammenarbeitet. Ansonsten gibt es zu berichten, dass der Leiterplattenhersteller Insolvenz angemeldet hat und Nager-IT nun auf der Suche nach einem ähnlich transparenten Lieferanten ist. Von neuen Projekten, die Fairness in der Elektronik zum Ziel haben, ist wenig zu vernehmen. Aus dem im letzten Heft erwähnten Workshop bei der *Maker Faire* ist ein Projekt für faires Lötzinn hervorgegangen. Der Plan des Crowdfunding-Projekts *Shift7,* ihr ab 77 Euro erhältliches Tablet fair zu produzieren, ist wohl schwieriger umzusetzen.

Die Aktualisierung des beliebten *Greenpeace*-Rankings *Guide to Greener Electronics* lässt seit November auf sich warten, aber bessere *Wie fair sind die Markenhersteller?*-Vergleichslisten sind inzwischen verfügbar. Zum einen wartet *Rank a brand* mit einer dreiteiligen Liste über Fairness, Klima- und Umweltschutz und einem *Greenwashing Alert* im *Sustainable Electronics Report 2014* auf. „*Insgesamt überzeugen in Ansätzen nur Fairphone, HP und Apple*", heißt es zum Thema faire Produktion. Eine australische Organisation hat fast zeitgleich einen umfangreichen Bericht namens *Behind the Barcode – Electronics Industry Trends* veröffentlicht, mit Schwerpunkt auf Sklaverei-artiger Arbeit und dem *living wage,* also ausreichendem Gehalt für die Ernährung einer kleinen Familie. Hier stach Nokia hervor. Das ist interessant, denn zum einen suchte Nokia (inzwischen ja die Mobilsparte von Microsoft) in der Vergangenheit immer wieder günstigere Arbeitnehmer – nach Deutschland, Rumänien und Indien nun in Vietnam – zum anderen war der größte Streik in Chinas Elektronikindustrie im letzten Jahr bei Nokia: wegen Gehaltsfragen.

Der Autor vor der deutschen NXP-Zentrale beim weltweiten Aktionstag, näheres unter http://blog.faire-computer.de/nxp-aktionstag-zum-mitmachen

Aber zurück zu den Rankings: Samsung landet bei diesen immer irgendwo im Mittelfeld. Zunehmend gerät der weltgrößte Handy- und Smartphone-Hersteller in den Blickpunkt der Kritiker, allen voran *China Labor Watch*. Sie schleusten zum wiederholten Male Undercover-Mitarbeiter in einen Samsung-Zulieferbetrieb ein und entdeckten – ebenfalls nicht zum ersten Mal – Beschäftigung unter 16-Jähriger, was in China wie auch International verboten ist. Als Samsung in seinem im Juni veröffentlichten Zuliefererbericht behauptete, bei seinen Auftragnehmern keine Kinderarbeit beobachtet zu haben, ging China Labor Watch an die Öffentlichkeit. Bald danach reduzierte Samsung das Auftragsvolumen bei eben diesem Zulieferer. Man befindet sich in schlechter Gesellschaft: Eine chinesische Elektronikfirma wurde behördlich geschlossen, nachdem dort gleich 200 Kinder bei der Arbeit entdeckt wurden.

Aber zurück zu Samsung: Es gab wochenlange Arbeiterproteste vor der Zentrale in Seoul nach dem Selbstmord eines Gewerkschaftsvertreters. Die Polizei hatte tatsächlich den Leichnam entführt und eingeäschert. An anderer Stelle gab es immerhin den ersten Tarifvertrag in der Geschichte des Konzerns. Auch das Thema Krebsfälle in der Samsung-Halbleiterherstellung ist noch aktuell. Derzeit laufen vertrauensvoll begonnene Gespräche zwischen der Opferorganisation *SHARPS* und Samsung.

Aber zurück zu den Enttäuschungen: Von der Dringlichkeit der Untersuchung dieser Fälle überzeugt auch ein anderer Artikel in diesem Heft. Wer weiß, wie viele unbekannte Fälle dieser Art es noch geben mag? Die Geschichte wiederholt sich nämlich: In den 1970er bis 90er Jahren gab es erste Berichte über Vergiftungen und Krebsfälle bei der Halbleiterindustrie im Silicon Valley (bei IBM), in Schottland (bei National Semiconductor) und in Taiwan (bei RCA). Gibt es denn keine Fortschritte?

Sebastian Jekutsch

Sebastian Jekutsch ist aktiv im *AK Faire Computer* des FIfF und *AK Faire Elektronik* in Hamburg. Wer sich für die Quellen der Nachrichten oder das Thema überhaupt interessiert sollte Kontakt aufnehmen über *fairit@fiff.de.*

Michael Leben

Krebserkrankung auf Samsungs Karriereleiter

Im Alter zwischen dreißig und vierzig Jahren kreisen private Gespräche meistens um die Kinder, den Partner oder den Job. Wenn aber das Telefon bei Frau Park Min-Suk *aus Südkorea klingelt, und sie nach langer Zeit von einem alten Freund angerufen wird, dann geht es oft um Krebserkrankungen. Im Jahr 2012 wurde auch bei Frau Park Brustkrebs festgestellt. Diese Telefonanrufe erweckten schließlich in ihr den Verdacht, ihr ehemaliger gemeinsamer Arbeitsplatz könnte der Auslöser für die vielen Erkrankungen sein. Sie arbeitete über sieben Jahre in der Halbleiterproduktion für* Samsung *in sogenannten Cleanrooms (Reinsträumen). Von den 18 Arbeitskollegen ihrer damaligen Schicht leiden mittlerweile sieben an Krebs und Unfruchtbarkeit. Zusammen mit* Dr. Kong Jeong-Ok *von der koreanischen Arbeitsschutzorganisation SHARPS, die uns bei der Übersetzung half, haben wir Park Min-Suk in Berlin getroffen.*

Park Min-Suk in Berlin, Mai 2014

FIfF: **Arbeiten Sie noch immer bei Samsung?**

Min-Suk Park: *Jetzt nicht mehr. Ich habe von 1991 bis 1998 in einer Fabrik von Samsung gearbeitet. Das macht sieben Jahre bei Samsung. Ich wurde 1973 geboren, und habe mit 18 Jahren begonnen, in der Fabrik zu arbeiten.*

FIfF: **Was war Ihre Aufgabe dort?**

Park: *Ich arbeitete in der Wafer-Produktion. In verschiedenen Prozessen, wie Trockenätzen und Nassätzen (Dry- und Wet-Etching), wobei man Chemikalien von den Wafern entfernen muss, zum Beispiel Fotolack, der auf den Wafer aufgebracht wurde, damit er sich entwickelt und dann zerschnitten werden kann. Der Wafer muss dann mit einigen Chemikalien gesäubert werden, das ist der Ätz-Prozess. Ich arbeitete auch mit Verfahren wie chemischer Gasphasenabscheidung und Dünnschichten. Ich wurde in unterschiedlichen Produktionslinien eingesetzt.*

Anfangs war es Parks Aufgabe, die Wafer zu säubern. Ein erfahrener Angestellter erklärte ihr die Arbeit. Wenn es um Schutzmaßnahmen ging, dann ausschließlich um solche zum Schutz der Wafer, von denen jeder „soviel wie dein Haus" kosten würde, wie ein dienstälterer Kollege betonte.

Park: *Aceton und Isopropylalkohol waren die Chemikalien, die wir am öftesten benutzten, um den Arbeitsplatz zu reinigen. Damit habe ich täglich hantiert.*

FIfF: **Wussten Sie, dass diese Chemikalien gefährlich sind?**

Park: *Ich wusste nichts über die Gefahren. Obwohl ich täglich mit verschiedenen Chemikalien und Gasen Umgang hatte, glaubte ich einfach, was die Firma uns sagte. Und die sagten, dass der Reinraum perfekt überwacht sei. Also dachten wir überhaupt nicht an chemische Gefahren. Ich hatte das leichte Gefühl, das es gefährlich sein könnte. Bevor ich dort arbeitete, hörte ich, dass die starken elektromagnetischen Felder in den Halbleiterfabriken bei Frauen Unfruchtbarkeit hervorrufen könnten.*

Halbleiter-Erzeugnisse werden in sehr komplexen Verfahren hergestellt. Meistens werden ätzende Chemikalien verwendet, damit die Schaltkreise auf einem Wafer entstehen. Ein Wafer ist eine dünne Scheibe aus Halbleitermaterial. Staub ist sehr gefährlich für die Chips, deshalb werden sie in Reinräumen hergestellt. Um die elektronischen Bauteile vor Staub, Haaren und Speichel zu schützen, tragen die Arbeiter Schutzanzüge, sogenannte *Bunny suits*, die man aus den Intel-Werbespots der 90er Jahre kennt. Obwohl diese Anzüge entfernt an Weltraumanzüge erinnern, sind sie keinesfalls dafür geschaffen, die Arbeiter zu schützen. Stattdessen verhindern sie, dass menschliche Partikel den Wafer kontaminieren, aber verhindern es keineswegs, dass der menschliche Körper mit Chemikalien in Berührung kommt.

Park arbeitete für Samsung in einer Halbleiterfabrik im südkoreanischen Giheung, wo sie Speichermodule herstellte, beispielsweise 64 MByte DRAM oder 256 KByte Fast SRAM. Wer damals einen handelsüblichen PC besaß, hatte darin sehr wahrscheinlich Speicherchips, die Park und ihre Kollegen hergestellt hatten. Heutzutage ist Samsung die Nummer 1 unter den Herstellern von Speicher.

FIfF: **Haben Sie mit Ihren Kollegen über die Chemikalien gesprochen?**

Park: *Die Mitarbeiter haben mir nichts darüber gesagt. Als wir in der Fabrik anfingen, unterwies uns ein dienstälterer Kollege – vertrauensvoll „Schwester" genannt. Er oder sie fungiert als Lehrer oder sogar wie ein Elternteil für die jungen Mitarbeiter. Wenn die nichts über Gefahren erwähnen, dann haben die jungen Mitarbeiter keinen Grund, Verdacht zu schöpfen.*

Die dienstälteren Mitarbeiter haben ihre Autorität zugunsten des Wafers eingesetzt. Und falls es einmal zu einem Unfall kom-

men sollte, dann hatte Samsung seine eigene Interpretation eines Evakuierungsplans, wie Park erklärt:

Park: *Die größte Gefahr, von der ich von einer der „Schwestern" hörte, war die einer Notabschaltung. Das bedeutet, dass die Produktionsanlagen wegen Wartungsarbeiten oder wegen eines Stromausfalls gestoppt werden. Sie sagten uns, dies sei der schädlichste Moment für die Wafer – nicht für die Angestellten – und aus so einer gefährlichen Situation zu flüchten, ohne sich vorher um den Wafer zu kümmern, könnte dazu führen, dass der Wafer durch zulange Einwirkzeiten der Chemikalien beschädigt wird. Der Wafer sollte noch evakuiert werden, bevor die Arbeiter die Anlage verlassen, daran sollten wir uns immer erinnern.*

Park erledigte ihre Arbeit so gut, dass sie bis zur Teamleiterin aufstieg. In den ersten drei Jahren bei Samsung hatte sie nicht viel Freizeit. Es wurde verlangt, dass die Angestellten jeden Tag arbeiteten, und nur einmal im Monat konnte ein Tag frei genommen werden, und auch nur dann, wenn ein anderer Mitarbeiter stattdessen die Schicht mitübernahm und so die Arbeit für zwei gleichzeitig verrichtete. Park und ihre Kolleginnen waren damals knapp 20 Jahre alt, einige von ihnen noch Teenager.

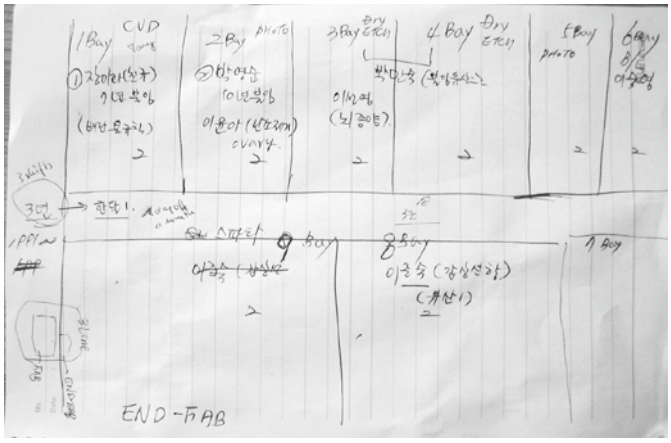
FIfF: **Wurden Sie während oder nach der Arbeit bei Samsung krank?**

Park: *Ich hatte starke Menstruationsschmerzen. Im Reinraum war der Luftdruck sehr hoch, sodass ich sehr müde wurde. Das einzige, woran ich mich vom Fabrikarbeiterleben erinnern kann, ist Arbeiten und zurück zum Schlafsaal zu gehen, um zu schlafen. Nur arbeiten und schlafen, nichts anderes, schon mit knapp 20 Jahren. Ich war sehr erschöpft. In den ersten drei Jahren, hatten wir nur einen einzigen Tag im Monat frei. Um diesen Tag frei zu bekommen, musste ein anderer doppelt arbeiten. Wir brauchten wirklich diesen freien Tag, aber wir konnten das nur einmal im Monat machen, weil man diese Doppelarbeit nur einmal im Monat durchhalten konnte. Ich habe die Fabrik verlassen, nachdem ich geheiratet habe. Ich konnte 4 Jahre lang kein Kind bekommen, in dieser Zeit hatte ich auch eine Fehlgeburt. Nachdem ich 2002 mein erstes Kind bekommen hatte, war alles gut, aber 2012, als ich 39 Jahre alt war, wurde bei mir Brustkrebs diagnostiziert.*

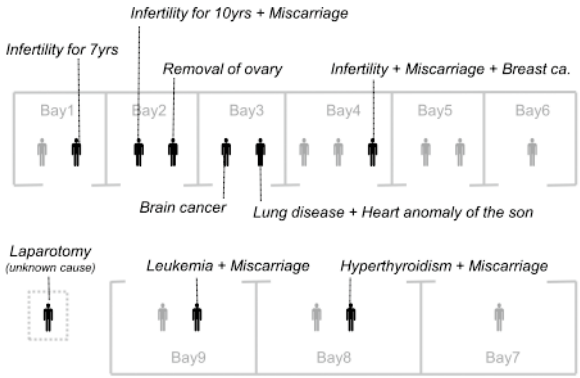
FIfF: **Ist so etwas auch Ihren Mitarbeitern passiert?**

Park: *Ja. Weil ich Teamleiter war, habe ich viel mitbekommen.*

Park fängt an, ein Diagramm der Fertigungslinie zu malen, an der sie in den ersten drei Jahren bei Samsung arbeitete. Es gibt neun Arbeitsplatzstationen, *bays* genannt, die meisten davon sind mit je zwei Mitarbeitern im Drei-Schicht-Betrieb besetzt, also ingesamt sechs Mitarbeiter je Arbeitsplatzstation.



Originalzeichnung der Fertigungslinie



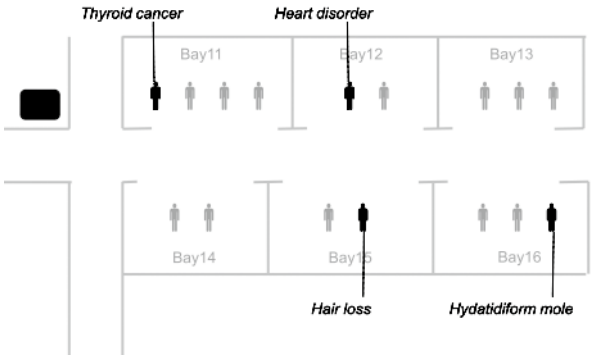
Endstufe der Fertigung von 1991 bis 1994 bei Samsung Semiconductor basierend auf der Skizze von Frau Park

Sie erzählt von den Schicksalen ihrer Teammitglieder und berichtet von Fruchtbarkeitsproblemen und Krebs. Von den 18 Arbeitern ihrer Schicht – die Fabrikbelegschaft war in drei Schichten eingeteilt – erkrankten sieben schwer. Das ist eine außergewöhnliche Häufung seltener Krankheiten.

Park: *Über die Gesundheit der 44 übrigen Arbeiter weiß ich nichts. In meinem Team gab es Fälle von Unfruchtbarkeit, für sieben Jahre und mehr, Gehirntumore, Leukämie, Schilddrüsenüberfunktion und Fehlgeburten, eine Frau ließ sich ihre Eierstöcke entfernen, bevor sie heiratete. 1994 installierte Samsung eine neue Produktionsanlage, mit einer anderen Anordnung von Arbeitern und Bays. Nachdem das passiert war, hatte ich Kollegen, die Schilddrüsenkrebs, Blasenmole und Haarausfall in sehr frühem Alter bekamen.*

Michael Leben

Michael Leben hat am Potsdamer Hasso-Plattner-Institut IT-Systems Engineering studiert und arbeitet als Software-Architekt in Berlin. Seine Interessensgebiete sind fair gehandelte Elektronik, Green-IT, Information Retrieval und maschinelles Lernen.



Fabrikerweiterung ab 1994. Vielen Dank an Dr. Kong für diese und die vorhergehende Zeichnung

FIfF: **Ist das alles in derselben Fabrik passiert?**

Park: *Ja, das sind alles Fälle aus einer einzigen Fabrik. An weiteren Produktionseinrichtungen gab es noch mehr Fälle. Im Januar 2014 starb eine Abteilungsleiterin, die Photochemie benutzte, im Alter von nur 42 Jahren an Magenkrebs. Ein anderer Produktionsingenieur im etwa gleichen Alter starb an Leukämie.*

FIfF: **Gab es durch Samsung Nachforschungen zu den Krankheitsfällen?**

Park: *Darüber habe ich nichts gehört. Ich erinnere mich nur daran, dass sie Spenden von den Mitarbeitern eingetrieben haben, um den Kampf eines Kollegen gegen eine Krankheit zu unterstützen. Die Firma führte eine Spendenaktion für ihren Angestellten durch.*

Normalerweise würde die staatliche Versicherungsagentur KCOMWEL *(Korea Workers' Compensation & Welfare Service)* die Arbeiter monetär für berufsbedingte Erkrankungen entschädigen. Da aber Samsung die Verantwortung für seine erkrankten Mitarbeiter ablehnte, wurden in den meisten Fällen keine Entschädigungszahlungen geleistet. In Südkorea werden durch die Krankenversicherungen die Kosten meistens nicht in voller Höhe erstattet. Patienten müssen einen Eigenanteil von manchmal bis zu 50 % erbringen. Deshalb haben sich viele der erkrankten Mitarbeiter durch ihre Behandlungskosten verschuldet.

FIfF: **Haben Sie Klage gegen Samsung eingereicht?**

Park: *Nein. Ich habe im Juli 2013 die Arbeiterentschädigung bei der Regierung beantragt. Sie haben bis jetzt, nach 10 Monaten, noch nicht geantwortet. Ich warte weiter. Samsung hat sich nie bei mir gemeldet.*

Erst kürzlich im Mai 2014 gab Samsung die Verantwortung für die Krankheitsfälle in einer halbherzigen Entschuldigung zu. Die zähen Verhandlungen über die Entschädigungszahlungen sind teils langlebiger als Parks ehemalige Kollegen, von denen etliche bereits tot sind.

Parks Krebserkrankung ist gegenwärtig unter Kontrolle. Sie arbeitet wieder: in einer Schule für behinderte Kinder. Sie sagt, dass sie dort glücklich sei.

Park Min-Suk in der Dokumentation „The Empire of Shame" (CinemaDAL, 2013)

Der Beitrag erschien zuerst auf Englisch im Blog *Faire Computer*, *http://blog.faire-computer.de/a-carcinogenic-career-at-samsung/*.

Stefan Hügel

Log 3/2014

Ereignisse, Störungen und Probleme der digitalen Gesellschaft

Immer wieder gibt es Ereignisse, Verlautbarungen und Entscheidungen, die im Zusammenhang mit dem fortschreitenden Abbau von Bürgerrechten stehen. Wir dokumentieren hier einige davon. Die Aufzählung ist sicherlich nicht vollständig; mit einigen besonders bedeutsamen Ereignissen wollen wir aber auf die weiterhin besorgniserregende Entwicklung hinweisen.

Mai 2014

4. Mai 2014: Nach Ansicht des hessischen Datenschutzbeauftragten Michael Ronellenfitsch ist die Vorratsdatenspeicherung ein geeignetes Mittel für die Bekämpfung von Terrorismus. Er erklärte, dass die Datenspeicherung für polizeiliche Zwecke und Kriminalitätsbekämpfung nicht sonderlich hilfreich sei, bei der Terrorismusbekämpfung aber sinnvoll sein könne (Quelle: Frankfurter Rundschau, Heise).

4. Mai 2014: Die deutsche Bundesregierung will dem NSA-Untersuchungsausschuss nur eingeschränkten Einblick in die Akten gewähren und lehnt einen Auftritt Edward Snowdens ab. Es gehe dabei um Informationen über die Verhandlungen über ein No-Spy-Abkommen und um Akten aus dem verfassungsrechtlich geschützten Kernbereich der exekutiven Eigenverantwortung und zur Zusammenarbeit der Geheimdienste. Bei der Frage der Vernehmung von Edward Snowden stellt die Bundesregierung offenbar außenpolitische Interessen und die interna-

tionale Zusammenarbeit über die Interessen des Bundestags, Menschenrechtsverletzungen aufzuklären (Quelle: Der Spiegel, Heise).

5. Mai 2014: Nach dem Transparenzbericht des E-Mail-Dienstleisters Posteo gab es im Jahr 2013 sieben Anfragen von Strafverfolgungsbehörden, davon eine Anfrage nach Verkehrsdaten. Fünf Abfragen wiesen formelle Fehler auf; insbesondere wurden Daten abgefragt, die nicht abgefragt werden durften. Zudem kritisiert Posteo das Vorgehen von Ermittlungsbeamten und fordert strafrechtliche Konsequenzen, unter anderem wegen Nötigung und Ermunterung zu rechtswidriger Kooperation (Quelle: Heise).

5. Mai 2014: Aus dem Transparenzbericht für 2013, der von der Deutschen Telekom vorgelegt wurde, wurden im Lauf des Jahres 49.796 Anschlüsse überwacht. Der überwiegende Teil davon wurde nach §100 StPO von Richtern oder Staatsanwälten angeordnet, der Rest geht auf das Artikel-10-Gesetz (G10) und auf Landespolizeigesetze zurück. Die Zahl der Verkehsdatensätze beträgt dabei 436.331. Im Rahmen der zivilgerichtlichen Verfolgung von Urheberrechtsverletzungen wurden in 946.641 Fällen nach §101 des Urheberrechtsgesetzes die Inhaber von IP-Adressen beauskunftet (Quelle: Heise).

5. Mai 2014: Auch nach einer NSA-Reform fordert US-Präsident Barack Obama Immunität für US-Provider, wenn sie Nutzerdaten an US-Geheimdienste weitergeben. Eine analoge Bestimmung gab es bereits im *Foreign Intelligence Surveillance Act* (FISA); auch hier hatte der damalige Senator Obama zugestimmt (Quelle: Guardian, Heise).

5. Mai 2014: Laut dem rheinland-pfälzischen Datenschutzbeauftragten Edgar Wagner gibt es in Deutschland mittlerweile rund 100.000 illegal montierte Überwachungskameras im Wald zur Beobachtung des Wildes. Diese Kameras beobachten auch Wanderer und verstoßen damit gegen Datenschutzbestimmungen. Wagner droht Jägern, die die Kameras trotz Aufforderung nicht entfernen, ein Bußgeld in Höhe von €5.000 an (Quelle: Heise).

6. Mai 2014: Aufgrund einer Sicherheitslücke bei einem Gewinnspiel von Kabel BW konnten Besucher persönliche Daten von Teilnehmen auslesen. Betroffen sind Klarnamen und Adressen. Das Leck wurde innerhalb eines Tages geschlossen (Quelle: Heise).

6. Mai 2014: Die Privacy Policy für die Fitness-App Moves wurden nach der Übernahme durch Facebook dahingehend verändert, dass nun persönlich identifizierbare Daten an Partner – einschließlich der neuen Konzernmutter – weitergegeben werden dürfen. Zuvor waren die Bestimmungen vergleichsweise datenschutzfreundlich; Daten wurden nur nach explizitem Einverständnis der Nutzer weitergeleitet (Quelle: Heise).

6. Mai 2014: Mails zwischen Vertretern von Google und dem ehemaligen NSA-Chef Keith Alexander deuten nach Ansicht von Al Jazeera auf eine enge Kooperation des Dienstleisters mit dem US-Geheimdienst hin. In Mails vom Juni 2012 gehe es um ein geheimes Treffen, bei dem Sicherheitsbedrohungen besprochen werden sollten. In einem weiteren Mailwechsel sei von einem Treffen die Rede, bei dem Erfolge der Kooperation und neue Ziele das Thema sein sollten (Quelle: Al Jazeera, Heise).

6. Mai 2014: Nach dem der EuGH die Vorratsdatenspeicherung im April verworfen hatte, zieht die EU-Kommission nun die Klage gegen Deutschland zurück (Rechtssache C-329/12). Die Kommission hatte geklagt, weil die europäische Richtlinie 2006/24/EG in Deutschland nicht umgesetzt worden war; dies ist durch die Entscheidung des EuGH hinfällig. Deutschland soll aber die Kosten des Verfahrens tragen (Quelle: Heise).

9. Mai 2014: Die Mehrheit der Regierungskoalition aus CDU/CSU und SPD hat im Bundestag gegen Initiativen gestimmt, keinen weiteren Vorstoß zur Einführung einer Vorratsdatenspeicherung zu unternehmen. Obwohl die Speicherung in ihrer bisherigen Form sowohl vom Bundesverfassungsgericht als auch vom Europäischen Gerichtshof abgelehnt worden sind, wollen sich die Regierungsparteien die Option Vorratsdatenspeicherung weiterhin offen halten (Quelle: Heise).

9. Mai 2014: Nach Einschätzung des ehemaligen NSA-Chefs, General Keith Alexander, trifft US-Präsident Barack Obama Entscheidungen zu nationalen Sicherheit „fast genauso" wie sein Vorgänger George W. Bush. Das ist nach Ansicht von Alexander auch der Grund, warum Obama das Programm zur Überwachung von Telefonaten habe weiterlaufen lassen (Quelle: Australian Financial Review, Heise).

12. Mai 2014: Internationale IT-Sicherheits-Experten haben auf Risiken der Internet-Wahlen in Estland hingewiesen und empfehlen die unverzügliche Rückkehr zu Wahlen mit Stimmzetteln aus Papier. Die Vorkehrungen zur Funktionssicherheit seinen für eine glaubwürdige Zählung nicht transparent genug und es gebe erhebliche Sicherheitslücken, die Angriffe von außen ermöglichten (Quelle: Heise).

12. Mai 2014: „Wir töten auf Basis von Metadaten", bestätigte nun auch der ehemalige Chef von NSA und CIA, Michael Hayden, auf einer Podiumsdiskussion. Er bestätigte damit die Aussagen des ehemaligen Drohnenpiloten Brandon Bryant, dass Verdächtige aufgrund von Verbindungsdaten geortet und umgebracht würden. Auch der Bundesnachrichtendienst (BND) gibt Handynummern an US-Behörden weiter, die demnach als Grundlage außergerichtlicher Tötungen dienen können. Der BND behauptet dagegen, die gelieferten Daten seien für eine zielgenaue Ortung nicht geeignet (Quelle: Heise).

13. Mai 2014: Einem Urteil des Europäischen Gerichtshofs (EuGH) zufolge kann der Suchmaschinenbetreiber Google verpflichtet werden, Webseiten mit sensiblen persönlichen Daten aus der Liste der Ergebnisse zu streichen. Dieses „Recht auf Vergessen" leite sich aus der EU-Datenschutzrichtlinie ab. Google argumentiert dagegen, der Zwang zur Entfernung bestimmter Links verstoße gegen die Grundrechte der Informations- und Meinungsfreiheit (Quelle: Heise).

13. Mai 2014: Durch ein Datenleck bei der ARD-Show Quizduell konnte auf die persönlichen Daten der Mitspieler zugegriffen werden. Von dem Leck sind über 50.000 Nutzer betroffen. Mit einem Trick konnten unter anderem Klarnamen, Wohnort, Geburtsdatum und Mail-Adressen ausgelesen werden (Quelle: Heise).

16. Mai 2014: Abgeordnete des Deutschen Bundestags kritisieren die im Zusammenhang mit der Edathy-Affäre bekannt gewordene umfassende Vorratsdatenspeicherung im Deutschen Bundestag. Abgeordnete erklärten, sie seien bisher davon ausgegangen, dass ihre Kommunikation sofort gelöscht werde. Daten werden aus dem aktuellen Monat und über drei Monate rückwirkend gespeichert; die Bundestagsverwaltung hat erklärt, dies sein ein „Service" für Abgeordnete, die so ihre Kommunikation nicht individuell sichern müssten (Quelle: Heise).

22. Mai 2014: Bei einer Anhörung des NSA-Untersuchungsausschusses haben die ehemaligen Verfassungsrichter Hans-Jürgen Papier und Wolfgang Hoffmann-Riem deutlich gemacht, dass staatliche Behörden eine Verpflichtung hätten, Bürgerinnen und Bürger vor der Ausspähung durch Geheimdienste zu schützen. Es gehe dabei darum, eine „Störung der öffentlichen Sicherheit" zu unterbinden; es gebe keinen Ermessensspielraum. Der Staat sei damit verpflichtet, eine grundrechtswahrende Informationsinfrastruktur zu schaffen. Auch der „Ringtausch" von sensiblen Informationen zwischen Sicherheitsbehörden sei grundrechtswidrig (Quelle: Deutscher Bundestag, Heise).

30. Mai 2014: Plänen des Bundesnachrichtendiensts (BND) zufolge sollen soziale Netzwerke in Echtzeit überwacht werden. Das Programm ist Teil der *Strategischen Initiative Technik* und wird als Echtzeitanalyse von Streaming-Daten bezeichnet. Zusätzlich sollen umfassend Verbindungsdaten ausgespäht werden. Zur Rechtfertigung dient einmal mehr der Hinweis, das Erfassen von Metadaten würden einen geringeren Eingriff bedeuten als Inhalte. Bundesjustizminister Heiko Maas erteilte einige Woche später der Totalüberwachung sozialer Netzwerke durch den BND eine Absage (Quelle: Süddeutsche Zeitung, Passauer Neue Presse, Heise).

Juni 2014

3. Juni 2014: Entgegen vorheriger Erklärungen will Generalbundesanwalt Harald Range nun doch Ermittlungen wegen des NSA-Skandals aufnehmen. Gegenstand der Ermittlungen soll aber nicht der massenhafte Menschenrechtsbruch gegen die deutsche Bevölkerung sein; der Generalbundesanwalt will lediglich wegen des abgehörten Mobiltelefons von Bundeskanzlerin Angela Merkel ermitteln. US-Behörden kritisieren die Ermittlungen und finden, dass solche Fragen auf diplomatischer Ebene geklärt werden sollten (Quelle: Heise).

5. Juni 2014: Aus der Antwort auf zwei Kleine Anfragen der Landtagsabgeordneten Katharina König geht hervor, dass der Thüringische Verfassungsschutz Briefe öffnet, ohne dabei Spuren zu hinterlassen. Warum die Briefe geöffnet würden, unterliege teilweise der Geheimhaltung, so das Thüringische Innenministerium (Quelle: Heise).

11. Juni 2014: Die Datenlieferungen des Verfassungsschutzes an die US-amerikanischen Behörden nehmen offenbar zu. 2013 soll der Verfassungsschutz in 1.163 Fällen Daten geliefert haben; in den vergangenen vier Jahren haben sich die Übermittlungen verfünffacht. Über wen die USA Informationen anfordern, ist unklar; aufgrund des Aufgabengebiets des Verfassungsschutzes als Inlandsgeheimdienst liegt die Annahme nahe, dass es sich um Informationen über deutsche Staatsbürger oder in Deutschland lebende Ausländer handelt (Quelle: NDR, WDR, Süddeutsche Zeitung, Heise).

17. Juni 2014: Die britische Regierung rechtfertigt die Massenüberwachung ihrer eigenen Bevölkerung formaljuristisch als rechtmäßig. Suchanfragen von Briten bei Google könnten als externe Kommunikation eingestuft werden, die nicht gesetzlich geschützt sei. Eigentlich sind auch Einwohner Großbritanniens gegen Überwachung rechtlich geschützt; durch die Einstufung ihrer Kommunikation als „extern" wird dieser Rechtsschutz ausgehebelt (Quelle: Heise).

19. Juni 2014: Die Drohne des südafrikanischen Herstellers Desert Wolf, Skunk genannt, hat das Ziel, Massenansammlungen unter Kontrolle zu bringen. Die Drohne ist dafür mit Laser, Lautsprecher und nicht-letalen Druckluftwaffen ausgestattet, mit denen Giftgas – in der Regel Pfefferspray – und Paintballs verschossen werden können. Die Drohne verfügt zusätzlich über zwei HD- und eine Wärmebildkamera. 25 Stück dieser Waffe wurden offenbar an einen internationalen Bergbaukonzern verkauft – in Südafrika kommt es häufig zu Streiks in Bergbaubetrieben (Quelle: Heise).

24. Juni 2014: Offenbar hat das Unternehmen *Hacking Team* einen Staatstrojaner für Smartphones entwickelt. Dies haben Untersuchungen von Kaspersky und dem Citizen Lab ergeben. Für die Spionage-Software gibt es den Berichten zufolge bereits Module für Andrion, iOS, Windows Mobile und Blackberry. Die Software ermögliche allumfassenden Zugriff auf die Funktionen der Geräte – wie Kameras, Mikrophone, GPS – und könne damit nahezu jeden Aspekt des Lebens der Zielpersonen ausspähen (Quelle: Heise).

25. Juni 2014: In den Jahren 2004 bis 2007 wurden offenbar jahrelang Daten eines Knotens in Frankfurt am Main an die NSA geleitet – mutmaßlich vom Internet-Knoten DE-CIX. Die Ko-

Stefan Hügel

Stefan Hügel, Vorsitzender des FIfF, studierte Informatik an den Universitäten Karlsruhe und Freiburg, wo er sein Studium mit der Diplomarbeit am Institut für Informatik und Gesellschaft abschloss. Er lebt in Frankfurt am Main und arbeitet als IT-Berater.

operation sei noch von der rot-grünen Bundesregierung unter Bundeskanzler Gerhard Schröder (SPD) und Vizekanzler Joschka Fischer (Grüne) – in Verantwortung des damaligen Kanzleramtschefs Frank-Walter Steinmeier (SPD) – eingeleitet worden. Später ist offenbar die Kooperation beendet worden, weil sie politisch „zu heikel" sei. Vertreter von DE-CIX dementierten später gegenüber der Tagesschau, dass im Zeitraum von 2004 bis 2007 ein ausländischer oder inländischer Geheimdienst einen Zugang zu von dem Unternehmen betriebenen Internetknoten und zugehörigen Glasfasernetzen hatte. Die Weiterleitung war offenbar ein Kompromiss (Quelle: Tagesschau, Süddeutsche Zeitung, NDR, WDR, Heise).

29. Juni 2014: Offenbar hat Facebook den Nachrichtenstrom hunderttausender Nutzer manipuliert, um damit eine Studie durchzuführen. Mit der Studie sollte untersucht werden, wie sich positive und negative Emotionen in Netzwerken ausbreiten. Das Ergebnis ist, dass Menschen, die in der Mehrzahl positive Einträge zu sehen bekamen, ebenfalls häufiger Nachrichten mit positivem Inhalt veröffentlichten – und umgekehrt. Die Manipulationen fanden im Januar 2013 statt; manipuliert wurden die Newsfeeds von ca. 690.000 Nutzern. Neben der Kritik aus ethischer Sicht wurde später auch die Aussagekraft der Studie in Zweifel gezogen. Durch eine Veröffentlichung von *Technology Review* wurde später bekannt, dass bei Facebook bereits seit Längerem mit den Daten experimentiert wurde. „Denn wer die Mechanik der sozialen Beeinflussung versteht, kann Online-Werbung noch eindrücklicher gestalten und damit bewirken, dass die Nutzer noch häufiger auf Anzeigen klicken" (Quelle: Technology Review, Heise).

Juli 2014

1. Juli 2014: Das Land Nordrhein-Westfalen will als erstes Bundesland Software für das *Predictive Policing* einsetzen. Zunächst soll untersucht werden, welche Software international für die vorausschauende Verbrechensbekämpfung eingesetzt wird. Data Mining soll eingesetzt werden, um „unerwartete Zusammenhänge" zu erkennen (Quelle: Heise).

1. Juli 2014: „Unter bestimmten Bedingungen" soll nun auch die Bundeswehr Kampfdrohnen einsetzen. Bundesverteidigungsminiterin Ursula von der Leyen spricht sich für die Entwicklung einer europäischen Drohne aus, wie sie bereits im Koalitionsvertrag vorgesehen ist. Bis 2023 soll die Bundeswehr über 16 waffenfähige Drohnen verfügen können (Quelle: Heise).

3. Juli 2014: Analysen des Quelltextes der Ausspähsoftware XKeyScore haben offenbar ergeben, dass Menschen, die sich mit der Anonymisierungssoftware Tor befassen, als Extremisten markiert und überwacht werden (Quelle: NDR, WDR, Heise).

3. Juli 2014: Untersuchungen der britischen Bürgerrechtsvereinigung *Open Rights Group* (ORG) zufolge wird offenbar ein Fünftel der beliebtesten Websites durch die britischen „Pornofilter" gesperrt, darunter Twitter. Damit wird ein erheblicher Teil auch nicht-jugendgefährdender Seiten durch die Filter zensiert. Der angebliche „Pornofilter" wurde im Juli 2013 durch Premierminister David Cameron vorgestellt und damit begründet, Kinder vor nicht altersgemäßen Inhalten schützen zu wollen (Quelle: Open Rights Group, Heise).

10. Juli 2014: Nachdem die Vorratsdatenspeicherung durch den Europäischen Gerichtshof (EuGH) verworfen wurde, will die britische Regierung nun dennoch schnell ein neues Gesetz im Eilverfahren beschließen lassen, damit die bereits gespeicherten Daten – durch die vom Gericht als unrechtmäßig abgelehnte Speicherung – nicht gelöscht werden müssen. Eine Woche später ist das Gesetz DRIP (*Data Retention and Investigation Powers Bill*) in beiden Kammern des Parlaments verabschiedet und auch von der Königin bestätigt (Quelle: Heise).

10. Juli 2014: Aufgrund der Spionageangriffe der US-Geheimdienste hat die Bundesregierung nun den Repräsentanten dieser Geheimdienste ausgewiesen. Zuvor war ein BND-Mitarbeiter festgenommen worden, der offenbar für die CIA spioniert hatte – unter anderem im Umfeld des NSA-Untersuchungsausschusses. Danach ist offenbar auch ein Spion im Bundesverteidigungsministerium aufgeflogen. In einer Stellungnahme versicherten die USA, dass die Partnerschaft mit Deutschland weiterhin einen hohen Stellenwert habe (Quelle: Heise).

10. Juli 2014: Gegen einen Studenten in Großbritannien ist eine sechsmonatige Beugehaft verhängt worden, weil er nicht bereit war, das Passwort für seinen verschlüsselten Rechner an die Behörden herauszugeben. In Großbritannien kann aufgrund des *Regulation of Investigatory Powers Act 2000* (RIPA) die Herausgabe von Passwörtern erzwungen werden. Auch in den USA gibt es mittlerweile solche Tendenzen – nachdem bisher vorherrschende Rechtsmeinung ist, dass die Herausgabe von Passwörtern unter das 5th Amendment der Verassung fällt, das das Recht auf Verweigerung der Aussage gegen sich selbst garantiert (Quelle: Chronicle, Heise).

14. Juli 2014: Zum Schutz vor Überwachung erwägt der NSA-Untersuchungsausschuss, mechanische Schreibmaschinen einzusetzen, um geheime Dokumente zu verfassen. Dies sei kein Scherz, erklärte der Vorsitzende des Ausschusses, Patrick Sensburg (CDU). „Anders als andere Untersuchungsausschüsse untersuchen wir einen laufenden Sachverhalt. Nachrichtendienstliche Tätigkeit läuft noch, findet statt. Und wir müssen natürlich versuchen, unsere interne Kommunikation sicher zu halten, verschlüsselte E-Mails senden, Krypto-Telefone benutzen und andere Dinge, die ich hier jetzt natürlich nicht sage" (Quelle: ARD, Heise).

24. Juli 2014: Einer Mitteilung der Europäischen Zentralbank in Frankfurt am Main zufolge sind Hacker in ihre Systeme eingedrungen und haben sich den Zugriff auf persönliche Daten, darunter 20.000 E-Mail-Adressen und in einigen Fällen Klarnamen, Adressen und Telefonnummern von Journalisten und anderen Personen verschafft. Finanzmarktdaten seien nicht betroffen (Quelle: Heise).

Klaus Haller

Ethische Überlegungen zum Einsatz von Data-Loss-Prevention-Tools in Unternehmen

Snowden, CDs von Schweizer Banken oder die fast vergessene Bonusmeilen-Affäre – manche MitarbeiterInnen ignorieren arbeitsvertragliche und strafrechtliche Normen. Mögliche Gründe sind Frust, Geltungssucht oder der Reiz des schnellen Geldes. Manchmal passiert „nur" ein Fehler. Eine Mitarbeiterin verliert einen USB-Stick mit Forschungsergebnissen oder ein Mitarbeiter schickt eine Kundenliste an eine falsche E-Mail-Adresse. Ein solcher Datenabfluss *ist in hochkompetitiven, wissensintensiven Sektoren wie der Pharma- oder Automobilbranche besonders kritisch. Ähnliches gilt für Branchen mit sensiblen Kundendaten. Beispiele sind das Gesundheitswesen, Banken und Versicherungen. Auch der Sicherheitssektor ist gefährdet. Wie schützen sich also Unternehmen vor einem Datenabfluss?*

1 Data Loss Prevention Tools in Unternehmen

Wer einen schlechten Rat sucht, findet ihn in dem guten Artikel *The NSA and Snowden – How better security measures could have stopped the leak* in den *Communications of the ACM* [Tox14]. Der Artikel erklärt, wie klassische IT-Security-Methoden (Zugriffsrechte, Zwei-Faktor-Authentifizierung, Vier-Augen-Prinzip, Verschlüsselung etc.) verhindern, dass Administratoren Klartextdaten sehen. Natürlich sollten Administratoren den Inhalt von Datenbanken oder Dokumentensammlungen nicht im Klartext sehen, doch ist die Sicht viel zu eng. Auch viele „normale" Mitarbeiter sind ein Risiko, weil sie mit sensiblen Daten arbeiten. Wer die Profitabilität von Kundenbeziehungen analysiert und Margen bei Projekten prüft, kann allein mit diesen Daten einem Unternehmen ernsthaft schaden. Nicht der Zugriff auf Daten, sondern ein Datenabfluss ist das Problem. Klassische Security-Maßnahmen scheitern bei solchen Themen. Ihr Schwerpunkt liegt beim Datenzugriff, nicht beim Datenabfluss. IT-Security-Abteilungen erfahren viel zu oft erst aus der Presse von einem Datenverlust. Daher kombinieren immer mehr Unternehmen klassische IT-Security-Maßnahmen mit *Data Loss Prevention* (DLP). DLP-Tools erkennen, melden oder blockieren Datenabfluss. Dazu durchsuchen sie E-Mails, Dateien, Instant Messages und den Netzwerkverkehr nach kritischen Inhalten. Schlüsselwörter wie *al-Qaida* oder *streng vertraulich* können verdächtig sein, andere Unternehmen suchen nach Mustern von IBAN-Nummern oder *Social Security Numbers*. Je nach Konfiguration warnt ein DLP-Tool Mitarbeiter vor Fehlverhalten, es dokumentiert Verdachtsfälle, alarmiert Vorgesetzte, unterbindet E-Mails oder verschiebt kritische Dateien in sichere Verzeichnisse [Hal14]. Solche Tools werden oft von DLP-Teams betrieben, die aus dem Risiko-Management und weniger aus der IT-Security kommen.

Aus Sicht der Mitarbeiter schnüffeln das DLP-Team, die Personalabteilung und Vorgesetzte mittels DLP-Tools in „ihren" E-Mails, Instant Messages und Dateien herum. Ist ein solcher Einsatz von DLP-Tools angemessen? Was ist höher zu gewichten, der Wunsch des Arbeitgebers, Geschäftsgeheimnisse zu schützen, oder der Wunsch der Mitarbeiter, nicht überwacht zu werden? Gesetze geben juristische Antworten, die für Unternehmen verbindlich sind. Doch neben dem juristischen gibt es auch einen ethischen Aspekt. Dieser Artikel geht nicht auf den Aspekt der empirischen, deskriptiven Ethik ein (Was machen Unternehmen heute? Warum?). Er nähert sich dem Thema aus Sicht der normativen Ethik, die Prinzipien für „gutes Handeln" aufzeigen möchte [GW]. Dazu wendet er bekannte ethische Konzepte zur Überwachung erstmals auf DLP-Tools in Unternehmen an. Als Grundlage dient die Arbeit *Surveillance Ethics* von Kevin Macnish [Mac11], die eine Vielzahl an Quellen zu Ethik und Überwachung zusammenfasst.

Der Artikel ist dabei wie folgt aufgebaut: Zunächst grenzt Abschnitt 2 den Anwendungsfall genauer ein, bevor Abschnitt 3 die Folgen von Überwachung und DLP-Tools auf Unternehmen und Mitarbeiter erklärt. Abschnitt 4 geht der Frage nach, ob Mitarbeiter ein Anrecht auf Privatsphäre haben, wenn sie in der IT-Infrastruktur eines Unternehmens arbeiten. Schließlich entwickelt Abschnitt 5 konkrete Kriterien für den ethischen Einsatz von DLP-Tools in Unternehmen. Abbildung 1 veranschaulicht diese Gliederung graphisch.

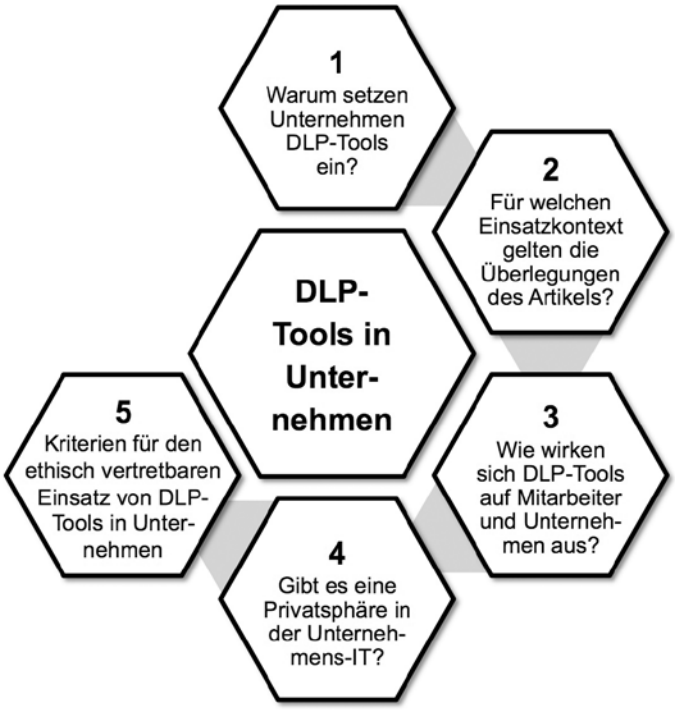


Abbildung 1: Themenüberblick

2 Berücksichtigter Einsatzkontext für DLP-Tools

Viele Technologien können missbraucht werden. Das gilt auch für DLP-Tools. Wer sie einsetzen möchte, muss zuerst ihre Missbrauchsrisiken und mögliche Gegenmaßnahmen analysieren. Dieser Artikel hilft dabei. Da DLP-Tools – wie fast jede Technologie – ethisch neutral sind, entscheidet der Einsatzkontext über „gut" oder „böse". Daher konkretisieren wir ihn mittels vier Annahmen:

1. Es geht um DLP-Tools in Unternehmen, nicht um staatliche Überwachung.

2. Das DLP-Tool soll Datenabfluss erkennen und unterbinden. Unternehmen messen nicht mittels DLP-Tools die Arbeitsleistung von Mitarbeitern und überwachen auch kein gewerkschaftliches Engagement.

3. Mitarbeiter werden nur innerhalb der Unternehmens-IT überwacht. Facebook, Xing etc. sind tabu, sofern kein Netzwerkverkehr über die Unternehmens-IT läuft.

4. Mitarbeiter können (teilweise) die Unternehmens-IT proaktiv vermeiden, auch während der Bürozeiten. Dazu verwenden sie private, mobile Geräte, die sich über das Mobilfunknetz mit dem Internet verbinden.

3 Überwachung durch DLP-Tools – Auswirkungen auf Mitarbeiter

Überwachung hat eine negative Konnotation, auch wenn sie teils im Interesse der Überwachten erfolgt. Macnish nennt als Beispiel Besitzer von Kreditkarten. Kreditkartenfirmen überwachen die Käufe ihrer Kunden. Weichen Einkäufe vom normalen Einkaufsverhalten ab, kann das ein Hinweis auf Kartenmissbrauch sein.

Doch nicht jede Überwachung erfolgt im Einvernehmen oder zum beiderseitigen Nutzen. Daher ist aus ethischer Sicht wichtig, wie sich Überwachung auf Menschen auswirkt. Macnish diskutiert unter anderem folgende Auswirkungen [Mac11]:

1. *Überwachung ersetzt Vertrauen* in Menschen und Mitarbeiter: Werden Menschen überwacht und drohen ihnen Sanktionen, verhalten sie sich meist korrekter als sonst. Wer Menschen überwacht, muss ihnen also weniger Vertrauen entgegenbringen.

2. Überwachung führt bei den Überwachten zu mehr *Stress*.

3. Überwachung kann übermäßige *Selbstzensur* bei der Kommunikation auslösen. Man ist vorsichtig und unterlässt Äußerungen oder Aktivitäten, um nicht gegen Regeln zu verstoßen oder aufzufallen (*chilling*).

4. Es gibt einen *Autonomieverlust* bezüglich der Selbstdarstellung. Dritte könnten durch die Überwachung Informationen erhalten, die man ihnen nicht geben würde.

5. Die eigene *Kommunikation* mit Dritten wird *befangener*. Man weiß nicht, was Gesprächspartner von eigenen Schwächen und Fehlern durch die Überwachung wissen.

6. Weniger Privatsphäre *erschwert, Vertrauensverhältnisse* aufzubauen.

3.1 Überwachung mit DLP-Tools – erwünschte Auswirkungen für Unternehmen

Drei der sechs Auswirkungen sind Gründe, warum Unternehmen DLP-Tools einsetzen. Konkret sind das Vertrauensersatz, Selbstzensur und Autonomieverlust. Vertrauensersatz ist besonders in großen Unternehmen ein Thema. Je mehr Mitarbeiter sensible Daten sehen, desto größer ist das Risiko, dass eine Person fahrlässig oder kriminell handelt und dabei Daten abfließen. DLP-Tools reduzieren das Risiko, indem sie transparent machen, wie Mitarbeiter mit sensiblen Daten umgehen. Das sorgt für Selbstzensur und Autonomieverlust. Mitarbeiter werden bei sensiblen Daten vorsichtiger und verzichten auf riskante Aktionen. Das hilft den Unternehmen.

Der letzte Absatz klingt nach einem Plädoyer für totale Überwachung – ‚DLP-Tools sind gut, weil sie Unternehmensziele durchsetzen'. Das ist zu einseitig. Jede Demokratie lebt von freier Meinungsäußerung. Es ist eine Katastrophe, wenn staatliche Überwachung zu Selbstzensur und Autonomieverlust führt. In diesem Artikel geht es aber nicht um einen demokratischen Staat, der seine Bürger überwacht. Es geht um Unternehmen, die durch Überwachung Datenabfluss verhindern wollen. Selbstzensur und Autonomieverlust beziehen sich auf einen engen Bereich der täglichen Arbeit – auf den Umgang mit sensiblen Daten, insbesondere in der elektronischen Kommunikation. Deswegen sind DLP-Tools in Unternehmen für Mitarbeiter weniger bedrohlich als staatliche Überwachung, die Bürger rund um die Uhr beobachtet. Trotzdem haben DLP-Tools natürlich auch in Unternehmen unerwünschte Folgen.

3.2 Überwachung mit DLP-Tools – Nebenwirkungen

Einige der von Macnish genannten Auswirkungen von Überwachung sind im Falle von DLP-Tools in Unternehmen unerwünscht. DLP-Tools beeinflussen Mitarbeiter und ihre Arbeitsweise. Abläufe im Unternehmen können ineffizienter werden oder bei Mitarbeitern *Stress wegen Überwachung* [MW00] auslösen. Genauso kann Stress entstehen, weil Mitarbeiter wissen, dass sie unzulässig mit sensiblen Daten umgehen. Eigene Bequemlichkeit kann der Grund sein, unpassende Prozesse und Tools ebenso. Hier decken DLP-Tools auf, wenn *Soll* und *Ist* abweichen. Doch Stress für Mitarbeiter trifft letztlich auch die Unternehmen, wenn Arbeitszufriedenheit und Leistung sinken.

Eine andere negative Auswirkung von DLP-Tools ist, dass sie die Teambildung erschweren können. Viele Unternehmen haben Teams, deren Mitarbeiter weltweit verteilt arbeiten. Informelle E-Mails oder Instant Messages über Urlaub und Hobbies helfen den Teammitgliedern, Vertrauen aufzubauen und Kontakte zu pflegen. Merken Mitarbeiter, dass ihre Vorgesetzten mittels DLP-Tools E-Mails und Instant Messages heimlich mitlesen, wird die *Kommunikation befangener. Vertrauensverhältnisse* sind *schwieriger* aufzubauen. Die Teamleistung droht schlechter zu werden.

Zusammenfassend lässt sich sagen: DLP-Tools sind für viele Unternehmen sinnvoll. Allerdings müssen die Risiken für die Arbeitsleistung beachtet werden, die von Überwachungsstress oder schlechterer Zusammenarbeit ausgehen können. Decken DLP-Tools Schwachstellen beim Umgang mit sensiblen Daten auf, hängt viel von der Unternehmenskultur ab. Es kann eine positive Dynamik entstehen sich zu verbessern, aber auch ein Klima der Angst.

Doch zunächst stellt sich eine andere Frage: Dürfen Mitarbeiter eine Privatsphäre beanspruchen, wenn es um Dateien, Instant Messaging oder E-Mails innerhalb der Unternehmens-IT geht?

4 Privatsphäre, DLP-Tools und die Unternehmens-IT

MitarbeiterInnen haben auch in Unternehmen ein Recht auf Privatsphäre. Dieses Recht gilt nicht uneingeschränkt. Wer im Supermarkt an der Kasse arbeitet, kann sich nicht auf seine Privatsphäre berufen, wenn sein Bargeldbestand geprüft wird. Für DLP-Tools ist also zu klären, ob sie Bereiche überwachen, die eigentlich zur Privatsphäre der Mitarbeiter gehören.

DLP-Tools überprüfen Dateien und E-Mails auf sensible Unternehmensdaten. Aus Sicht der Privatsphäre ist das zentrale Problem, dass DLP-Tools wie Schleppnetze beim Fischfang arbeiten. Im Schleppnetz verfangen sich viele Fische, die man verkaufen kann. Daneben gibt es „Beifang", unverkäufliche Fische oder Müll. Man möchte ihn nicht, doch er ist unvermeidlich und kostet Zeit und Geld. Egal wie gut DLP-Tools arbeiten und wie integer das DLP-Team ist, auch bei DLP-Tools gibt es Beifang, die *False Positives*. DLP-Tools filtern aus E-Mails, Dateien, und Netzwerkverkehr mittels Regeln und Heuristiken Verdachtsfälle heraus (Abbildung 2). Verdachtsfälle sind Dateien oder E-Mails mit potenziell unerlaubten, sensiblen Daten. Stellt sich ein Verdachtsfall als harmlos heraus, ist er ein *False Positive*. Doch vorher hat ein Mitarbeiter des DLP-Teams die konkrete E-Mail möglicherweise gelesen. Ist die E-Mail aus Sicht des Unternehmens harmlos, enthält aber private Daten, ist die Privatsphäre eines Mitarbeiters verletzt. Doch warum haben Mitarbeiter überhaupt private Daten in der Unternehmens-IT? Ein Blick zurück in die 1960er Jahre gibt die Antwort.

In den Schwarzweißfilmen der 1960er Jahre gibt es Kaffeeklatsch im Pausenraum und in Büros mit vielen Aktenordnern. Die Aktenorder enthalten Briefe und Gesprächsprotokolle. Es ist normal, wenn Vorgesetzte Akten einsehen. Nicht akzeptabel sind heimliche Tonbandaufnahmen im Pausenraum. Das flüchtige, gesprochene Wort im Pausenraum und archivierte Briefe und Protokolle in Aktenordnern sind zwei getrennte Welten. Diese Zeiten sind heute vorbei. Verträge, Protokolle, Austausch von Ideen und Smalltalk, alles geht über die gleichen elektronischen Kanäle. Die Trennung – Akten sind für alle einsehbar, Gespräche sind privat – existiert nicht mehr. Verlieren nun Mitarbeiter ihr Recht auf Privatsphäre, weil in Unternehmen formale und informale Kommunikation über die gleichen Kanäle laufen? Das ist mehr als fraglich. Neben vermeidbarer privater Kommunika-

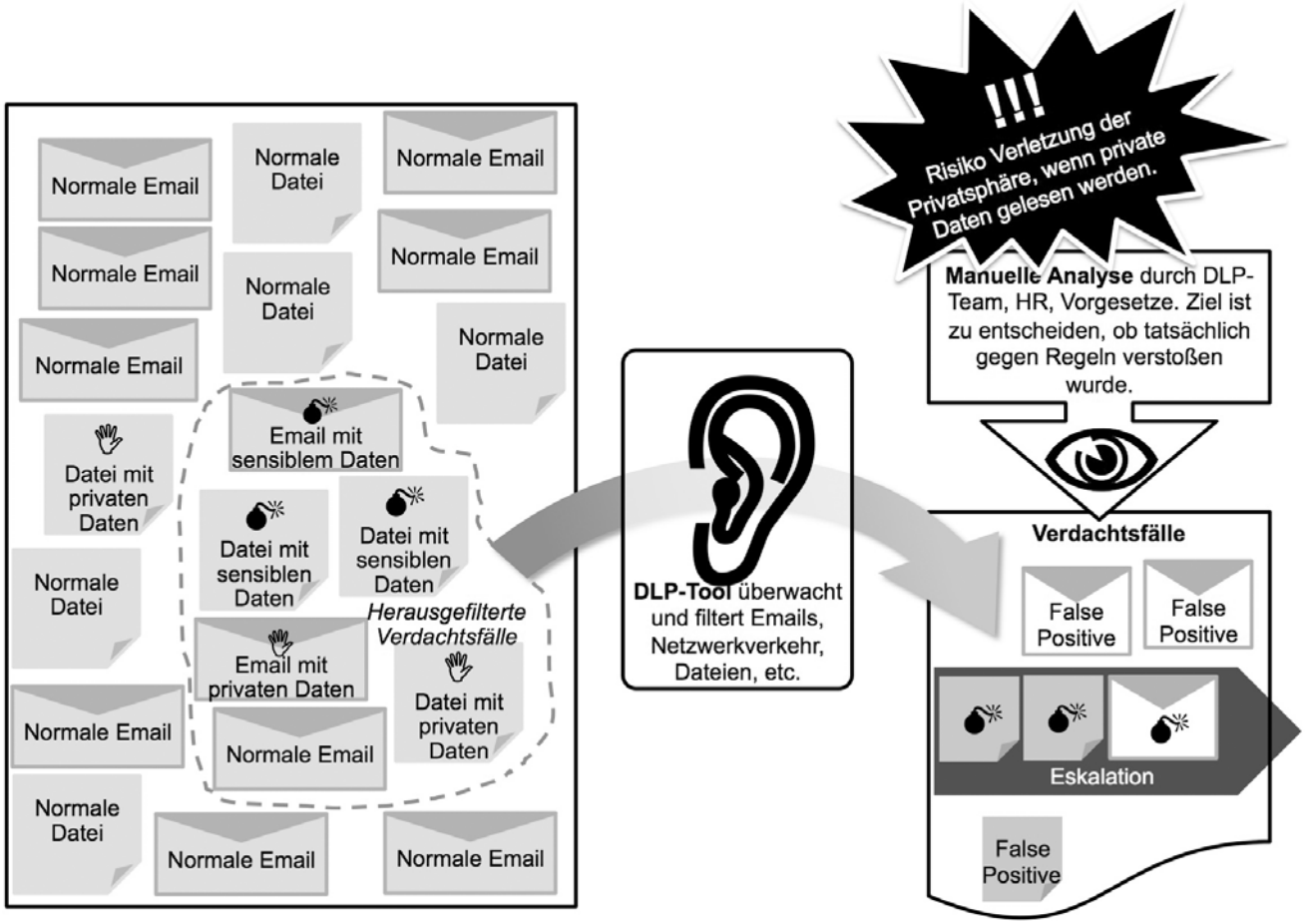


Abbildung 2: Funktionsweise von DLP-Tools und (Haupt-)Risiko der Privatsphären-Verletzung

tion gibt es nämlich *geduldete, geförderte und sogar notwendige private Kommunikation* im Unternehmensnetzwerk. Dazu vier Beispiele:

- *Informale Gespräche und Smalltalk*. Details aus privaten Aktivitäten oder Fotos werden mit Kollegen geteilt. Damit sind sie in der Unternehmens-IT. Teams bauen so leichter persönliche Beziehungen und Vertrauen auf. Das Unternehmen profitiert. Die Mitarbeiter riskieren aber, dass die Kommunikation peinliche Momente enthält. Filtert das DLP-Tool zufällig den peinlichen Moment als „Beifang", verbreitet er sich möglicherweise im Unternehmen. Chancen und Risiken für Mitarbeiter und Unternehmen wären so nicht fair verteilt.

- *Regelungen kleinerer persönlicher Angelegenheiten*, die nur zu Bürozeiten möglich sind und IT-Infrastruktur benötigen. Beispiele sind telefonische Rückfragen zu Online-Formularen oder zum Online-Banking, für die man auch die eigenen Daten sehen muss. Erledigen Mitarbeiter solche Anliegen schnell (!) am Arbeitsplatz anstelle Urlaub nehmen zu müssen, vermeidet das Störungen betrieblicher Abläufe aufgrund von Abwesenheiten.

- *Persönlich-geschäftliche Daten* wie E-Mails mit Bezug zu Personalthemen (Gehalt, Urlaub, Abwesenheiten wegen Krankheit). Die Kommunikation erfolgt zwingend innerhalb der Unternehmens-IT. Trotzdem muss das Unternehmen solche persönliche Daten der Mitarbeiter besonders schützen.

- Bei *bring your own device* (BYOD) arbeitet ein Mitarbeiter auf seinem eigenen Laptop. Mitarbeiter können erwarten, dass E-Mails bei Webmail-Anbietern und private Dateien nicht überwacht werden. Das DLP-Tool des Unternehmens darf private Laptops nicht beliebig durchsuchen.

Die Beispiele zeigen, dass Mitarbeiter aus ethischer Sicht eine Privatsphäre erwarten dürfen, auch in der Unternehmens-IT, selbst wenn das Unternehmen jede private Nutzung verbietet. Folgende Fragen helfen, die Situation und die Erwartungen zu klären:

1. Ist informale Kommunikation unter MitarbeiterInnen über elektronische Kanäle im Intranet erlaubt, geduldet oder erwünscht? Für welche Mitarbeiter gilt dies? Gilt es für E-Mails, Instant Messaging und auch für private Fotos und Videos?

2. Ist informale Kommunikation mit Kunden über elektronische Kanäle erwünscht? Für welche Mitarbeiter gilt dies? Gilt es für E-Mails, Instant Messaging und auch für private Fotos und Videos?

3. Müssen sensible Personalthemen oder andere Themen im privat-beruflichen Grenzbereich über das Intranet abgehandelt werden? Welche? Geht es um elektronische Kommunikation und/oder um Dateien? Wer ist betroffen?

4. Wie sieht die Abgrenzung bei BYOD zwischen privater und beruflicher Kommunikation beziehungsweise bei Dateien aus?

Das Management, die Rechts- und die Personalabteilung müssen bindende Antworten geben. Das DLP-Team hat eine rein beratende Funktion.

5 Ethische Voraussetzungen für DLP-Tools in Unternehmen

Manche Autoren lehnen jede Überwachung von Mitarbeitern ab (siehe z. B. [Int03]). Das ist sehr einseitig. Natürlich können DLP-Tools die Privatsphäre von Mitarbeitern verletzen, doch genauso können sie sowohl Unternehmen als auch Mitarbeitern helfen. Will ein Mitarbeiter versehentlich sensible Daten per E-Mail an eine private Adresse schicken, kann ein DLP-Tool davor warnen. Das hilft dem Mitarbeiter und dem Unternehmen. DLP-Tools können existenzbedrohende Datenverluste verhindern. Davon profitieren das Unternehmen und alle Mitarbeiter, deren Arbeitsplätze nicht gefährdet werden. Daher nimmt der Artikel an, dass DLP-Tools ethisch angemessen sein *können*, aber Motiv und Ausgestaltung pro Einzelfall zu prüfen sind. Basierend auf [Mac11] formulieren wir fünf Prüfanforderungen: lauteres Motiv, Befugnis, Notwendigkeit, Angemessenheit und Organisation (siehe Abbildung 3). Ein Unternehmen muss stets alle fünf Anforderungen erfüllen, nicht nur einzelne.

Abbildung 3: Voraussetzungen für ethische Überwachung, zum Beispiel durch DLP-Tools in Unternehmen

5.1 Lauteres Motiv

Zentral für die ethische Beurteilung von Überwachung ist ihr Zweck (*purpose*) [Mac11]. Hat ein Unternehmen ein lauteres Motiv für die Überwachung? Das ist für DLP-Tools gegeben, wenn ein Unternehmen Datenabfluss erkennen und verhindern will. Ein unlauteres Motiv wäre, E-Mails von Mitarbeitern aus Neugierde zu lesen oder gewerkschaftliche Aktivitäten auszuspionieren.

5.2 Befugnis

Macnish spricht von einer Befugnis für das Überwachen (*authority*) [Mac11]. Das ist für staatliche Institutionen leicht zu erklären. Soll ein Nachrichtendienst Terroristen und die organisierte Kriminalität beobachten, sammelt er spezifische Daten über sie und nicht Daten über Falschparker, Raser oder Politiker. Das Konzept lässt sich auf DLP-Tools in Unternehmen übertragen. Ein DLP-Team betreibt das DLP-Tool und bearbei-

tet Verdachtsfälle. Dafür braucht es eine Befugnis als Auftrag. Ein DLP-Team kann sich nicht selbst ermächtigen. Falls die Unternehmensleitung nicht gerade einen „Blanko-Scheck" ausstellt, ist eine *kombinierte Befugnis* von Linienvorgesetzten und Dateneigentümern erforderlich.

Die *Linienvorgesetzten* müssen zustimmen, wenn ein DLP-Tool ihre Mitarbeiter überwachen soll. Die *Dateneigentümer* (*Data Owners*) entscheiden, welche Daten sensibel sind. Interne Sicherheitsrichtlinien (siehe zum Beispiel [Mtu11]) regeln solche Aufgaben. Welche Daten sensibel sind, hängt vom Kontext ab. Das können Kundenlisten, Forschungsergebnisse oder Angebote für Kunden sein. Klassifizieren Unternehmen konsequent, wie vertraulich ihre Dokumente und Daten sind – zum Beispiel „öffentlich", „intern", „vertraulich" – ist das eine Grundlage für DLP-Tools. Sie könnten so konfiguriert werden, dass sie als vertraulich klassifizierte Daten finden, aber möglichst nicht als öffentlich oder intern klassifizierte Daten.

5.3 Notwendigkeit

Notwendig ist eine Überwachungsmaßnahme, wenn das Schutzziel entweder nur mit ihrer Hilfe sinnvoll erreicht werden kann oder wenn alle Alternativen (noch) mehr Nachteile haben [Mac11].[1] Bei DLP-Tools ist zunächst zu klären, ob die Suchalgorithmen E-Mails und Dateien mit sensiblen Daten dieses Unternehmens aufspüren können. Außerdem sind Alternativen zu einem DLP-Tool zu prüfen. Kann man sensible Daten auf einem isolierten Rechner ohne Netzwerkanbindung ablegen? Kann man den Personenkreis mit Zugriff auf sensible Daten verkleinern? Vielleicht reicht es, einzelne Teams zu überwachen anstelle aller Mitarbeiter.

Zur Notwendigkeit gehört bei DLP-Tools auch die Frage, ob und wann der Mitarbeiter, seine Vorgesetzten, das DLP-Team, IT-Security oder die Personalabteilung informiert werden. Wer sieht Metadaten wie Dateinamen oder die Empfänger der E-Mails? Wer liest E-Mails oder Instant-Messaging-Protokolle oder schaut sich Dateien an? IT-Security muss nicht zwangsläufig den Inhalt verdächtiger E-Mails sehen, gerade wenn E-Mails automatisch blockiert werden und keinerlei Verdacht auf kriminelles Fehlverhalten vorliegt.

5.4 Angemessenheit

Angemessenheit verlangt eine Abwägung zu treffen. Rechtfertigen die Risiken, denen ein Unternehmen ausgesetzt ist, einen Eingriff in die Privatsphäre der Mitarbeiter? Es gibt drei Aspekte zu beurteilen:

1. Verhältnismäßigkeit
2. Diskriminierungsfreie, sachgerechte Auswahl, wer und was überwacht wird
3. Absolute Schranken der Überwachung

Verhältnismäßigkeit – proportionality und *discrimination* – fragt, ob die Stärke des Eingriffs in die Privatsphäre und die Anzahl der überwachten Personen angemessen sind [Mac11]. Ein DLP-Tool zum Schutz von Kundendaten ist nicht per se verhältnismäßig. Können alle Mitarbeiter auf eine CRM-Applikation zugreifen und Kundenlisten ausdrucken, ist fraglich, ob ein DLP-Tool alleine das Risiko eines Datenverlustes genug reduziert, um die Überwachung zu rechtfertigen. Haben weltweit nur fünf Personen Zugriff auf eine solche Kundenliste, ist der Fall anders zu beurteilen.

E-Mails und Dateien, die überwacht werden, müssen *diskriminierungsfrei und sachgerecht* ausgewählt werden. Soziale Vorurteile dürfen keinen Einfluss haben.[2] Eine Risikoanalyse muss entscheiden, welche Teams, Unternehmensteile und -standorte oder Management-Ebenen das DLP-Tool (nicht) überwacht.

Weiter sind *absolute Schranken der Überwachung* (*impermissible surveillance*) eine zentrale Forderung. Sie verhindern, dass die Überwachung schleichend ausgeweitet wird und inakzeptable Formen annimmt („function creep") [Mac11]. Absolute Schranken sind partielle Verbote von Überwachung. Ein solches kann beispielsweise für Daten der Personalabteilung gelten oder für Instant Messaging innerhalb des Unternehmens. Absolute Schranken vermeiden ethische Probleme, Rechtsverstöße und Spannungen zwischen Unternehmen und Mitarbeitern. Möchte das DLP-Team eine absolute Schranke aufweichen, muss die Befugnis (Abschnitt 5.2) angepasst werden.

5.5 Organisation

Setzen Unternehmen DLP-Tools ein, überwachen Mitarbeiter andere Mitarbeiter. Sie lesen private E-Mails und weisen Mitarbeiter auf Fehler hin. Bei Bedarf leiten sie disziplinarische Maßnahmen ein. Dafür brauchen sie psychologisches Geschick. Überwachung soll Risiken verkleinern, nicht die Firmenkultur zerstören. Macnish diskutiert dafür das Konzept der Distanz.

Distanz hat zwei gegensätzliche Pole. Einerseits sollen Mitarbeiter mit Überwachungsaufgaben keine einseitige, negative Sicht auf die anderen Mitarbeiter entwickeln. Die Gefahr ist besonders bei automatisierten Überwachungsmaßnahmen ohne Kontakt zwischen Überwachern und Überwachten groß. Andererseits hilft Distanz den Überwachten. Für sie bedeutet es weniger Stress, wenn sie nicht persönlich mit ihrem Fehlverhalten konfrontiert werden. Eine E-Mail mit Bitte um Antwort ist für sie angenehmer [Mac11]. Folglich sollte ein DLP-Team örtlich und organisatorisch von anderen Mitarbeitern getrennt sein.

Mit *situativem Verständnis* vermeidet ein DLP-Team eine zu negative Sicht auf andere Mitarbeiter. Situatives Verständnis verlangt, dass das DLP-Team versteht, wie die übrigen Mitarbeiter in ihrer täglichen Arbeit mit sensiblen Daten umgehen. Unternehmen erreichen dies durch die richtige Auswahl von Mitarbeitern. Nicht technische IT-Security-Spezialisten sind für ein DLP-Team gefragt, sondern Mitarbeiter mit Verständnis für betriebliche Abläufe, Risikomanagement und für sensible Daten. Gerade in größeren Unternehmen kann die Organisation eine Herausforderung sein. Die Unternehmen müssen entscheiden, ob sie ein zentrales DLP-Team für das ganze Unternehmen wollen oder kleinere Teams pro Standort, Land oder pro Geschäftseinheit.

Aus der Diskussion lassen sich folgende Fragen für ethisch verantwortungsvolle Unternehmen ableiten:

- Warum soll ein DLP-Tool E-Mails, Dateien und Netzwerkverkehr überwachen? Ist das Motiv lauter? (Abschnitt 5.1)
- Wer mandatiert den Einsatz des DLP-Tools? Dateneigentümer und Linienvorgesetze müssen explizit oder implizit zustimmen. (Abschnitt 5.2)
- Ist die Überwachung mittels DLP-Tool risikominimierend oder gibt es Alternativen, die weniger in die Privatsphäre von Mitarbeitern eingreifen? (Abschnitt 5.3)
- Ist der Einsatz verhältnismäßig? Sind die Überwachungsziele diskriminierungsfrei gewählt? Sind absoluten Grenzen definiert? (Abschnitt 5.4)
- Ist die Organisation des Einsatzes von DLP-Tools derart, dass das DLP-Team situatives Einfühlungsvermögen für die Überwachten hat und gleichzeitig eine räumliche und organisatorische Trennung besteht? (Abschnitt 5.5)

6 Fazit

Verlieren Unternehmen sensible Daten, kann das ihre Existenz gefährden. DLP-Tools reduzieren solche Risiken. Dafür greifen sie in die Privatsphäre von MitarbeiterInnen ein. Das wirft die Frage nach der ethischen Zulässigkeit auf. Dieser Artikel bietet Unternehmen eine Liste von Fragen für eine Selbstbeurteilung. Mit ihrer Hilfe können sie existierende Lösungen evaluieren oder neue Lösungen ethisch akzeptabel konzipieren.

Die Überwachung von Mitarbeitern ist allerdings auch ein gesellschaftlich relevantes Thema. Entscheidungen zur Mitarbeiterüberwachung in Unternehmen dürfen nicht nur vom ethischen Gewissen einzelner Manager abhängen. Es geht um fundamentale Überwachungsverbote (absolute Schranken), die kein Unternehmen überschreiten darf. Weiter geht es um Verantwortlichkeit. Wer im Unternehmen muss garantieren, dass ein DLP-Tool nicht missbraucht wird? Die normativen Grundlagen gesellschaftlichen Zusammenlebens sind hier weiterzuentwickeln. Ansonsten behält Dieter Hildebrandt vielleicht doch Recht mit seinem Satz: „Politik ist nur der Spielraum, den die Wirtschaft ihr lässt."

Referenzen

[GW] Springer Gabler Verlag (Herausgeber), Gabler Wirtschaftslexikon, Stichwort: Ethik, http://wirtschaftslexikon.gabler.de/Archiv/2794/ethik-v9.html

[Hal14] Haller, K.: When Data Is a Risk: Data Loss Prevention Tools and Their Role within IT Departments, login (Usenix), Vol. 39, No. 1, February 2014

[Int03] Introna, L. D.: Workplace surveillance 'is' unethical and unfair. Surveillance & Society, 1(2), 210-216, 2002

[Lan06] Lango, J.: Last resort and Coercive Threats: Relating a Just War Principle to a Military Practice, Joint Services Conference on Professional Ethics, 2006

[Mac11] Macnish, K.: Surveillance Ethics, Internet Encyclopedia of Philosophy, http://www.iep.utm.edu, last update of the article: August 9, 2011

[Mtu11] Michigan Technological University, Information Technology Services and Security: Information Security Roles & Responsibilities, July 2nd, 2011, http://security.mtu.edu/policies-procedures/ISRolesResponsibilities.pdf , last retrieved July 26th, 2014

[MW00] Miller, S, Weckert, J.: Privacy, the Workplace and the Internet. Journal of Business Ethics, 28. Jg., Nr. 3, S. 255-265, 2000

[NA99] Norris, C., Armstrong, G.: CCTV and the social structuring of surveillance. Crime prevention studies, 10. Jg., Nr. 157-178, S. 1, 1999

[Tox14] Toxen, B.: The NSA and Snowden: Securing the All-Seeing Eye. Communications of the ACM, Vol. 57, No. 5, May 2014

Anmerkungen

1 *Mit eigenen Smartphones oder Tablets kann man sich nahezu überall per Mobilfunknetz mit dem Internet verbinden. Möchte man in Arbeitspausen private E-Mails oder soziale Netzwerke nutzen, gibt es keinen Grund, die Unternehmens-IT zu nutzen. In diesem Bereich können Mitarbeiter proaktiv ihre Privatsphäre schützen.*

2 *Macnish verwendet die Kriterien „feasibility standard" und „awfulness standard". Sie gehen auf Lango zurück, der sie im Zusammenhang mit „gerechtfertigten Kriegen" entwickelt hat [Lan06].*

3 *Macnish verweist auf die Gefahr, dass Vorurteile zu einer verstärkten Überwachung einer sozialen Gruppe führen können. Selbst wenn die Gruppe nicht krimineller ist als jede andere, hat man überproportional viele Vorkommnisse aus dieser Gruppe aufgrund der höheren Überwachungsdichte. Dadurch wird das – falsche – Vorurteil vermeintlich bestätigt. Er verweist auf eine Studie von Norris und Armstrong zur Videoüberwachung [NA99].*

Klaus Haller

Klaus Haller arbeitet im Consulting in den Bereichen IT-Risiko, Information-Security und Testorganisationen. Er verfügt über praktische Erfahrung in der Konzeption, Implementierung und Betrieb von Data-Loss-Prevention-Lösungen. Alle Äußerungen im Artikel geben seine Meinung als Privatperson wieder. Mehr zu ihm auf seiner Homepage *http://www.klaushaller.net.*

Joachim Jakobs

Die Kraft der Metadaten: Wie ein Geheimdienst-Chef Opfer seiner Überwachungsdoktrin wurde

Der frühere CIA-Direktor David Petraeus bekundete 2012 seine Absicht, die Menschen dabei zu beobachten, wie sie das Licht in ihrem Wohnzimmer mit Hilfe ihres „intelligenten" Telefons einschalten. Bedauerlicherweise muss Petraeus dieses Vergnügen seinem Nachfolger überlassen: Der CIA-Chef stolperte über eine außereheliche Beziehung mit seiner Biographin Paula Broadwell.

„Um die Nadel zu finden, braucht man den Heuhaufen", so die angebliche Überzeugung von NSA-(*National Security Agency*) Direktor *Keith Alexander*. *Ira Hunt*, Chef-Techniker der *Central Intelligence Agency* (CIA) wird konkreter: *„Mehr ist immer besser … da man Punkte nicht verknüpfen kann, die man nicht hat, versuchen wir grundsätzlich alles zu sammeln, was wir sammeln können und behalten es für immer. Es liegt in sehr greifbarer Nähe, dass wir in der Lage sind, jede von Menschen verursachte Information zu verarbeiten."*

Ist Hunt womöglich nur ein Großmaul? Für den Verschlüsselungsexperten *Bruce Schneier* offenbar nicht. Er hat Zugang zu den Snowden-Dokumenten und sagt nach deren Durchsicht: „Wir wissen nicht exakt, was gesammelt wird, aber es darf als gesichert unterstellt werden, dass alles gesammelt wird. Computer generieren Transaktionsdaten als Abfallprodukt ihrer Rechnerei. Und da so ziemlich alles, was wir tun, mit Hilfe von Computern geschieht, produzieren wir mit allem was wir tun, personenbezogene Daten. Die NSA versucht alle dieser Daten zu sammeln. – Sie sollten dabei an Alles denken: Surfen, Einkaufen, Chatten, Kontakte zu Freunden. Denken Sie ans Telefonieren und wo Sie sich dabei aufhalten. Denken Sie an Alles, was nicht mit Hilfe von Bargeld abgewickelt wird, und so weiter, und so weiter. Wir wissen, dass alles von der NSA gesammelt und in Datenbanken wie PRISM gespeichert wird."

Um jegliche durch Menschen verursachte Information verarbeiten zu können, spannen die USA 2000 Firmen ein. Eine davon ist *Convera* mit seiner Suchmaschine *RetrievalWare* – ein Werkzeug mit besonderen Fähigkeiten: Sie erstellt „Profile" wahlweise von Personen, Objekten oder Orten und kann dazu nicht nur Textdokumente online und offline nach Schlagworten durchsuchen, sondern auch „Zusammenhänge erfassen": „Durch den Gebrauch von stabilen semantischen Netzen und Taxonomien, die viele Sprachen und fachspezifische Interessensgebiete abdecken, erkennt und verarbeitet *RetrievalWare* Worte, Sätze und Konzepte in ihrem spezifischen Kontext."

Das wissenschaftliche Spezialgebiet wird als *Complex Event Processing* (CEP) bezeichnet. *Bernhard Seeger*, Professor im Fachbereich Mathematik und Informatik der Universität Marburg erläutert: „Ähnlich wie bei RSS-Feeds abonniert die CEP-Anwendung Datenströme bei einer oder mehreren unabhängigen Informationsquellen. Die Datenströme bestehen aus einer potenziell unendlichen Folge zeitlich geordneter Elemente beziehungsweise einfacher Events, die neben den fachlichen Informationen über einen Zeitstempel verfügen. Ein Beispiel für einen Datenstrom sind die Nachrichten, die zwischen Applikationen auf einem *Enterprise Service Bus* ausgetauscht werden und beispielsweise per Zeitstempel bekanntgeben, wann der Sender die Nachricht erzeugt hat."

Die relevanten „Ereignisse" können von *RetrievalWare* „in bestimmte Ansichten abgebildet werden, die die personalisierten Wissensbedürfnisse, Rollen und Perspektiven eines jeden Nutzers widerspiegelt". So beschreibt es die *Convera Corporation* in ihrem „FORM 10-K"-Bericht – einem nüchternen, vorgeschriebenen – Bericht an die US-Börsenaufsicht SEC im Jahr 2006.

von David Petaraeus (links) zu John Brennan (rechts) (ehemaliger und aktueller Direktor der CIA) Fotos: offizielle Portraits der CIA

Langweilig mögen andere Berichte sein – der von *Convera* ist es nicht: Das System ist polyglott und soll 45 Sprachen beherrschen. Es ist außerdem in der Lage, Bilder, Audio- und Videoinhalte sowie 200 weitere Datenformate zu verarbeiten. Es kooperiert mit Systemen wie Lotus Notes, Microsoft Exchange, Microsoft SQL Server, Oracle, DB2, Sybase, Informix, Teradata und „jeder ODBC- kompatiblen Datenbank".

Im *FileRoom* lassen sich gescannte Dokumente, Bilder und Texte laden, indexieren und verwalten. Graphiken, Diagramme, handschriftliche Notizen und Unterschriften in den Suchtreffern sind sofort zugänglich.

Der *Screening Room* erlaubt es unter anderem, die Inhalte analoger und digitaler Videos „leistungsfähig" zu erschließen. Er bietet skalierbaren Zugang, Suche und Abruf von Videoinhalten von jedem Arbeitsplatz. In Verbindung mit *RetrievalWare Search* ist es möglich, Videoinhalte zu erfassen, verschlüsseln, analysieren, katalogisieren, durchzustöbern und aufzurufen – und zwar alles in Echtzeit: In dem Augenblick, in dem das Video verfügbar ist, wird es auch schon im *Screening Room* verarbeitet – Untertitel genauso wie gesprochene Konversationen. Hinzu kommen die Metadaten über Firmen-Netze. Die Anwender können aus den Videos heraus „einfach" „intelligente" Video-Drehbücher erstellen und in jedem Standard-Video-Dateiformat abspielen. Dadurch sollen sich die Inhalte beim nächsten Mal präzise und automatisch durchpflügen, durchsuchen und aufrufen lassen ohne das Material insgesamt erneut ansehen zu müssen.

RetrievalWare soll bereits vor acht Jahren über 4 Millarden Dokumente indexiert haben. In der Wahl seiner Quellen ist das System flexibel: „Der *RetrievalWare Profiling Server* filtert, speichert und verteilt eingehende Daten von vielen Quellen einschließlich Echtzeit News-Feeds, relationalen Datenbanken, Papierablagen und dem *RetrievalWare Internet Spider*“, wie es in dem SEC-Bericht heißt.

Der *Internet Spider* wiederum ist ein multimedialer, Hochleistungs-Webcrawler, mit dessen Hilfe sich die Such-Fähigkeiten von *RetrievalWare* ergänzen lassen – unabhängig davon, ob es als Einzelplatz-System betrieben oder in einer anderen Anwendung integriert ist. Das wirkt komfortabel – jede Veränderung im Netz wird verfolgt – und zwar ebenfalls „in Echtzeit“: In dem Augenblick, in dem die Internetseite geändert wird, nimmt *RetrievalWare* davon Notiz, aktualisiert das Profil und informiert einem Bericht der *Washington Post* zufolge den zuständigen Sachbearbeiter. Neben HTML-basierten Webseiten durchpflügt er auch PDF-Dokumente und multimediale Inhalte einschließlich Audio, Video und Bildern.

Auch verbal kann das System glänzen: Die Englische Sprachversion des semantischen Basisnetzes von *RetrievalWare* bietet 500.000 Wortbedeutungen, 50.000 Sprachphrasen und 1,6 Millionen Wortkombinationen. Die Anwender stellen umgangssprachliche Suchanfragen, die automatisch erweitert werden, um verknüpfte Ausdrücke und Konzepte zu finden. Auf diese Weise soll die Wahrscheinlichkeit erhöht werden, relevante Ergebnisse zu erhalten. Außerdem bietet *RetrievalWare* fachspezifische Komponenten an – etwa für die Disziplinen Biologie, Chemie, EDV, Elektronik, Finanzwissenschaft, Lebensmittelwissenschaft, Geographie, Geologie, Gesundheitswissenschaft, Informationswissenschaft, Recht, Mathematik, Medizin, Militär, Öl, Erdgas, Pharmazie, Physik, Kunststoffe und Telekommunikation. Für andere Fächer ließen sich unternehmensspezifische semantische Netze mit Hilfe von *Convera* entwickeln.

Die 185 Kunden von *RetrievalWare* sollen zu 70 Prozent Behörden US-amerikanischen Ursprungs gewesen sein – unter anderem die Bundespolizei FBI, die Geheimdienste CIA und NSA, das Heimatschutz- und das Verteidigungsministerium. Aber auch „über ein Dutzend ausländische Geheimdienste“.

Offenbar war die Anzahl der Kunden nicht ausreichend, um das Unternehmen am Leben zu erhalten: 2007 wurde die Software an den Wettbewerber *Fast Search & Transfer* verkauft, der einige Funktionen in eigene Anwendungen implementiert hat, aber dann selbst 2008 von Microsoft übernommen wurde. Heute firmiert das Unternehmen als *Microsoft Development Center Norway*. Microsoft leistet allerdings heute nur noch Service und Support.

Schenkt man Wikipedia Glauben, so ist *Convera* ein Kind des Risikokapitalgebers *In-Q-Tel* (IQT). Dieser wiederum gehört zum Geheimdienst CIA. Und In-Q-Tel hält Beteiligungen an dutzenden Firmen wie *Convera*, die – so *Christopher Tucker*, Chefstratege von *In-Q-Tel* bei deren Gründung 2001, „dem Dienst dabei helfen, seine Mission zu erfüllen“. Im Bereich Suchmaschinen sind es *PiXlogic*, *Endeca*, *Inxight*, *MetaCarta*, *Attensity*, *NetBase*, *Platfora* und *Intelliseek*.

Die *In-Q-Tel*-Beteiligung *Palantir* hilft dabei, die gewonnenen Erkenntnisse weiterzuverarbeiten: Seit 2011 kooperieren Palantir und SAP im Dienste der öffentlichen Sicherheit: SAP verkauft *Palantir*s Software weltweit an die Behörden. *Huddle* wiederum ermöglicht es, die Daten in der Cloud zu halten. Die Firmen *Mohomine* und *Stratify* helfen dabei, die riesigen Datenmassen zu bewältigen.

Visual Sciences will „marktführend darin sein, rechtzeitige, genaue, verständliche und gerichtsfähige Beweise zu liefern, die von unseren Kunden benötigt werden, um belastbare und wirtschaftliche Entscheidungen mit Hilfe ihrer riesigen Datenbestände in Echtzeit zu treffen.“

Dazu gehören die Auswertung von Telefondaten und -gesprächen und die Internetaktivitäten. Mit der Analyse von Daten beschäftigen sich außerdem die *In-Q-Tel*-Beteiligungen *Spotfire*, *ReversingLabs*, *RecordedFuture*, *Platfora* und *Geosemble*.

Die Arizona State University hilft dabei, Handschriften zu erkennen; dabei ist die Technik nicht nur in der Lage, handschriftlichen Notizen eine Bedeutung zuzuweisen, sondern auch den Urheber dieser Notizen zu identifizieren.

Carnegie Speech und der *CallMiner* analysieren menschliche Sprache. Da ist es konsequent, dass die US-Sicherheitsbehörden neben Kameras auch Mikrofone im öffentlichen Raum installieren – zuletzt in 55 Bussen in Portland, im US-Bundesstaat Oregan. In Washington sollen es 300 Sensoren auf 20 Quadratmeilen (~ 52 km²) sein, 70 Städte beobachteten die Einwohner auf diese Weise 2012. Aber wie erhalten die belauschten Gespräche eine Bedeutung? Die Menschen auf der Straße sind doch anonym? Da könnten abgehörte Telefonate hilfreich sein – so schreiben Wissenschaftler der Bina Nusantara University in Jarkata in einem Aufsatz: „Die Methoden der Spracherkennung nutzt die allgemein üblichen Schritte: Merkmalserkennung (Hier: Belauschen von Gesprächen, Anm. d. Autors), Sprachmusterdatenbank und Mustervergleich.“ Das heißt die bisher geführten Telefonate des „Verdächtigen“ können als Referenzdaten genutzt werden, um die Zielperson bei ihren Gesprächen in der Öffentlichkeit zu identifizieren. Genauso eignet sich der Webbrowser *Google Chrome* als Referenz: Dessen Mikrofon läßt sich – vom Nutzer unbemerkt! – von außen als Wanze nutzen.

Die IQT-Firmen *Basis Technology*, *Language Weaver* und *Lingotek* wollen Sprache übersetzen. Deren Branche hat viel vor: Automatische Sprachverarbeitung soll heute in Echtzeit möglich sein, und zwar in „78 Sprachen“, verspricht die Werbung.

Ähnlich sieht es bei der Verarbeitung von Bildern aus – ab April 2014 wird die Gesichtserkennung in den USA „radikal“ ausgebaut: So will das *Janus*-Programm nicht nur auf Fahndungsfotos, sondern auch auf Bilder des realen Lebens – etwa von Überwachungskameras – zugreifen. Mit solchen Kameras ist nicht nur in der Luft, auf Bahnhöfen, Flughäfen und vor privaten Immobilien zu rechnen, sondern auch in Umkleidekabinen, auf dem Straßenstrich, an Bushaltestellen, in Schwimmbädern und Schultoiletten sowie in Schaufenstern, E-Litfaßsäulen und E-Plakaten. Nur sind die Kameras nicht immer dicht: Leck sind sowohl zigtausende öffentliche

IP-Überwachungskameras weltweit als auch die Videokonferenzsysteme in Vorstandsbüros, Forschungseinrichtungen und Anwaltskanzleien – wobei letztere mitunter durch eine bemerkenswerte Bildqualität bestechen: Auf Zetteln notierte Passwörter sollen sich auf eine Distanz von sechs Metern erkennen lassen.

Interessant ist die Bilderkennung auch für die glücklichen Anwender von Spieleboxen: Der Journalist *Glenn Greenwald* behauptet, Microsoft habe den Behörden NSA, FBI und CIA Zugang zu den verschlüsselten Video-, Audio- und Text-Daten gewährt. So ist durchaus plausibel, dass die Bilder aus der *Xbox* von Microsoft den Diensten zugänglich sind.

Die Datenbrille *Google Glass* ist bereits durch ein Loch aufgefallen. Die Sicherheitsfirma *Symantec* meint, Kriminelle hätten an Nutzerdaten kommen können. Das wäre nicht nur für den problematisch, der die Brille trägt, sondern auch für den, der an dieser Brille vorbeiläuft. Der Berliner Beauftragte für den Datenschutz orakelte bereits in seinem Jahresbericht 2011: „Videoüberwachung pervertiert zum Volkssport". Kein Wunder: Videodrohnen mit vier Rotoren gibt's bereits für 29,95 US-Dollar.

Wer den Ereignissen einen geographischen Bezug zuweisen möchte, kann das womöglich mit Hilfe der *In-Q-Tel*-Beteiligungen *GeoIQ* oder *TerraGo* tun.

Die IQT-Firma *Digital Reasoning* – ein Spezialist bei der Verarbeitung „unstrukturierter Daten" wie Mails oder Bildern – unterstützt IBM zusammen mit dutzenden weiteren Firmen bei der Verarbeitung der vielen Daten. Bei solchen Datenmengen gibt's schnell Dopplungen: Ist der Autor einer Mail identisch mit der Person, die an einer Überwachungskamera vorbeigelaufen ist, oder tragen die beiden unterschiedlichen Personen nur zufällig beide den Namen „Müller-Lüdenscheid"? Solche Unklarheiten lassen sich mit Hilfe von *Identity Resolution Software* aufklären. IBM hat dazu bereits vor Jahren den Spezialisten *SRD* von *In-Q-Tel* übernommen.

Seinen bunten Technikstrauß hat IBM in Hardware gegossen. Das Ergebnis heißt *Watson*; wie mächtig die Kiste ist, demonstrierte der Konzern 2011 in der Quizsendung *Jeopardy*: Bereits damals war das System in der US-amerikanischen Version von *Wer wird Millionär?* in der Lage, die Fragen des Moderators – in natürlicher Sprache! – schneller zu beantworten als seine menschlichen Wettbewerber – immerhin beide „Champions" dieses Wettbewerbs. *Zdnet.com* spekulierte damals darüber, ob *Watson* „unser Computer-Oberherr" würde. Jetzt jedenfalls will der Konzern Kapital aus *Watson* schlagen – Ärzte sollen ihre Diagnosen mit der neuen *Watson*-Technologie „diskutieren" können; Architekten können Statik- und Designvorschläge erhalten; der Chefsyndikus von *Big Blue* stellt den Anwälten einen „digitalen Assistenten" mit einer „gewaltigen, eigenständigen Datenbank" in Aussicht „die alle interne und externe Informationen enthält, die für die täglichen Aufgaben nötig sind." Die Liste läßt sich fortsetzen. Das alles steht demnächst als Service übers „intelligente" Telefon bereit. Und der Heuhaufen schwillt merklich an.

Unter anderem wegen der biotechnischen Spuren, die er hinterläßt – Dutzende weitere *In-Q-Tel*-Engagements beschäftigen sich mit der Aufbereitung, dem Erhalt und der Aufklärung dieser Spuren:

Biomatrica entwickelt eine kostengünstige Technik, mit deren Hilfe die Geheimdienste biologische Proben bei Raumtemperaturen lagern können, *T2 Biosystems* will die medizinische, Arcxis die molekularbiologische Diagnostik voranbringen. Die *febit group* und *Boreal Genomics* rücken den Geheimnissen des Genoms zu Leibe.

Und die Dienste wollen auch an unser Oberstübchen – der Bestsellerautor und Geheimdienst-Experte *James Bamford* berichtete bereits 2009: Die NSA entwickle mit *AQUAINT* „ein Werkzeug, das George Orwells Gedankenpolizei nützlich gefunden hätte: Ein künstlich-intelligentes System, um Zugang zum Denken der Menschen zu erhalten."

Dafür könnten die genannten und weitere Datenquellen hilfreich sein: Zahlreiche Unternehmer in den Bereichen Elektrizität, Elektronik, Video, Datenzentren und Sicherheits-Tests erfreuen sich der geheimdienstlichen Unterstützung durch IQT.

AdaptiveEnergy entwickelt Technik fürs *Energie Harvesting*; dabei werden kleine Mengen von elektrischer Energie aus Quellen wie Umgebungstemperatur, Vibrationen oder Luftströmungen für mobile Geräte mit geringer Leistung gewonnen. *Miserware* hilft dem Notebook-Nutzer Strom zu sparen.

Nanosys will die Qualität von LED-Bildschirmen mit Hilfe von Nanotechnik verbessern. *Wispry* entwickelt Chips für Mobiltelefone.

Joachim Jakobs

Joachim Jakobs ist einer der Autoren von *Vom Datum zum Dossier – Wie der Mensch mit seinen schutzlosen Daten in der Informationsgesellschaft ferngesteuert werden kann*. Als Journalist schreibt er auch für *konstruktion.de, tab.de* und *security-insider.de* und verfasst für *itespresso.de* eine monatliche Kolumne *SicherKMU* mit der er kleinen und mittelständischen Unternehmen zu helfen versucht, den Alltag sicher zu bewältigen. Zuvor war er für IBM in Schottland, Pressesprecher bei der Fraunhofer-Gesellschaft und der Free Software Foundation Europe (FSFE).

Das Jungunternehmen *Perceptive Pixel* beschäftigte sich mit berührungsempfindlichen Bildschirmen und wurde 2012 an Microsoft verkauft. Heute bietet der Konzern sowohl berührungsempfindliche Eingabegeräte wie auch Fingerabdruckscanner an. Nicht nur die Überwachung ist dabei bedrohlich: Fingerabdrücke lassen sich auf Latexhandschuhe übertragen – sagt das Bundeskriminalamt; und sie werden auch mal unbeabsichtigt von Behörden im Netz veröffentlicht oder gestohlen.

PlateScan bietet Software zur Erkennung von Autokennzeichen, um diese dann mit den Einträgen in behördlichen Datenbanken zu vergleichen. Vom Zeitpunkt der Nummernschild-Erkennung bis zum Datenbankabgleich benötigt das System angeblich nur eine Sekunde.

Die *Ember Corporation* und *Tendril Networks* helfen beim Stromsparen im intelligenten Haushalt mit Hilfe mobiler Sensoren. Im RFID-Markt bewegen sich außerdem die IQT-Investitionen *Paratek*, *Streambase* und *Thingmagic*.

Ob diese Unternehmen und ihre Produkte von der CIA und anderen Geheimdiensten als Vehikel genutzt werden, um deren Kunden auszuspähen, ist nicht bekannt. ZDNet berichtete jedenfalls kürzlich darüber, dass die NSA PC, Router und Festplatten infiziert haben soll.

Der frühere CIA-Direktor *David Petraeus* bekundete 2012 seine Absicht, die Menschen dabei zu beobachten, wie sie das Licht in ihrem Wohnzimmer mit Hilfe ihres „intelligenten" Telefons einschalten. Bedauerlicherweise muss Petraeus dieses Vergnügen seinem Nachfolger überlassen: Der CIA-Chef stolperte über eine außereheliche Beziehung mit seiner Biographin Paula Broadwell.

Diese kam durch eine Analyse von Metadaten ans Licht: Die US-Bundespolizei FBI beobachtete ein elektronisches Postfach, von dem belästigende Mails verschickt wurden. Diese ließen sich auf ein WLAN-Netz in einem Hotel zurückverfolgen und mit der Gästeliste des Hotels vergleichen. Schließlich korrespondierten Broadwell und Petraeus gleichzeitig über den Entwurfs-Ordner eines zweiten Postfachs über ihre Liebesbeziehung miteinander. Die belästigenden Mails an die vermeintliche Nebenbuhlerin und die Nachrichten der verliebten Broadwell kamen von ein und derselben IP-Adresse.

In der Informationsgesellschaft ist kein Heuhaufen mehr nötig, um ein Opfer zu Fall zu bringen; insbesondere für die „Großkopferten" kann eine Nadel völlig ausreichen.

Originalquelle: ZDNet, *http://www.zdnet.de/88185358/die-kraft-der-metadaten-wie-ein-geheimdienst-chef-opfer-seiner-ueberwachungsdoktrin-wurde/*

Joachim Jakobs

Vernetzte Bedrohungen verlangen nach vernetzten Verteidigungsstrategien

Die Sicherheit der Sicherheitsbehörden ist bedroht: Insbesondere beim BND stehlen die US-Dienste wie die Raben. Jetzt werden wieder Schreibmaschinen angeschafft. Die amtliche Hilflosigkeit ist kein Einzelfall – tatsächlich sind die Kombinationsmöglichkeiten aus Angreifern, Angriffsmitteln/-wegen und Angegriffenen endlos.

Geheimdienste, Mafiosi, Industriespione, Terroristen – oder auch Cyber-Söldner – klauen analoge Daten auf Papier und digitale Informationen auf elektronischen Speichern, physikalisch (per Einbruchdiebstahl) oder übers Internet. Mal mit, mal ohne die Unterstützung von „Innentätern" – bei Behörden und Unternehmen. Und zwar seit Jahren – nur wollten wir es nicht sehen. Die Scherben unserer Ignoranz fallen uns jetzt vor die Füße.

Auch die Leistungsfähigkeit gehört dazu: Immer mehr Informationen können auf immer kleinerem Raum gespeichert und immer schneller übertragen werden. Die Angreifer nutzen künstliche Intelligenz, um damit verbundene menschliche und technische Schwächen automatisiert auszunutzen, die Angegriffenen meinen, sie hätten nix zu verbergen. Dieser digitale Graben droht explosionsartig zu wachsen – die Dinge sollen „intelligent" werden: Im kommenden Internet „der Dinge" (IPv6) verfügt rein rechnerisch jeder der 80 Millionen Bundesbürger über 62,5 Trillionen IPAdressen. Damit ließe sich jede der 100 Billionen Körperzellen eines jeden Bundesbürgers 625.000.000 Mal weltweit einmalig – durchnummerieren. Diese Leistungsfähigkeit ermöglicht es, Politik, Wirtschaft und Gesellschaft in beliebiger Detailtiefe zu vernetzen. „Smart" soll sie sein, die Zukunft.

Möglichkeiten und Wünsche sollten im Einklang stehen mit den Fähigkeiten derer, die Entscheidungen zur Informationsgesellschaft fällen, oder auf Basis dieser Entscheidungen Software entwickeln, implementieren oder nutzen, um diese „intelligenten" Anlagen zu steuern oder personenbezogene Daten zu verarbeiten.

Ansonsten könnten uns Dritte das Fell über die Ohren ziehen: *Bonesaw* kennt jedes Endgerät am Internet – samt seiner Löcher. *Turbine* kann diese Geräte infizieren. Die Inhalte von Texten, gesprochener Sprache, Bildern, Handschriften und Videos lassen sich maschinell erkennen und die beteiligten Personen können anhand ihrer biometrischen Merkmale identifiziert werden. Die Beute aus dem einen Raubzug läßt sich kombinieren mit der aus beliebig vielen Anderen. Der Verschlüsselungsexperte Bruce Schneier ist der Ansicht: „Bald wird alles was wir tun, on- und offline, aufgenommen und für immer gespeichert. Die einzig verbleibende Frage ist, wer Zugang zu all den Informationen hat."

Solche Informationen werden heute vielfach mit Hilfe von SAP verarbeitet: Kaum ein DAX-Konzern kommt ohne die Software

der Walldorfer – für Funktionen wie dem Controlling oder dem Personalwesen – aus. Zwei Dutzend Branchenanwendungen treiben die Produktivität in Wirtschaft und Verwaltung. Künftig werden aber auch Gebäude, Heizungen oder Fahrzeuge vernetzt. Wirbt SAP. Die „Dinge" bieten sich Spionen und Saboteuren an. So debattieren Experten derzeit, ob sich ein ganzes Land mit Hilfe eines „Generalschlüssels" zu SAP lahmlegen ließe – für Innentäter mit den Fähigkeiten von Edward Snowden sicher ein Kinderspiel. Wobei: „SAP" ließe sich austauschen – etwa durch „Windows".

Die US-Bundespolizei (FBI) meint, sie würde den Cyberkrieg „nicht gewinnen". Die Angreifer scheinen schneller zu lernen als die Angegriffenen – und könnten ähnliche Schäden verursachen wie am *11. September*.

Wir haben es offenbar mit einer vernetzten Bedrohung zu tun. Daher sind vernetzte Antworten gefordert – nicht unbedingt von denen, die über Geld, Macht und/oder Einfluss verfügen. Aber diese Spezies sollte dafür sorgen, dass das Gespräch in Gang kommt – etwa zur Frage, wie die 4482 Seiten *IT-Grundschutz* vom *Bundesamt für die Sicherheit in der Informationstechnik* (BSI) in Millionen Institutionen in unserem Land implementiert werden können.

Tatsächlich kommen die Maßnahmen nur schleppend in Gang: Ein Verband ist stolz auf 2000 Teilnehmer seines Projekts *(m)IT Sicherheit*. Bei 30 Millionen Arbeitnehmern ein Tropfen auf den heissen Stein.

Und ob von diesen 2000 Personen auch nur eine in der Lage wäre, den Europäischen Computerführerschein ECDL zu absolvieren oder bei ihrem Arbeitgeber ein Projekt für ein Sicherheitsoder ein Notfallkonzept angeschoben und erfolgreich abgeschlossen hat?

Eine der Ursachen dieses Erfolgsmangels liegt sicher darin, dass sich die Mittelstands-Maßnahmen gegenseitig kannibalisieren. Hinzu kommen Angebote für die Hoteliers und die Handwerker. Und natürlich die Ärzte. Die *Kassenärztliche Vereinigung Rheinland-Pfalz* bietet 2014 vier Termine an, bei denen den dortigen Ärzten DatenschutzInformationshäppchen im Viertelstunden-Takt geboten werden. Bildung in einem einzelnen Bundesland in der 15-Minuten-Terrine!

Die zweite Mängelursache besteht in der künstlichen Trennung der natürlichen Vernetzung und das auch noch nach Bundesländern separiert!

Der Höhepunkt des Aufklärungs-Aktionismus: Der *Deutschland sicher im Netz e. V.* will Anwälte und Steuerberater dazu gewinnen, die Sensibilität ihrer Klienten zu erhöhen. Hoffentlich hat der Bock eine Umschulung genossen, bevor er seine Tätigkeit als Gärtner aufgenommen hat!

Das Klein-Klein führt dazu, dass die Medien nicht berichten – das Argument der Macher: „Wenn ich diese eine Veranstaltung vorstelle, wollen fünf andere auch genannt werden." Die Debatte über Fähigkeiten und Verantwortung der Handelnden bleibt aus. Der umworbene Mittelstand nimmt das Angebot nicht einmal zur Kenntnis. Und die Veranstaltungen bleiben leer: Die Resonanz ist so schlecht, dass Journalisten nicht einmal an den Veranstaltungen der Ärzte teilnehmen dürfen. Das Ergebnis des Gewurschtels dokumentiert eine Pressemeldung Ende Mai: „Nach einer aktuellen Umfrage von Deutschland sicher im Netz (DsiN) führen nur 28 Prozent der Unternehmen regelmäßige Schulungen für Mitarbeiter durch. Damit ist dieser Wert seit 2011 unverändert, obwohl die Digitalisierung des geschäftlichen Alltags im selben Zeitraum zugelegt hat." Andere formulieren ihre Erkenntnis knackiger: „Mittelständler sind stark bedroht und schlecht gerüstet."

Wir müssen unkonventionelle Wege gehen, wenn wir nicht alle zur Schreibmaschine zurückkehren wollen: Ich versuche das mit *SicherKMU* und *Frei+Fit im Web 2.0*. Beim ersten Projekt handelt es sich um eine monatliche Kolumne, die Aspekte vom BSI-Grundschutz anschaulich aufgreifen, die Zusammenhänge erläutern und eine Lösung vorschlagen soll. Im Rahmen der zweiten Initiative will ich mit einem *Datenschutzmobil* durchs Land fahren und die Teilnehmer der Informationsgesellschaft für ein Sicherheitsbewußtsein begeistern. Jeder ist aufgerufen, diese öffentliche Debatte mit eigenen Vorschlägen zu fördern – und wer immer mich dabei unterstützen möchte, kann mir gern schreiben an *info@privatsphaere.org*.

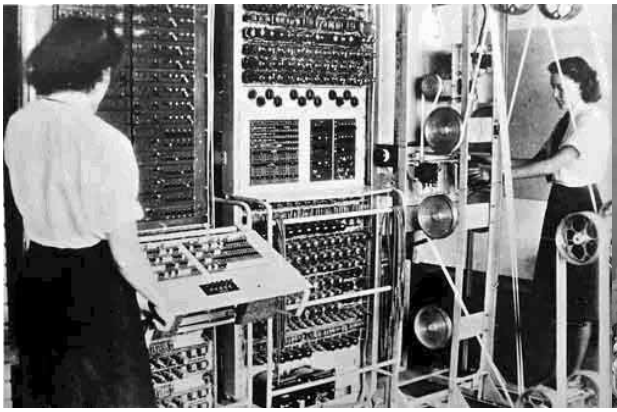
Originalquelle: security-insider.de, *http://www.security-insider.de/themenbereiche/sicherheits-management/compliance/articles/453913/*

Das Datenschutzmobil – Blickfang und idealer Werbeträger 3DModell: Dosch Design Grafik: Hannes Fuß, CC BY-NC-ND

„Dieses Fahrzeug hoffen die Initiatoren von einem Hersteller zu erhalten. Weitere 15 Investoren sollen jeweils 15.000 Euro beitragen, um so die Kosten für Personal und Marketing der einjährigen Kampagne zu finanzieren. Eine deutschlandweit vertretene Hotelgruppe soll tageweise Räume zur Verfügung stellen, um die Veranstaltungen durchzuführen. Somit hätten viele der Adressaten am jeweiligen Ort die Chance, bei einem der Vorträge zuzuhören. Projektleiter Jakobs hofft, die Geldgeber in den entsprechenden Branchen schnell zu finden: ‚Die Werbewirksamkeit des Projekts ist extrem hoch'."

http://privatsphaere.org/2012/11/05/frei-fit-im-web-2-0-will-freiberufler-fit-fur-die-informationsgesellschaft-machen/

Die Deutschland-Tournee scheiterte mangels Investoren und Datenschutzmobil.



Britta Schinzel und Sara Stadler

Gender und Informatik – Editorial zum Schwerpunkt

Dass es notwendig ist, im Zusammenhang mit Informatik über Gender zu sprechen, bedarf eigentlich keiner langen Erklärung. Trotz Fortschritten bei der Gleichstellung von Frauen im Informatik-Studium und Beruf sind im deutschsprachigen Raum die Hörsäle und Führungsetagen ebenso weitgehend männlich dominiert wie die Hackerspaces. Insbesondere Feminist_innen sind in der Netzwelt prominentes Ziel unter anderem sexistischer und homophober Angriffe und die Technik, die uns alltäglich umgibt, spiegelt nicht selten das sexistische Designparadigma wider, dass sich Frauen nur dann an einen Computer trauen, wenn er pink ist.

Die Beiträge des Schwerpunkts tragen der Themenvielfalt in diesem Bereich Rechnung und beleuchten die Rolle von Gender in der Informatik in verschiedenen Bereichen und aus unterschiedlichen Perspektiven. Zu den identifizierten Ausschließungen und Angriffen werden dabei jeweils Gegenstrategien vorgetragen, aber es bleibt viel zu tun.

Ein Teil der Beiträge beschäftigt sich mit dem nach wie vor durch wirkmächtige gesellschaftliche Stereotype und institutionalisierten Sexismus eingeschränkten Zugang von Frauen zur Informatik-Bildung und entsprechenden Berufen, wobei sie jeweils unterschiedliche Bereiche fokussieren.

In dem Text *Alumnae tracking* beschreiben *Schmid et al.* die Ergebnisse einer sehr akribisch geführten differenzorientierten Untersuchung von Studierenden und Ehemaligen der Fakultät Wirtschaftsinformatik und Angewandte Informatik an der Universität Bamberg, die exemplarisch Ursachen für die geringe Anzahl von Frauen in Führungspositionen in Deutschland herausfinden sollte. Dazu wurde in einer Fragebogenaktion einerseits nach den Kompetenzen für Leitungsberufe im IT-Bereich und andererseits nach Prioritäten in Bezug auf die eigene Lebensplanung gefragt. Während sich die Einschätzung der eigenen Leistungsfähigkeit nach Geschlecht kaum unterscheidet, und diese, sowie die Abschlussnoten, sogar zugunsten der Frauen sprechen, zeigen sich hinsichtlich der Bewertung der Relevanz der Arbeitssituation leichte Unterschiede, auch wenn diese die Unterschiede bei der Erreichung von Führungspositionen nicht erklären können. Es zeigt sich eine gewisse Blindheit der männlichen Befragten gegenüber den Problemen von Frauen in diesen Berufen: Während die befragten Frauen eine eher aufgabenorientierte, statt aufstiegsorientierte weibliche Arbeitsweise sowie Vereinbarkeitsprobleme von Familie und Beruf als Grund für geringere Aufstiegsmöglichkeit von Frauen ansehen, bestätigen die befragten Männer zwar die unterschiedliche Arbeitsweise und Vereinbarkeitsprobleme (übrigens auch für sich selbst), sehen diese jedoch nicht als Aufstiegshindernisse für Frauen an. Auch allen weiteren von Frauen angeführten Gründen für schlechtere Aufstiegschancen wird seitens der Männer eine signifikant geringere Bedeutung beigemessen – wie auch, es ist ja nicht ihr Problem.

Während dieser Text also in erster Linie die Notwendigkeit aufzeigt, der Unterrepräsentation von Frauen im Informatikbereich entgegenzuwirken und Zugangshürden abzubauen, zeigen die Texte von *Stefanie Nordmann* sowie *Julia Hoffmann* und *Natalie Sontopski* entsprechende Strategien auf.

Stefanie Nordmann beschreibt in ihrem Beitrag *Eine neue Zielgruppe für die Informatik* die Konzeption, Bewerbung und den Erfolg eines an der Hochschule für Technik und Wirtschaft Berlin seit dem Wintersemester 2009/10 etablierten Bachelor-Frauenstudiengangs für Informatik und Wirtschaft. Dabei konnte unter anderem auf Erfahrungen aus dem Bremer Frauenstudiengang zurückgegriffen werden, die auf entsprechende Anforderungen für die Motivation, günstigere Studienformen und integrative Eigenschaften der angebotenen Lehre eingehen. Der Erfolg gibt den Initiatorinnen Recht: es konnten mehr Frauen gewonnen werden als dies ohne die monoedukative Form gelungen wäre, ohne dass die parallelen koedukativen Studiengänge an Frauen verloren hätten; die Zufriedenheit der Studierenden ist groß und die Wirtschaft schätzt die gegenüber den klassischen Studiengängen erweiterten Kompetenzen der Abgängerinnen sehr.

Julia Hoffmann und *Natalie Sontopski*, Gründerinnen der *Code Girls Leipzig,* setzen in erster Linie auf Selbstorganisation. In ihrem Text *Du nennst es Programmieren, ich nenne es Rock'n'Roll* berichten sie davon, wie sie vor nunmehr zwei Jahren die *Code Girls* gegründet und im Lauf der Zeit weiter etabliert haben, und warum sich das trotz aller Widrigkeiten gelohnt hat. In einem beachtlichen Marathon haben sie das erreicht, wozu sie voller Tatendrang von einem Besuch des internationalen Technik-Festivals *Campus Party* aufgebrochen sind: dass

„mehr Mädchen und Frauen, Programmier- und Scriptsprachen als Ausdrucksmittel entdecken und unsere digitale Welt mitgestalten."

Dass Stereotype und Diskriminierungen nicht nur für den Zugang zum Informatikbereich, sondern auch für informationstechnische Produkte von Bedeutung sind, veranschaulichen die folgenden Beiträge.

Im Kontext der Softwareentwicklung werden, wie in jedem anderen gesellschaftlichen Bereich, Sexismen und stereotype Rollenbilder durch Wiederholung verfestigt. *Jasmin Link*, *Elisabeth Büllesfeld* und *Nicola Marsden* heben in ihrem Beitrag *Personas: Vermeidung von Stereotypen im Softwareentwicklungsprozess* die Bedeutung hervor, die den in nutzungszentrierter Gestaltung eingesetzten fiktiven Personen zukommt. Da im Zusammenhang mit Personas die Möglichkeit zur Identifikation und Empathie von zentraler Bedutung ist, stellt das Vermeiden von Stereotypen aber gerade in diesem Bereich eine Herausforderung dar, da *„die Möglichkeit zur Identifikation mit und Sympathie für eine Persona (und damit die mögliche Empathie) unter anderem vom Sexismus der Betrachtenden bestimmt"* wird. Die Autorinnen schlagen jedoch verschiedene Ansätze vor, die das Vorhandensein von Stereotypen und Sexismen im Erstellungsprozess von Personas sichtbar und diskutierbar machen. Inwieweit damit das Vorkommen stereotyper Geschlechterbilder in der Softwareentwicklung reduziert werden kann, wird der situative Einsatz zeigen.

Doris Allhutter beleuchtet in ihrem Text *User Experience: Was uns Geschlechter-Technikverhältnisse zeigen* die User Experience (UX), ein soziotechnisches Konzept, dem es um die *„Wahrnehmungen, Emotionen und psychologischen und physiologischen Reaktionen von Nutzer_innen bei der Interaktion mit einem System"* geht, aus der Perspektive verschiedener geschlechtsspezifischer Ansätze. Dabei macht sie ein soziomaterielles UX-Konzept stark, das die *„Gesellschaftlichkeit, Geschichtlichkeit und das prozesshafte Werden von Subjekten in Relationalität mit Technik"* sichtbar macht und dadurch die Möglichkeit eines gesellschaftspolitisch engagierten UX-Designs eröffnet. Für die konkrete Umsetzung von Design-Entscheidungen bedeutet das, Annahmen über Zielgruppen auf stereotype Zuschreibungen zu hinterfragen und Diversität innerhalb der Nutzer_innengruppe mitzudenken.

Die folgenden Beiträge thematisieren Hacktivismus und Netzkultur hinsichtlich der Beteiligung von Frauen, aber auch deren (und anderer Gruppen) Ausgrenzung durch Sexismus, Rassismus und andere Diskriminierungen.

Im Text von *Leonie Tanczer* geht es um eine qualitative Studie zum sogenannten *Hacktivismus*, des politisch und sozial motivierten Hackertums, das ebenso wie die Hackercommunity stark männlich stereotypisiert ist. Diese Stereotype werden dadurch verstärkt, dass die Mitwirkung von Frauen unerwähnt bleibt und der Gender-Bias sprachlich im Alltag und in den Medien verstärkt wird. Tanczer führte Interviews mit fünf weiblichen und fünf männlichen Hacktivist_innen und unterzog die Ergebnisse einer Diskursanalyse. Im Ergebnis zeigte sich, dass der *Male-Only*-Stereotyp durch die männlichen Aktivist_innen sprachlich verselbstständlicht wird und die Selbstidentifizierung als Hacktivisten untermauert. Gegen diese Norm bauten Hacktivistinnen hingegen Widerstände rund um ihre weibliche Identität auf, indem sie feministische oder frauenspezifische Themen in ihrer Hacktivist_innen-Tätigkeit hervorheben. Die Effekte um die Vereinzelung in einer Gruppe anderer wird als *Tokenism* bezeichnet: die selbstverständliche Norm braucht nicht erwähnt zu werden, die Abweichung von der Norm (hier Hacker-Frau) wird als auffällig wahrgenommen und muss gerechtfertigt werden. Die weiblichen Tokens werden ihrerseits stereotypisiert, entweder als kompetente Ausnahmen oder als Vertreterinnen der homogenen Gruppe *Frau*, der IT-Kompetenz abgesprochen wird. Tanczer beschreibt weitere Zugangshürden für Frauen und erwähnt mögliche Gegenstrategien.

Dass das Netz entgegen ersten Gleichheits- und Freiheits-Utopien kein Raum ohne Diskriminierungen und auch kein post-gender-Raum ist, ist hinlänglich bekannt geworden. Nicht nur haben sich Maskulinisten auf Genderforscherinnen und Feminstinnen eingeschossen – das geht bis hin zu Vergewaltigungs- und Morddrohungen –, sondern öffentliche Äußerungen von Frauen allgemein erscheinen als beliebter Ort für diskriminierende, diffamierende und verletzende Rede. *Sylvia Pritsch* analysierte exemplarisch die *Troll*-Attacken während der Bloggermesse *Re:publica* im April 2010 und die Reaktionen darauf. Der Chat zu einer per Livestream übertragenen Podiumsdiskussion dieser Messe unter dem Titel *Das andere Geschlecht – Sexismus im Netz* wurde mit Spam-Attacken überhäuft und blockiert, wobei zunächst diskutiert wurde, ob es sich dabei um Sexismus handelte oder „nur" um Trollbeiträge, die einfach provozieren sollten. Diese Trennung wurde aber schließlich als unproduktiv und verharmlosend aufgegeben. Nach einiger Auseinandersetzung um mögliche Gegenstrategien, wurden im behandelten Beispiel Enttabuisierungsstrategien gewählt, die darauf abzielten, sexistische Äußerungen als solche zu benennen und zu veröffentlichen. Im Folgenden erreichten die *#Aufschrei*-Kampagne und feministische Netz-Communities die öffentliche Thematisierung und Einordnung sexistischer Rede als verletzend und als eine Form von Gewalt. Eine besondere Verletzbarkeit im Netz zeigt sich mit der Adressierung, der wiedererkennbaren Internet-Adresse, die angreifbar ist, z. B. durch Spam-Attacken oder Stalking. Wirklich wirksame Gegenstrategien gegen solche Attacken sind noch nicht entwickelt.

Mit der Bandbreite der angesprochenen Themen gelingt es dem Schwerpunkt, so hoffen wir, Anstöße für eine tiefer gehende Auseinandersetzung mit dem Thema zu liefern. Der Fokus liegt in diesem Heft zumeist auf dem deutschsprachigen Raum und auf Ausschließung und Diskriminierung entlang von Geschlecht, ohne detaillierter auf Heteronormativität, Mehrfachdiskriminierungen und Wechselwirkungen mit anderen Machtstrukturen einzugehen. Dass damit viele Aspekte der Ausgrenzung außen vor bleiben, steht außer Frage. Gerne nehmen wir Zuschriften und Ideen für zukünftige Ausgaben entgegen.

Bildnachweis: Colossus codebreaking computer in operation, 1943; Dr. Mae C. Jemison, First African-American Woman in Space – GPN-2004; Universal Automatic Computer Model 120 – Foto vom Department of Interior, Bureau of Mines, 1961

Anja Gärting-Daugs, Silvia Förtsch und Ute Schmid

Alumnae Tracking

Frauenkarrieren in der Informatik

Projektbeschreibung und -ziele

Das vom Europäischen Sozialfonds und dem Bayerischen Staatsministerium für Arbeit und Sozialordnung, Familien und Frauen finanzierte Forschungsprojekt *Alumnae Tracking* verfolgt das Ziel, Ursachen für geschlechtsspezifische Segregation im Berufsleben aufzudecken und den Anteil von Frauen in Führungspositionen und in zukunftsorientierten Bereichen zu erhöhen [7].

Im europäischen Vergleich ist der Anteil von Frauen in Führungspositionen in Deutschland branchenübergreifend gering. So waren in der Privatwirtschaft 2010 nur etwa 30 % der Führungspositionen mit Frauen besetzt [11]. Betrachtet man lediglich die Besetzung der Top-Positionen in den größten börsenorientierten Unternehmen, so liegt der Frauenanteil mit 18 % noch deutlich niedriger [6, 9]. In der IT-Branche beträgt der Frauenanteil im Top-Management sogar nur rund 7 % [12].

Ein Grund dafür ist im vergleichsweise niedrigen Anteil weiblicher Studierender in der Informatik zu sehen. Trotz steigender Zahl von Studienanfängerinnen sind Frauen mit einem Anteil von 22,1 % an allen Studierenden im 1. Fachsemester Informatik noch immer unterrepräsentiert [13]. Von diesen erreichen bislang nur wenige Frauen eine Führungsposition [5].

Im Rahmen des Alumnae-Tracking-Projekts wird untersucht, ob Informatikerinnen in einem männlich dominierten Arbeitsumfeld auf dem Weg nach oben an eine gläserne Decke stoßen [4, 8] oder ob weibliche Informatikabsolventinnen aufgrund ihrer individuellen Gewichtung von privaten und beruflichen Zielen keine Führungsposition anstreben.

Methodik und Fragestellungen

Innerhalb der Projektlaufzeit von Oktober 2012 bis März 2015 werden Studierende und Ehemalige der Fakultät Wirtschaftsinformatik und Angewandte Informatik (WIAI) der Otto-Friedrich Universität Bamberg zu drei Zeitpunkten schriftlich befragt. Auf diese Weise sollen Veränderungen in der beruflichen Position sowie in der Lebensplanung mit ihren jeweiligen Einflussfaktoren erfasst und Geschlechterunterschiede aufgedeckt werden.

Als theoretische Grundlage für die Erhebung und deren Auswertung dient das Rahmenmodell der Lebensplanung in Beruf und Privatleben (vgl. Abbildung 1), das von Abele (2002) entwickelt wurde. Entsprechend diesem Modell hängt die berufliche und private Entwicklung neben soziodemografischen Variablen von motivationalen Faktoren, Fähigkeiten, Interessen und dem Selbstkonzept einer Person ab. Zusätzlich ist die Zielerreichung durch förderliche und hinderliche Bedingungen im privaten und beruflichen Umfeld bedingt [1].

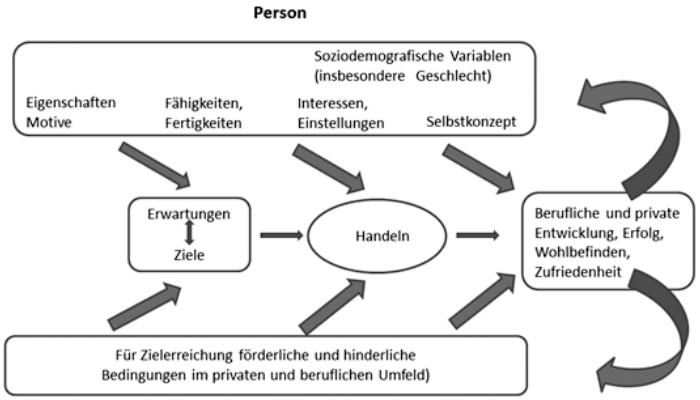


Abbildung 1: Rahmenmodell der Lebensplanung in Beruf und Privatleben, Quelle: Abele, A. (2012), S. 111, eigene Darstellung

In diesem Beitrag werden ausgewählte Ergebnisse zu den Fähigkeiten und Fertigkeiten der Befragten, den jeweiligen Zielen sowie hinderlichen Faktoren für das Erreichen einer Führungsposition dargestellt. Darüber hinaus wird untersucht, ob sich die Befragten in ihrer Berufszufriedenheit hinsichtlich Geschlecht und Führungsposition unterscheiden. Tabelle 1 gibt einen Überblick, mit welchen Fragen die soziodemografischen Variablen wie Geschlecht und familiärer Status sowie die Konstrukte Fähigkeiten und Fertigkeiten, Ziele, hinderliche Bedingungen im beruflichen Alltag, Führungsposition und Berufszufriedenheit operationalisiert wurden.

Führungsposition

Als Führungskraft werden im vorliegenden Beitrag alle Personen mit leitender Funktion aufgefasst. Demgegenüber ist der Begriff der Führungskraft im Führungskräftemonitor der DIW weiter gefasst. Dort werden auch Beschäftigte mit hoch qualifizierten Tätigkeiten, wie beispielsweise wissenschaftliche Angestellte oder Ingenieure, zu den Führungskräften gezählt [11]. Gemäß der eingangs erwähnten Zahlenlage untersuchen wir, ob auch unter den Absolventen unserer Fakultät weitaus mehr männliche Befragungsteilnehmer als Frauen eine Führungsposition innehaben.

Fähigkeiten und Fertigkeiten

Es wird betrachtet, ob sich der geringe Anteil von Frauen in Führungspositionen durch unterschiedliche Befähigung zur Führung erklären lässt. Generell gelten gute Noten, Fachwissen und soziale Kompetenzen als förderlich für einen erfolgreichen Berufseinstieg und -aufstieg [16]. Es wird deshalb untersucht, ob sich Informatikerinnen und Informatiker in ihrer universitären Abschlussnote sowie in der subjektiven Einschätzung ihrer Fach- und Führungskompetenzen unterscheiden.

Konstrukt	Operationalisierung	Skala/Merkmalsausprägung
Soziodemografische Variablen		
Geschlecht	Geschlecht	männlich weiblich
Familiärer Status	Anzahl Kinder unter 18 Jahren	keine 1 Kind 2 Kinder 3 Kinder mehr als 3 Kinder
Fähigkeiten und Fertigkeiten		
Objektive Fachkompetenz	Studiumsabschlussnote	1,0 bis 4,0
Subjektive Einschätzung der Fachkompetenz [1)]	Spezielles Fachwissen	5-stufige Likertskala (1: in sehr geringem Maße; 5: in sehr hohem Maße)
	Breites Grundlagenwissen	5-stufige Likertskala (1: in sehr geringem Maße; 5: in sehr hohem Maße)
Subjektive Einschätzung der Führungskompetenz [1)]	Kommunikationsfähigkeit	5-stufige Likertskala (1: in sehr geringem Maße; 5: in sehr hohem Maße)
	Verhandlungsgeschick	5-stufige Likertskala (1: in sehr geringem Maße; 5: in sehr hohem Maße)
	Organisationsfähigkeit	5-stufige Likertskala (1: in sehr geringem Maße; 5: in sehr hohem Maße)
	Führungsqualitäten	5-stufige Likertskala (1: in sehr geringem Maße; 5: in sehr hohem Maße)
	Kooperationsfähigkeit	5-stufige Likertskala (1: in sehr geringem Maße; 5: in sehr hohem Maße)
	Verantwortungsfähigkeit	5-stufige Likertskala (1: in sehr geringem Maße; 5: in sehr hohem Maße)
	Konfliktmanagement	5-stufige Likertskala (1: in sehr geringem Maße; 5: in sehr hohem Maße)
Lebens- und Arbeitsziele [2)]		
Wichtigkeit aus subjektiver Sicht	Gut verdienen	5-stufige Likertskala (1: gar nicht wichtig; 5: sehr wichtig)
	Leitende Funktion übernehmen	5-stufige Likertskala (1: gar nicht wichtig; 5: sehr wichtig)
	Sich der Familie widmen	5-stufige Likertskala (1: gar nicht wichtig; 5: sehr wichtig)
	Das Leben genießen	5-stufige Likertskala (1: gar nicht wichtig; 5: sehr wichtig)
	Beruf und Familie vereinbaren	5-stufige Likertskala (1: gar nicht wichtig; 5: sehr wichtig)
	Anerkennung im Beruf erwerben	5-stufige Likertskala (1: gar nicht wichtig; 5: sehr wichtig)
	Einen sicheren Arbeitsplatz haben	5-stufige Likertskala (1: gar nicht wichtig; 5: sehr wichtig)
	Gute Arbeitsbedingungen haben	5-stufige Likertskala (1: gar nicht wichtig; 5: sehr wichtig)
	Interessante berufliche Tätigkeit	5-stufige Likertskala (1: gar nicht wichtig; 5: sehr wichtig)
Hinderliche Faktoren für berufliche Entwicklung [3)]		
Zutreffen aus subjektiver Sicht	Zu wenig weibliche Vorbilder	5-stufige Likertskala (1: trifft gar nicht zu; 5: trifft stark zu)
	Männlich geprägte Kultur	5-stufige Likertskala (1: trifft gar nicht zu; 5: trifft stark zu)
	Aufgabenorientiertes Arbeiten	5-stufige Likertskala (1: trifft gar nicht zu; 5: trifft stark zu)
	Benachteiligung bei der Stellenbesetzung	5-stufige Likertskala (1: trifft gar nicht zu; 5: trifft stark zu)
	Geringe Förderung durch männliche Vorgesetzte	5-stufige Likertskala (1: trifft gar nicht zu; 5: trifft stark zu)
	Probleme bei Vereinbarkeit von Familie und Beruf	5-stufige Likertskala (1: trifft gar nicht zu; 5: trifft stark zu)
	Geringere prestigeträchtige Arbeitsfelder	5-stufige Likertskala (1: trifft gar nicht zu; 5: trifft stark zu)
Führungsposition	Führungsverantwortung für Anzahl Mitarbeiter	unter 10 10 bis unter 50 50 bis unter 200 200 bis unter 500 Über 500

Quellen:
1) Schaeper, H./Briedis, K. (2004), Kompetenzen von Hochschulabsolventinnen und Hochschulabsolventen, berufliche Anforderungen und Folgerungen für die Hochschulreform, HIS-Projektbericht, Hannover.
2) Hochschul-Informations-System GmbH (2009), Hochqualifiziert und auf dem Weg. Eine Befragung von Masterabsolventinnen und Masterabsolventen des Prüfungsjahrgangs 2008/2009, Hannover.
3) Langfeldt, B./Mischau, A. (2013), Geschlechterdisparitäten in Berufs- und Karriereverläufen von MathematikerInnen und PhysikerInnen innerhalb und außerhalb klassischer Beschäftigungsmodelle, Hamburg/Bielefeld/Berlin.

Tabelle 1: Operationalisierung der soziodemografischen Variablen und untersuchten Konstrukte, eigene Darstellung

Lebens- und Arbeitsziele

Ferner gehen wir davon aus, dass der Karriereverlauf und die Zufriedenheit mit der erreichten beruflichen Position auch von den Lebens- und Arbeitszielen der Befragten, die das individuelle Anspruchsniveau an die berufliche Tätigkeit definieren abhängig ist und dem Ausmaß, inwieweit dieses erreicht wurde. Auch hier werden Unterschiede zwischen männlichen und weiblichen Informatikabsolventen unterstellt. Eine berufliche Karriere anzustreben, ist gemäß einer Befragung durch *Allmendinger* und *Haarbrücker* (2013) Männern nach wie vor wichtiger als Frauen. Jedoch stieg der Anteil der Frauen, die Karriereziele haben, gegenüber der vorangegangen Erhebung im Jahr 2007 deutlich an. Insbesondere gute gebildete Frauen, wie dies auch auf Informatikabsolventinnen zutrifft, streben nach dem Chefsessel [3].

Hinderliche Faktoren für die Karriereentwicklung

Als hinderliche Faktoren für einen beruflichen Aufstieg von Frauen werden im MINT-Bereich vielfach fehlende weibliche Vorbilder, eine männlich geprägte Berufskultur mit einer einhergehenden Bevorzugung von Männern bei Stellenbesetzungen und einer fehlenden Förderung von Frauen durch männliche Vorgesetzte, eine eher aufgaben- anstelle einer aufstiegsorientierten weiblichen Arbeitsweise sowie Vereinbarkeitsprobleme von Familie und Beruf angeführt [5, 14, 15]. Es wird untersucht, ob und inwieweit diese Gründe auch als Barriere für einen erfolgreichen beruflichen Aufstieg von den Absolventinnen der Fakultät WIAI aufgeführt werden.

Beschreibung der Stichprobe

Der Beitrag basiert auf den Daten der ersten Welle der schriftlichen Absolventenbefragung. Anfang des Jahres 2013 wurden 751 Fragebögen an alle Absolventen der Fakultät WIAI verschickt. Die Beantwortung der Fragen war schriftlich oder online möglich. Insgesamt gingen bis Dezember 2013 204 ausgefüllte Fragebögen ein, davon 179 Männer und 25 Frauen. Dies entspricht einer Rücklaufquote von 27,2 %. Der Anteil weiblicher Teilnehmer beträgt 12,3 %.

Die nachfolgenden Ergebnisse werden nach Geschlechtern und teilweise nach beruflicher Stellung für die Gesamtstichprobe (179 männlich, 25 weiblich) differenziert dargestellt. Falls abweichende Stichprobengrößen angegeben werden, geben diese die Anzahl der Studierenden an, die das jeweilige Item beantwortet haben. Die höhere Fallzahl in Tabelle 2 ist auf die Erfassung von Mehrfachabschlüssen zurückzuführen. Anhand des *Mann-Whitney-U-Tests* wurde auf Unterschiede zwischen Männern und Frauen getestet.

Tabelle 2 gibt einen Überblick über die Zusammensetzung unserer Stichprobe nach Studiengang und Abschlussjahr.

Die zahlenmäßig stärkste Gruppe stellen demnach Absolventinnen und Absolventen der Wirtschaftsinformatik dar. Bei der Betrachtung der Arbeitsbereiche, in denen die Befragten tätig sind (vgl. Tabelle 3), zeigt sich, dass annähernd gleich viele Personen in der Softwareentwicklung wie auch in der Beratung tätig sind. Damit unterscheiden sich unsere Befragten von Absolventinnen und Absolventen eigenständiger Informatikstudiengänge, die zumeist im Bereich der Softwareentwicklung beschäftigt sind [17].

Arbeitsbereich (aktuelle Stelle)	Geschlecht		Total
	Männer	Frauen	
Softwareentwicklung	47	86	55
Beratung, Systemeinrichtung	59	6	65
Schulen	8	0	8
Universität, Hochschule	17	2	19
Forschungseinrichtungen	5	2	7
Sonstiges	24	3	27
Total	160	21	181

Tabelle 3: Arbeitsbereich der Befragten nach Geschlecht, Datenquelle: Projekt Alumnae Tracking Ehemaligenbefragung, eigene Darstellung

Ergebnisse

Führungsposition und familiärer Status

Die deskriptive Analyse der Daten zeigt auf, dass 51,47 % der ehemaligen Studierenden in einer leitenden Position tätig sind (96 Männer und 9 Frauen). Das bedeutet, dass 53,6 % der befragten Männer und 36 % der befragten Frauen eine Führungsposition innehaben. Allerdings sind Frauen nur in Positionen anzutreffen, in denen ihnen im Vergleich zu männlichen Führungskräften weniger Mitarbeiter unterstehen (vgl. Tabelle 4).

Studiengang	Abschlussjahr													Anzahl gesamt
	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	
Dipl.-Wirtschaftsinformatik	1	1		12	10	16	20	15	21	6	10	3	4	119
BA-Wirtschaftsinformatik											3	4	4	11
MA-Wirtschaftsinformatik						2	2	2	3	7	7	8	8	39
BA.-Angewandte Informatik										1	2	4	2	9
MA-Angewandte Informatik								1	2		4	2	2	11
Dipl-Wirtschaftspädagogik mit Schwerpunkt WI				1			2	1	2	5	1	2		14
MA-Wirtschaftspädagogik mit Schwerpunkt WI							1		2		1	1	2	7
														210

Tabelle 2: Aufteilung der Teilnehmer nach Studiengang und Abschlussjahr, Datenquelle: Projekt Alumnae Tracking Ehemaligenbefragung, eigene Darstellung

Anzahl unterstellter Mitarbeiter	Geschlecht		Total
	Männer	Frauen	
Unter 10	77	6	83
10 bis unter 50	13	3	16
50 bis unter 200	4	0	4
200 bis unter 500	2	0	2
Über 500	0	0	0
Total	96	9	105

Tabelle 4: Führungsposition nach Geschlecht und Anzahl der unterstellten Mitarbeiter, Datenquelle: Projekt Alumnae Tracking Ehemaligenbefragung, eigene Darstellung

Diese Befunde stehen in Einklang mit den Ergebnissen des Führungskräftemonitors und des Branchenmonitors von Hoppenstedt, demzufolge weniger Frauen als Männer in der IT-Branche eine leitende Position einnehmen [12] und Frauen im Vergleich zu Männern nur Führungsverantwortung für eine kleinere Mitarbeiterzahl übernehmen [11].

Bei den befragten Frauen in leitenden Positionen handelt es sich keineswegs um kinderlose Karrierefrauen oder Frauen mit bereits volljährigen Kindern: 44,4 % dieser Frauen (4 von 9 Frauen) haben mindestens ein minderjähriges Kind. Der Anteil von Vätern in Führungspositionen entspricht demgegenüber 30,2 % (29 von 75 Männern).

Fähigkeiten und Fertigkeiten

Im nächsten Schritt sind wir der Frage nachgegangen, ob der geringere Anteil von Frauen in Führungspositionen auf unterschiedliche Fähigkeiten und Fertigkeiten von Männern und Frauen zurückzuführen ist. Hierzu wurde zusätzlich zur subjektiven Einschätzung der fachlichen Kompetenz durch die Befragten die Studiumsabschlussnote als objektives Kriterium betrachtet.

Aus der Datenanalyse der Absolventen- und Absolventinnenbefragung geht hervor, dass die Studiumsabschlussnote im Mittel (vgl. Abbildung 3) bei Männern und Frauen bis auf die zweite Kommazahl identisch ist (weiblich 1.88; männlich 1.82; U = -0.795; p = 0.42). Allerdings unterscheidet sich die Notenverteilung zwischen Männern und Frauen (vgl. Abbildung 2). Während männliche Absolventen überwiegend mit der Note 1 oder 2 abschließen, haben zwar etwas mehr Frauen als Männer eine 1 als Abschlussnote, aber ein Viertel der Frauen schließt das Studium mit der Note 3 ab.

Bei der subjektiven Einschätzung auf einer 5-stufigen Likert-Skala (1: in sehr geringem Maße; 5: in sehr hohem Maße) zum vorhandenen speziellen Fachwissen (weiblich 3.52; männlich 3.49; U = -0.043; p = 0.97) und Grundlagenwissen nach Abschluss des Studiums (entnommen aus [10]) schätzen sich die Frauen sogar besser ein (weiblich 4.12; männlich 3.95; U = -1.367; p = 0.17).

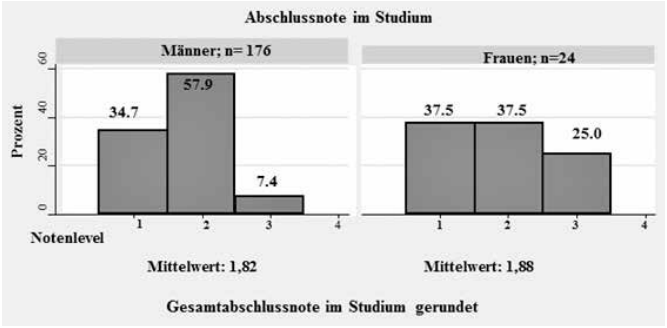


Abbildung 2: Studiumabschlussnote, Datenquelle: Projekt Alumnae Tracking Ehemaligenbefragung, eigene Darstellung

Einen deutlicheren Unterschied gibt es hingegen bei der Einschätzung von Führungsmerkmalen (entnommen aus [19]). Frauen schätzen auf einer 5-stufigen Likert-Skala (1: in sehr geringem Maße; 5: in sehr hohem Maße) ihre Führungskompetenzen durchweg höher ein als Männer.

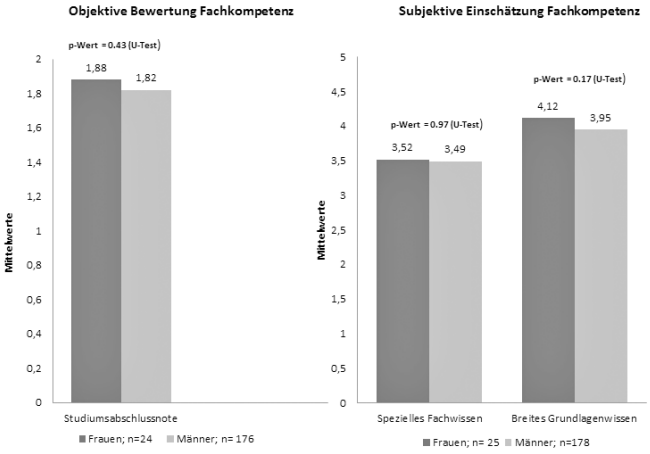


Abbildung 3: Objektive und subjektive Fachkompetenz, Datenquelle: Projekt Alumnae Tracking Ehemaligenbefragung, eigene Darstellung

Die deutlichsten Unterschiede zeigen sich in der Einschätzung der Organisationsfähigkeit (weiblich 4.24, männlich 3.67, U = -2.74, p < 0.01), der Verantwortungsfähigkeit (weiblich 4.08, männlich 3.62, U = -2.17, p = 0.03), der Fähigkeit, Konflikte zu lösen bzw. zu vermeiden (weiblich 3.28, männlich 2.88, U = -2.04, p = 0.04) und der Kommunikationsfähigkeit (weiblich 3.76, männlich 3.4, U = -1.75, p = 0.08).

Aus den Befunden lässt sich schließen, dass sich ehemalige Informatikstudierende objektiv in ihrer fachlichen Kompetenz bezüglich Geschlecht kaum unterscheiden. In der subjektiven Einschätzung des Fach- und Grundlagenwissens und in speziellen Führungscharakteristiken scheinen die Absolventinnen sogar einen Vorteil gegenüber den Absolventen zu haben. Dennoch nimmt auch unter den befragten Informatikerinnen nur ein kleiner Anteil eine Führungsposition ein. Deswegen wird der Frage nachgegangen, inwieweit seitens der Frauen überhaupt ein Interesse an einer Führungsaufgabe zu verzeichnen ist. Hierzu wurden die Befragten gebeten, die Wichtigkeit unterschiedlicher Lebens- und Arbeitsziele auf einer 5-stufigen Likert-Skala (1: gar nicht wichtig; 5: sehr wichtig) einzuschätzen. Nachfolgend werden die Antworten hierzu auf Geschlechterunterschiede hin untersucht.

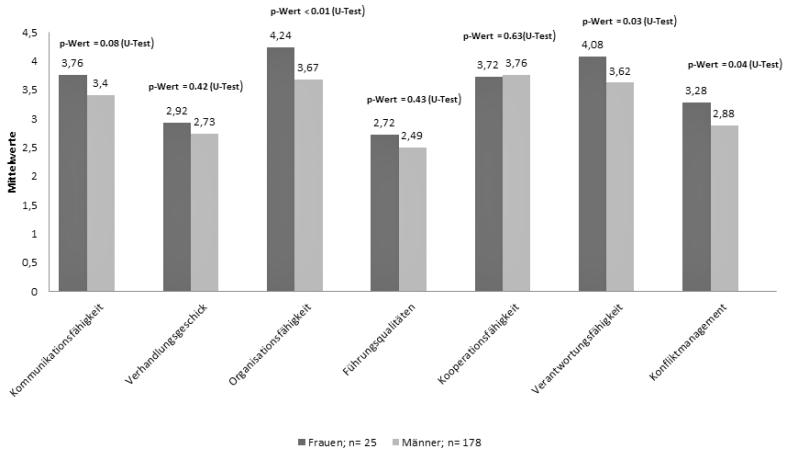


Abbildung 4: Subjektive Einschätzung der Führungskompetenzen, Datenquelle: Projekt Alumnae Tracking Ehemaligenbefragung, eigene Darstellung

einem Mittelwert von 3.16 von den Frauen immerhin als mäßig wichtig eingestuft.

Um Aufschlüsse zu erhalten, welche Gründe aus Sicht der Befragten am ehesten zu einer Unterrepräsentanz von Frauen in führenden Positionen führen, wurden die Befragten gebeten, vermeintliche Karrierehindernisse (entnommen aus [14]) auf einer 5-stufigen Likert-Skala (1: trifft gar nicht zu; 5: trifft stark zu) auf ihr Zutreffen einzuschätzen.

Als bedeutendste Gründe für den geringen Anteil von Frauen in Führungspositionen erachten die befragten Frauen die eher aufgabenorientierte, statt aufstiegsorientierte weibliche Arbeitsweise (MW = 4.0) sowie Vereinbarkeitsprobleme von Familie und Beruf (MW = 3.92).

Lebens- und Arbeitsziele

Informatikabsolventinnen legen größten Wert darauf, Beruf und Familie zu vereinbaren (MW = 4.8), das Leben zu genießen (MW = 4.75) und gute Arbeitsbedingungen (MW = 4.54) zu haben. Sie möchten sich der Familie widmen können (MW = 4.48), ohne dabei beruflich zurückstecken zu müssen. Anerkennung für ihre Leistungen zu erhalten (MW = 4.44), wiegt für die weiblichen Befragungsteilnehmer in der Bedeutung sogar noch etwas höher, als sich mit interessanten Tätigkeitsinhalten zu befassen (MW = 4.4) und einen sicheren Arbeitsplatz zu haben (MW = 4.32). Demgegenüber spielen der Verdienst (MW = 3.68) und das Erreichen einer Führungsposition (MW = 3.16) nur eine nachrangige Bedeutung.

Männliche Befragungsteilnehmer möchten in erster Linie einer interessanten Tätigkeit nachgehen (MW = 4.47) und ebenso wie Frauen das Leben genießen (MW = 4.4). Allerdings messen sie dem zweitgenannten Ziel signifikant weniger Bedeutung zu als Frauen (weiblich 4.75, männlich 4.4, U = -2.38, p = 0.02). Sie legen großen Wert auf eine Vereinbarkeit von Familie und Beruf (MW = 4.4), gute Arbeitsbedingungen (MW = 4.38), berufliche Anerkennung (MW = 4.21) und Arbeitsplatzsicherheit (MW = 3.94). Ebenso wie bei den weiblichen Befragten sind Verdienst (MW = 3.77) und Führungsposition (MW = 3.53) nur von nachrangiger Bedeutung, wenngleich das Erreichen einer Führungsposition den männlichen Absolventen deutlich wichtiger ist als den befragten Frauen (weiblich 3.16, männlich 3.53, U = 1.67, p = 0.09).

Hinderliche Faktoren für die Karriereentwicklung

Wie aus der vorangegangenen Analyse hervorgeht, stellt das Erreichen einer Führungsposition für die weiblichen Informatikabsolventinnen kein vorrangiges Lebens- und Arbeitsziel dar. Dennoch wird dieses Ziel mit

Entsprechend geben bei der Frage, welche Probleme im Berufsleben auftreten bzw. bereits einmal auftraten, auch 66,7 % der Frauen mit Kindern an, dass ihr beruflicher Alltag durch die Vereinbarkeit von Familie/Partnerschaft und Beruf geprägt ist bzw. war. Dies trifft sowohl auf Frauen zu, die aktuell eine Führungspositionen bekleiden, als auch auf Frauen ohne Personalverantwortung. Bei Männern geben 45,8 % der Väter, die sich in einer Führungsposition befinden, und 50 % der Väter ohne Personalverantwortung Vereinbarkeitsprobleme an.

Die weibliche Arbeitsweise hingegen, die sich durch eine stärkere Aufgabenorientierung anstelle einer Aufstiegsorientierung auszeichnet, wird von den befragten Männern insgesamt (MW = 2.8) und auch von denen, die selbst eine leitende Position innehaben (MW = 2.84) und damit Personalentscheidungen zu treffen haben, nicht als Karrierehindernis für Frauen angesehen.

Eine mittelstarke Bedeutung für den geringen Anteil weiblicher Führungskräfte in der Informatik messen Frauen weiterhin der

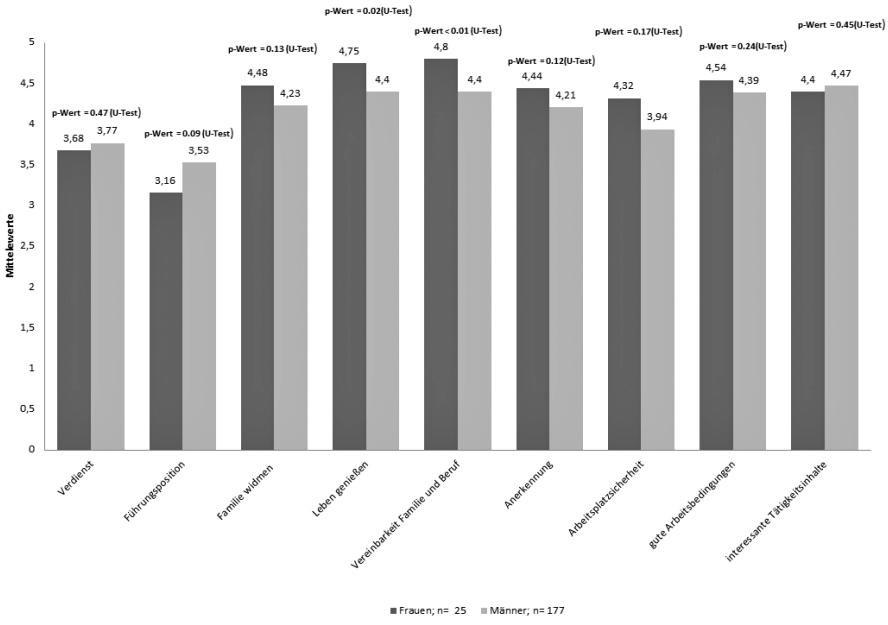


Abbildung 5: Bedeutung verschiedener Lebens- und Arbeitsziele, Datenquelle: Projekt Alumnae Tracking Ehemaligenbefragung, eigene Darstellung

Wahl weniger prestigeträchtiger Arbeitsfelder (MW = 3.4) zu, einer geringeren Förderung durch männliche Führungskräfte (MW = 3.32), fehlenden weiblichen Rollenbildern (MW = 3.28), einer Bevorzugung von Männern bei der Stellenbesetzung trotz gleicher Qualifikation der Frau (MW = 3.17) sowie einer geringeren Anerkennung der Leistungen (MW = 3.17). Eine eher untergeordnete Rolle spielt aus ihrer Sicht der Grund, dass Frauen aufgrund einer männlich geprägten Unternehmenskultur im Bereich der Informatik auf eine Karriere verzichten (MW = 2.76). Aus der Gegenüberstellung der Einschätzungen, inwieweit die angeführten Gründe zu einer Unterrepräsentanz von Frauen in führenden Positionen führen, ist jedoch ersichtlich, dass durchwegs allen Gründen seitens der Männer eine zumeist signifikant geringere Bedeutung beigemessen wird (Aufgabenorientiertes Arbeiten: weiblich 4.0, männlich 2.8, $U = -5.00$, $p < 0.00$; Probleme bei der Vereinbarkeit von Familie und Beruf: weiblich 3.92, männlich 3.36, $U = -2.2$, $p = 0.03$; Wahl weniger prestigeträchtiger Arbeitsfelder: weiblich 3.4, männlich 2.55, $U = -3.35$, $p < 0.01$; geringere Förderung durch männliche Führungskräfte: weiblich 3.32, männlich 2.44, $U = -3.35$, $p < 0.01$; Benachteiligung von Frauen bei der Stellenbesetzung: weiblich 3.17, männlich 2.36, $U = -2.90$, $p < 0.01$; geringere Anerkennung für Leistungen: weiblich 3.17, männlich 2.33, $U = -3.21$, $p < 0.01$). Diese Unterschiede in der Wahrnehmung könnten ein weiterer Grund dafür sein, dass sich das berufliche Vorankommen von Frauen in einer männlich konnotierten Arbeitswelt nach wie vor schwierig gestaltet.

Diskussion

Der Anteil von Informatikerinnen in Führungspositionen unter den Befragungsteilnehmern ist in Übereinstimmung mit anderen Untersuchungen ([5, 12]) vergleichsweise niedrig.

Die Ergebnisse unserer Befragung legen nahe, dass sich die Arbeits- und Lebensziele von Informatikerinnen und Informatikern unterscheiden. Informatikerinnen streben deutlich seltener als ihre männlichen Kollegen eine Führungskarriere an. Hingegen möchten sie in deutlich stärkerem Umfang ihr Leben genießen sowie Beruf und Familie miteinander vereinbaren können. Allerdings zeigen die Ergebnisse ebenfalls, dass Informatikerinnen im Beruf eher Probleme haben, die Vereinbarkeit mit der Familie zu realisieren als ihre Kollegen. Dies könnte auf die für den Informatikbereich charakteristische Projekttätigkeit mit hohem Termindruck zurückzuführen sein. Trotz vielfach gegebener flexibler Arbeitsmöglichkeiten machen erforderliche Überstunden im Projektgeschäft die Vereinbarkeit von Familie und Beruf oftmals schwierig [8]. Um das Vereinbarkeitsproblem von Familie und Beruf lösen zu können, muss sich auf gesellschaftlicher Ebene die Vorstellung von der Rolle als Frau innerhalb der Gesellschaft ändern [20]. So lautet das Ergebnis einer Studie, die Wippermann im Auftrag des Sinus-Instituts durchführte. In einer repräsentativen Befragung von Führungskräften privatwirtschaftlicher Unternehmen untersuchte er deren Einstellungen a) zu Frauen in Führungpositionen sowie b) zu politischen Maßnahmen für eine gleichberechtigte Teilhabe von Frauen und Männern an Führungspositionen. Bei einer Frau in Führungsposition wird klischeeartig davon ausgegangen, dass sie nicht genügend Zeit hat, Kinder zu erziehen und den Haushalt zu organisieren. Dagegen wird bei einem Mann in Führungsposition der Background einer intakten Familie mit Kindern als karriereförderlich angesehen. Um hier ein Umdenken zu erreichen, muss die Botschaft folgendermaßen lauten: Familie und Führungsposition sind im Unternehmen für Frauen vereinbar. Die Vereinbarkeit von Beruf und Familie ist auch eine Aufgabe für Männer in Führungspositionen [20]. Damit Frauen bereit sind, in die Führungsetage aufzusteigen, ist es außerdem erforderlich, dass Frauen nicht gezwungen werden, sich wie Männer zu verhalten und sich entsprechend zu

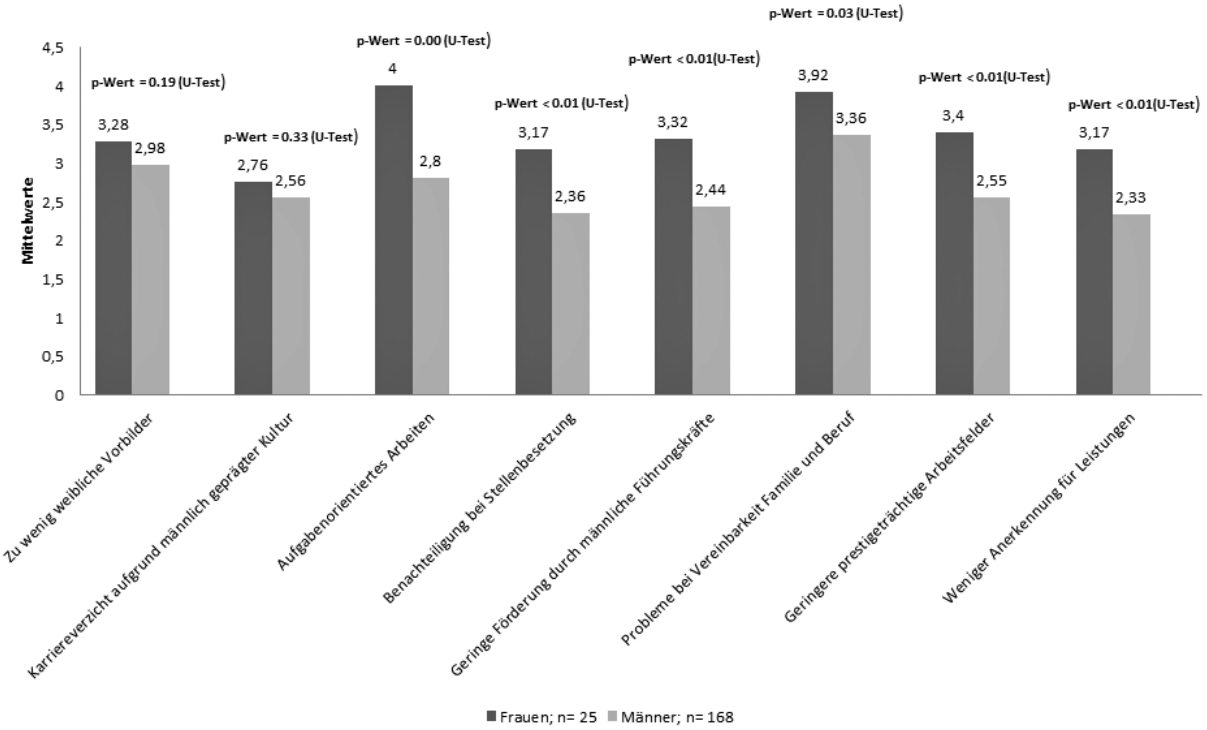


Abbildung 6: Gründe für die weibliche Unterrepräsentanz in Führungspositionen, Datenquelle: Projekt Alumnae Tracking Ehemaligenbefragung, eigene Darstellung

kleiden. Es sollte akzeptiert werden, dass Frauen Aufgaben anders angehen und einen anderen Führungsstil zeigen [18].

Seit Langem wird auf politischer Ebene und auf Ebene der Unternehmen über Maßnahmen diskutiert, die die Situation optimieren sollen. Im MINT-Bereich wird unterstellt, dass aufgrund der stark männlich geprägten Arbeitswelt das berufliche Vorankommen für Frauen erschwert ist [2, 8]. Die Bedürfnisse und Ansprüche der Frauen werden von den Unternehmen bislang nur unzureichend wahrgenommen. Dies zeigen auch unsere Ergebnisse. So schreiben die befragten Männer in unserer Studie den möglichen Gründen für die weibliche Unterrepräsentanz in Führungspositionen durchwegs geringere Bedeutung zu als die befragten Frauen.

Erst wenn es gelingt, Hemmnisse abzubauen, und dadurch mehr Frauen gewillt sind, Führungspositionen anzustreben, und ihr Ziel auch erreichen, wird sich die Chefetage und damit die gesamte Unternehmenskultur ändern. Der Umbruch von einem männlich konnotierten Führungsstil zu einer Diversity-orientierten Personalentwicklung vollzieht sich in den Unternehmen nur langsam. Dazu braucht es gezielte Fördermaßnahmen, die den Bedürfnissen der Frauen gerecht werden.

Danksagung

Wir danken den Studentinnen Bettina Finzel, Susanne Gall, Elke Heidel und Verena Pfeiffer sehr herzlich für ihre Unterstützung bei der Dateneingabe und Datenaufbereitung. Diese Arbeit entstand im Rahmen des Projekts *Alumnae Tracking*, gefördert durch ESF und den Freistaat Bayern.

Referenzen

[1] Abele, A.: Ein Modell und empirische Befunde zur Laufbahnentwicklung unter besonderer Berücksichtigung des Geschlechtsvergleichs. In: Psychologische Rundschau 53, S. 109–18 (2002).

[2] Ahuja, A.: Women in the information technology profession: a literature review, synthesis and research agenda. In: European Journal of Information Systems 11, S. 20–34 (2002).

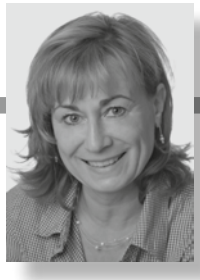
[3] Allmendinger, J.; Haarbrücker, J.: Lebensentwürfe heute. Wie junge Frauen und Männer in Deutschland leben wollen. Kommentierte Ergebnisse der Befragung 2012. Berlin 2013.

[4] Bain, O.; Cummings, W.: Academe`s Glass Ceiling: Societal, Professional/Organizational, and Institutional Barriers to the Career Advancement of Academic Women. In: Comparative Education Review 44, S. 493–514 (2000).

[5] Endres, H.: Karriere technisch unmöglich. URL: http://www.spiegel.de/karriere/berufsleben/studie-trotz-fachkraeftemangels-keine-chance-fuer-mint-frauen-a-914507.html. Abrufdatum 24.06.2014.

[6] Europäische Komission: Datenbank über die Mitwirkung von Frauen und Männern an Entscheidungsprozessen. URL: http://ec.europa.eu/justice/gender-equality/gender-decision-making/database/business-finance/executives-non-executives/index_de.htm. Abrufdatum 24.06.2014.

[7] Europäischer Sozialfonds, B.S.f.A.u.S.F.u.F.: Förderhinweise für Projekte zur Erhöhung des Anteils von Frauen in Führungspositionen und in zukunftsorientierten Berufen. Europäischer Sozialfonds 2007 – 2013. 2013.



Silvia Förtsch, Anja Gärtig-Daugs und Ute Schmid

Silvia Förtsch studierte Bildungswissenschaft (B.Sc.) an der Fern-Universität Hagen und Empirische Bildungsforschung (M.Sc.) an der Otto-Friedrich-Universität Bamberg. Seit 2011 ist sie wissenschaftliche Mitarbeiterin der Frauenbeauftragten der Fakultät WIAI, zunächst im Rahmen des Mentorinnenprogramms für Informatikstudentinnen und seit 2012 im ESF-Projekt Alumnae Tracking. Ihr Forschungsinteresse liegt im Bereich der längsschnittlichen Analyse von Bildungsverläufen, Lebensverlauf- und Genderforschung.

Anja Gärtig-Daugs studierte Gesundheitsökonomie (Dipl.) an der Universität Bayreuth und promovierte dort nebenberuflich zum Dr. rer. pol. Nach dem Studienabschluss arbeitete sie zunächst als Epidemiologin am bevölkerungsbezogenen Krebsregister Bayern sowie als Lehrbeauftragte an der Otto-Friedrich-Universität Bamberg. Seit 2012 ist sie wissenschaftliche Mitarbeiterin im ESF-Projekt Alumnae Tracking. Ihr Forschungsinteresse liegt im Bereich der Berufs- und Lebenszufriedenheit, Lebensverlaufs- und Genderforschung.

Dr. rer. nat. **Ute Schmid** ist Professorin für Angewandte Informatik, insb. Kognitive Systeme. Sie studierte Psychologie und Informatik an der EHW Landau sowie an der TU Berlin. 1994 wurde sie an der TU Berlin im Bereich Informatik promoviert, im Jahr 2002 folgte die Habilitation für das Fach Informatik. Ihr Forschungsinteresse liegt hauptsächlich in den Bereichen Intelligente Agenten, Machine Learning sowie Kognitive Modellierung. In ihrer Funktion als Frauenbeauftragte der Fakultät WIAI organisiert sie regelmäßig Workshops für Schülerinnen mit dem Ziel, den Anteil weiblicher Informatikstudentinnen zu steigern. Seit 2012 ist sie Leiterin des Forschungsprojekts Alumnae Tracking, das vom Europäischen Sozialfonds gefördert wird.

[8] Fisher, J.; Lang, C.; Craig, A.: Women in the IT workplace: learnings for managers. In: ECIS 2013 Proceedings, S. 1–12 (2013).
[9] Hans-Böckler-Stiftung: Gender: Acht Frauen mehr in DAX-Vorständen, 2. Auflage. Düsseldorf 2013.
[10] Hochschul-Informations-System GmbH: Hochqualifiziert und auf dem Weg. Eine Befragung von Masterabsolventinnen und Masterabsolventen des Prüfungsjahrgangs 2008/2009. Hannover 2009.
[11] Holst, E.; Busch, A.; Kröger, L.: Führungskräfte-Monitor 2012. Update 2001 – 2010. Berlin 2012.
[12] Hoppenstedt: Branchenmonitor "Frauen in der IT-Branche". Frauenmangel in den Chefetagen der IT-Branche. Darmstadt 2012.
[13] Kompetenzzentrum Technik – Diversity – Chancengleichheit e.V.: Studienanfängerinnen und Studienanfänger der Fächergruppe Mathematik, Naturwissenschaften im Studienjahr 2012. URL: http://www.kompetenzz.de/Daten-Fakten/Studium#astudienanfaengerinnen_und_studienanfaenger_1_der_faechergruppe_mathematik_naturwissenschaften_im_studienjahr_2012_2. Abrufdatum 24.06.2014.
[14] Langfeldt, B.; Mischau, A.: Itembatterie zum Projekt "Geschlechterdisparitäten in Berufs- und Karriereverläufen von MathematikerInnen und PhysikerInnen innerhalb und außerhalb klassischer Beschäftigungsmodelle", e-Mail (2012). Hamburg/Bielefeld.
[15] Mischau, A.; Langfeldt, B.; Griffiths, K.; Reith, F.: Geschlechterdisparitäten in Berufs- und Karriereverläufen von MathematikerInnen und PhysikerInnen. Neues Forschungsprojekt am IFF. In: IFFOnZeit 2, S. 67–75 (2012).
[16] Neumann, V.: Nicht nur gute Noten sind entscheidend. Soft Skills für den Aufstieg. URL: http://www.access.de/karriereplanung/karriere-blog/soft-skills-fuehrungskraefte-8576. Abrufdatum 24.06.2014.
[17] plus Media GmbH: Nach dem Studium (Informatik). URL: http://www.studieren-studium.com/studium/Informatik. Abrufdatum 30.06.2014.
[18] Rohwetter, M.: Internet: "Es beschützt uns". Das Internet von morgen werde die Menschen vor Fehlern bewahren, sagt Padmasree Warrior. Die Topmanagerin des US-Technologiekonzerns Cisco spricht über Netzwerke, digitale Enthaltsamkeit und Frauen im Silicon Valley. 2013.
[19] Schaeper, H. K.: Kompetenzen von Hochschulabsolventinnen und Hochschulabsolventen, berufliche Anforderungen und Folgerungen für die Hochschulreform. HIS-Projektbericht. Hannover 2004.
[20] Wippermann, C.: Frauen in Führungspositionen. Barrieren und Brücken. Mehr Frauen – mehr Vielfalt in Führungspositonen. 2010.

Stefanie Nordmann

Eine neue Zielgruppe für die Informatik

An der Hochschule für Technik und Wirtschaft Berlin existiert seit dem Wintersemester 2009/10 ein Studiengang, der sich ausschließlich an Frauen richtet. Es handelt sich um den sechssemestrigen Bachelorstudiengang Informatik und Wirtschaft*. Der Studiengang wurde unter anderem eingerichtet, um mehr Frauen für ein Studium im MINT[1]-Bereich im Allgemeinen und in der Informatik im Speziellen zu gewinnen. Dass und wie dieses Ziel erreicht wird, werde ich im Folgenden aufzeigen.*

1 Einleitung

Als im Wintersemester 2009/10 an der Hochschule für Technik und Wirtschaft (HTW) Berlin der Studiengang *Informatik und Wirtschaft für Frauen* (FIW) erfolgreich mit 40 Studentinnen beginnen konnte, war ein erstes Etappenziel erreicht. Für den Studiengang hatten sich mehr als doppelt so viele Frauen beworben, als Plätze vorhanden waren, und somit sind die Werbemaßnahmen für den Studiengang als positiv und erfolgreich zu bewerten.

Einen monoedukativen Studiengang zu konzeptionieren und zu bewerben, stellt eine besondere Herausforderung dar, da es schwierig ist, einzuschätzen, wen das Studienangebot anspricht, welche Studieninhalte und -formate von der potenziellen Zielgruppe am ehesten angenommen werden und wie Werbung für diese unbekannte Personengruppe am ansprechendsten aussieht. So gibt es zu Beginn ziemlich viele Unbekannte, Vermutungen, Mutmaßungen und Annahmen[2] – doch im Fall des monoedukativen Studienangebots an der HTW Berlin auch den Rückgriff auf Erfahrungen anderer. So wurden die erfolgreichen *Women´s Colleges* aus Amerika als Inspirationsquelle genutzt, und auch der monoedukative Informatikstudiengang in Bremen[3] diente als Vorbild.

Im Folgenden soll dargestellt werden, wie der Studiengang *Informatik und Wirtschaft* in Berlin beworben wurde und welche Besonderheiten er aufweist, um daran anschließend aufzuzeigen, welche Frauen dieses monoedukative Angebot anspricht. Es wird dargestellt werden, dass eine neue Zielgruppe von Frauen in diesem Informatikstudiengang immatrikuliert wird und somit die Anzahl der Frauen, die Informatik studieren, erhöht werden konnte.

2 Werbung und Öffentlichkeitsarbeit

Um Frauen für die Informatik zu gewinnen, wurde in der Konzeptionsphase des Studiengangs bereits darüber nachgedacht, welche Bedürfnisse und Wünsche Frauen aufgrund ihrer Sozialisation haben könnten und auf welche gesellschaftlichen Gegebenheiten sie im späteren Berufsleben treffen.[4] Aufgrund bestimmter gesellschaftlicher Rahmenbedingungen (z. B. die nach wie vor stärkere Zuschreibung von Reproduktionsarbeit an Frauen) wurden die folgenden drei Werbeslogans[5] entwickelt[6]:

1. Informatik von Null an: Da viele Frauen ihr Wissen und ihre Fähigkeiten im Bereich Informatik manchmal unterschätzen und ihr Selbstbewusstsein in Bezug auf dieses Thema durch Vergleich mit „den Männern"[7] nicht so groß ist, wird darauf Bezug genommen, indem deutlich gemacht wird, dass keine IT-Vorkenntnisse notwendig sind. In der Regel startet zwar jeder (Informatik-)Studiengang bei Null und bringt alle Studierenden auf einen vergleichbaren Wissensstand. Jedoch scheint den Frauen das im Kontext dieses monoedukativen Studiengangs glaubwürdiger.

2. Mütter willkommen: Da Frauen – wie oben schon angesprochen – in unserer Gesellschaft immer noch mehrheitlich für die Reproduktionsarbeiten verantwortlich gemacht werden und sich zum Teil auch selbst so sehen, wird mit diesem Werbeslogan deutlich gemacht, dass Frauen mit familiären Verpflichtungen willkommen sind und ihnen die Vereinbarkeit von Studium, Familie (und Beruf) ermöglicht wird. In der Umsetzung sieht das so aus, dass der Studiengang familienfreundliche Studienzeiten in der Zeit von 9-16 Uhr anbietet.

3. Fragen erwünscht: Mit diesem Werbespruch wird darauf aufmerksam gemacht, dass Kommunikation wichtiger Bestandteil der Informatik ist und Fragen zu stellen erwünscht ist, zumal innerhalb der Informatik oft viele Abkürzungen und eine besondere Neigung zur Fachsprache (technisches Vokabular) vorherrschen. Deshalb werden die Studentinnen ermutigt, so oft wie möglich Fragen zu stellen.

3 Das Curriculum und die Besonderheiten des Studiengangs

Das Curriculum des monoedukativen Studiengangs ist dem der koedukativen Informatikstudiengänge sehr ähnlich[8], jedoch wird das Studium anders organisiert[9]. Die Frauen des monoedukativen Studiengangs sind am Ende ihres Studiums genauso gut ausgebildet wie die Männer und Frauen, die sich für einen koedukativen Studiengang entschieden haben. Dies zeigt sich unter anderem daran, dass viele der FIW-Studentinnen nach ihrem Bachelorabschluss in den koedukativen Informatik-Masterstudiengängen ihr Studium fortführen können und sich dort erfolgreich bewähren.

Veronika Oechtering (1998) hat sieben zentrale Ansatzpunkte[10] herausgearbeitet, die berücksichtigt werden sollten, um das Interesse von Frauen in einzelnen Studienphasen in technischen Studiengängen zu steigern. Auf zwei davon, die unter anderen[11] auch im Studiengang FIW umgesetzt werden, möchte ich im Folgenden genauer eingehen:

1. Neukonzeption von Lehrveranstaltungen: Im ersten Semester werden alle Frauen auf den gleichen Wissensstand gebracht. Um den Studentinnen die Ehrfurcht vor dem Rechner zu nehmen, startet die Lehrveranstaltung Rechnerarchitektur/Betriebssysteme damit, Computer auseinander- und wieder funktionstüchtig zusammenzubauen. Dabei sehen einige Frauen zum ersten Mal in ihrem Leben eine Festplatte, das Mainboard oder die CPU – das Herzstück eines Rechners.

2. Vom ersten Semester an finden neben den regulären wöchentlich stattfindenden Kursen auch Blockkurse in den Semesterferien (z. B. Hackathon) statt, Präsenzveranstaltungen werden durch E-Learning-Angebote ergänzt und neben normalen, eher frontal angelegten, Lehrveranstaltungen finden auch innovative andere Formen der Lehrvermittlung, wie z. B. Projektarbeit (s. unten), Gruppenarbeit, Exkursionen und Lernteamcoaching statt.[12] Um diese Angebote bestmöglich umsetzen zu können, bilden sich die ProfessorInnen des Studiengangs regelmäßig weiter, achten bei der Besetzung von DozentInnen auf deren Lehrkompetenz und beraten diese auch vor, während und nach dem Semester.

3. Praxisintegration ins Studium: In vielen Studiengängen gibt es mittlerweile Projektveranstaltungen, um den Studierenden ein praxisnäheres Studium anbieten zu können. Das Besondere am FIW ist jedoch, dass die Kontakte mit der Wirtschaft zweimal im Verlauf des Studiums geknüpft werden und beim ersten Kontakt, der im 3. Semester stattfindet, die Studentinnen auch sehr frühzeitig mit echten Arbeitgebern ein umfangreiches Projekt bearbeiten. Dabei arbeiten Frauen aus dem 3. und 5. Semester in gemischten Teams zusammen. Für die Frauen aus dem 5. Semester bietet die Zusammenarbeit den Vorteil, dass sie ihr Wissen über (Miss-)Erfolge aus der Erfahrung in ihrem ersten Projekt mit einbringen und reflektieren können. Die Studentinnen des 3. Semesters können sich an den höhersemestrigen Frauen orientieren, die ihnen Halt bieten und mit denen sie sich identifizieren können.

4. Im 4. Semester absolvieren die Studentinnen ihr Praktikum, was ebenfalls als sehr frühzeitig im Studienverlauf angesehen werden kann. Durch das vorhergehende Projekt im 3. Semester können einige Frauen direkt in dem Unternehmen ihr Praktikum absolvieren, für das sie im Projekt gearbeitet haben.

5. Im sechsten und damit letzten Bachelorsemester schreiben die Studentinnen ihre Bachelorarbeit. Durch das vorgeschaltete Projekt im 5. Semester kommt es auch in diesem Fall gelegentlich dazu, dass die Frauen ihre Bachelorarbeit bei dem Unternehmen schreiben, bei dem sie ihr Projekt absolviert haben.[13]

6. Diese Ineinanderverzahntheit ist auch für die Arbeitgeber sehr attraktiv, da sie die Möglichkeit haben, ein echtes Projekt bearbeiten zu lassen und währenddessen die Studentinnen und ihre Fähigkeiten näher kennenlernen können und einschätzen lernen. Wenn eine Studentin sich als geeignet

Stefanie Nordmann

Stefanie Nordmann, M.A., hat Gender Studies und Germanistische Linguistik an der Humboldt-Universität zu Berlin studiert und promoviert derzeit an der TU Berlin zu dem Thema Motivation von Frauen für ein Informatikstudium. Dabei untersucht sie, ob es Unterschiede zwischen den Frauen gibt, die Informatik koedukativ und denen, die Informatik monoedukativ studieren.
Kontakt: *Stefanie.nordmann@campus.tu-berlin.de*

erweist, kann sie frühzeitig im Studienverlauf in das Unternehmen eingeführt werden und dort möglicherweise ihren Berufseinstieg vollziehen, was in Zeiten des Fachkräftemangels für die Unternehmen sehr vorteilhaft ist.

Über die zentralen Ansatzpunkte von Oechtering hinaus möchte ich noch einen wichtigen Punkt ansprechen: Eine weitere Besonderheit des Studiengangs ist, dass derzeit zwei *Professorinnen* und ein Professor für den Studiengang verantwortlich sind und in diesem lehren, so dass die Studentinnen auch hier Informatikerinnen als Rollenvorbilder erleben. Die drei ProfessorInnen werden in ihrer Lehre durch ProfessorInnen anderer Studiengänge der HTW Berlin und durch Lehrbeauftragte unterstützt, wobei sehr häufig Frauen anzutreffen sind.

Wegen all dieser Besonderheiten, die der Studiengang an der HTW bietet, wurde die Hochschule mit dem Preis *Digital Impact Organisation of the Year 2013* ausgezeichnet

4 Die Studentinnen

Bisher konnte gezeigt werden, welche Werbemaßnahmen erfolgversprechend sind, um Frauen für dieses Studienangebot zu begeistern, und welche Besonderheiten der Studiengang aufweist.

Im Folgenden soll dargestellt werden, welche Frauen sich von dem Angebot angesprochen fühlen und sich bewerben bzw. welche Frauen dann auch immatrikuliert werden. In jedem Wintersemester sind 40 Plätze zu vergeben und seit der Studiengang existiert, haben sich jedes Jahr mehr als doppelt so viele Frauen beworben, wie es Plätze gibt. Im Wintersemester 2013/14 wurden die neu immatrikulierten Frauen mithilfe eines Fragebogens befragt und es konnte eine Vollerhebung durchgeführt werden. Alle 41 Frauen haben ihren Bogen beantwortet und an die Untersuchungsleiterin zurückgegeben.[14]

Besonders interessant ist, dass sich 15 der 41 Frauen ausschließlich auf den monoedukativen Studiengang Informatik und Wirtschaft beworben haben, und 10 Frauen haben sich neben diesem Studiengang auf fachlich nicht verwandte Studiengänge[16] beworben. 10 weitere haben sich auf verwandte Fächer[15] beworben und 6 Frauen haben sich sowohl auf verwandte als auch auf nicht verwandte Fächer beworben (Abbildung 1: Bewerbungen für Studiengänge, in absoluten Zahlen).

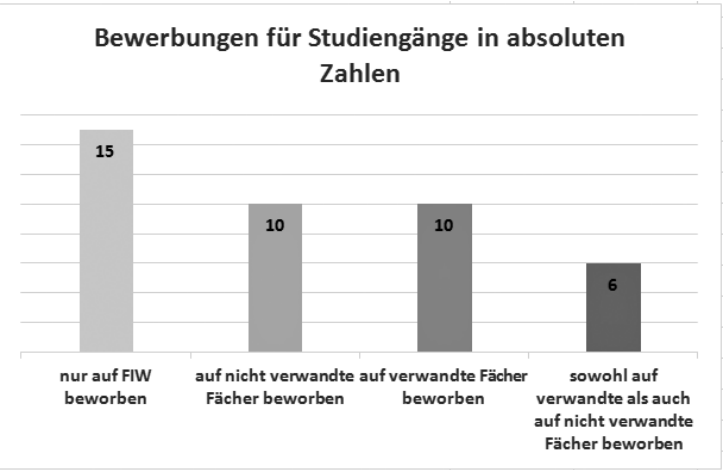


Abbildung 1: Bewerbungen für Studiengänge, in absoluten Zahlen

Dies legt den Schluss nahe, dass ohne das monoedukative Angebot mindestens 25 Frauen NICHT Informatik studiert hätten. Diejenigen, die sich ausschließlich auf FIW beworben haben, hätten mutmaßlich zu diesem Zeitpunkt kein Studium aufgenommen und diejenigen, die sich ausschließlich auf nicht verwandte Fächer beworben haben, hätten möglicherweise ein anderes Fach studiert. Interessant ist auch, dass die nicht mit Informatik und/oder Wirtschaft verwandten Alternativ-Studiengänge, auf die sich die Frauen beworben haben, dem geschlechtsspezifisch als weiblich konnotiertem Bereich angehören.

Außerdem gaben die Frauen, die neben FIW noch weitere Studiengangszusagen erhalten haben, mehrheitlich an, dass FIW ihre erste Wahl war. Ebenso wichtig erscheint mir aber auch, zu betonen, dass in den anderen Informatikstudiengängen der HTW Berlin[17] der Anteil der Studentinnen im 1. Fachsemester nicht abgenommen hat (Abbildung 2: Anzahl Studentinnen im 1. Fachsemester nach Studiengang). Somit wird deutlich, dass mit dem monoedukativen Studienangebot eine neue Zielgruppe erschlossen wird.

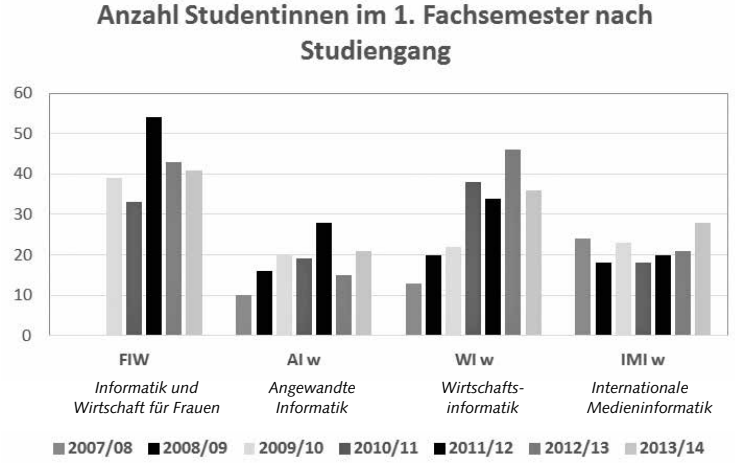


Abbildung 2: Anzahl Studentinnen im 1. Fachsemester nach Studiengang

5 Zusammenfassung und Ausblick

Es konnte gezeigt werden, welche Werbemaßnahmen auf eine bestimmte Gruppe von Frauen attraktiv wirken können und welche Besonderheiten der Studiengang aufweist, um Frauen zu gewinnen und zu halten.

Durch die im WS 2013/14 durchgeführte Fragebogenerhebung konnte festgestellt werden, dass eine nicht zu unterschätzende Anzahl von Frauen Informatik ohne das monoedukative Angebot zu diesem Zeitpunkt nicht studiert hätte und somit kann geschlussfolgert werden, dass eine neue Zielgruppe angesprochen wird. Dass in den koedukativen Informatikstudiengängen der HTW der Anteil an eingeschriebenen Frauen nicht gesunken ist, bestätigt, dass der Frauenanteil in der Informatik an der HTW Berlin erhöht werden konnte.

Um die Vorerfahrungen, Vorkenntnisse und die Motivation der Frauen noch genauer in Erfahrung bringen und auch miteinander vergleichen zu können, werde ich im Rahmen meiner Dissertation leitfadengestützte qualitative Interviews sowohl mit den Frauen aus dem monoedukativen als auch aus drei koedukativen Informatikstudiengängen an der HTW Berlin durchführen.

Untersucht werden soll in diesem Zusammenhang auch, ob sich durch die Einführung monoedukativer Studienangebote im MINT-Bereich der Frauenanteil in diesem männerdominierten Feld erhöhen lässt und welche Handlungsempfehlungen sich daraus ableiten lassen könnten.

Anmerkungen

1 MINT steht für Mathematik, Informatik, Naturwissenschaften und Technik.

2 So wurde auch im Laufe der Zeit das Konzept des Studiengangs überarbeitet, nachgebessert und angepasst. Beispielsweise wurde im WS 2009/10 der Kurs Programmierung als E-Learning-Angebot offeriert, um den Studentinnen das Lernen von zu Hause aus zu ermöglichen. Es stellte sich jedoch heraus, dass insbesondere dieser Kurs als E-Learning-Angebot nicht so günstig ist, da viele Fragen auftauchen und Übungen das Erlernte festigen müssen. So werden heute andere Fächer als E-Learning-Kurse angeboten, Programmierung jedoch als Präsenzveranstaltung.

3 Vgl.: Homepage des monoedukativen Studiengangs in Bremen: http://www.hs-bremen.de/internet/de/studium/stg/ifi/.

4 Es gibt Kompetenzen und Fähigkeiten, die in unserer Gesellschaft Frauen zu- und Männern abgeschrieben werden und umgekehrt. Entscheidend ist dabei nicht, ob die oder der Einzelne dann tatsächlich über diese Kompetenzen verfügt, „sondern daß diese Stereotype unser Bild und auch das der Personalverantwortlichen prägen." (Tischer 1998, S. 44).

5 Vgl.: Ripke, Marita/Nordmann (2010).

6 Siehe: Homepage des monoedukativen Studiengangs in Berlin: http://fiw.htw-berlin.de/

7 Ich setze „den Männern" in Anführungszeichen, um deutlich zu machen, dass es sich dabei nur um eine Verallgemeinerung handelt. In den Medien werden Informatiker mehrheitlich als Männer, gern dann auch als Nerds, dargestellt, was auf manche Frauen abschreckend wirkt. Und auch im schulischen Umfeld wirken die Jungen durch ihr selbstbewusstes Auftreten in Bezug auf den Computer kompetenter auf Mädchen, wodurch diese vermuten, dass die Jungen einen großen Wissensvorsprung haben, dem sie sich selbst nicht aussetzen wollen.

8 Das wird u. a. auch dadurch gewährleistet, dass die Studentinnen im monoedukativen Studiengang in vielen Kursen von den selben DozentInnen unterrichtet werden, wie die Studierenden in den koedukativen Studiengängen und dann auch die gleichen Klausuren schreiben.

9 Siehe die oben erwähnten familienfreundlichen Studienzeiten, aber auch die Lehrmethodenvielfalt ist größer sowie die Bestärkung der Frauen in ihrer Informatikkompetenz und in ihrem Selbstbewusstsein (Empowerment).

10 Dazu zählen „die Neugestaltung der Studienvorbereitungs- und Einführungsphase, der Erwerb oder die Auffrischung von Kenntnissen mathematischer, programmiertechnischer oder fachpraktischer Grundlagen, die Neukonzeption von Lehrveranstaltungen, der Erwerb von Berufsfähigkeiten, die Praxisintegration in das Studium, monoedukative Lehre sowie Weiterbildungsangebote für Frauen" (Oechtering 1998, S. 118).

11 1. Die Neugestaltung der Studienvorbereitungs- und Einführungsphase wurde bereits oben durch die Ansprache der potenziellen Studentinnen in der Öffentlichkeitsarbeit dargestellt. Darüber hinaus beteiligt sich die HTW Berlin am Girls Day, veranstaltet die Mädchen-machen-Technik-Tage und bietet ein Mentoringprogramm für Schülerinnen an. Auch wird den Studentinnen in der ersten Semesterwoche die Gelegenheit gegeben, sich gut kennenzulernen. 2. Der Erwerb oder das Auffrischen von Kenntnissen mathematischer, programmiertechnischer oder fachpraktischer Grundlagen wird in Studienvorbereitungskursen ermöglicht. 3. Der Erwerb von Berufsfähigkeiten wird im Rahmen des Studienangebots und darüber hinaus durch Weiterbildungsangebote des Career Service der HTW Berlin abgedeckt. 4. Monoedukative Lehre wird im Rahmen des gesamten Studiengangs angeboten. 5. Weiterbildungsangebote für Frauen werden ebenfalls vom Career Service angeboten.

12 Ausführlicher bei: Siegeris/Krefting (2014).

13 Durch die vielen Praxiskontakte im Studienverlauf wird den Studentinnen die Chance gegeben, viele Unternehmen ein Stück weit kennenzulernen und Einblicke zu erhalten. Dadurch bekommen die Studentinnen mit, was ihnen an ihrem potenziellen zukünftigen Arbeitgeber gefällt und was nicht.

14 Ich habe die Fragebogenerhebung im Rahmen meines Promotionsprojekts an der TU Berlin mit dem Titel „‚Eigentlich wollte ich was ganz anderes machen …' – Eine vergleichende Untersuchung der motivationalen Ausgangslage von IT-Studentinnen in monoedukativen und koedukativen Studiengängen" durchgeführt und bin dazu in eine Lehrveranstaltung gegangen, die in der ersten Semesterwoche stattfand. Nach ca. 20 Minuten Bearbeitungszeit habe ich die Fragebögen wieder eingesammelt.

15 Die gewählten Studiengänge sind folgenden Studienrichtungen zuzuordnen: Sozialwissenschaften, Medien und Kommunikation, Kulturen, Sprachen und Literatur, Recht, Naturwissenschaften, Lehramt, Medizin und Gesundheit, Ingenieurwissenschaften, Land- und Forstwirtschaft.

16 Dazu gehören u. a. Wirtschaftsinformatik, Medieninformatik, Verwaltungsinformatik, Betriebswirtschaftslehre, Public Management, Volkswirtschaftslehre, Wirtschaftswissenschaften.

17 AI = Angewandte Informatik, WI = Wirtschaftsinformatik, IMI = Internationale Medieninformatik.

Referenzen

Homepage des monoedukativen Studiengangs in Berlin: http://fiw.htw-berlin.de/, letzter Zugriff: Juli 2014

Homepage des monoedukativen Studiengangs in Bremen: http://www.hs-bremen.de/internet/de/studium/stg/ifi/, letzter Zugriff: Juli 2014

Ripke, Marita/Nordmann, Stefanie : Explizit und ausschließlich für Frauen – Informatik und Wirtschaft an der HTW Berlin.. In: Rundbrief, Gesellschaft für Informatik, 2010.

Oechtering, Veronika: Frauengerechte Hochschulausbildung in technischen Studiengängen. In: Oechtering, Veronika/Winker, Gabriele (Hrsg.): Computernetze Frauenplätze. Frauen in der Informationsgesellschaft, Leske + Budrich: Opladen 1998, S. 115-132.

Siegeris, Juliane/Krefting, Dagmar: Lehrmethodenvielfalt im Curriculum des Studiengangs Informatik und Wirtschaft – Ein Erfahrungsbericht. In: Carmen Leicht-Scholten/Ulrik Schroeder (Hrsg.): Informatikkultur neu denken – Konzepte für Studium und Lehre. Integration von Gender und Diversity in MINT-Studiengängen, Springer Verlag: Wiesbaden 2014, S. 127-140.

Tischer, Ute: Neue Beschäftigungsfelder und weibliche Qualifikationspotentiale, in: Winker, Gabriele; Oechtering, Veronika (Hrsg.): Computernetze, Frauenplätze. Frauen in der Informationsgesellschaft, Leske + Budrich: Opladen 1998, S. 33-55.

Julia Hoffmann, Natalie Sontopski

Code Girls Leipzig – Du nennst es Programmieren, ich nenne es Rock'n'Roll

Die Code Girls *wurden vor zwei Jahren von Natalie Sontopski und Julia Hoffmann gegründet und verstehen sich als Stammtisch, Zweites Zuhause, Geekette-Paradies, Diskutierkreis, Programmier-Zirkel. Bei diesem Artikel handelt es sich um einen praxisorientierten Erfahrungsbericht, bei dem wir auf die Darstellung von Statistiken zur Unterrepräsentation von Frauen in der IT-Branche verzichten und die Notwendigkeit als gegeben annehmen, mehr Mädchen und Frauen für das Programmieren und Codieren zu begeistern und ihnen einen Zugang zu virtuellen Ausdrucks- und Gestaltungsmöglichkeiten zu vermitteln, und dass es dafür essenziell ist, dass sich mehr IT-interessierte Frauen in Netzwerken zusammenschließen und in der Öffentlichkeit sichtbar werden.*

Ausgangspunkt für die Gründung der *Code Girls* war der Besuch des internationalen Technik-Festivals *Campus Party*, für das Natalie Karten gewonnen hatte. Zwischen Robotern, Cyborgs und Vorträgen über Astrophysik taten es uns besonders die *Rails Girls* an, die in Berlin Einsteiger-Workshops für Web-App-Programmierung mit *Ruby on Rails* organisieren. Bisher hatten wir uns zwar individuell mit Grundlagen des Webdesigns und Programmierens auseinandergesetzt, vor allem um eigene Blogs zu verschönern. Das Studieren von Online-Kursen und Tutorials war aber nach der ersten Anfangseuphorie schnell an seine Grenzen geraten und die Mischung aus D.I.Y. (*Do it yourself-*) Philosophie, Gemeinschaft und ansprechender Ästhetik, die die *Rails Girls* präsentierten, motivierte uns, ein eigenes Netzwerk zu gründen. Da wir uns jedoch nicht auf *Ruby on Rails* beschränken wollten, entscheiden wir uns eine Gruppe zu bilden, die sich nach den Programmier- und Codierinteressen der Mitglieder richten sollte und so fuhren wir voller Tatendrang nach Leipzig zurück.

Aller Anfang ist schwer

Nach anfänglichen Diskussionen, ob wir mit Mitte bis Ende Zwanzig eigentlich noch als „Girls" durchgehen können und dadurch die richtige Zielgruppe erreicht wird, stand der Name *Code Girls* schnell fest.

Als erstaunlich unproblematisch erwies sich die Suche nach Räumlichkeiten für die regelmäßigen Treffen. Auf der Suche nach Mitstreiterinnen inserierten wir einen Aufruf auf einer lokalen Kleinanzeigenseite und wurden kurz danach von Mitgliedern des lokalen Vereins *Sublab e. V.* angeschrieben und gefragt, ob wir uns bei ihnen treffen möchten. Bis heute findet unser zweiwöchiges Treffen in dem loftartigen Sublab-Hackerspace im Leipziger Westen statt und wir haben das große Glück, Räume und Technik kostenlos nutzen zu dürfen.

Weniger einfach gestaltete sich die Mitgliedersuche. Zwar konnten wir durch Flyer, Poster und Werbung auf unserer Facebook-Seite interessierte Frauen versammeln. Unser Plan, möglichst wenige Inhalte vorzugeben und die Projekte, an denen wir in den zweiwöchigen Treffen arbeiten, gemeinsam zu entwickeln, führte zu einer hohen Mitgliederfluktuation. Wir fingen zunächst damit an, Kurse auf der Lernplattform *Codecademy* gemeinsam durchzugehen und durch das für Jugendliche entwickelte Lernprogramm *Scratch* einen Zugang zum Programmieren zu finden. Sowohl Codecademy als auch Scratch sind hervorragende Einstiegshilfen, stellten sich aber für den Gebrauch im Gruppenkontext als nicht optimal heraus, weil die Lerngeschwindigkeit innerhalb der Code Girls sehr unterschiedlich war und die Motivation nach unserer Erfahrung schnell nachlässt.

Rails Girls und Neustrukturierung

Da wir mit unserem Vorankommen nach einigen Monaten nicht zufrieden waren, beschlossen wir, einen Rails-Girls-Workshop in Leipzig zu veranstalten, was sich als Initialzündung für eine neue, organisiertere Phase der Code Girls erweisen sollte. Das Konzept der zweitägigen, kostenlosen Ruby-on-Rails-Workshops stammt aus Finnland und hat mittlerweile auf der ganzen Welt Anhängerinnen gefunden. Das Rails-Girls-Netzwerk stellt sowohl Werbe- als auch Workshopmaterialien zur Verfügung und steht jederzeit hilfreich zur Seite; die Organisation vor Ort wird von den lokalen Gruppen übernommen. In unse-

Abbildung 1: Teilnehmerinnen und Coaches des Rails-Girls-Leipzig-Workshops 2013 Foto: Natalie Sontopski

Abbildung 2: Teilnehmerinnen und Coaches des Rails-Girls-Leipzig-Workshops 2013 – Foto: Natalie Sontopski

rem Fall gehörte dazu das Finden der Räumlichkeiten, die Suche nach Coaches, Pressemitteilungen zu versenden, Sponsoren für Coaches-Dinner, Catering und Druckmaterialien anzuwerben und Interviews in den Lokalmedien zu geben. Der Arbeits- und Kostenaufwand für einen Rails-Girls-Workshop ist nicht zu unterschätzen: Für die Vorbereitungen benötigten wir ungefähr zwei Monate, empfehlenswert ist jedoch eine längere Vorlaufzeit, da Unternehmen die Vergabe von Sponsorengeldern oft weit im Voraus planen. Auch das Beantworten von E-Mails, die Erstellung der lokalen Website (besonders wenn man noch nie auf der Entwicklerplattform *Git* gearbeitet hat) und die Werbung für das Event erfordern ein hohes Maß an Engagement. Diese Arbeit zahlt sich jedoch definitiv aus. Nicht nur die glücklichen Gesichter bei der Vorstellung der Web-Apps am zweiten Workshop-Tag entschädigten für den ein oder anderen nahenden Nervenzusammenbruch. Wir lernten bei der Veranstaltung unseren derzeitigen Chefcoach *Lucas* kennen, der uns seitdem bei den regulären *Code-Girls*-Treffen mit Rat und Tat zur Seite steht.

Gemeinsam mit Lucas entwickelten wir ein eigenes Kursprogramm für die *Code Girls*, das die Integration von neuen Mitgliedern erleichtert und in kleinen Einheiten spielerisch die Grundlagen für HTML/CSS und JavaScript vermittelt *(http://codegirls.github.io/materials/).*

Je nach Interesse kann ein kleiner, individuell anpassbarer Blog gestaltet werden oder die Teilnehmerinnen nähern sich den Grundlagen von JavaScript in Form kleiner Aufgaben und am Ende durch die Erstellung eines Text-*Adventures*. Besonders wichtig war es uns, die Kurse frei zugänglich und in englischer Sprache zur Verfügung zu stellen, damit möglichst viele Personen von ihnen profitieren können, und um in den Aufgaben Anregungen zum eigenen Experimentieren zu geben. Ergänzt werden diese Programme durch Feiertagsspecials, wie das „Hacken" von Online-Adventskalendern, Vorträgen von ProgrammiererInnen, z. B. zu HTML5 und individuellen Beratungen von unseren Coaches zu eigenen Projekten wie Blogs oder Websites.

Mit dieser Mischung haben wir gute Erfahrungen gesammelt und in der Zwischenzeit einen kleinen, aber stabilen Kreis von *Code Girls* und Coaches aufgebaut, wobei wir uns freuen würden, den einen oder anderen weiblichen Coach bei uns begrüßen zu dürfen. Für die nähere Zukunft möchten wir unsere Tutorials, besonders die Webdesign-Einheit, weiter ausbauen, uns mit weiteren netz- und technikaffinen Gruppen in Leipzig vernetzen und, wenn es Zeit und Energie ermöglichen, mehr Vorträge anbieten. Außerdem steht die Suche nach Fördermöglichkeiten weit oben auf der Agenda.

Fazit

Die Gründung und Etablierung einer Programmieranfängerinnen-Gruppe ist eher ein Marathon als ein Sprint, wie wir in den zwei Jahren seit unserer Gründung festgestellt haben. Wider unserer anfänglichen Hoffnungen sind wir noch keine vielgebuchten Programmiererinnen und Speakerinnen und haben manchmal das Gefühl, dass die technische Entwicklung in Lichtgeschwindigkeit verläuft, während wir uns die Codier- und Programmier-Grundlagen im Schildkrötentempo aneignen.

Auch wenn unsere Erfolge von außen betrachtet überschaubar aussehen, hat sich der Aufwand für uns gelohnt. Neben

Natalie Sontopski und Julia Hoffmann

Natalie Sontopski (*1984) studierte zwischen 2005 und 2009 Soziologie und Geschichte mit dem Schwerpunkt Kultursoziologie an der Universität Konstanz und von 2009-2012 im Master-Studiengang European Studies an der Universität Leipzig. Derzeit arbeitet sie als Content Managerin beim Leipziger Unternehmen Spreadshirt. Im Netz zu finden mit dem eigenen Blog Endemittezwanzig.
Kontakt: *natalie@codegirls.de*

Julia Hoffmann (*1988) interessierte sich während ihres Studiums der Kommunikations- und Medienwissenschaft an der Universität Leipzig (2007-2013) besonders für Partizipationsmöglichkeiten durch und Identitätsarbeit mit Medien. Nach Redaktionstätigkeiten für verschiedene Printmedien arbeitet sie derzeit als Forschungsassistentin am Deutschen Zentrum für integrative Biodiversitätsforschung (iDiv). Im Netz zu finden unter *hellojuliahoffmann.tumblr.com.*
Kontakt: *julia@codegirls.de.*

Webdesign-, *Ruby on Rails*- und JavaScript-Kenntnissen, konnten wir Erfahrungen im Projektmanagement, inkl. PR, Sponsorenakquise, Mediengestaltung, Pädagogik und Teamleitung gewinnen, die uns nicht zuletzt in unseren alltäglichen Jobs zu Gute kommen und uns zu mehr Souveränität und Selbstbewusstsein verholfen haben. Auf professioneller Ebene konnten wir außerdem an Konferenzen teilnehmen, Artikel veröffentlichen und somit am öffentlichen Diskurs teilhaben.

Aber besonders die *Code Girls*, Coaches und UnterstützerInnen aus der Tech-Szene, die wir in dieser Zeit kennengelernt haben und wahrscheinlich ohne unsere Gruppe nie getroffen hätten, motivieren uns immer wieder, mit unserer Arbeit weiter zu machen und gemeinsam etwas dafür zu tun, dass mehr Mädchen und Frauen, Programmier- und Scriptsprachen als Ausdrucksmittel entdecken und unsere digitale Welt mitgestalten.

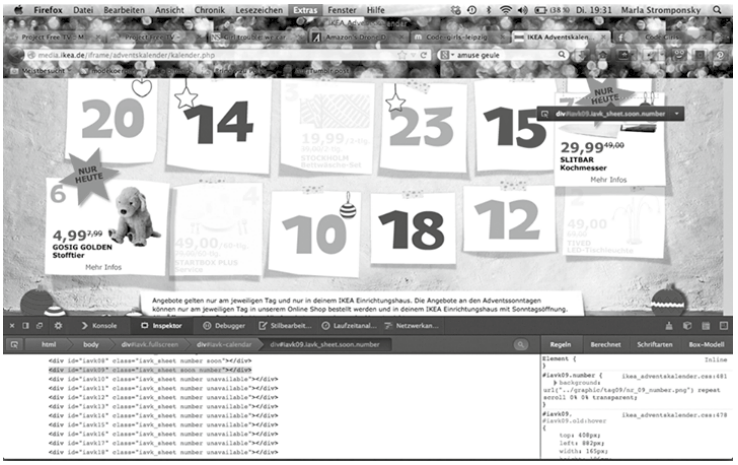


Abbildung 3: Die Code Girls hacken den Ikea-Weihnachtskalender
Foto: Natalie Sontopski

Jasmin Link, Nicola Marsden und Elisabeth Büllesfeld

Personas: Vermeidung von Stereotypen im Softwareentwicklungsprozess[1]

In der Softwareentwicklung und in nutzendenzentrierten Gestaltungsprozessen werden Personas eingesetzt: „Steckbriefe", die fiktive Personen beschreiben, um bei den Mitgliedern des Entwicklungs- oder Designteams das Verständnis für die Nutzenden zu erhöhen. Dabei werden Gruppen von Nutzern und Nutzerinnen oder Nutzungsrollen durch eine oder mehrere, oft detailliert ausgestaltete Personas repräsentiert.
In diesem Artikel wird erörtert, inwieweit dabei Stereotypen zum Einsatz kommen, welche Auswirkungen dies – insbesondere unter Genderaspekten – hat, und wie Ansätze für den Umgang mit Geschlechterstereotypen bei der Nutzung von Personas aussehen können.

Persona-Methode

Die Persona-Methode hat ihre Wurzeln im Marketing, in der Zielgruppenanalyse. Sie basiert auf der Tatsache, dass es uns Menschen zumeist sehr leicht fällt, uns in andere Menschen hinein zu versetzen – eine Fähigkeit die wir im Alltag ständig nutzen, sei es im direkten Umgang mit anderen oder beim Lesen von Geschichten und beim Filmeschauen.

Der Mechanismus funktioniert auch bei fiktiven Charakteren, die sowohl in der Arbeit eines Design- oder Entwicklungsteams genutzt werden können, als auch im Kontakt mit Kundinnen und Kunden, um eine Nutzungssituation zu beschreiben und den Beteiligten zu ermöglichen, mit geringem Aufwand in die Rolle einer konkreten Person zu schlüpfen.

Der Vorteil ist, dass sich alle Beteiligten gemeinsam die jeweilige Persona in einer konkreten Situation vorstellen können, und nicht nur abstrakt über „den User" reden und ganz verschiedene unausgesprochene Vorstellungen von dieser Person haben. Diese verschiedenen Vorstellungen werden idealerweise zusätzlich zu Marktforschungsdaten über die Zielgruppe oder Nutzenden im Erstellungsprozess der Personas berücksichtigt. Manchmal werden auch personaübergreifende Szenarien oder *User Stories* geschrieben.

Detaillierte, ansprechende Beschreibung

Dabei kommt dem Detaillierungsgrad und dem Realismus der Beschreibung der Persona eine große Bedeutung zu: Sehr einfache Personas bestehen aus einem Foto einer Person, ihrem Alter und Geschlecht und ein paar Schlagwörtern. Detailliertere Personas haben einen Hintergrund, sie haben eine Geschichte und Erfahrungen, Ziele, Pläne und Erwartungen, Eigenschaften, die sich mit der Zeit verändern. So ergibt sich ein differenziertes, ganzheitliches Bild einer Person.

Eine weitere Rolle spielt die Anforderung, dass eine Persona ansprechend sein soll. Denn dann fällt es leicht, sich mit der Persona zu identifizieren, und ein Interesse zu haben, sich bewusst mit ihr und ihrem Verhalten zu beschäftigen. Bei einer unsympathischen oder stark überzeichneten Persona sinkt die Bereitschaft dazu[2].

Aus der Perspektive des Gender Mainstreamings kann die Persona-Methode eine sehr positive Auswirkung haben. Denn während in unserem Sprechgebrauch das generische Maskulinum verbreitet ist und Frauen oft mit gemeint aber nicht mit gedacht werden (vgl. Abschnitt: Sprachliche Bezeichnung), tauchen in den Persona-Sets konkrete weibliche Personen auf.

Duale Informationsverarbeitung: Bewusst vs. Automatisiert

Eine weitere wichtige Rolle in der Wahrnehmung von Personen und Personas spielen die bewusste und die automatisierte Informationsverarbeitung.

Duale Informationsverarbeitungsmodelle zeigen Folgendes auf: Wenn wir unsere Wahrnehmung nicht bewusst kontrollieren, verarbeiten wir Informationen automatisiert und greifen als Default auf Stereotype zurück. Die aufmerksame, zentrale Verarbeitung von Informationen macht den Einsatz von Stereotypen unwahrscheinlicher. Studien zeigen, dass sowohl die Möglichkeit/Fähigkeit zur Aufnahme (z. B. ohne Zeitdruck oder Ablenkung) als auch die Motivation (z. B. bei persönlicher Relevanz des Themas oder beim Wunsch, vorurteilsfrei wahrzunehmen) die zentrale, bewusste Informationsverarbeitung stärken.

Damit Personas gut funktionieren, sollten also folgende Voraussetzungen erfüllt sein: Die Persona sollte ansprechend und detailliert genug sein, um als ganzheitliche Persönlichkeit wahrgenommen zu werden. Und nur bei aufmerksamer Wahrnehmung (kontrollierter Verarbeitung) ist eine wirkliche Auseinandersetzung mit der Persona gegeben. Unter Zeitdruck oder Ablenkung wird jede noch so sorgfältig erarbeitete Persona auf Basis von Stereotypen wahrgenommen.

Geschlechterbezogene Aspekte

Welche Mechanismen laufen beim Erstellen und Nutzen von Personas ab? Welche Rolle spielen geschlechtsbezogene Aspekte beim Einsatz von Personas?

Um auf diese Frage einzugehen, werden im Folgenden einige Punkte bezüglich Sprache, sozialer Identität und geschlechtsbezogener Personenwahrnehmung erläutert:

Sprachliche Bezeichnung

Personengruppen nicht näher bestimmten oder gemischten Geschlechts werden im Deutschen entsprechend dem generischen Maskulinum meist mit der männlichen Bezeichnung beschrieben, z. B. „die Entwickler“ oder „die Monteure“. Auch in der Einzahl wird mit „der User“, oder „der Kunde“ eine zwar grammatikalisch neutral gemeinte, aber doch männlich assoziierte Form gewählt. Unter dem sprachlichen Gesichtspunkt ist es von Vorteil, wenn in einem Persona-Set konkrete weibliche Personen auftauchen. Dadurch kommt auch eine Userin vor, es wird auch über die Kundinnen gesprochen, und deren Handeln antizipiert.

Soziale Identität und Personenwahrnehmung

Die Theorie der sozialen Identität besagt, dass Mitglieder der eigenen Gruppe positiver wahrgenommen werden als Mitglieder der Fremdgruppe („*ingroup favoritism*“, „*out-group discrimination*“). Bei der Betrachtung des Entwicklungsprozesses von Personas ist zu erwarten, dass es in der Beschreibung von Personas eine Tendenz gibt, sie in Kategorien zu beschreiben, in der die Eigengruppe besonders gut dasteht, und solche Kategorien außen vor zu lassen, in denen die Fremdgruppe positiver und die Eigengruppe negativer dastehen würde bzw. in denen sich beide Gruppen ähnlich sind.

Hat eine Gruppe eine hohe Kompetenz in einem Bereich, tendiert sie dazu, die Fremdgruppe durch das Fehlen dieser Kompetenz zu beschreiben. Bei Personas ist, besonders auch unter Berücksichtigung der Tatsache, dass sie meist durch sehr technikaffine Menschen definiert werden, z. B. Technikaffinität eine Eigenschaft, die in diesen Bereich fallen könnte.

Auch die eigene Geschlechtszugehörigkeit als herausragendes Merkmal sozialer Identität dürfte eine Rolle spielen.

Andere Personen – und somit auch Personas – werden also grundsätzlich anders beurteilt, je nachdem, ob sie zur Eigen- oder zur Fremdgruppe gehören. Personas stehen somit in einer intergruppalen Interaktion mit den Personen, die sie betrachten, und denen, die sie erstellt haben. Sie stehen allerdings auch in Interaktion miteinander: Personas eines Sets können nicht isoliert betrachtet werden – die anderen im gleichen Kontext vorhandenen Personas dienen als Referenzrahmen für intergruppale Vergleiche.

Geschlechtsbezogene Personenwahrnehmung

Die Forschung zur Personenwahrnehmung und zur Eindrucksbildung zeigt, dass das Geschlecht, mit dem eine Person „ausgestattet“ wird, die Beurteilung dieser Person in vielfältiger Hinsicht beeinflusst.

Werden bei identischen Beschreibungen nur die Namen oder das Geschlecht ausgetauscht, so wird die gleiche Person als unterschiedlich kompetent oder sympathisch beurteilt. Die negative Bewertung eines Abweichens von den für das Geschlecht als typisch wahrgenommenen Verhaltensweisen zeigt folgendes Beispiel: Hypothetische Personen, die in Teilzeit arbeiten wollten, werden im Vergleich zu Frauen als Mann deutlich negativer beurteilt.

Ambivalenz von Geschlechterstereotypen

Im Kontext von Geschlechterstereotypen wurde ausführlich erforscht, dass Vorurteile und Stereotypen nicht gleichzusetzen sind mit Antipathie, sondern dass beim Phänomen des „benevolenten“ Sexismus solchen Mitglieder des anderen Geschlechts, die rollenkonform wahrgenommen werden, eine besondere Zuneigung entgegengebracht wird, während rollenabweichendes Verhalten Ablehnung auslöst.

Sexistische Wahrnehmung zeigen sowohl Männer als auch Frauen, sowohl gegenüber dem eigenen wie auch dem anderen Geschlecht. Für den Umgang mit Personas bedeutet dies, dass Eigenschaften, die eine weibliche Persona sympathisch machen, eine männliche unsympathisch machen können und umgekehrt.

Da die Möglichkeit zur Identifikation mit und Sympathie für eine Persona (und damit die mögliche Empathie) unter anderem vom

Sexismus der Betrachtenden bestimmt wird, stellt die Erstellung einer nicht rollenkonformen Persona einen Balanceakt dar.

Vermeidbarkeit von Stereotypen

Bezüglich der Frage, ob Stereotypen vermeidbar sind, wird in der Literatur auf das Spannungsfeld zwischen dem Nutzen von und den Einschränkungen durch Stereotype eingegangen: Es muss zwischen individuellen Besonderheiten und der nötigen Reduzierung von Komplexität abgewogen werden. Untersuchungen zeigen auch, dass im Entwicklungsteam neben der schriftlichen Repräsentation der Personas in Diskussionen sehr häufig Stereotype verbalisiert werden[3].

Genderbewusste Entwicklung und Nutzung von Personas

Die Repräsentation von Personas und die Auseinandersetzung mit Geschlechterstereotypen im Entwicklungsprozess interaktiver Systeme und Zukunftsszenarien können, genauso wie das Vorkommen dieser Phänomene in der Alltagskultur, entweder zum Beibehalten, Wiederholen und Festigen von Rollenbildern und Stereotypen beitragen – oder, beim aufmerksamen Umgang mit Stereotypen, zur Flexibilisierung von Rollen und Identitäten.

Im Sinne des in der Europäischen Forschung verankerten Gender Mainstreaming ist die Beachtung geschlechter- und geschlechterrollen-spezifischer Faktoren z. B. in öffentlichen Institutionen und Forschungsprojekten verpflichtend, und ein bewusster Umgang mit diesen Faktoren gerade im Bereich von Innovationen ein wichtiger Aspekt, dessen soziale, politische sowie ökonomische Auswirkungen berücksichtigt werden sollten, um eine Entwicklung von Produkten und Systemen zu gewährleisten, die genderspezifischen Unterschieden gerecht wird.

Aus folgenden Gründen ist es wichtig, die handelnden Personen nicht einseitig darzustellen:

Zum einen werden Rollenzuschreibungen durch ihre Wiederholung gefestigt, dabei werden Vorurteile und Klischees oft unreflektiert übernommen. Durch das Vorhandensein und das Betonen geschlechterstereotyper Zuschreibungen werden die Handlungsspielräume von sowohl Männern als auch Frauen eingeschränkt, z. B. hinsichtlich ihres Selbstverständnisses, ihrer Anwendung von Technik, ihrer Berufswahl.

Zum anderen wird durch die Verknüpfung eines Themas mit nur einem der Geschlechter der Transfer von Innovationen in die mit diesem Geschlecht nicht assoziierten Bereiche weniger suggeriert, was möglicherweise eine verlangsamte Entwicklung „innovationsferner" Bereiche zur Folge hat.

Beim Entwurf von Personas wird deren Geschlecht oft eine untergeordnete Rolle zugeordnet. Meist wird ein binäres Geschlechtersystem angenommen. Die Zuschreibung von „für Männer" und „für Frauen" als typisch wahrgenommenen Eigenschaften und Verhaltensweisen ist entsprechend wahrscheinlich. Deshalb sollten bei Szenarien und Persona-Sets folgende Punkte kritisch beleuchtet werden:

Die soziale Identität und der Status der Personas: Alter, Geschlecht, Beschäftigungsstatus, persönliche und soziale Beziehungen zu anderen Personas.

Der Hintergrund und Detaillierungsgrad und die Basis, auf der die Beschreibungen entstanden sind, sowie das Vorkommen stereotyper Beschreibungen.

Jasmin Link, Nicola Marsden und Elisabeth Büllesfeld

Jasmin Link ist wissenschaftliche Mitarbeiterin in der Abteilung Web-Application-Engineering und Human-Computer-Interaction am Fraunhofer IAO in Stuttgart. Im von ihr geleiteten Interaktionslabor wird die Interaktion mit allen Sinnen erforscht und weiterentwickelt. Ihre Tätigkeit als Beauftragte für Chancengleichheit trug dazu bei, Genderaspekte auch im Bereich von Informatik und Medien zu betrachten.

Nicola Marsden ist Professorin für Sozialpsychologie in der Informatik an der Hochschule Heilbronn. Sie lehrt und forscht in den Bereichen Human-Computer-Interaction computervermittelte Kommunikation, Gender, Motivation und Einstellungsänderung.

Elisabeth Büllesfeld ist wissenschaftliche Mitarbeiterin in der Abteilung Web-Application-Engineering und Human-Computer-Interaction am Fraunhofer IAO in Stuttgart. Sie beschäftigt sich mit Zukunftskonzepten von Automaten und der Gestaltung von und Interaktion mit Prozessen im Gesundheitswesen.

Darüber hinaus gibt es eine Vielzahl von Faktoren, die Einfluss darauf haben, ob eine Persona bzw. ein Persona-Set Geschlechterstereotype verstärkt oder vermeidet:

Es hängt ab von der Beschreibung der Persona selbst, dem Informationsverarbeitungsmodus der Person, die die Personas erstellt, dem Informationsverarbeitungsmodus der Person, die die Personas einsetzt, d.h. davon ob Informationen elaboriert oder automatisch verarbeitet werden. Es hängt außerdem ab von der Gruppenzugehörigkeit der Person, die die Persona einsetzt und erstellt, d.h. der Frage, ob es sich um ein Eigen- oder ein Fremdgruppenmitglied handelt, von Kontakten oder Freundschaften zu Mitgliedern der Gruppe, der die Persona angehört, vom sozialen Umfeld – sowohl des Design- oder Entwicklungsteams, das die Persona verwendet, als auch vom Umfeld der Persona, also des Persona-Sets, vom Detaillierungsgrad und Realismus in dem die Beschreibung vorliegt, und davon, inwieweit sich die Personen, die mit ihr arbeiten, mit der beschriebenen Persona identifizieren können.

Lösungsansätze

Um in Persona-Sets und Szenarien Geschlechterstereotype zu vermeiden oder bewusst damit umzugehen, werden im Folgenden vier Lösungsansätze diskutiert, die direkt mit dem Erstellungsprozess und dem Einsatz der Personas zusammenhängen. Welchen Einfluss die Geschlechterverteilung des Entwicklungsteams hat, wird nicht erörtert.

Repräsentation in direkter Ansprache

Eine Repräsentation in direkter Ansprache bedeutet, dass Szenarien, Rollen oder Personas in Ansprache der Lesenden formuliert werden: „Stellen Sie sich vor, Sie haben gerade Ihre Ausbildung als Fachkraft im Vertrieb abgeschlossen, und sind auf Stellensuche." Bei dieser Abwandlung der Persona-Methode werden bestimmte (Haupt-)Attribute der Persona, beispielsweise das Geschlecht und das Alter, weggelassen und durch die Person, die mit der beschriebenen Situation konfrontiert wird, bewusst oder unbewusst ergänzt. Durch diese Formulierung kann ein hohes Maß an persönlichem Bezug hergestellt werden, das z. B. für die Öffentlichkeitsarbeit durch die „ansprechende" Ausdrucksweise von Vorteil sein kann. Doch der Vorteil für Gruppendiskussionen, eine Persona beim Namen nennen zu können, entfällt.

Gleichgeschlechtliches Persona-Set

Beim Einsatz von Personas in Testsituationen kann den Testpersonen ein Persona-Set präsentiert werden, das dem eigenen Geschlecht entspricht. Da in unserer Gesellschaft weitgehend ein binäres Geschlechtersystem angenommen wird, würde in der praktischen Umsetzung Männern eine Anzahl verschiedener Männer präsentiert werden, den Frauen die Personas in ihrer weiblichen Form.

Dabei kann es passieren, dass sowohl beim Erstellen, als auch im Umgang mit der Persona festgestellt wird, dass eine Persona mit einem anderen Geschlecht „nicht funktioniert". An diesen Stellen lohnt es sich, besonders genau hinzuschauen, welches die Ursachen dafür sind – ob durch eigene (Vor-)Urteile und Stereotypen die Kombination ungewohnt aussieht, ob die Gründe in den sozialen, mehr oder weniger wandelbaren Geschlechterrollen liegen oder wodurch die Kombination ausgeschlossen wird.

Es ist zu beachten, dass stark von gewohnten Rollen abweichende Personas einerseits vom Entwicklungsteam als unglaubhaft wahrgenommen werden können, andererseits die Aufmerksamkeit erhöhen.

Es wäre zu untersuchen, ob sich die Testpersonen bei gleichgeschlechtlichen Personas besser in die Situationen einfühlen können: So wird bei der Berufswahl von Jungen und Mädchen die Wichtigkeit von *role-models* betont, vielleicht ist dieses Konzept auch auf Bereiche wie den Einsatz von Personas übertragbar.

Zufällige Verteilung des Geschlechts

Beim Erstellen der Personas wird das Geschlecht, ähnlich wie beim Erstellen eines Charakters in einem Rollenspiel, durch Würfeln zufällig bestimmt. Hierbei ist vorher festzulegen, welche Ausprägungen vorkommen sollen, und ob diese quotiert sind. Beim Festlegen dieser Rahmenbedingungen muss auch diskutiert werden, welcher Einfluss des Faktors Geschlecht auf die Persona im vorliegenden Kontext angenommen wird und welcher Stellenwert diesem beigemessen wird. Auch bei dieser zufälligen Verteilung kann der Effekt auftreten, dass Teammitglieder der Meinung sind, dass das Geschlecht zu anderen definierten Eigenschaften nicht „passe". Aus der Diskussion, woran das liegt, können auch hier wichtige Schlüsse gezogen werden, welchen Einfluss der Faktor Geschlecht im Umgang mit einer Anwendung oder einem System hat oder welcher Einfluss ihm unterstellt wird.

Normalverteilte, repräsentative Personas

Um in Projekten, bei denen nicht auf Marktforschungsdaten zurückgegriffen werden kann, trotzdem eine objektive Basis an demographischen Daten zugrunde zu legen, könnte ein Persona-Set erstellt werden, das z. B. die in Deutschland lebende Bevölkerung in ihrer Gesamtheit repräsentiert, vgl. auch *Sinus-Milieus*. Um den Entwickelnden einen Eindruck von der Spannbreite an Lebenssituationen zu geben, müsste ein solches Set sehr umfangreich sein.

Käme dieses Set für ein konkretes Projekt zum Einsatz, würden zwar nur ein paar der Personas herausgegriffen werden, aber trotzdem würde noch ein guter Teil der Vielfalt und des Realismus des Ursprungssets erhalten bleiben.

Fazit und Ausblick

Bei der Gestaltung und dem Einsatz von Personas greifen wir auf Stereotypen und Automatismen der Wahrnehmung zurück, die auch durch das Geschlecht einer Persona beeinflusst werden. Da es sich hierbei häufig um unbewusste Prozesse handelt, sind diese häufig schwer zu fassen und es fällt schwer, im Entwicklungsteam darüber zu sprechen. Die Mechanismen, die hier

greifen, sind vor allem automatisierte Informationsverarbeitung, internalisierte Geschlechterstereotypen und die Interpretation von Verhalten und Eigenschaften auf Basis der eigenen Gruppenzugehörigkeit. Es lohnt also das genaue Hinschauen, um vor allem beim Entwickeln von Personas nicht den eigenen Wahrnehmungsfehlern zum Opfer zu fallen und mit Stereotypen oder Sexismen gespickte Personas zu entwerfen.

Um vorhandene Geschlechterstereotypen nicht in Personas festzuschreiben, können die oben genannten Methoden genutzt werden, um die geschlechtsbezogene Wahrnehmung aufzudecken und damit diskutierbar zu machen sowie den Einsatz von Stereotypen zu reduzieren. Durch einen engagierten Umgang mit den Personas kann sichergestellt werden, dass die Verarbeitung von Informationen in der Entwicklung und beim Einsatz der Personas ausreichend detailliert geschieht. Und dass durch eine Auseinandersetzung mit dem Faktor Geschlecht im aktuellen Projekt zumindest bewusstes „Doing Gender" betrieben wird.

Anmerkungen

1 *Dieser Artikel basiert auf dem Beitrag „Personas und stereotype Geschlechterrollen" vom April 2014, von Nicola Marsden, Hochschule Heilbronn und Jasmin Link und Elisabeth Büllesfeld, Fraunhofer IAO, Stuttgart, erschienen in Nicola Marsden & Ute Kempf (Eds.), GenderUseIT – HCI, Web-Usability und User Experience unter Gendergesichtspunkten. Berlin: DeGruyter.*

2 *Siehe dazu Grudin 2006, Nielsen 2013.*

3 *Siehe Turner&Turner 2011.*

Referenzen

Grudin, John. (2006). Why personas work: The psychological evidence. In John Pruitt and Tamara Adlin (eds.)

The persona lifecycle: Keeping people in mind throughout the product design, 642-664. Morgan Kaufman.

Turner, Phil & Turner, Susan (2011). Is Stereotyping Inevitable When Designing With Personas? Design Studies, 32(1), 30-44.

Nielsen, Lene (2013). Personas – User Focused Design. Springer.

Plant, E Ashby & Devine, Patricia G. (1998). Internal and external motivation to respond without prejudice. Journal of Personality and Social Psychology, 75(3), 811.

Weitere Quellen siehe Konferenzbeitrag.

Für weitere Untersuchungen über Personas in Persona-Sets und Szenarien sind wir, ein kleines Team Forschender am Fraunhofer IAO, auf der Suche nach Daten die wir auswerten dürfen. Wir interessieren uns für Beschreibungen von Personas aus Entwicklungs- oder Design-Projekten, für Szenario-Berichte und Zukunftsszenarien.

Für weitere Informationen oder Zusendungen wenden Sie sich bitte an *jasmin.link@iao.fraunhofer.de*. Vielen Dank.

Doris Allhutter

User Experience: Was uns Geschlechter-Technikverhältnisse zeigen[1]

User Experience (UX) umfasst mehr als bloß instrumentelle Anforderungen an eine Computeranwendung. Es geht um „subjektive, situierte, komplexe und dynamische Begegnungen" [1:59]. UX ist ein Effekt der Wahrnehmungen, Emotionen und psychologischen und physiologischen Reaktionen von Nutzer_innen bei der Interaktion mit einem System in einem bestimmten Nutzungskontext. Welche Aspekte werden aber konkret als subjektiv erlebte Produktqualität angesprochen? Welche Wahrnehmungsmodi bedenken UX-Konzepte mit, welche schließen sie aus? In wie weit werden gesellschaftliche Verhältnisse in die Charakterisierung von Nutzungskontexten einbezogen? Eine Geschlechterperspektive eröffnet eine Annäherung an zentrale offene Fragestellung zu Konzeptualisierung, Design und Evaluierung von UX.

Seit den frühen 1990er Jahren erweiterten sich Qualitätsvorstellungen im Interaktionsdesign von einem stark technikzentrierten Fokus auf *User Performance* und *Usability* hin zu einem erweiterten Konzept von subjektiv empfundener *User Experience*. Die Interaktion mit einem System oder einer Anwendung soll dabei nicht nur eine Funktion erfüllen, sondern sie soll für die Nutzer_innen affektiv und emotional von Bedeutung sein. UX umfasst dabei die Gesamtheit der Effekte, die von Nutzer_innen als Ergebnis des Nutzungskontexts und der Interaktion mit einem Produkt wahrgenommen oder gefühlt werden. Als mögliche emotionale Wirkungen werden Freude, Spaß, Überraschung oder Bindung genannt und „auch tiefere emotionale Faktoren wie Selbstausdruck, Identität, ein Gefühl, an der Welt Teil zu haben, oder Stolz, etwas zu besitzen" [2:59]. Hassenzahl et al. [3] schlagen vor, die „Essenz" von positiven Erlebnissen zu sogenannten *experience patterns* zu destillieren, also die Struktur von freudvollen Erlebnissen herauszuarbeiten, um sie dann in Artefakte einzuschreiben. Pohlmeyer [4] arbeitet mit ihrem *model of continuous UX* unterschiedliche Zeitebenen heraus, indem sie unmittelbare Effekte und Kurzzeit- und Langzeit-Effekte differenziert (*anticipated experience, use experience, reflective experience, repetivite experience, retrospective experience, proscpective experience*). In ihrem Modell spielen Erinnerungen an vorgängige Erfahrungen eine zentrale Rolle für das Produktdesign. In Anlehnung daran betonen Kujala et al. [5] die Bedeutung einer *long-term UX*. Die zeitliche Vielschichtigkeit von UX einzubeziehen erlaube es erstens, UX als eine Reihe von Erfahrungen zu begreifen, die nicht nur episodische Konsequenzen für Nutzer_innen sondern auch langfristige und gesellschaftliche Auswirkungen haben. Zweitens zieht diese Sicht in Betracht, dass Zeit den Kontext und die Bedeutung einer Erfahrung radikal verändern kann. Dementsprechend wird ein Interaktionsdesign unterschiedliche Nutzer_innen-Erlebnisse hervorrufen. Wie oft betont wird, sei es deshalb notwendig, Zielgruppen-spezifische Designs auf der Basis eines soliden Wissens über diese Zielgruppen zu entwickeln.

Was bringt Geschlechtertheorie?

In der Technikforschung dienen unterschiedliche Ansätze dazu, das Verhältnis zwischen Gesellschaft und Technik zu erklären. Daran anknüpfend zielt feministische Technikforschung darauf ab, entsprechend in Geschlechter-Technikverhältnisse zu intervenieren.

Ansätze wie *social construction of technology* (SCOT) oder *social shaping of technology* (SHOT) verstehen Technik als sozial geformt. Sie gehen davon aus, dass sich gesellschaftliche Vorstellungen durch eine Konfiguration von zukünftigen Nutzer_innen und Nutzungskontexten in informatische Artefakte einschreiben. Entwickler_innen greifen bei Designentscheidungen und deren Implementierung oft auf eigene Anforderungen oder Kenntnisse zurück (*I-methodology*) oder treffen implizit Annahmen über zukünftige Nutzer_innen, die als Scripts in Anwendungen einfließen [6;7]. Beide Vorgehensweisen führen tendenziell zum Ausschluss von Nutzer_innengruppen, die nicht als User mitgedacht werden. Oder Sie können Frauen und Männer aufgrund gesellschaftlicher Zuschreibungen durch Produktdesign, Funktionalitäten oder Produktkommunikation auf stereotypisierende Weise unterschiedlich ansprechen. Eine Analyse von *Gender Scripts*, die in Anwendungen eingeschrieben sind, intendiert ein Aufbrechen von Geschlechterstereotypen und asymmetrischen Zuschreibungen. Ansätze, die die Diversität von Nutzer_innengruppen und Lebens-/Nutzungskontexten einbeziehen, stellen Zuschreibungen an ‚Frauen' und ‚Männer' in Frage, indem sie diese vermeintlich einheitlichen Gruppen durch Aspekte wie Alter, Sexualität und soziale Bezugsfelder, Behinderung/Befähigung, sozio-ökonomische und kulturelle Herkunft differenzieren. Dabei wird hinterfragt, welche Geschlechterbilder in technischen Kontexten hegemonial sind, und welchen vergeschlechtlichten Vorstellungen damit auch in der Entwicklung Relevanz eingeräumt wird. In Bezug auf UX bieten diese Ansätze einen Weg, das durch Annahmen, Interviews oder Beobachtungen gewonnene „solide Wissen" über unterschiedliche Zielgruppen und entsprechende Evaluationsverfahren kritisch auf Geschlechter- und soziale Biases hin zu überprüfen. Verortet man UX allerdings nicht im Design oder dessen direkten Folgen sind hier Grenzen gesetzt.

Ko-konstruktivistische Ansätze gehen davon aus, dass Technik und Gesellschaft einander wechselseitig konstituieren. Es wird gefragt, wie Vorstellungen über Geschlecht durch Technik mitgeformt werden und wie Technikentwicklung und -nutzung Bereiche wie Arbeit, Freizeit und Alltag geschlechtlich strukturieren. Technische Konzepte und Methoden, die Entwicklung von Systemen und ihre Nutzung, das Reden über Technik in der Gesellschaft – all diese immer wieder wiederholten Praktiken stellen laufend Geschlechterdifferenz[2] her. Um ein duales Geschlechterverständnis in der Technik in Frage zu stellen, sind daher Entwicklungspraktiken grundsätzlich als soziotechnisch zu verstehen. In der Technikforschung werden technische Paradigmen durch die Auflösung von Gegensatzpaaren wie Objektivität/Subjektivität oder Technik/Gesellschaft als vergeschlechtlicht sichtbar gemacht.

Auch soziomaterielle Ansätze setzen voraus, dass Gesellschaft und Technik kontinuierlich in Relation zueinander entstehen. Soziotechnische Praktiken werden allerdings stärker auch als materiell beschrieben – als Praktiken, in denen nicht nur gesellschaftliche Diskurse und Strukturen, sondern auch Materialitäten wie Programme, Code aber auch Körper eine Rolle spielen und aktiv sind. Auf diese Weise werden Geschlecht und Technik als koemergent, d.h. als schrittweise gegenseitige Inkraftsetzung beschrieben [8]. Durch eine Analyse von Entwicklungsprozessen wird zum Beispiel sichtbar gemacht, wie etwa Software-Qualität, Requirements-Engineering oder konkrete Implementierungen vergeschlechtlicht sind. Eine Möglichkeit der Intervention in Geschlechter-Technikverhältnisse bietet daher ein grundsätzliches Infragestellen von dualen Geschlechtervorstellungen und den damit verknüpften Dichotomien in technischen Konzepten, Methoden und Praktiken (z. B. [9]). Eine soziomaterielle Sichtweise geht dabei einen Schritt weiter und setzt sich damit auseinander, wie Geschlechter-Technikverhältnisse verkörpert und materialisiert werden [10]. In Bezug auf UX eignet sich dieser Ansatz, um Anwender_innen-Erlebnisse als affektive Phänomene zu beleuchten.

Affekt und soziomaterielle Technikverhältnisse

Die Affektivität von Interaktionen stellt in der Literatur zu UX einen zentralen Bezugspunkt dar (z. B. [11;12]). Dabei wird Affekt als eine durch Design erzeugte Beziehung mit einem Artefakt verstanden. Obwohl UX kein Produktmerkmal ist, sondern (affektiv) im Kontext einer bestimmten Nutzung durch konkrete Nutzer_innen entsteht, beschreiben es Designkonzepte oft vereinfacht als ihr Ziel, den Nutzer_innen positive Erfahrungen bereit zu stellen. Den Ursprung von emotionalen Erlebnissen allein in der situativen Interaktion mit dem technischen Artefakt zu verorten, verkürzt allerdings die Sichtweise, die Ansätze zu Affekt anbieten.

Ein Anwender_innen-Erlebnis ist ein soziomaterielles Phänomen, in dem Eigenschaften eines Computersystems, Handlungen, die mit dem System durchgeführt werden und die sich auf vorgängige Praktiken beziehen, und die Körper der Nutzer_innen, die sich durch Wahrnehmungen, Interaktionen, Affekte und Emotionen in diese Praktiken involvieren, etwas miteinander hervorbringen: ein bestimmtes Technikverhältnis. Solche relationalen Phänomene manifestieren sich in Objekten und in Körpern: Nutzer_innen involvieren sich und werden sensorisch, emotional und körperlich involviert. Bestimmte Interaktionen werden damit bedeutsam – oder, wie Karen Barad [13] es formuliert hat, erlangen bestimmte verkörperte Konzepte Bedeutung und materialisieren sich (in Artefakten und Subjekten).

Sara Ahmed [14] erklärt in ihren Arbeiten zu Affekt und dem Verhältnis mit Objekten, wie die Welt durch den Kontakt zwischen Körpern und Objekten eine bestimmte Form annimmt. Sie beschreibt diese Beziehung als Orientierungen. Orientierungen gestalten, welche Dinge für uns Bedeutung erlangen und sie bezeichnen Richtungen, die wir einschlagen: wir orientieren uns mehr hin zu manchen Objekten als zu anderen [14:247]. Die Orientierung hin zu einem Objekt steckt den Raum ab, den wir in der Gesellschaft einnehmen. So hat die feministische Technikforschung etwa den Umgang mit bestimmten technischen Objekten und Technikentwicklung als ‚männlich' bewohnten Raum beschrieben (z. B. [15]). Die Nähe von Körpern und Dingen zueinander gestaltet die Form dieser Körper und Dinge mit. Was in

dieser Nähe zueinander in einem bestimmten Moment passiert, ist offen, meint Ahmed [14:240]. Wir wissen nicht immer, wie Dinge einander affizieren oder wie wir von ihnen affektiv berührt werden. Susan Kozel [16] hat dies als Resonanz zwischen Objekten und Menschen beschrieben. Resonanzen entstehen zwischen Objekten und Körpern. Sie verbinden das Sensorische und Affektive und zeigen sich als Momente des Affiziert-Werdens.

Affekt wird in queer-feministischen Ansätzen nicht wie in kognitionswissenschaftlichen Ansätzen als neurophysiologischer Zustand einer Person verstanden, der durch einen Stimulus ausgelöst wird. Affekt wird dagegen als *Modus der Involviertheit* [17] beschrieben – als Involviertheit in gesellschaftliche Strukturen und in Materialitäten. Wie weiter oben beschrieben, entwickeln sich Gesellschaft und Technik in Relation zueinander. Sie entstehen ineinander verschränkt in einem fortlaufenden Prozess, in dem auch technische Objekte oder ein Involviert-Sein der Menschen in soziotechnische Verhältnisse eine aktive Rolle spielen. Historisch gewachsene Geschlechter-Technikverhältnisse spiegeln daher bestimmte gesellschaftliche Machtverhältnisse wider, in denen Körper unterschiedlich affiziert werden.

Affektive Erfahrungen sind daher nicht nur individuell und subjektiv, sondern sie werden aufgrund ihres Entstehens in einem gesellschaftlichen Zusammenhang auch durch Empathie und Imagination mit anderen Menschen geteilt. Sie verweisen auf ein Zusammenwirken von materiellen Körpern und Gesellschaft. Ahmeds [14:245] Konzept der Orientierungen erklärt die Geschichtlichkeit oder das Geworden-sein und ständige Werden von Körpern und Affekten auch als Tendenz zu etwas hin. Bestimmte Tendenzen oder die Nähe zu bestimmten Objekten haben wir schon geerbt, etwa eine Nähe zu den geschlechterdifferenten Räumen, die wir ‚bewohnen'.

UX: ein verkörpertes Konzept

Vor diesem theoretischen Hintergrund und auch auf Basis meiner empirischen Untersuchung zu Affekten und Orientierungen in Anwender_innen-Erlebnissen [10;18] zeigt sich, dass UX als verkörpertes Konzept begriffen werden muss, das als situiertes Phänomen in einem konkreten soziomateriellen Verhältnis zutage tritt und dem eine Geschichtlichkeit vergeschlechtlichter Subjekte zugrunde liegt. Reale Anwender_innen-Erlebnisse machen Interaktionen mit technischen Objekten als affektiven Prozess deutlich, der die Körper der Nutzer_innen (auch) geschlechtlich adressiert. Momente der Affizierung sind dabei vielschichtig, unvorhersehbar und verlaufen nicht innerhalb definierter Geschlechtergrenzen. Durch erworbene Orientierungen in Geschlechter-Technikverhältnissen tendieren Menschen aber zu unterschiedlichen affektiven Bezügen (in denen neben Geschlecht auch weitere Diversitätsaspekte wirksam werden). Interaktionsdesign kann daher als ein Prozess verstanden werden, in dem Geschlechter-Technikverhältnisse differentiell in Kraft gesetzt werden.

In Bezug auf Konzeptualisierung, Design und Evaluierung von UX lassen sich zwei Aspekte zusammenfassen: Erstens macht ein soziomaterielles UX Konzept, wie ich es hier skizziert habe, nochmals deutlicher, was in einigen Konzeptionen von UX schon angelegt ist, aber in Design-Ansätzen nicht in letzter Konsequenz vollzogen wird: die Auflösung der Dichotomie eines subjektiven Nutzer_innen-Erlebnisses und einer objektiven, quantitativ messbaren *User Experience*. Die Fortschreibung dieser Dichotomie zeigt sich in den disziplinären Zugängen und analytischen Bezugsrahmen, die Forschung zu UX heranzieht. Im Allgemeinen beziehen sich ergonomische, kognitionswissenschaftliche und psychologische Ansätze auf quantitative individuelle Wirkungszusammenhänge, die verallgemeinert und objektiviert werden. Die Gesellschaftlichkeit, Geschichtlichkeit und das prozesshafte Werden von Subjekten in Relationalität mit Technik wird dadurch nicht sichtbar. Damit bleiben diese Aspekte auch in der praktischen Umsetzung und Evaluierung von UX eine Leerstelle. Dagegen eröffnet ein Sichtbarmachen dieser Aspekte Denkräume für eine gesellschaftspolitisch engagierte Gestaltung von Informationssystemen und vergeschlechtlichten Technikverhältnissen.

User Experiences sind soziomaterielle Phänomene, die sich unter wirklichen, geschichtlichen und kulturell spezifischen gesellschaftlichen Bedingungen und als Teil von konkreten gesellschaftlichen Technikverhältnissen entfalten. Daher ist es zweitens von Bedeutung, wie ein soziomaterielles Konzept wie UX in konkreten Design-Entscheidungen umgesetzt wird. Literatur zu UX bezieht sich oftmals auf eine Liste von Emotionen und affektiven Wirkungen, die eine Interaktion mit einer Anwendung oder einem System auslösen soll. Oft wird auch versucht eine generelle Struktur von emotionalen Erlebnissen zu definieren. Diese Herangehensweisen gehen von verallgemeinerten menschlichen Wahrnehmungen und emotionalen und psychologischen Reaktionen aus. Es ist darüber hinaus aber produktiv, die unterschiedliche Situiertheit von Menschen in gesellschaftlichen Technikverhältnissen einzubeziehen. Emotionen und Affekte folgen keinem Reiz-Reaktionsschema und sind nicht Ausdruck der Interaktionen, die ein System anbietet. Sie sind auf unvorhersehbarere

Doris Allhutter

Doris Allhutter, Mag.a Dr.in, ist Elise-Richter Senior Postdoc am Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften. Sie beschäftigt sich mit der Frage, welche Rolle Ideologien und vergeschlechtlichte Konzepte und Methoden bei der Entwicklung von Informationssystemen spielen.

Weise mit Körpern, Materialitäten und ihren Geschichtlichkeiten verwickelt. Einen Ansatzpunkt bieten hier „long-term UX" Konzepte, die unterschiedliche Zeitlichkeiten und Erinnerungen einbeziehen. Anhand der Geschlechterperspektive zeigt sich in diesem Zusammenhang noch genauer, wie vergangene, gegenwärtige und zukünftige Technikverhältnisse in Nutzer_innen-Erlebnissen ineinanderfließen. Erhebungs- und Umsetzungsmethoden für ein diversitätsorientiertes UX-Design, ebenso wie Evaluierungsmethoden müssen daher geschichtlich gewachsene Orientierungen hin zu bestimmten Objekten und Interaktionen stärker in den Blick nehmen. Ein eventuell zugrunde liegendes Konzept von „Zielgruppen-spezifischem" Design sollte dabei auf Stereotypisierung und geschlechtliche Normierungen hinterfragt werden.

Referenzen

[1] Hassenzahl, M., & Tractinsky, N. (2006). User experience-a research agenda. Behaviour & Information Technology, 25(2), S. 91-97.

[2] Hartson, R., & Pyla, P. S. (2012). The UX Book: Process and guidelines for ensuring a quality user experience. Elsevier.

[3] Hassenzahl, M., Eckoldt, K., Diefenbach, S., Laschke, M., Lenz, E., & Kim, J. (2013). Designing moments of meaning and pleasure. Experience design and happiness. International Journal of Design, 7(3), 21-31.

[4] Pohlmeyer, A. E., & Maschinensysteme, V. U. (2011). Identifying Attribute Importance in Early Product Development. Technische Universität Berlin, Doktorarbeit.

[5] Kujala, S., Vogel, M., Pohlmeyer, A. E., & Obrist, M. (2013, April). Lost in time: the meaning of temporal aspects in user experience. In CHI'13 Extended Abstracts on Human Factors in Computing Systems, 559-564. ACM.

[6] Akrich, M. (1995). User representations: practices, methods and sociology. Managing technology in society. The approach of constructive technology assessment, 167-184.

[7] Rommes, E. (2014). Feminist Interventions in the Design Process. Gender in Science and Technology. Interdisciplinary Approaches, 41-55.

[8] van der Velden, M., & Mörtberg, C. (2012). Between Need and Desire Exploring Strategies for Gendering Design. Science, Technology & Human Values, 37(6), 663-683.

[9] Allhutter, D., & Hofmann, R. (2010). Deconstructive design as an approach for opening trading zones. Thinking Machines in the Philosophy of Computer Science: Concepts and Principles, Hershey: IGI Global, 175-192.

[10] Allhutter, D., & Hofmann, R. (2014). Affektive Materialitäten in Geschlechter-Technikverhältnissen. Handlungs- und theorie-politische Implikationen einer antikategorialen Geschlechteranalyse. Freiburger Zeitschrift für Geschlechterstudien, 20(2), (in Druck).

[11] Desmet, P. M., & Hekkert, P. (2007). Framework of product experience. International Journal of Design, 1(1), 57-66.

[12] Norman, D. A. (2007). Emotional design: Why we love (or hate) everyday things. Basic books.

[13] Barad, K. (2003). Posthumanist performativity: Toward an understanding of how matter comes to matter. Signs, 28(3), 801-831.

[14] Ahmed, S. (2010). Orientations Matter. New Materialisms. Ontology, Agency, and Politics. Duke University Press, 234-257.

[15] Faulkner, W. (2007). Nuts and Bolts and People. Gender-Troubled Engineering Identities. Social studies of science, 37(3), 331-356.

[16] Kozel, S. (2007). Closer: performance, technologies, phenomenology. MIT Press.

[17] Bargetz, B. (2013). Markt der Gefühle, Macht der Gefühle. Österreichische Zeitschrift für Soziologie, 38(2), 203-220.

[18] Allhutter, D. (2014). Vergeschlechtlichte Anwender_innen-Erlebnisse und User Experience als soziomaterielles Konzept. In: Marsden, N./ Kempf, U. (Hg.): Gender-UseIT. HCI, Usability und UX unter Gendergesichtspunkten. München: De Gruyter Oldenbourg, S. 15-25.

Anmerkungen

1 Eine längere Version dieses Beitrags wurde von Nicola Marsden und Ute Kempf in ihrem kürzlich erschienenen Buch „Gender-UseIT. HCI, Usability und UX unter Gendergesichtspunkten" herausgegeben und ist bei De Gruyter Oldenbourg frei zugänglich [18].

2 Gemeint ist die ständig wiederholte Ideologie, dass Männer und Frauen von Natur aus verschieden sind und es eine „weibliche" und „männliche" Identität gibt. Diese Identität lässt sich aber nur in Abgrenzung von dem anderen definieren: in diesem Sinne ist eine Frau „nicht männlich", ohne sagen zu können, was „weiblich" bedeutet.

Leonie Maria Tanczer

Hacking + Aktivismus = Männlich?

Anonymous, LulzSec oder Edward Snowden sind gegenwärtig Bestandteil der medialen Berichterstattung. Sie werden vielfach mit dem Begriff Hacktivismus assoziiert, eine Verschmelzung von Hacking und Aktivismus, die politisch motiviertes Hacking beschreibt[1]. Diese Bezeichnung ist häufig vorurteils- und stereotypenbehaftet, weshalb ich mich im Rahmen meiner Forschung mit der Wahrnehmung befasst habe, alle HacktivistInnen seien junge Männer.

HacktivistInnen verwenden dieselben Techniken wie HackerInnen. Ihre Aktivität und Motivation stützen sich jedoch nicht auf persönliche Ziele oder Interessen, sondern vielmehr darauf, politische oder soziale Veränderungen zu bewirken.[2] Deibert und Rohozinski[3] betonen, dass HacktivistInnen oft innovative Technologien zur Sicherung von Privatsphäre, Umgehung von Filtermechanismen sowie zur Unterstützung von Individuen und sozialen/zivilgesellschaftlichen Bewegungen generieren. Ähnlich zur HackerInnen-Community ist auch unter HacktivistInnen ein Geschlechterungleichgewicht[4] zugunsten der Männer evident sowie ein *Male-Only*-Stereotyp – sprich alle HacktivistInnen seien Männer.

Stereotypisierung ist als Prozess der sozialen Kategorisierung einer Gruppe auf Basis prototypischer Eigenschaften zu verstehen.[5] Zwar entspringen Stereotype einer sozialen Realität und

Es reihen sich vielfältige Stereotype rund um HackerInnen und HacktivistInnen.

sind in einer gesellschaftlichen Wirklichkeit verortet, jedoch wird als Konsequenz eines Stereotyps die gesamte Gruppe als eine homogene Einheit wahrgenommen.[6] Dies hat zur Folge, dass z. B. generalisiert angenommen wird, Frauen könnten nicht Auto fahren, oder Hacktivisten seien immer Männer. Abweichungen von solchen Normen müssen sich gegen diese Annahme behaupten, werden jedoch oft ignoriert. Im Falle von Hacktivismus bleibt daher die Mitwirkung von Frauen unerwähnt und der Gender-Bias wird vor allem sprachlich im Alltag und in den Medien verstärkt.

Auf Basis des genannten Stereotyps hat sich die bisher unveröffentlichte qualitative Studie zum Ziel gesetzt, die Gruppenidentität sowie -aktivität von selbst-definierten HacktivistInnen zu untersuchen. Ein Schwerpunkt wurde dabei auf Konsequenzen des *Male-Only*-Stereotyps gelegt. Die Untersuchung des Zusammenhangs von Gender und politisch motiviertem Hacking lag nahe, da soziale und politische Motive das Engagement von HacktivistInnen vorantreiben und Taylor[7] dem Hacktivismus ein Potenzial zur Minimierung des Gender-Gaps in der Informationstechnologie-Branche (IT) zuschreibt. Für die Studie wurden 2013 Interviews mit fünf weiblichen und fünf männlichen HacktivistInnen durchgeführt und die Daten daraufhin einer Diskursanalyse[8] unterzogen. Aus den Interviews wurden sprachliche Dynamiken extrahiert, die auf das enge Zusammenspiel von Geschlecht und Selbstidentifizierung als HacktivistIn hinweisen. Im folgenden Abschnitt soll nun auf einige der Resultate eingegangen werden, um darauf folgend Zugangshürden für Frauen und mögliche Gegenstrategien zu diskutieren.

Studienergebnisse

Eine zentrale Einsicht, die durch diese Studie gewonnen wurde, ist, dass der *Male-Only*-Stereotyp durch Sprache innerhalb der Interviews perpetuiert wird und die Selbstwahrnehmung der Interviewten beeinflusst. Männliche Hacktivisten sprachen im Zuge der Interviews keine geschlechtsbezogenen Aspekte an. So nutzen sie ausschließlich männliche Pronomen und verglichen sich mit anderen Männern wie etwa Jeremy Hammond oder mit Organisationen. Im Kontrast dazu waren die Interviews mit Hacktivistinnen von geschlechtsbezogenen, feministischen Themen dominiert. Diese Unterdrückung der weiblichen Form bzw. die Inexistenz einer geschlechtsneutralen Formulierung[9] deutet auf eine einseitige, männlich-zentrierte Wahrnehmung von Männern hin und ist mitverantwortlich für die Themensetzung der weiblichen Interviewten. Diese in der Studie als männlicher „Unachtsamkeitsdiskurs" bezeichnete Dynamik offenbart sich weiterhin durch eine um Macht, Militarisierung und Heroisierung kreisende Sprache im Zusammenhang mit ihrem politischen Engagement:

> *"And that's why we are Anonymous – basically we are like ah one… we are like a small kid who is really muscled and so all full of muscles and he does not even know it yet. It's like he is hitting the wall and is then "wow!" I did that. And that's why I think of Anonymous as one kid, who got all this power but does not even know it yet."*

Demgegenüber zeigt sich in den Interviews mit Hacktivistinnen ein Prozess, der als weibliche Gegenstrategie fungiert und in der Studie als „Widerstandsdiskurs" zusammengefasst wird. Der Diskurs hat zwei Ausprägungen. Eine spezifische Form und Resultat der Verdrängung des Weiblichen ist, dass Frauen sich mit dem Stereotyp des männlichen Hackers/Hacktivisten ständig konfrontiert sehen. In den Interviews wird deutlich, dass Hacktivistinnen als Konsequenz dieser gesellschaftlichen Ausblendung sowohl ihre Aktivität als auch ihre Identität als Hacktivistinnen rund um ihre weibliche Identität aufbauten. Daraus folgt, dass sie feministische oder frauenspezifische Themen in ihrer HacktivistInnen-Tätigkeit hervorheben. Die Interviewten sprachen den *Male-Only*-Stereotyp gezielt an und waren entschlossen, sich im Rahmen ihres Hacktivismus gegen Ungleichheiten, Sexismus und Diskriminierung stark zu machen:

> *"I actually pay attention to the women around me. (…). I think that people within, people within power-groups often…are completely ignorant of the activities of the people in the non-power-groups. (…) the men are simply used to play with other men. And all their friends are men. And when they go out and do things – even if there's a woman sitting right next to them – they're oblivious, because they only pay attention to the person who is like them. Ahm and it takes a certain sort of… ahm enlightenment to be able to realise, to be part of a power-group and realise that the people outside your power-group exist (…)."*

Diese verkürzte Zusammenfassung einiger Ergebnisse lässt sich auf eine weitverbreitete gesellschaftliche Dynamik übertragen: Männer müssen sich ihres Geschlechts nicht bewusst sein; Männlichkeit gleicht der Norm. Frauen hingegen, und dies zeigt sich vor allem in männerdominierten Feldern wie Hacktivismus, sind viel eher dazu angehalten, sich mit ihrer geschlechtlichen Identität auseinanderzusetzen, da sie scheinbar von der Norm abweichen. Exemplarisch kann der Prozess so erklärt werden: Während ein Informatiker nie oder zumindest sehr selten seine Männlichkeit im Kontext seiner Identität als Informatiker rechtfertigen muss, wird die Arbeit und Identität einer Informatikerin sehr viel häufiger mit ihrem Geschlecht in Verbindung gebracht. Ist sie überdurchschnittlich gut, ist sie die *beste Frau* in der Bran-

che. Zeigt sie jedoch Schwächen, ist ihr (Nicht-)Können mit ihrem Frausein verbunden. Diese Zusammenhänge wurden daher auch in der hier vorgestellten Studie gefunden.

Zugangshürden für Frauen

Die präsentierten Ergebnisse sind Effekte viel fundamentalerer gesellschaftlicher Ungleichheiten. Obwohl Zugangshürden für Frauen sowie anderer unterrepräsentierter Gruppen in Bezug auf politisch motiviertes Hacken bis dato noch unerforscht sind, kann davon ausgegangen werden, dass ähnliche Barrieren wie in den Forschungen zu STEM (Science, Technology, Engineering, and Mathematics; dt: MINT) von Bedeutung sind.

In Hinblick auf Gender-Stereotypen ist die gesellschaftliche Vorstellung, Männer seien in technischen Belangen besser als Frauen, zentral.[10] Männern und Frauen werden dabei unterschiedliche Persönlichkeitsmerkmale zugeschrieben, die auch mit geschlechtsspezifischen Rollenbildern einhergehen. Durch die Annahme, dass Männer z. B. besser in Mathematik seien, wird eine selbsterfüllende Prophezeiung vorangetrieben. Spence, Helmreich, und Stapp[11] zeigen dies anhand ihrer Studie zu Vorstellungen über Männlichkeit und Weiblichkeit. Männer sollen demzufolge wetteifernd, dominant und handlungsfähig, Frauen dagegen liebevoll, sensibel und warmherzig sein. Darauf aufbauend zeigen jüngste Untersuchungen, dass Frauen in männlichen Berufssparten oft vorgeworfen wird, traditionelle Rollenbilder zu verletzen. Interessanterweise werden diese Frauen bei Umfragen dann von Männern und Frauen gleichermaßen mit Feindseligkeit und geringer Sympathie bewertet.[12] Aspekte wie diese erschweren es Frauen, in diesen Branchen Fuß zu fassen und Wertschätzung zu erhalten.

Die Problematik wird zusätzlich durch den sogenannten *Stereotype Threat* vergrößert. Dieser bezeichnet die Sorge eines einem gewissen Stereotyp unterliegenden Menschen, genau diesen negativen Stereotyp zu erfüllen. Das Wissen um diesen Stereotyp hat hierbei zur Konsequenz, dass die Leistung der/des Betroffenen beeinflusst wird.[13] Studien zeigen, wie der *Stereotype Threat* somit auch negative Effekte für die eigene berufliche Laufbahn zur Folge haben kann. Einsichten wie diese scheinen legitim, berücksichtigt man, dass Frauen in entsprechenden Studien vermehrt negative Haltungen gegenüber Mathematik artikulieren,[14] sowie zusätzlich Belege dieses Gender-Bias im Rahmen von *Computer Self-Efficacy*- sowie *Computer-Anxiety*-Tests[15] zu finden sind.

Im Kontext der hier vorgestellten Hacktivismus-Studie scheinen ebensolche Mechanismen eine Rolle zu spielen. Sie werden durch die Konnotation von *Hacking* als männliche Domäne[16] weiter erhöht. Zwar hatten alle weiblichen Interviewten ein hohes Maß an technischem Know-How, doch unterlagen sie genau solchen Ausgrenzungen:

> *"If we work with men – and maybe they are our boyfriends or something – you know – ahm other people don't see our contributions as legitimate. So, I am doing something, I am being an activist and my male boyfriend is doing it too – for example – then really he is the real one, and I am just helping. – In other people's minds. In other people's minds they don't see me as having agency,… because of my gender."*

Die Barrieren sind also facettenreich und häufig subtil. Es spielt deshalb nicht nur eine Rolle, dass Frauen sich selbst nicht als ausreichend befähigt sehen, sondern dass gesellschaftliche Zwänge Frauen die Fähigkeit abschreiben, gut in technischen Belangen zu sein.

Gegenstrategien

Trotz der erwähnten Zugangshürden finden sich vermehrt Studien, die darauf hindeuten, dass sich der Gender-Gap z. B. durch die steigende Häufigkeit der Computer-Verwendung schließt.[17] Gezielte Förderung und Sensibilisierung scheinen somit erste Früchte zu tragen. Es bedarf jedoch weiterer Bemühungen, die Rollenbilder, Diskriminierungen und Ausgrenzungen sowie geschlechtliche Sozialisierungen zu minimieren.

Das Wissen um z. B. den *Saying-Is-Repeating*-Effekt[18], dass also Stereotype durch Kommunikation sowohl entstehen als auch beibehalten werden, ist deshalb zentral. Alltagssprache, aber auch die mediale Berichterstattung haben einen wesentlichen Einfluss auf unsere Vorstellungen und Realitätswahrnehmungen. Deshalb kann angenommen werden, dass durch das Sichtbarmachen von Frauen und anderen unterrepräsentierten Gruppen ein Umdenken herbeigeführt wird. Die öffentliche Repräsentation von Frauen als HacktivistInnen mag daher von Bedeutung sein. Hier ist aber darauf zu achten, dass dieses Sichtbarmachen nicht in Alibiaktionen endet. Frauen sollen zu keinen „*Token*", sprich Vorzeigefrauen werden, denen in Folge alle Hacktivistinnen gerecht werden müssen.[19]

Daneben ist es wichtig, Frauen überhaupt den Schritt in den Hacktivismus oder in die IT-Branche zu ermöglichen. Dazu bedarf es grundlegenderer Änderungen, die im frühsten Kindesalter beginnen müssen. Mädchen, genauso wie Jungen, sollten verstärkt dazu angehalten werden sich mit Technik auseinanderzusetzen. Dafür ist sowohl die Unterstützung der Erziehungsberechtigten, des Bildungssystems als auch der Werbeindus-

Leonie Maria Tanczer

Leonie Maria Tanczer ist Doktorandin an der School of Politics, International Studies and Philosophy, Queen's University Belfast und Fellow am Alexander von Humboldt Institut für Internet und Gesellschaft in Berlin. Ihre Arbeitsschwerpunkte sind u. a. Gender Studies, Online Collective Action und Internet Governance. Sie twittert unter @leotanczt und steht für Rückfragen zur Verfügung.

trie vonnöten. Geschlechterstereotypes Spielzeug und Vorbilder in Filmen oder Büchern täuschen Mädchen und Jungen unterschiedliche Interessen und Fähigkeiten vor. Diese sind jedoch viel mehr anerzogen denn angeboren. Gefragt ist deshalb ein allumfassendes gesellschaftliches Umdenken, das nicht zuletzt den gegenwärtigen und zukünftigen HacktivstInnen eine Stütze sein kann.

Anmerkungen

1 *Jordan, T. (2002). Activism!: Direct action, hactivism and the future of society. London: Reaktion Books Ltd.*

2 *Milone, M. G. (2002). Hacktivism: Securing the national infratructure. The Business Lawyer, 58(1), 383-413.*

3 *Deibert, R. J., & Rohozinski, R. (2008). Good for liberty, bad for security? Global civil society and the securitization of the internet. In R. J. Deibert, J. Palfrey, R. Rohozinski & J. Zittrain (Eds.), Access denied: The practice and policy of global internet filtering (pp. 123-149). Cambridge: MIT Press.*

4 *Taylor, P. A. (2005). From hackers to hacktivists: Speed bumps on the global superhighway? New Media & Society, 7(5), 625-646.*

5 *Ashmore, R. D., & Del Boca, F. K. (1981). Conceptual approaches to stereotypes and stereotyping. In D. L. Hamilton (Ed.), Cognitive process in stereotyping and intergroup behavior (pp. 1-35). Hillsdale: Erlbaum.*

6 *Hoffman, C., & Hurst, N. (1990). Gender stereotypes: Perception or rationalization? Journal of Personality and Social Psychology, 58(2), 197-208.*

7 *Taylor, P. A. (2003). Maestros or misogynists? Gender and the social construction of hacking. In Y. Jewkes (Ed.), Dot. cons: Crime, deviance and identity on the internet (pp. 126-146). Cullomptom: Willan.*

8 *Taylor, P. A. (2003). Maestros or misogynists? Gender and the social construction of hacking. In Y. Jewkes (Ed.), Dot. cons: Crime, deviance and identity on the internet (pp. 126-146). Cullomptom: Willan.*

9 *Pusch, L. F. (1984). Das Deutsche als Männersprache. Frankfurt am Main: Suhrkamp Verlag.*

10 *Moorman, P., & Johnson, E. (2003). Still a stranger here: Attitudes among secondary school students towards computer science. Paper presented at the 8th Annual SIGCSE Conference on Innovation and Technology in Computer Science Education, Thessaloniki, 35(3) 193-197.*

11 *Spence, J. T., Helmreich, R., & Stapp, J. (1975). Ratings of self and peers on sex role attributes and their relation to self-esteem and conceptions of masculinity and femininity. Journal of Personality and Social Psychology, 32(1), 29-39.*

12 *Lawson, K. M., & Lips, H. M. (2014). The role of self-perceived agency and job attainability in women's impressions of successful women in masculine occupations. Journal of Applied Social Psychology, 44(6), 433-441.*

13 *Lawson, K. M., & Lips, H. M. (2014). The role of self-perceived agency and job attainability in women's impressions of successful women in masculine occupations. Journal of Applied Social Psychology, 44(6), 433-441.*

14 *Steele, J. R., & Ambady, N. (2006). "Math is hard!" The effect of gender priming on women's attitudes. Journal of Experimental Social Psychology, 42(4), 428-436.*

15 *Steele, J. R., & Ambady, N. (2006). "Math is hard!" The effect of gender priming on women's attitudes. Journal of Experimental Social Psychology, 42(4), 428-436.*

16 *Turkle, S. (1984). The second self: Computers and the human spirit. London: Granada.*

17 *Imhof, M., Vollmeyer, R., & Beierlein, C. (2007). Computer use and the gender gap: The issue of access, use, motivation, and performance. Computers in Human Behavior, 23(6), 2823-2837.*

18 *Bratanova, B., & Kashima, Y. (2014). The "Saying is repeating" effect: Dyadic communication can generate cultural stereotypes. The Journal of Social Psychology,154(2), 155-174.*

19 *Kanter, R. M. (1977). Some effects of proportions on group life: Skewed sex ratios and responses to token women. American Journal of Sociology, 82(1), 965-990.*

Sylvia Pritsch

Zur sexistischen Gewalt im Netz

Sexismus als alltägliche Erfahrung scheint inzwischen im Mainstream-Bewusstsein angekommen, nicht zuletzt dank der #Aufschrei-*Kampagne, die sich 2013 über den Netzdienst Twitter formierte und rasant verbreitete. Mit dieser Diskussion über alltäglichen Sexismus, die durch einen Zeitungsbericht ausgelöst und innerhalb und außerhalb des Netzes weitergeführt wurde, fanden mediale Grenzüberschreitungen statt, die als „Brückenschlag zwischen digitalem Resonanzraum und arrondierenden publizistischen Leistungen" im Sinne einer „neuen, verzahnten On- und Offline-Debattenkultur" gewürdigt wurden.*[1]

Weniger prominent, aber mit zunehmender öffentlicher Resonanz setzte sich ebenfalls die Einsicht durch, dass auch das Netz kein *post-gender*-Raum ist, sondern entsprechend anderen sozialen Räumen sexistische, rassistische und andere diskriminierende Strukturen aufweist.[2] Diese Erkenntnis ist keineswegs neu, allerdings hat es eine Weile gedauert, bis entsprechende Phänomene nicht nur als lästig, sondern als sexistisch und tatsächlich gewaltförmig in einer breiteren Öffentlichkeit thematisierbar waren. Verbunden mit einem persistenten Netz-Mythos eines weitgehend eigenständigen (*virtuellen*) Raums *freier* Kommunikationsmöglichkeiten gab es dafür eine Reihe von Gründen, von denen einige kurz skizziert werden sollen. Als Ausgangspunkt dient hier die Szenerie der Troll-Attacken während der Bloggermesse *Re:publica* im April 2010 und die Reaktionen darauf, die einige Dilemmata im Umgang mit Sexismus im Netz verdeutlichen sollen. Einschneidend war dieses Ereignis weniger aufgrund der Tatsache, dass sich solche Angriffe gegen feministische Akteur_innen richteten – Susan Herring et al. beschrieben dies bereits für die ersten feministischen Newsgroups des USENET Mitte der 90er Jahre – sondern vielmehr wegen der relativ hohen Öffentlichkeit für das Thema, die Netz-Aktivistinnen in der Folge bewirkt haben.[3]

1 Trollen und/als Sexismus

Eine deutliche Demonstration, wie unerwünscht bzw. unmöglich die Thematisierung von Sexismus im Netz war (und immer noch ist), lieferten Spam-Attacken anlässlich einer per Video Livestream übertragenen Podiumsdiskussion der Messe unter dem Titel *Das andere Geschlecht – Sexismus im Netz*.[4] Binnen kürzester Zeit kam es zur Blockierung des Chats durch eine Vielzahl von sinnlosen bis beleidigenden, sexistischen, rassistischen, insgesamt die Veranstaltung, Feministinnen bzw. Frauen* diffamierenden Beiträgen. Erschwert wurde die Bewertung und damit der Umgang mit diesen Äußerungen dadurch, dass ihr Status zunächst im Unklaren blieb: Handelt es sich bei diesen Attacken um einen „der besten Beweise für den real existierenden Sexismus – gegen Frauen! – im Internet", wie das *Piratenweib* im gleichnamigen Blog titelte, oder „nur" um Trollbeiträge, von denen auch andere betroffen sind?[5] Sollten diese Äußerungen mitsamt ihren beleidigenden und verletzenden Wirkungen überhaupt ernst genommen werden? Darüber wurde auch in den Blog-Kommentaren gestritten: *„[...] Das ist Pöbelei, im Netz auch gerne Trollerei genannt. Wichtig ist nur das Krakeelen gegen die Werte der Mehrheit. [...] Die einzige Überzeugung ist die Provokation, gemessen in Follow-Ups. Das ist armselig, aber nicht sexistisch."*[6]

Die Beantwortung der Frage, ob es sich um destruktive und verletzende Sprechhandlungen handelt, die als Sexismus identifiziert und geahndet werden müssten, oder aber um Provokationen, die ignoriert werden sollten, wurde erschwert durch die im Netz verbreitete Maxime *„don't feed the troll"*. Was als Schutz vor Spam-Attacken gedacht war, nämlich einen möglichst baldigen Abbruch von als Provokation gewerteten Äußerungen durch das Ignorieren derselben zu erreichen, erwies sich allzu oft als nachteilig für die entsprechend adressierten Personen, die sich mit einer Flut verletzender Angriffe bis hin zu Bedrohungen allein gelassen sahen und sich nicht selten aus öffentlichen Diskussionen zurückzogen. Die genannte Empfehlung richtete die Aufmerksamkeit auf individuelles Verhalten, nicht auf die strukturelle Dimension der Angriffe. Dass Beiträge von Frauen*, v.a. mit feministischen und anderen politischen Themen, verstärkt Angriffspunkte für verletzende Äußerungen sind, war eine grundlegende Erfahrung beispielsweise von Bloggerinnen[7] – öffentlich anerkannt war es nicht.

2 Enttabuisierungs-Strategien

Genau hier setzten im Folgenden die Strategien an, nämlich mit der Dokumentation und Benennung der Rede als sexistisch. Unmittelbar nach den als *shitstorm* titulierten Angriffen im Kontext der *Re:publica*-Veranstaltung wurden sie auf dem Blog *Piratenweib* veröffentlicht, mit dem Effekt, dass sich die Angriffe zum Teil wortwörtlich wiederholten. In der Auseinandersetzung damit wurde ein weiteres Dilemma sichtbar, nämlich inwieweit solchen Attacken durch Sperrung der Kommentarfunktion bzw. durch Selektion der Beiträge beizukommen wäre, ohne jedoch Vorwürfe zu bestätigen, „Zensur" ausüben zu wollen. Herring et. al. nannten einen ideologischen Konflikt als einen zentralen Grund dafür, weshalb das Unterbinden von Trollbeiträgen speziell einem feministischen Forum schwer fiele.[8] Sie führten dies auf ein „liberal-libertäres Ethos" von Internet-Foren zurück, das die freie Meinungsäußerung als höchstes Gut setzt und Konflikte innerhalb der Diskussionsgruppe lösen will. Dieses Ethos stehe in einem widersprüchlichen Verhältnis zum feministischen Anspruch, einen geschützten Raum anzubieten, in dem alle das Wort ergreifen könnten, ohne dafür aufgrund ihres Geschlechts persönlich angegriffen zu werden. Troller seien nun häufig die Gewinner, indem sie diese Spannung ausnutzten, sei es, weil die Vertreterinnen einer offenen Debatte sich durchsetzen, wodurch die Troller in ihrem Tun fortfahren könnten, oder sei es durch die Denunziation von Sperrungen bestimmter Nutzer als Zensur, wodurch ein beliebter Generalvorwurf – *„Feministinnnen sind intolerant"* – bestätigt würde. Das *Piratenweib* entschied sich letztlich für einen Mittelweg: Die ersten Kommentare, etwa ein Drittel aller Einträge, wurden unzensiert freigeschaltet, die restlichen gefiltert.

In der weiteren Auseinandersetzung konnte diese Verunsicherung jedoch überwunden werden und es galt, sexistische Äußerungen als solche zu benennen und zu veröffentlichen, was auf verschiedenen Seiten geschah.[9] Die Alternative, verletzende Äußerungen als Sexismus *oder* Trollen einzuordnen, wurde als unproduktiv und verharmlosend erkannt.[10] Letztlich lassen sich, wie bereits Herring et. al beschrieben, Trollbeiträge und sexistische Attacken allgemeiner Art oder aus maskulistischem Umfeld nicht wirklich unterscheiden.

3 Gewalt der Adressierung

Inzwischen wird zunehmend sexistische Rede als verletzend klassifiziert und als eine Form von Gewalt thematisiert. Unter einer sprachtheoretischen Perspektive wird eine spezifische Verletzbarkeit im Netz sichtbar, die sich im Akt der *Adressierung* zeigt:[11] Die Adresse, die generell der Identifizierung und Individualisierung einer Person dient, fächert sich im Netz auf. Als Erkennungs- bzw. Lokalisierungsmerkmal innerhalb des digitalen Raumes fungieren an der Benutzeroberfläche die weltweit einmaligen Domain- oder E-Mail-Adressen. Donna Haraway bezeichnete E-Mail-Adressen als machtvolle Technologien *„through which identities ebb and flow in the net of technoscience"*.[12] Für die Etablierung einer Internet-Identität ist die Wiedererkennbarkeit

Sylvia Pritsch

Dr. **Sylvia Pritsch** ist Literatur- u. Kulturwissenschaftlerin. Aktuell ist sie als wissenschaftliche Mitarbeiterin am Zentrum für interdisziplinäre Frauen- und Geschlechterforschung der Universität Oldenburg tätig.

über den Namen elementar – nicht nur für eine individuelle Erreichbarkeit, sondern auch für eine Positionierung an den Aufmerksamkeitsmärkten des Internets. Andererseits sind mit diesen Internet-Identitäten nicht immer Personen außerhalb der Online-Welt identifizierbar, zumindest kann auf der Benutzeroberfläche oder über Verschlüsselungstechnologien eine anonymisierte Distanz bewahrt werden. Die gewählten Namen weisen also nicht direkt auf die Klarnamen der Absender zurück, die in einem nicht-öffentlichen Raum verbleiben können. An diesem Verhältnis von *privatem* und *öffentlichem* Namen setzen die beschriebenen Diffamierungs-Strategien an. Sie polarisieren dieses Verhältnis, indem sie selbst aus einer Anonymität heraus, die in diesem Fall als ein geschützter Ort in der Wirrnis der Internet-Öffentlichkeit erscheint, die Klarnamen anderer preisgeben und damit öffentlich zugänglich machen oder den Angegriffenen – wie beim zum Stalking – zu verstehen geben, dass sie die Grenzen ihrer Privatsphäre nicht einzuhalten gedenken. Die Botschaft, die hier übermittelt wird, ist eine doppelte: Die Warnung, die zur Drohung werden kann, lautet „*Du bist lokalisierbar*" (und damit angreifbar, z. B. durch Spamattacken oder Stalking). Damit wird ebenfalls suggeriert: „*Du hast keine Kontrolle über Deinen Namen/Deine Adresse*", die zu einem öffentlichen Ort gemacht oder entwendet werden können. In dieser Adressierung lässt sich die Gewaltförmigkeit der Ansprache in zugespitzter Form ablesen, insofern sie zeigt, dass die verletzende Rede den anderen zwar einen sozialen Ort zugesteht, nicht aber die Verfügungsgewalt über die Verortung im *privaten* bzw. *öffentlichen* Raum.

Eine Reaktion war daher auch, den Spieß umzukehren, indem die Aufdeckung von Klarnamen gefordert wurde.[13] Auch Verbote und Ausschlüsse waren in der Diskussion. Diese bieten zwar, insbesondere, wenn sie strafrechtlich verankert sind, eine rechtliche Handhabe für den Umgang mit Beleidigungen, Morddrohungen, Stalking. Allerdings, darauf wies Sibylle Krämer hin, ist ein verrechtlichter Begriff von Gewalt stets mit der Aporie verbunden, dass diejenigen Mittel, die Gewalt einschränken sollen, „*letztlich Formen von Gewalt zuarbeiten, sie verstärken, mithin soziale und politische Kontrolle verfestigen und persönliche Freiheiten einschränken*".[14] Auch wenn solche Maßnahmen u.U. zum Schutz Einzelner ergriffen werden, eine Lösung für das Problem struktureller Diskriminierung bieten sie erstmal nicht. Dass Beiträge von Frauen*, insbesondere mit geschlechterpolitischen Inhalten, eine besondere Verletzbarkeit aufweisen, hatten Herring et. al. bereits für die 90er Jahre konstatiert. Positionen, die dort vertreten werden, würden vom Mainstream stigmatisiert bzw. diskriminiert. Zudem gälten Frauen generell als schwächer, so dass sie ein attraktives Ziel für Troll-Attacken darstellten.[15] Das heißt also in der Konsequenz, öffentliche Äußerungen nicht nur von Feministinnen, sondern von Frauen* allgemein erscheinen als sanktionierter Ort, als kultureller Topos, für diskriminierende, diffamierende, verletzende Rede.

Dies erkannt und in eine netzübergreifende Öffentlichkeit getragen zu haben, so dass „*Netzpolitik und Politik im ‚richtigen' Leben keine getrennten Sphären (mehr) [sind]*",[16] ist das Verdienst von feministischen Netz-Communities, die sich seit 2011 in verschiedenen Formen entwickelt und neu gegründet haben.[17] Weit über die #*Aufschrei*-Kampagne hinaus ist Sexismus auch für digitale Räume von sozialen Netzwerken über Blogs und Twitter bis hin zu selektiven Suchmaschinen-Ergebnissen heute medienübergreifend ein Thema.

Anmerkungen

1 So die Begründung für die Verleihung des Grimme Online Awards („Spezial") 2013, www.grimme-institut.de/html/index.php?d=1667#c10914 (abgerufen 10.07.2014).

2 Bereits zwei Jahre zuvor hatte eine Umfrage der Bremer Frauenseiten unter 500 Internet-Nutzerinnen ergeben, dass sich etwa die Hälfte von sexistischen und beleidigenden Äußerungen belästigt fühlt (http://frauenseiten.bremen.de/gefaellt_uns_nicht/internet---ist-doch-nur-spass-23584654, zuletzt aufgerufen 10.07.2014).

3 Herring, Susan/ Job-Sluder, Kirk/ Scheckler Rebecca/ Barab; Sasha (2002): Searching for Safety Online: Managing "Trolling" in a Feminist Forum. In: The Information Society: An International Journal. Jg. 18, H. 5, S. 371 – 384.

4 Die Podiumssdiskussion mit Anne Roth, Anna Berg, Klaus Schönberger ist archiviert unter http://www.youtube.com/watch?v=-3LKBARD10E; zur Reaktion vgl. u. a. die Diskussion auf www.maedchenmannschaft.de; www.annalist.de.

5 Piratenweib (15.04.2010): „re:publica – se:xisticum … oder warum ein Livestream mit parallelem Chat einer der besten Beweise für den real existierenden Sexismus – gegen Frauen! – im Internet ist", mit anschließenden Kommentaren (http://www.piratenweib.de/republica-sexisticum) [10.02.2011] – im Folgenden zitiert unter „PW".

6 PW: vorbeisurfer, 2010, 16.4. 11:46.

7 Vgl. Tabler, Nele (10.2.2010): „Gewalt gegen bloggende Frauen" (http://www.karnele.de/gewalt-gegen-bloggende-frauen/) [10.02.2011].

8 Herring et.al. 2002, a.a.O., S. 374.

9 Zur Strategie der Monetarisierung bei hatr.org u. a. vgl. Schmidt, Francesca: Trolljaner im Netz – Wie ist Sexismus, Rassismus und Homophobie beizukommen?, in: Digitale Intimität, die Privatsphäre und das Netz – #public_life, hg. v. Heinrich-Böll-Stiftung, Berlin 2011 [http://www.gwi-boell.de/de/2011/04/27/trolljaner-im-netz-wie-ist-sexismus-rassismus-und-homophobie-beizukommen; abgerufen 10.07.2014].

10 Vgl. etwa den Blog-Beitrag „Troll oder Sexismus? von Katrin Rönicke, 06.12.201 [http://blog.katrin-roenicke.net/?p=565; abgerufen 07.07.2014].

11 Siehe hierzu genauer Pritsch, Sylvia: Verletzbarkeit im Netz – Zur sexistischen Rhetorik des Trollens, in: Feministische Studien, Jg. 29, Nr. 2 2011, S. 232-247.

12 Haraway, Donna: Modest_Witness@Second_Millenium.FemaleMan©_Meets_ OncoMouseTM. London/NewYork 1997, S. 4.

13 Vgl. Rönicke, a.a.O.

14 Krämer, Sibylle (2010): ‚Humane Dimensionen' sprachlicher Gewalt oder: Warum symbolische und körperliche Gewalt wohl zu unterscheiden sind, in: dies./Koch, Elke (Hrsg.): Gewalt in der Sprache. Rhetoriken verletzenden Sprechens. München, 21-44, S. 27). Zur rechtlichen Diskussion um das Verhältnis von Privatheit/ Öffentlichkeit siehe Ganz, Kathrin: Feministische Netzpolitik. Perspektiven und Handlungsfelder (i. Auftrag d. Gunda-Werner-Institut) Berlin 2014, 13ff [http://www.gwi- abboell.de/sites/default/files/uploads/2013/04/ganz_feministische_netzpolitik_web.pdf; abgerufen 05.07.2014].

15 Herring et.al. 2002, a.a.O., S. 373.

16 Reimann, Bärbel: Sexismus gibt es im Netz – Gegenstrategien aber auch, frauenseiten.bremen.de 22.11.2011 [http://frauenseiten.bremen.de/gefaellt_uns_nicht/sexismus-gibt-es-im-netz---gegenstrategien-aber-auch-23679412; abgerufen 10.07.2014].

17 Vgl. die Überblicke in „Jahresrückblick Netzpolitik" für die Jahre 2011-13/14, hg. v. iRights.Lab, irights-media.de/webbooks/dasnetz.

Stefan Hügel

Weltweite Ausspähung der Bevölkerung: Rechtliche Bewertung und Handlungsoptionen

Zum dritten Mal wurde am 20. und 21. Juni 2014 in Rastatt das Gustav-Heinemann-Forum ausgerichtet, in dem sich die Humanistische Union den Defiziten unserer Verfassungsordnung widmet – seien sie national, europäisch oder international bedingt. In diesem Jahr befasste sich das Gustav-Heinemann-Forum mit einer besonders gravierenden Verletzung der freiheitlichen Verfassungsordnung: der von US-amerikanischen, europäischen und deutschen Geheimdiensten und weiteren Behörden seit dem zweiten Weltkrieg betriebenen Ausspähung und Überwachung der Bevölkerung.

In einer der drei Sessions war das FIfF umfassend vertreten: *Instrumente und Konsequenzen: Was ist heute technisch möglich? Worin besteht die Bedrohung? Ist die Technik heute noch demokratisch beherrschbar?* Die Praxis der Überwachung wird nicht nur von den (rechts-)politischen Vorgaben, sondern auch von der Entwicklung der Kommunikationstechnik geprägt. Mit den heutigen Möglichkeiten digitaler, vernetzter Kommunikation sind auch neue Möglichkeiten der Überwachung entstanden. Verstärkt wird dieser Trend dadurch, dass Menschen das Internet und seine Dienste jeden Tag nutzen – vielen ist es inzwischen zu einer Form von Lebenswelt geworden.

Damit stellt sich die Frage nach dem Grundrechtsschutz im Internet. In dem Panel sollten die technischen Möglichkeiten der Überwachung im Rahmen der technischen Entwicklung und ihre Auswirkungen auf die verfassungsmäßigen Rechte ausgelotet werden. Es ging dabei um Veränderungen wie vernetzte Datenbanken mit den Möglichkeiten der Verknüpfung, Datenanalysetechniken, die unter dem Stichwort *Big Data* diskutiert werden, Sensoren, die im „Internet der Dinge" allgegenwärtig sind, die heute praktisch unbegrenzte Speicherkapazität und die Automatisierung von Abläufen und damit weitere Datenbanken, -speicher und Zugriffsmöglichkeiten.

Beispiele dafür sind Datenspeicher für Sozial- und Gesundheitsdaten, wie z. B. bei der elektronischen Gesundheitskarte oder der Erhebung von Sozialdaten, Smart Meter zur exakten Ermittlung des Energieverbrauchs, Datenspeicher für die Strafverfolgung wie bei der Vorratsdatenspeicherung oder Datenzugriffe wie bei der Bestandsdatenauskunft, Nachrichtendienstliche Datenauswertung, wie z. B. bei PRISM, Tempora, XKeyScore oder wirtschaftlich genutzte Daten, z. B. in sozialen Netzwerken oder bei Internet-Suchmaschinen.

Die Diskussion führten *Stefan Hügel* als Moderator, *Sylvia Johnigk*, die die technischen Möglichkeiten der Überwachung und die Konsequenzen daraus betrachtete und *Dietrich Meyer-Ebrecht*, der die Möglichkeiten – und vor allem die Hindernisse – untersuchte, Technik demokratisch zu gestalten und zu kontrollieren. Die Diskussion sollte sich an folgenden Leitfragen orientieren:

- Welchen Umfang und welche Überwachungstiefe erlauben die heutigen technischen Möglichkeiten der Kommunikationsüberwachung?

- Inwieweit werden Menschenrechte durch die Technik gefährdet? Welchen Einfluss hat die technische Entwicklung der Überwachungsmöglichkeiten auf die Freiheitsrechte der Betroffenen? Welche Folgen für Demokratie und Freiheit ergeben sich daraus? Welche politische Bedeutung hat der Schutz der Privatsphäre?

- Welche Anforderungen an die Technikgestaltung ergeben sich aus den grundrechtlich verbürgten Freiheitsgarantien? Insbesondere: Wie weit muss die Auswahl und der Einsatz legitimer Überwachungstechniken für die Öffentlichkeit transparent gemacht werden? Wie kann eine menschenrechtskonforme Nutzung der Technik überprüft und sichergestellt werden?

Sylvia Johnigk fragte in ihrem Referat nach dem Überwachungspotenzial der heutigen Kommunikationstechnik. Genutzt wird von Geheimdiensten und Militär die Verpflichtung von Anbietern zur *lawful Interception* und die weitergehende Kollaborationsbereitschaft von Unternehmen – damit haben sie weitgehenden Zugriff auf die Informations- und Kommunikationstechnik und können Online-Dienste zur flächendeckenden Überwachung nutzen. Geschwächt werden sie, wenn Nutzer-

innen und Nutzer sicher kommunizieren und dazu beispielsweise Kryptoprodukte nutzen.

Für geheimdienstliche Operationen stehen eine Reihe von Methoden und Werkzeugen zur Verfügung:

- die Kompromittierung von Geräten und Infrastruktur, z. B. indem Rechner online mit Schadsoftware verseucht oder Botnetze zur Überwachung aufgebaut werden,
- der Einbau zusätzlicher „Features" in Produkten, z. B. indem bestellte Geräte auf dem Postweg abgefangen und mit Überwachungstechnik ausgestattet werden,
- Desinformation und Propaganda, indem Informationen verfälscht und Aktivisten und Kritiker diskreditiert werden.

Sylvia Johnigk kritisierte in diesem Zusammenhang die Bundesregierung und weitere Exekutivorgane. Durch mangelnde Aufklärung, Kooperation mit der NSA und Befürwortung massenhafter und flächendeckender Ausspähung leisteten sie Beihilfe zu geheimdienstlichen Aktionen, die gegen internationale Menschenrechte und die deutsche Verfassung verstießen. Dies führe zu einer Reihe von Bedrohungen für Zivilgesellschaft und Demokratie: Kommunikation ist nicht mehr vertraulich und unbeobachtet, Geräte sind nicht mehr vertrauenswürdig und Internetdienste können nicht mehr unbeobachtet genutzt werden. Die informationelle Selbstbestimmung ist verletzt, keine freie demokratische Willensbildung mehr möglich.

Weitere Details sind in dem ausführlichen Beitrag von Sylvia Johnigk ab Seite 58 nachzulesen.

Dietrich Meyer-Ebrecht stellte in seinem Referat fest, dass sowohl der Staat als auch die Bürgerinnen und Bürger bei der Abwehr der Ausspähung gefordert sind. Notwendig ist der politische Wille der Verantwortlichen, den Schutz vor Ausspähung und Überwachung durchzusetzen. Dazu ist gesellschaftlicher Druck notwendig, um die Politik zu den notwendigen Entscheidungen zu bringen.

Drei Faktoren sind dafür maßgeblich:

1. Die Innen- und außenpolitische Dimension: Die Ausspähung ist ein wesentliches Element des Cyberwarfare – will die Regierung dem Schutzauftrag gegenüber ihren Bürgerinnen und Bürgern nachkommen, müsste sie die Befugnisse der Nachrichtendienste einschränken und bereit sein, die transatlantischen Beziehungen hintanzustellen – angesichts internationaler Abkommen ein schwieriges Unterfangen.
2. Die gesellschaftliche Dimension: Auch die Gesellschaft wird lieb gewonnene Verhaltensmuster und wirtschaftliche Interessen aufgeben müssen. Der Gesetzgeber kann uns nicht schützen, wenn wir legislative Schutzmaßnahmen durch leichtfertigen Umgang mit unseren Daten unterlaufen, weil wir auf Komfort oder wirtschaftlichen Gewinn nicht verzichten wollen.
3. Die psychologische Dimension: Die Überwachung ist *counterintuitive* – wir können es uns nicht vorstellen, dass aus der Masse an Daten ausgerechnet „unsere" herausgefischt werden. Dabei ist das Gegenteil der Fall – je größer die analysierten Datenmengen, desto größer die Wahrscheinlichkeit, dass vorgegebene Muster in den Daten – auch unseren – gefunden werden.

Sylvia Johnigk, Stefan Hügel und Dietrich Meyer-Ebrecht
Foto: Sven Lüders

Fazit ist, dass wir uns der Gefahren aus der Datenverarbeitung bewusst werden und daraus die Voraussetzungen schaffen, politischen Druck aufzubauen. Dies ist ein langwieriger Prozess – der erste Schritt ist, zum Selbstschutz zu greifen, z. B. durch Nutzung sicherer Kommunikationsmethoden und Verschlüsselung. Wir müssen uns bewusst machen, dass wir uns damit ein Stück Freiheit zurückerobern.

Der vollständige Beitrag von Dietrich Meyer-Ebrecht ist ab Seite 60 nachzulesen.

Weitere Sessions konzentrierten sich auf verfassungsrechtliche Fragen der Ausspähung: *Ausspähung in Lichte des Grundgesetzes – kann die nationale Verfassung Freiheit und Menschenrechte noch effektiv schützen?* und die Handlungsmöglichkeiten: *Was sind unsere Handlungsoptionen, um Demokratie und Freiheit effektiv zu schützen?* Die Zeitschrift **vor***gänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik* wird in ihrer Ausgabe 206/207 ausführlich darüber berichten.

Im Rahmen des Verbandstags der Humanistischen Union wurde am gleichen Abend der Fritz-Bauer-Preis an Edward Snowden verliehen. Mit dem Fritz-Bauer-Preis würdigt die Humanistische Union herausragende Verdienste um die Humanisierung, Liberalisierung und Demokratisierung der Rechtsordnung. Der Preis ist benannt nach dem früheren Hessischen Generalstaatsanwalt *Fritz Bauer*, der als Wegbereiter einer juristischen Aufarbeitung des NS-Unrechts und Reformer des Strafrechts wie des Strafvollzuges gilt.

> *„Edward Snowden steht für eine außergewöhnliche Zivilcourage bei der Aufdeckung grund- und menschenrechtswidriger Überwachungspraktiken. Gemeinsam mit anderen Engagierten enthüllte er, in welchem Ausmaß die geheimdienstliche Überwachungspraxis heute rechtliche Schranken, die Grenzen des Vorstellbaren sowie des moralisch Vertretbaren überschreitet",*

begründete der Bundesvorsitzende der Humanistischen Union, *Werner Koep-Kerstin*, die Vergabe des Preises.

Snowden, der aus bekannten Gründen den Preis nicht persönlich entgegen nehmen konnte, dankte für die Verleihung mit einer Grußbotschaft aus Moskau, in der er unter anderem ausführte:

> *„What we have, as a public, accomplished in one year is to reveal to the world the reality of new restrictions on our rights, on our freedom to speak and associate, even to think and to be. But more critically, we revealed that it is not we the people who changed, but our policies, and that this occured in secret, without neither public consent nor debate. This clandestine movement of government away from the participatory state toward one that is closed and technocratic, I think, cannot survive the light thrust upon it. We say, ‚Always a citizen, never a subject.'"*

Die vollständige Botschaft und weitere Informationen zur Verleihung des Fritz-Bauer-Preises sind auf den Internet-Seiten der Humanistischen Union zu finden.[1]

Anmerkung

1 *http://www.humanistische-union.de/nc/aktuelles/aktuelles_detail/back/aktuelles/article/auszeichnung-fuer-einen-wertvollen-beitrag-zur-wahrung-unserer-grundrechtsordnung/*

Sylvia Johnigk

Bürgerrechte nach dem NSA-Skandal

Geheimdienste und Militär nutzen die Verpflichtung von Telekommunikationsunternehmen zur Lawful Interception *und die Kollaborationsbereitschaft von Unternehmen aus, um flächendeckend Informationen abzuschnorcheln. Somit dienen die Informations- und Kommunikationstechnik und insbesondere das Internet und die Online-Dienste zur massenhaften und flächendeckenden Ausforschung und Überwachung.*

Geheimdienste und Militär wollen unsere Metadaten

Dabei stehen Netzknotenpunkte im Fokus, wie zum Beispiel der weltweit größte Internetknotenpunkt DE-CIX, der in Frankfurt betrieben wird. Dieser wird von verschiedenen Betreibern unterhalten, unter anderem ist auch *Level(3)* dabei, ein Kollaborateur des britischen Geheimdienstes GCHQ. Ferner werden Glasfaserkabel an zentralen Orten wie den transatlantischen Unterseekabeln nahezu vollständig auf Metadaten und partiell auf Inhaltsdaten abgeschnorchelt.

Insbesondere interessieren sich die Geheimdienste für die Metadaten. Es scheint so, als wappneten sie sich schon jetzt für die Zukunft. In den nächsten Jahren werden immer mehr Metadaten erzeugt, *Smart Phone*, *Smart Pad*, *Smart TV*, *Smart Grid*, *Smart Fridge*, *Smart Power*, *Smart Car*, *Smart App*. Das sind unfassbar viele Informationen, die die Geheimdienste zu einem gigantischen Verhaltensprofil zusammen führen wollen.

Geheimdienste und Militär schwächen unsere IT

Geheimdienste und Militär schwächen aktiv Software-, Krypto- und Hardwareprodukte, indem sie bei den herstellenden Unternehmen bewusst Schwachstellen einbauen lassen, die sie für ihre Zwecke nutzen.

Zusätzlich werden gezielt Endgeräte, Netzwerkgeräte, Server, Tastatur, Monitor, USB, Smartphone, etc. von Nutzern durch die Geheimdienste mit Wanzen und anderem Ungeziefer ausgestattet. Der Bestellvorgang im Online-Shop und die Bezahlung per Kreditkarte erleichtern es den Geheimdiensten, gezielt die bestellte Ware einer bestimmten Person auf dem Versandweg abzufangen und zu infiltrieren.

Sylvia Johnigk bei ihrem engaierten Referat, Foto: Sven Lüders

Hierfür gibt es für Geheimdienste einen Bestellkatalog[1], aus dem sie die richtigen Tools für ein bestimmtes Gerät auswählen können. Eine weitere Möglichkeit ist das Erzeugen von *Windows*-Fehlermeldungen und so das potenzielle Abgreifen von privaten Informationen über die Versendeoptionen *Melden des Fehlers* an den Provider.

Die aktuelle Konzeption und Implementierung von IuK-Netzwerken und IuK-Technik sind offen für das Ausspähen von Daten. Viele Endgeräte sind aktuell nicht sicher, so dass es schwierig ist, auf diesen Endgeräten Krypto- und andere Sicherheitsanwendungen sicher zu installieren und zu benutzen.

Geheimdienste und Militär betreiben *Bot-Netze* und infizieren 100.000 private Rechner, um sie im Ernstfall für einen Cyberangriff nutzen zu können.[2]

Fälschen, Täuschen und Propaganda sind ihre Kernkompetenzen

Geheimdienste und Militär betreiben gezielt Desinformation und Propaganda. Hierzu gehört es, Informationen zu Bedrohungen oder Schwachstellen einseitig zu färben, zu fälschen oder irreführend, verharmlosend oder übertrieben darzustellen. Hier stehen nicht nur die Geheimdienste in der Kritik, sondern auch die Regierung und andere exekutive Organe der Bundesrepublik.

Zum Beispiel proklamiert die Bundesregierung per Gesetz, dass *DE-Mail* sicher ist. Fakt ist, dass es sich bei DE-Mail lediglich um eine Transport-Verschlüsselung handelt. Auf den Servern der TK-Anbieter liegen die Mails unverschlüsselt. Da TK-Anbieter dem Staat *Lawful-Interception*-Schnittstellen zur Verfügung stellen müssen, können die Geheimdienste bei Bedarf die E-Mail unverschlüsselt absaugen.

Teilweise verbreiten kollaborierende (Sicherheits-) Unternehmen diese Informationen, um ihnen in dieser Tarnung mehr Glaubwürdigkeit zu verleihen.

Geheimdienste verbreiten zudem Desinformation und Propaganda, um Aktivisten und Kritiker zu diskreditieren. Im Rahmen der Veröffentlichungen von Snowden tauchte ein Dokument auf, welches einen Plan des britischen Geheimdienstes offenbarte, dem zu Folge unliebsame Personen diskreditiert werden sollten. Es ist nicht bekannt, ob diese Pläne jemals ausgeführt wurden.[3]

Bundesregierung glänzt im Kleinreden

Bundesregierung und andere Exekutivorgane lassen die Bevölkerung (und die Unternehmen) im Regen stehen. Sie boykottieren eine Aufklärung und schweigen zur Affäre. Ausdrücklich befürworten sie dagegen eine Kooperation mit der NSA. Die NSA unterhält in Deutschland unter anderem den wichtigsten Knotenpunkt für ihre Aktivitäten auf dem alten Kontinent. Zudem genießen Geheimdienstmitarbeiter Diplomatenstatus und sind somit nahezu unantastbar.

Unsere Bundesregierung befürwortet die massenhafte und flächendeckende Ausspähung. Sie spricht bei der Vorratsdatenspeicherung von Erfolgen bei Ermittlungen, von Verstößen gegen das Grundgesetz dagegen gar nicht.

Das Grundrecht auf *Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* dient dem Schutz von persönlichen Daten, die in informationstechnischen Systemen gespeichert oder verarbeitet werden. Dieses Recht wird im Grundgesetz zwar nicht explizit genannt. Es wurde allerdings 2008 durch das Bundesverfassungsgericht als spezielle Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 1 Abs. 1 GG, Art. 2 Abs. 1 i.V.m.) aus den vorhandenen Grundrechtsbestimmungen abgeleitet. Nach dem Urteil des Bundesverfassungsgerichts ist zudem die heimliche Infiltration informationstechnischer Systeme nur dann zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Diese Infiltration kann nur durch einen richterlichen Beschluss herbeigeführt werden.

Mit diesem Urteil sollte klar geworden sein, dass das massenhafte, anlasslose Ausspähen in vielerlei Hinsicht einen massiven Bruch der Grundrechte in Deutschland darstellt, der mit nichts zu rechtfertigen ist.

Die Bundesregierung leistet Beihilfe zu Menschenrechtsverletzungen

Die Bundesregierung und andere Organe der Exekutive leisten Beihilfe bei geheimdienstlichen Aktionen, die sowohl gegen internationale Menschenrechte als auch die deutsche Verfassung verstoßen, indem Menschen in Menschen und Terroristen/Terrorverdächtigte eingeteilt werden. Dabei wird akzeptiert, dass geheime Algorithmen/Analyseverfahren (z. B. X-Keyscore) darüber bestimmen, wer Terrorist oder Terrorverdächtigter ist.

Terroristen und Terrorverdächtige können festgesetzt und in einen Staat verschleppt werden, in dem sie ihre Menschenrechte verlieren – auch wenn nur ein Verdacht vorliegt. Kann man Terrorverdächtige gleich (durch Drohnen) töten, ohne ein Recht auf einem fairen Prozess? Kann man sie in Foltergefängnisse wegsperren, ohne dass sie jemals ein Recht auf einen fairen Prozess haben? Darf man sie foltern, *waterboarden*, stundenlang, tagelang mit lauter Musik beschallen und grellem Licht bestrahlen, auf dem nackten Boden schlafen lassen, in kalten nassen Räumen unterbringen oder ohne Schatten im Freien? Alles ohne eine Chance auf Verteidigung? Ohne einen fairen, offenen Prozess? Lebenslang verdächtig weggesperrt? Wenn das heimlich geschieht, verschwindet man einfach vom Erdboden und oft erfahren Angehörige nichts davon.

Die CIA hat in Deutschland mit Hilfe des Unternehmens CSC den deutschen Staatsbürger *al Masri* in ein Foltergefängnis verschleppen lassen. Nachdem bekannt wurde, dass einige Regierungsmitglieder darüber informiert gewesen waren, gerieten

Sylvia Johnigk

Sylvia Johnigk studierte Informatik an der TU-Berlin und befasste sich schon im Studium mit Themen wie Datenschutz und Informationssicherheit, arbeitete fünf Jahre in der Forschung am Thema Informationssicherheit und acht Jahre bei einem Finanzdienstleister als IT-Security Consultant in Frankfurt am Main. Seit Mitte des Jahres 2009 ist sie selbständig und leitet ein kleines Unternehmen in München, das sich auf Beratung von Unternehmen zum Thema Informationssicherheitsmanagement mit dem Schwerpunkt Mitarbeitersensiblisierung spezialisiert hat.

diese in Kritik. Wegen des Drucks von Außen und der erwiesenen Unschuld kam *al Masri* nach mehreren Monaten wieder frei. Man hat ihn übrigens, nachdem der Fehler bemerkt wurde, nicht zurück nach Deutschland geflogen, sondern in einem Wald nahe der albanischen Grenze ausgesetzt.

Wir lassen uns von Menschen, von Geheimdienstmitarbeitern mittels nicht überprüfbarer Algorithmen und Verfahren die Menschenrechte absprechen.

Die flächendeckende Ausspähung wird zwar mit dem weltweiten Terror begründet, doch lediglich 35 % des Budgets ist für die Terrorbekämpfung vorgesehen. Ein Schelm, wer Böses dabei denkt.

Wichtige Fragen, die wir uns im Zusammenhang mit dem NSA Skandal stellen müssen

Wie dehnbar wird der Begriff des Terroristen/Terrorverdächtigten in der Zukunft werden?

Wollen wir in einer Gesellschaft mit zwei Klassen von Menschen leben, Menschen mit Menschenrechten und Menschen ohne Menschenrechte?

Wollen wir akzeptieren, dass Geheimdienste diese Entscheidungen im Verborgenen und nahezu ohne transparente Kontrolle treffen?

Wollen wir akzeptieren, dass ausländische Geheimdienste auf dem Boden von Deutschland/Europa unsere/andere Daten abziehen?

Wollen wir akzeptieren, dass wir keine Antworten aus den USA bekommen, obwohl sie in die Autonomie der BRD eingreifen (falls die Regierungen dies nicht schon über Geheimverträge abgetreten haben)?

Wollen wir akzeptieren, dass wir unter dem Deckmäntelchen des Terrorismus massenhaft und flächendeckend ausgespäht werden?

Anmerkungen

1 *http://www.spiegel.de/netzwelt/netzpolitik/interaktive-grafik-hier-sitzen-die-spaeh-werkzeuge-der-nsa-a-941030.html*
2 *http://www.chip.de/news/NSA-Geheimdienst-nutzt-infizierte-PCs-als-Botnetz_66586085.html*
3 *http://www.spiegel.de/netzwelt/netzpolitik/gchq-greenwald-veroeffentlicht-weitere-snowden-dokumente-a-955488.html*

Dietrich Meyer-Ebrecht

Besteht die Chance einer demokratischen Gestaltung und Kontrolle unserer Kommunikationsnetze?

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.
Bruce Schneier[1]

Edward Snowden hat uns mit seinen Enthüllungen gelehrt: Geheimdienste, allen voran die NSA, sind mit der Massivität ihrer personellen und finanziellen Mittel, mit ihrer Aggregation an Expertise und Kreativität in der Lage, jeden Datenstrom anzuzapfen, sich Zugang zu jeder Datensammlung zu verschaffen. Nur mit einem unverhältnismäßig hohen Aufwand und mit erheblichen Einschränkungen könnten wir uns dagegen schützen, und es bleibt offen, ob ein 100 %iger Schutz überhaupt erreicht werden kann. Bürgerrechte im Digitalen – so können wir Bruce Schneiers Statement interpretieren – sind nicht technisch zu haben, sie sind zwischen Politik und Gesellschaft auszuhandeln.

Nicht verhandelbar in einer freiheitlichen Gesellschaft ist die Privatsphäre. Der Schutz der informationellen Privatsphäre stellt jedoch eine ganz besondere Herausforderung dar. Anders als im Physischen gibt es im Digitalen zwischen öffentlichem Raum und privatem Raum keine Türen, die verriegelt werden können. Die Abgrenzung ist eher eine Art semipermeable Membran, vergleichbar mit der Hülle einer biologischen Zelle. Denn für den Informationsaustausch bedarf es einer selektiven Durchlässigkeit, wenn die Optionen der Kommunikationsnetze sowohl einen individuellen als auch einen gesellschaftlichen Nutzen haben sollen. Schutz und Nutzen zugleich können jedoch nur gewährt werden, wenn die digitale Außenwelt demokratischen Spielregeln folgt, einer demokratischen Kontrolle unterzogen wird. Dies fordert den Staat. Der Schutz seiner Bürger muss durch eine angemessene Gesetzgebung – und ihre Durchsetzung! – garantiert sein. Dazu gehört ein politischer Wille. Unverzichtbar ist aber auch das gesellschaftliche Engagement. Beides ist derzeit schwer zu haben. Wollen wir die Chancen für eine demokratische Gestaltung und Kontrolle der Netze abwägen und Lösungswege skizzieren, müssen wir uns mit den Problemen und Missverständnissen auseinander setzen, die diesem Ziel im Wege stehen, die gleichsam als *Bedrohung von innen* wirken.

Die Politik – handlungsunfähig?

Hier treffen wir auf drei Komplexe. Der erste ist die innen- und außenpolitische Dimension: das Thema betrifft die Sicherheits-

politik. Ausspähung ist ein wesentliches Element der Cyberwarfare, der digitalen Kriegsführung. Die wiederum ist eine zentrale Säule der strategischen Doktrin für eine neue, technologieorientierte Kriegsführung. Aus dieser Sicht müssen wir die gegenwärtige ungebremste Ausspähung staatlicher Institutionen, Wirtschaft und Industrie, Forschungseinrichtungen und privater Personen bereits als *kalten* Cyberkrieg verstehen. Sie dient dem Erkennen der Absichten des potenziellen Gegners – oder auch Freundes – und dem Anlegen geheimer Zugänge zu dessen Netzwerken. Dies auch als Vorbereitung aggressiverer Maßnahmen, die damit beginnen, dem Gegner mit spürbaren Operationen *die digitalen Muskeln zu zeigen* bis zu Operationen, die den Gegner schwächen sollen, wie Sabotageakte oder die Übernahme der Kontrolle über kritische Systeme. All diese hoch geheim gehaltenen Operationen schwimmen gleichsam mit in den zivilen Informationsströmen. Sie stellen ein Fundamentalrisiko für die Zivilgesellschaft dar!

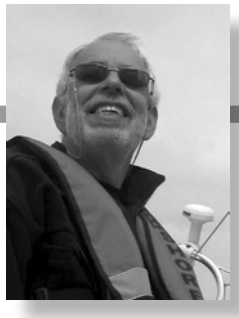
Militärische Überlegungen waren zwar der Ursprung des Internet. Längst ist es aber zu einem kaum verzichtbaren Instrument der Zivilgesellschaft geworden. Mit der regelmäßigen Nutzung für militärische Cyberoperationen unterliegt es spätestens heute wieder eindeutig militärischen Herrschaftsansprüchen und militärischen Denkkategorien. Militärisches Denken bestimmt bereits die Ausspähungsaktivitäten. Kennzeichnend dafür sind die Erfolgskriterien: Sie sind nicht wie im Zivilen orientiert am bestmöglichen Erreichen eines Ziels unter möglichst geringen Schäden – der Erfolgsfall ist, wenn das Ziel überhaupt erreicht wird, unter Inkaufnahme jedweder Kollateralschäden. Verständlich wird unter dem militärischen Aspekt auch die üppige Ausstattung der Geheimdienste. Und auch die Freistellung von zivilrechtlichen Normen. Als US-Präsident George W. Bush unmittelbar nach dem 9/11-Attentat den damaligen Direktor der NSA, *Michael V. Hayden* fragte, „*was braucht ihr, damit so etwas nie wieder geschieht?*“, war es unter anderem die Autorisierung, US-amerikanische Bürger auch gegen geltendes Recht ausspähen zu dürfen. Und er bekam, was er sich wünschte, an allen demokratischen Institutionen vorbei.

Einer wirksamen parlamentarischen Kontrolle entziehen sich auch unsere eigenen Geheimdienste. Aus Snowdens Enthüllungen wurde auch offensichtlich, dass sich BND und NSA gegenseitig darin zuarbeiten, Bürger und Institutionen auszuspähen. Dies bestätigte auch *William Binney*, früherer technischer Direktor der NSA, heute ihr vehementer Kritiker, in einer Anhörung im NSA-Ausschuss des Deutschen Bundestages. Die Zusammenarbeite des BND mit US-Geheimdiensten hat historische Wurzeln. Sie stützt sich auf schon sehr alte bilaterale Verträge, Zusatzabkommen zum Nato-Truppenstatut und, wie kürzlich im SPIEGEL berichtet, auf Geheimverträge zwischen BND und NSA – ein Tabuthema für unsere Politik! „*Deutschland braucht dringend einen Snowden aus dem BND*“, empfahl in einem Interview kürzlich *Thomas Drake*, als Whistleblower der NSA ein Vorgänger von Snowden.[2] Unsere Gesellschaft muss Aufklärung einfordern, um einschätzen zu können, wo politische Hebel angesetzt werden müssen. Derzeit kann unsere Regierung ihrem Schutzauftrag gegenüber uns Bürgern gar nicht nachkommen, denn sie müsste den Diensten die Arme binden und damit gegenüber den amerikanischen Freunden vertragsbrüchig werden. Ohne sehr massiven gesellschaftlichen Druck wird sich eine Bewegung in der Politik auf diesem Feld nicht erzielen lassen.

Die Gesellschaft – veränderungsunwillig?

Leider lässt sich auch die Gesellschaft dazu kaum bewegen – der zweite Komplex. Denn wir werden auch etwas aufgeben müssen. Zur Disposition stehen private Verhaltensmuster und wirtschaftliche Interessen. Wir haben uns an den Komfort und den Effizienzgewinn gewöhnt, die uns die Netze bieten, und wir sträuben uns gegen jede Einschränkung. Wir wollen ja nicht wieder Briefe schreiben müssen und versenden deshalb weiterhin vertrauliche Information unverschlüsselt, für den *man-in-the-middle* ohne große Mühe mitlesbar. Oder wir *posten* sie samt intimen Bildern gleichsam an Anschlagbrettern auf öffentlichen Plätzen. Schon wird es schwierig, sich dem sozialen Druck zu entziehen, die private Kommunikation nur noch über soziale Netze abzuwickeln, Bilder und Videos auf Plattformen wie Flickr oder YouTube zu *teilen*, regelmäßig *Lebenszeichen* zu tweeten.

Unsere persönlichsten Daten laden wir in die *Cloud*, um von überall her darauf zugreifen zu können. Aber so wolkig wie der Name sind unsere Vorstellung davon, wo und wie unsere Daten gespeichert werden, wie sicher unsere Daten dort bewahrt werden. Ein Beispiel, wie wohlfeil Ausspähtechnologie ist: Auf ihren Webseiten bietet die russische Firma *Elcomsoft* ein Programm an, mit dem man in die Cloud-Backups von iOS- und Blackberry-Geräten einbrechen kann, in der *forensischen* Version auch, ohne die Kontrolle über die Geräte zu besitzen – für nicht einmal 400 €.[3] Und wer unter den Smartphone-Besitzern jetzt noch keine weichen Knie hat und meint, in den Gigabytes an Songs, Fotos und Filmchen sind seine wenigen interessanten Dokumente doch gut versteckt: Elcomsoft bietet auch gleich die notwendigen Softwarewerkzeuge an, um für ein schnelles Herausziehen der vermutlich interessanten Dokumente die Spreu vom Weizen zu trennen. Auch in der Wirtschaft kommen inzwischen viele Geschäftsprozesse ohne die *Cloud*, ohne Plattformen für das kooperative Arbeiten und ohne Online-Datenbanken gar



Dietrich Meyer-Ebrecht

Prof. (em) Dr.-Ing. **Dietrich Meyer-Ebrecht** war von 1984 bis 2004 Inhaber des Lehrstuhles für Bildverarbeitung an der RWTH Aachen, zuletzt mit dem Forschungsschwerpunkt digitale Bildanalyse für medizinische Anwendungen. Seit 2001 ist er Mitglied des FIfF-Vorstandes.

nicht mehr aus. Das sind hoch ergiebige Angriffsziele! Wir reichen den Geheimdiensten unsere vertraulichen Informationen quasi auf dem Silbertablett.

Und wenn wir schon bei den Tabletts sind: Smartphones und Tabletcomputer, demnächst auch Smartwatches, ausgestattet mit GPS-Lokalisierung, Mikrofon, Kamera und Mobilfunkzugang, tragen wir als potenzielle Taschenwanzen beständig mit uns herum. Die NSA-Experten sollen, wie aus den von Snowden enthüllten NSA-Dokumenten hervorgeht, gejubelt haben, als die Smartphones den Markt eroberten, und kaum war das erste iPhone erschienen, war es bereits gehackt. Wer etwa die Babyphone-App einschaltet – mit Ton und Bild! – oder die App zum Auffinden des eigenen Telefons, macht sich vermutlich wenig Gedanken darüber, dass dabei u. a. gerade die technischen Eigenschafen dieser Geräte genutzt werden, die die Geräte bestens geeignet zur Ausspähung unserer Intimsphäre und unserer Bewegungsmuster machen. Wer Heizung oder Herd per Smartphone aus der Ferne steuert, denkt vermutlich kaum daran, dass das heimische IT-Netz durch die dafür notwendigen Öffnungen in seiner Firewall angreifbarer wird.

Es muss aber gar nicht sofort in unsere Geräte und Systeme eingegriffen werden, für eine *aktive* Überwachung. Die *passive* Überwachung, die Beobachtung des aus den Netzen abgegriffenen Datenverkehrs unserer Mobiltelefone, gibt bereits Auskunft über unsere Kommunikationspartner, über unsere Aufenthaltsorte und mehr. Dazu kommen Suchanfragen, Internetkäufe, Finanztransaktionen und Schlüsselwörter in unseren E-Mails. Allein die Auswertung dieser Metadaten und Datenspuren liefert bereits sehr detaillierte persönliche Profile.

Nun könnte auch der willigste Gesetzgeber uns nicht wirksam schützen, wenn wir alle potenziellen Schutzmaßnahmen durch leichtfertigen Umgang mit unseren Daten unterlaufen würden. Weil wir auf den privaten Komfort nicht verzichten wollen. Weil wir dem wirtschaftlichen Gewinn Priorität einräumen. Weil wir uns den Kommunikationstrends nicht verweigern möchten oder uns einem sozialen Druck schon nicht mehr entziehen können. Seinerseits wird der Gesetzgeber jedoch nicht tätig werden, solange der Willen der Gesellschaft nicht erkennbar wird, durch Veränderung von Verhalten und Konsum ihrerseits einen Beitrag zum Schutz der Privatheit zu leisten.

Unser Ego – im Selbstbetrug bequem eingerichtet?

Und dann ist da noch ein dritter Komplex: unsere Psyche. Was sich in den digitalen Netzen abspielt und dahinter, in den Superrechnern der Geheimdienste, entzieht sich weitgehend unseren Vorstellungen. „*Wir hätten es wissen können, …*“ schreibt die GI in einem Aufruf an ihre Mitglieder. Aber nicht einmal wir InformatikerInnen und IngenieurInnen haben das Ausmaß und die Tiefe der Ausspähung sehen wollen. Dabei lassen wir uns auf interessante Widersprüchlichkeiten ein: Mit geschickt kombinierten Suchbegriffen lassen wir uns durch Google genau die gerade benötige Information in dem unüberschaubaren Datenuniversum des Internet suchen – und in Sekunden finden. Geht es aber um unsere eigenen Daten, verlassen wir uns gerne auf das Gefühl, „je mehr Daten, desto unwahrscheinlicher, dass zufällige unsere eigenen herausgefischt werden“. Und dieser Glaubenssatz ist falsch: Je umfassender die abgegriffenen Daten, desto größer wird sogar die Wahrscheinlichkeit, dass Daten, die mit vorgegebenen Merkmalen und Mustern korrelieren, identifiziert werden – und dass wir durch das Zusammenspiel von Zufällen unbescholten ins Fadenkreuz geraten können. Das widerspricht der Intuition, ist *counterintuitive*, und damit schwer vermittelbar.

Unsere Vorstellungen hängen noch an Bildern aus Gestapo- und Stasi-Zeiten – Geheimdienstmitarbeiter, die Briefcouverts unter Wasserdampf öffnen, um unsere Post zu lesen –, Bilder, die wir ins Digitale übertragen. Mediale Darstellung nähren diese Vorstellungen eher, als dass sie uns darüber aufklären, dass längst nicht mehr Analysten anhand von gegebenen Verdachtsmomenten ermitteln, sondern Big-Data-Tools mit hoch entwickelten Statistikmethoden und komplexen Mustererkennungsverfahren. Der Verdacht wird gleichsam erzeugt, konstruiert, von Automaten! Sie analysieren alle erfassten Daten unmittelbar, suchen nach Korrelationen, stellen Verknüpfungen her, berechnen Gewichtungen für die Verdächtigkeit aller erfassten Personen. Diese *scores* hängen z. B. von den *scores* der Personen ab, mit denen wir kommuniziert haben, und sogar von deren Kommunikationspartnern, die wir nicht einmal kennen müssen. Sie hängen – über unsere Geodaten – von Personen ab, neben denen wir zufällig im Café gesessen haben, von Ländern, die wir bereist haben, von den Suchbegriffen unserer Internet-Recherchen.

Wir werden zu gewichteten Punkten in einem Beziehungsnetz, dem so genannten *social graph*, und je enger das Netz, desto ergiebiger wird es. Nachvollziehbar daher die Sammelwut der Dienste: „*Mehr ist immer besser […]. Da man Punkte, die man nicht besitzt, nicht verknüpfen kann, versuchen wir grundsätzlich, alles zu sammeln und behalten es für immer*“, sagt *Ira Hunt*, Chef-Techniker der CIA. Geheim bleibt, welche Faktoren relevant sind, mit welchen Algorithmen ausgewertet wird, welche Annahmen der *Verdachtskonstruktion* zu Grunde liegen.

Soweit sprechen wir von *passiver* Überwachung, die wir nicht spüren, von der wir nicht erfahren – muss sie uns dann überhaupt kümmern? „Ich haben ja nichts zu verbergen“, das kann ein fataler Irrtum werden. Denn gezielt nehmen sich die Dienste Personen vor, die von den Automaten ausgesiebt werden, weil ihr *score* einen Schwellwert überschritten hat. So kann jeder von uns in die *aktive* Überwachung geraten, ohne sein Wissen, einfach durch die Kombination von dummen Zufälligkeiten – mit ziemlich ungemütlichen Konsequenzen.

Wie ernst wir dieses persönliche Risiko nehmen, ist vielleicht jedes Einzelnen Sache. Ein allgemeines, die Gesellschaft betreffendes Risiko ist jedoch, dass Gleichgültigkeit und Unwissen dazu zu führen droht, dass wir in einen totalen Überwachungsstaat abgleiten. Können wir wirklich davon ausgehen, dass unsere westlichen Demokratien immer stabil genug bleiben, reaktionären Kräften zu widerstehen, die sich der Überwachungseinrichtungen als willkommenes Werkzeug für eine Machtergreifung bedienen? Selbst wenn wir uns auf ein solches Szenario nicht einlassen wollen – führt nicht, wie *Rolf Gößner* anlässlich der Verleihung des Berliner Preises für Zivilcourage an Edward Snowden ausführte, bereits das Bewusstsein, überwacht zu werden, über eine allmähliche Änderung des kollektiven Verhaltens zu einer unfreien Gesellschaft?

Und dennoch – es gibt Handlungsoptionen!

Was tun? Die Technik muss vor der Übermacht des Angriffspotenzials passen, unsere Regierung will ihre innen- und außenpolitischen Positionen nicht aufgeben, die Gesellschaft will auf das Gewohnte nicht verzichten. Hinzu kommen sozialer Druck und Unverständnis gegenüber den Risiken. Die Hände in den Schoß legen? Veränderung können wir erreichen, aber wir müssen dazu auf allen Ebenen ansetzen, konzertiert – Politik, Gesellschaft, Technik sind gleichermaßen aufgerufen.

Einmischen in die Politik, Kampagnenarbeit für eine gesellschaftliche Bewusstmachung sind zwei unverzichtbare Komponenten. Jedoch, genau wie die Politik sich nicht rühren wird, bevor die Gesellschaft ihren Veränderungswillen demonstriert, so wird sich die Gesellschaft nicht bewegen, ohne dass ihr technische und funktionale Alternativen an die Hand gegeben werden, die akzeptable Kompromisse zwischen dem ‚weiter so' und dem Verzicht auf eingespielte Prozeduren und lieb gewonnene Gewohnheiten bieten. Insofern muss Bruce Schneiers vorangestelltes Statement relativiert werden: Auch die Technik muss Beiträge leisten, um Wege zu ihrer demokratischen Gestaltung und Kontrolle zu ebnen, auf mehreren Ebenen:

Offene Systeme sind die Grundlage für Kontrollierbarkeit. Erst wenn der Programmcode von Betriebssystemen und Anwendungsprogrammen offengelegt wird, kann Software wirkungsvoll auf Hintertüren und versteckte Schadfunktionen geprüft werden. Opensource-Software ist mittlerweile etabliert, findet aber immer noch nicht die wünschenswerte breite Akzeptanz. Mit komfortableren Installationspaketen für Betriebssysteme auf gängigen PCs, Notebooks, Tablets und Smartphones könnte die Schwelle zum Umstieg reduziert werden. Besser noch, wenn Aufklärung eine marktrelevante Käuferschicht für Produkte entstehen lässt, die bereits mit einer kompletten Grundausstattung offener Software ausgeliefert werden. Dies gilt nicht nur für den privaten Konsum, sondern ebenso für Unternehmen, die schon aus wirtschaftlichen Erwägungen interessiert sein sollten, Sicherheitsrisiken zu reduzieren.

Wahlmöglichkeiten innerhalb eines Angebots alternativer Dienste sind eine Voraussetzung für eine Abkehr von den derzeitigen monopolistischen sozialen Netzen, Suchmaschinen, Clouds, App-Stores. Dass für alternative Dienste bereits heute Bedarf ist, beweist eine Vielzahl kleiner und mittlerer Unternehmen, die E-Mail-Konten, Upload-Speicherplatz, Webhosting etc. anbieten. Wichtig ist die Etablierung öffentlicher Kontrollinstanzen. Es sollte ein von den Kunden eingefordertes Qualitätskriterium werden, dass sich die Unternehmen freiwillig regelmäßigen Sicherheitsaudits unterziehen.

Digitaler Selbstschutz ist eine Sofortmaßnahme. Er sollte so selbstverständlich werden wie das Anbringen eines Sicherheitsschlosses an der Wohnungstür. Auch hier wieder obliegt es der Käufergemeinde, eine Grundausstattung an Mitteln für den digitalen Selbstschutz bereits bei der Auslieferung von Neugeräten zu erwarten (kein Vermieter wird heute eine Wohnung ohne Türschloss anbieten …). Bis dies erreicht ist, kann mit bereits heute erreichbaren Werkzeugen begonnen werden, wenigstens mit den einfachsten. Auch wenn gegen aktive Ausspähung vermutlich alle uns realistischerweise verfügbaren Mittel versagen, erschweren ‚Hausmittel' zumindest die passive Ausspähung. „*Macht es den Geheimdiensten schwer, verdunkelt das Netz!*", ist die Parole der Initiative *Reset the Net*, die dazu eine Grundausstattung an einfach zu handhabenden Schutzfunktionen anbietet.[2] Aufwändiger, aber auch wirkungsvoller ist die E-Mail-Verschlüsslung. Erforderlich ist jedoch die Installation der Verschlüsslungssoftware auf *beiden* Seiten der Kommunikation. Für Verbreitung muss daher geworben werden. Dazu müssen Installation und Handhabung mit guten Anleitungen leicht gemacht werden. Einen hilfreichen Beitrag dazu leistete nun, gerade ein Jahr nach Snowdens Enthüllungen, die *Free Software Foundation.*[5]

Wir haben es in der Hand …

Es läge an den Bürgern selbst, Überwachung zu stoppen, schrieb Edward Snowden. Und dies sei mithilfe der Naturgesetze einfacher als mit staatlichen Gesetzen. Letztlich hat die Gesellschaft den Schlüssel für eine Veränderung in der Hand. Loslösen müssen wir uns von der verführerischen Annehmlichkeit des scheinbaren Umsonst von Internetdienstleistungen und -werkzeugen. Sicherheit kostet. Und auch ein Stück Komfort müssen wir bereit sein aufzugeben. Denn, so schreibt Ulrike Meyer, Professorin für IT-Sicherheitsforschung an der RWTH Aachen, „*Sicherheit kostet oft auch die Benutzerfreundlichkeit eines Programms.*" Die erforderlichen neuen Produkte werden eine Herausforderung an die Wirtschaft sein. Und so wird vermutlich schneller als die Politik der Markt reagieren, sobald sich eine sicherheitsbewusste Käuferschicht etabliert. Der politische Einfluss der betroffenen Wirtschaft wird dafür sorgen, dass die Politik nachzieht. Aber beginnen müssen *wir*!

Selbst tätig zu werden, andere dazu zu ermutigen, zu unterstützen – das hat mindestens zwei Effekte über den konkreten Nutzen hinaus: Wir erfahren Technik und ihre Mechanismen, wir holen die Technik ein Stück heraus aus ihrer Abstraktheit. Und uns wird bewusst, dass wir uns ein Stück Freiheit zurückerobern. Denn „*beobachtet werden macht unfrei*", sagt uns Glenn Greenwald.

Erweiterte Fassung eines Vortrag auf dem 3. Gustav-Heinemann-Forum der Humanistischen Union, Rastatt, 20./21.06.2014, „Weltweite Kommunikationsüberwachung: Rechtliche Bewertung & politische Handlungsoptionen.

Anmerkungen

1 *Bruce Schneier, US-amerikanischer Experte für Computersicherheit, Vorwort seines Buches „Secrets and Lies", 2000*

2 *„Ihr braucht einen Snowden aus dem BND!", Thomas Drake, Interview in FR 10.06.2014*

3 *Elcomsoft Phone Password Breaker, http://www.elcomsoft.de/eppb.html*

4 *Initiator der Kampagne war Fred Barlow, Mitbegründer der Electronic Frontier Foundation, http://resetthenet.org*

5 *Inzwischen ist unter Mitwirkung des FIfF auch eine deutsche Fassung der Anleitung der FSF für die Installation und Handhabung der (freien!) GnuPG-Software für das heute standardmäßig verwendete PGP-Verfahren verfügbar, https://emailselfdefense.fsf.org/de/*

Ute Bernhardt, Ingo Ruhmann

Revolution von oben – Der Weg in die Informationsgesellschaft

Die Weiterentwicklung der Informations- und Kommunikationstechnologie (IuK-Technologie) soll uns in den nächsten Jahren Veränderungen erheblichen Ausmaßes bescheren. Von „Dritter Industrieller Revolution" bis zum „Bit Bang" scheint kein Begriff eindringlich genug, um Bedeutung und Tiefe des Wandels einer Industrie- in eine Informationsgesellschaft zu beschreiben. Es geht um nichts weniger als unsere Arbeit, unser Geld, unsere Rechte, unsere Staatsform und die Art und Weise unseres zukünftigen Lebens. Bei all dem stehen nach Ansichten der Experten revolutionäre Änderungen an. Womit wird dies begründet, wer treibt die Entwicklung voran?

Was in Deutschland mit dem unglücklichen Begriff *Datenautobahn* bezeichnet wird, lehnt sich an die von US-Vizepräsidenten *Al Gore* verkündeten Vorschläge einer erst nationalen, dann globalen Informations-Infrastruktur an. Das erklärte Ziel ist die Infrastruktur für die Gesellschaftsform der Zukunft: Die Informationsgesellschaft.

Die Informationsgesellschaft fußt auf Mythen. Sie geht auf die Idee der post-industriellen Gesellschaft zurück, die *Alain Touraine* bereits 1969 publizierte. Wenige Jahre später beschrieb *Daniel Bell* die post-industrielle Gesellschaft durch Wissensarbeit, Ressourcenschonung und die Verschiebung der Arbeit vom Produktions- in den Dienstleistungssektor. Aus Bells Ideen erwuchs, was uns heute als Informationsgesellschaft vermittelt wird. Die Informationsgesellschaft ist Resultat der Erfahrungen der späten Sechziger und frühen Siebziger – samt des damals ungebrochenen Glaubens an die Technik. Energie- und Umweltprobleme, soziale Krisen gab es erst in Ansätzen. Daraus folgt die Frage: Ist eine solche Vision heute überhaupt tragfähig?

Nach dem Ende des Ost-West-Konflikts suchte die bis dahin gut von den Fördermitteln des Pentagon lebende Computerindustrie der USA ein neues Ziel ihrer Anstrengungen. Als Fokus ökonomischer Aktivitäten wurde 1989 von einem Konsortium von 13 Unternehmern der US-Computerbranche eine Informations-Infrastruktur vorgeschlagen und als *Perspectives on the National Infrastructure* veröffentlicht. Damit war ein neues Thema für einen technologischen Wettlauf vorgegeben. Japan gilt dabei als „technologisch rückständig" und abgeschlagen, Europa als Markt der Zukunft. Auch hier wurde eine Industriellen-Gruppe gebildet, es entstand ein nach seinem Auftraggeber benanntes *Bangemann-Papier*, an dem sich Kommission und Parlament der EU nun abarbeiten. In der Bundesrepublik hat „Zukunftsminister" Rüttgers eine schmale Dokumentation zum Thema Multimedia erarbeitet. Der Innovationsrat der Bundesregierung hat die Veröffentlichung seiner Ergebnisse mehrfach verschoben.

Deutschland Position ist günstig, weil es sowohl über wohlhabende, gut ausgebildete KundInnen als auch über eine sehr gut ausgebaute Infrastruktur verfügt. In der Bundesrepublik gibt es zahlreiche multimediale Pilotprojekte unterschiedlichen Zuschnitts. Nach ersten Projekten auf kommunaler Ebene – in Berlin und Stuttgart – werden landesweite Projekte – *Bayern online* und Planungen in NRW – vorbereitet. Sie zeichnen sich – trotz partieller Probleme – durch sehr unterschiedliche Techniken, Produkte und Dienstleistungen aus und gehören zu den größten der Welt. Ihre Vielzahl macht sie zu einem kaum vergleichbaren Experimentierfeld. In den USA werden dagegen von den derzeit 28 Pilotprojekten über 80 % nicht wie geplant starten.

Unterschiedliche Voraussetzungen

Trotz Einigkeit über die hohen ökonomischen Ambitionen gibt es wichtige Unterschiede. In den USA ist das Internet Grundlage der Fortentwicklung, Ziel sind neuartige Angebote. In der Bundesrepublik hingegen werden neben den Versuchen für Daten-Hochgeschwindigkeitsstrecken auch Projekte auf Fernseh-Kabelnetzen – Beispiel Baden-Württemberg – durchgeführt. Damit lebt die Diskussion um Medienmacht, Verteil- oder Wählnetze wieder auf.

Die USA nutzen ein neues elektronisches Kommunikationsmedium, um damit ihren riesigen Kontinent – mit einheitlicher Sprache, aber weit auseinandergezogenen Märkten – zusammenzubinden. Aus der Not Europas, im Gegensatz dazu keine einheitliche Sprache und einen zersplitterten Markt zu haben, versucht die EU, eine Tugend zu machen. Die mit Hochdruck verfolgte elektronische Kopplung besonders der Verwaltungen in der EU dient drei Zielen:

- Erstens sollen Sozial-, Agrarbehörden, Zoll und viele andere transnational wichtige Stellen verbunden werden, um ein geeintes Europa der Behörden zu schaffen,
- Zweitens soll damit die Ausgabenseite unter Kontrolle gebracht werden,
- Drittens lässt sich diese Kopplung anordnen und damit auch ohne Marktakzeptanz vielsprachliche, transnationale und EU-weite Dienste aufbauen, die Kern weiterer Angebote sein sollen.

Zusätzlich gibt es sehr vielfältige technische – z. B. ISDN als Infrastruktur – und inhaltliche – z. B. CD-ROM für Behinderte in der EU als Versuch für mehrsprachige Systeme – Projekte, mit denen die EU die Entwicklung vorantreibt. Bemerkenswert ist auch, dass – allen Beteuerungen zum Trotz, nicht der Staat sondern die Industrie werde die Investitionen übernehmen – derzeit in den USA und der EU hunderte von Milliarden staatlicher Gelder in die Projekte gepumpt werden.

Im Aktionsplan der EU-Kommission nimmt der Ausbau von Satelliten und terrestrischen Verteilnetzen für Medienangebote weiten Raum ein. Die EU favorisiert also den Ausbau von Verteilnetzen. Die Kommission verschafft damit Medienkonzernen die Basis für das Recycling ihrer technisch geschönten Bild- und Tonkonserven und läuft gleichzeitig Gefahr, die Entwicklung innovativer neuer Medien und ihrer Nutzung zu verschlafen.

Damit lassen sich bereits drei wichtige Unterschiede zwischen den USA und der Bundesrepublik bei den Voraussetzungen für eine Informationsgesellschaft benennen:

1. Forschung und Entwicklung in der IuK-Technologie wurden bei uns weder so stark gefördert noch so stark auf militärische Fragen ausgerichtet wie in den USA. Das Interesse an einer Umorientierung auf hohem Niveau ist deshalb hier geringer.

2. Die sprachlichen, kulturellen und politischen Differenzen zwischen Europa insgesamt und den USA führen zu unterschiedlicher Nutzung. Uneinheitliche Sprache und Kultur engen das Volumen des europäischen Markts ein. Andererseits benötigt das dicht besiedelte Europa geringere Investitionen zur Anbindung entlegener Regionen.

3. Die Netztopologien – Internet als freies, interaktives Wählnetz in den USA gegenüber konsumorientierten Multimediaprojekten auf den TV-Kabelverteilnetzen in der Bundesrepublik – legen die Projekte auf bestimmte Nutzungsmöglichkeiten fest.

Die Informationsgesellschaft beginnt also zwar mit oft derselben Technik, aber unterschiedlichen Nutzungsvorstellungen und -bedingungen. Der Innovationsrat der Bundesregierung beklagt sich über passive Mediennutzung, die Bundesregierung lässt sich dennoch nicht davon abbringen, Konzepte mit eingeschränkter Interaktivität und deutlichen Kapazitätsunterschieden zwischen Hin- und Rückkanal zu verfolgen. Die Informationsgesellschaft wird sich daher keineswegs überall gleich entwickeln.

Die attraktiven Seiten der Informationsgesellschaft

Die Informationsgesellschaft ist eine Initiative von Akteuren aus Politik und Wirtschaft, eine Revolution von oben. Die von der G7-Konferenz benannten Ziele sind die Entwicklung einer kritischen Masse durch staatliche Initiative und damit vorrangig die Entwicklung von Märkten, sowie die Überzeugung der unnötigerweise skeptischen Bevölkerung, wie Bundesregierung und EU-Kommission nicht müde werden zu betonen. Eben dazu werden gängigerweise vier Argumentationsmuster genutzt, die teilweise miteinander verwoben werden. Keines dieser Muster erweist sich bei näherem Hinsehen als schlüssig.

Erstes Argument: Arbeit

Neue Arbeitsplätze sind das Argument, mit dem die Informationsgesellschaft bevorzugt beworben wird. Die genannten Zahlen von über 10 Millionen neuer Arbeitsplätze in der EU, zwei Millionen allein in der Bundesrepublik, fußen auf wenigen Studien, deren Autoren sich mittlerweile von diesen Prognosen distanzieren. Von EU-Kommissar Bangemann war auf einer Veranstaltung zu hören, die schönen Zahlen seien eine Setzung. Was also stimmt am Arbeitsplatzargument?

Natürlich entstehen neue Arbeitsfelder durch neue Technik. Wichtig ist jedoch der Nettoeffekt. Wenn, wie in den digital umgerüsteten Rundfunkanstalten 135 verschiedene Berufe auf etwa ein Dutzend neue Berufsbilder schrumpfen, so ist der Nettoeffekt verheerend. Auch die Digitalisierung des Telekommunikationssektors hat zehntausende von Arbeitsplätzen gekostet, 30.000 davon allein bei der Telekom. Dies sind jedoch Einzelbetrachtungen.

Nicht alle Arbeitslosen wurden zwar durch die IuK-Technologie verursacht, aber Strukturkrisen sind allein genauso wenig zur Erklärung geeignet. So kommt die OECD-Beschäftigungsstudie zu dem Schluß: „*Technologie ist eine der Ursachen der steigenden Arbeitslosigkeit*“. Rationalisierungsgewinne bei den sich verschlankenden Unternehmen von über 25 % in den letzten Monaten sind nur durch die konsequente Nutzung der Rationalisierungspotenziale vorhandener IuK-Technik in den Betrieben möglich geworden. Der Innovationsrat der Bundesregierung geht bei der positiven Bilanzierung der wirtschaftlichen Effekte der IuK-Technologie von weiteren Rationalisierungspotenzialen in Höhe von 20 % aus.

Die Debatte um die Arbeitsplatzfolgen des Computereinsatzes wurde schon in den 80er Jahren mit Vehemenz geführt. In Ermangelung exakter Studien über die Rationalisierungseffekte und die vielschichtigen Gründe der derzeitigen Arbeitslosigkeit lässt sich nur das Resümee ziehen, dass die Pessimisten der 80er Jahre mit ihren Prognosen näher an der heutigen Wirklichkeit auf dem Arbeitsmarkt lagen als die Optimisten und Technikprotagonisten.

Nach Ansicht der Befürworter der Informationsgesellschaft ist dies eine natürliche Folge der Weiterentwicklung des Produktionssektors. Die Informationsgesellschaft erst schafft neue Arbeitsplätze im Dienstleistungssektor. Wissensarbeit und neue Formen von Dienstleistungen besonders bei Informations- und Kommunikationsdiensten sollen die alten Arbeitsplätze ersetzen. Wissensarbeit und Dienstleistung sind jene Formen von Arbeit, die Bell entwarf und die bis heute die Grundlage der optimistischen Szenarien geblieben sind.

Wissensarbeit – nach Bell Forschung und Entwicklung allgemein – ist heute vor allem auf die IuK-Technologie bezogen. Abgesehen davon, wie tragfähig dies für eine Gesellschaft als Ganzes sein kann, zeigen sich gegenläufige Effekte. In der Bundesrepublik werden Forschung, Entwicklung und Software-Design zunehmend ausgelagert, das Management ausgedünnt. Statt zu wachsen, schrumpfen die entsprechenden Bereiche. Dienstleistungen nehmen zwar noch zu, aber auch hier gibt es Probleme, die auf zwei Feldern zu beobachten sind: Die herkömmlichen Dienstleistungen und die neuen, sogenannten Informationsdienstleistungen.

Wer heute die Dienstleistungen, die früher die Bank ausführte, am heimischen PC per Bankensoftware selbst erledigt, kann nachvollziehen, was der Club of Rome bereits 1982 erkannte: Weil „der sekundäre und der tertiäre Sektor gleichzeitig automatisiert werden“, könne der (tertiäre) Dienstleistungssektor nicht alle freigesetzten Arbeitskräfte aufnehmen. Die Produktivitätssteigerung im herkömmlichen Dienstleistungssektor gilt heute als Quelle zusätzlicher Arbeitslosigkeit. Allein die elektronische Unterschrift und der elektronische Austausch von Dokumenten kann 250.000 Angestellte überflüssig machen, die bisher die entsprechenden Papiere bearbeiteten. Für das Bankgewerbe haben Studien den Wegfall von einem Siebtel der Arbeitsplätze prognostiziert, in Verwaltungen wird von 30 % ausgegangen. Herkömmliche Dienstleistungen scheiden damit als Quelle für neue Arbeitsplätze aus.

Netze entkoppeln die Arbeit vom Ort ihrer Ausführung – Teleworking oder virtuelle Firmen sind die entsprechenden Begriffe. Netze heben Zeit-Schranken auf: Arbeit kann über die Welt verteilt rund um die Uhr geleistet werden. Zum zusätzlichen Problem wird damit die globale elektronische Vernetzung, die die zu

erledigende Arbeit zu den preisgünstigsten ArbeiterInnen bringt. Von der Stadtverwaltung bis zur Programmierung wird die Arbeit der Zukunft global ausgeschrieben und erledigt. Erst Globalisierung *und* Technisierung von Arbeit verbinden den Arbeitsmarkt der Bundesrepublik mit dem Indiens oder Argentiniens. Damit werden lokale Schutzrechte bedeutungslos. Tarifverträge, Gesundheitsschutz, ArbeitnehmerInnen-Organisation verflüchtigen sich auf einem global vernetzten Arbeitsmarkt, dem die Beschäftigen nichts Gleichwertiges entgegenzusetzen haben.

Die erhofften neuen Informationsdienstleistungen sind dabei die unbekannte Größe. Im Multimedia-Sektor etwa nennen offizielle Prognosen einen Bedarf von 5200 Arbeitskräften jährlich. Die Realität sieht dagegen so ernüchternd aus, dass einige der neu geschaffenen Ausbildungsgänge schon wieder eingestellt wurden. Die Forschung an intelligenten Assistenten und autonomen Agenten für Informationsdienstleistungen der Zukunft schränken gerade die Bereiche, in denen Arbeit geschaffen werden könnten, ein. Auch auf diesem Feld sind die Aussichten auf Arbeit vage.

Statt neuer Arbeit werden daher vor allem in den USA neue Formen der Arbeitsorganisation intensiv diskutiert. Diese Studien betrachten – im Gegensatz zur Lage hier – auch die Folgen des Einsatzes der IuK-Technologie. Ihr Fazit ist:

- Arbeit für die Masse der Bevölkerung wird es nicht mehr geben,
- Arbeit wird von immer mehr temporär Beschäftigten geleistet,
- die Schere zwischen qualifizierter und unqualifizierter Arbeit weitet sich,
- weite Teile der Beschäftigten werden marginalisiert.

Tagelöhnerei, Saisonarbeit und in jeder Form unwürdige Arbeitsverhältnisse werden unter neuen Namen wieder möglich. Ohne Arbeit bricht in unserem Wirtschaftssystem nicht nur der Sozialstaat zusammen, es fehlt auch an Kaufkraft. Daraus ziehen Experten zwei Konsequenzen: Deutschland lebt auf einem „zu hohen Wohlstandsniveau" und: Ohne Kaufkraft rechnet sich die Informationsgesellschaft nicht.

Zweites Argument: Die Wirtschaft

Als Grund für Staat und Wirtschaft, in die Informationsgesellschaft zu investieren, wird die internationale Wettbewerbsfähigkeit genannt. Nur die Beteiligung an globalen Datennetzen mache einen Industriestandort sicher, die Teilhabe am prognostizierten Markt der Zukunft möglich. Nur wer als erster die neuen Möglichkeiten ergreift, werde auch die Arbeitsplätze der Zukunft ernten. Eile sei geboten. Die Aussicht auf Gewinne bestimmt derzeit die Aktivitäten und verdeckt das Nachdenken über Probleme, Ziele und Alternativen.

Auch die überwiegende Mehrzahl der Unternehmen kann kein Konzept für ihr Engagement in neue Informations- und Kommunikationstechniken angeben. In Gesprächen äußern die Strategen, ihre Planungen hätten bestenfalls eine Gültigkeit von sechs bis neun Monaten, alles andere solle nur die Geldgeber beruhigen.

Mit der Informationsgesellschaft sind grundlegende ökonomische Veränderungen verbunden, die das gesamte Sozial- und Gesellschaftssystem in Frage stellen. Unser demokratisches System hängt damit untrennbar zusammen. Schon warnen selbst Technikbefürworter, mit dem Abschied von Wohlstand und Sozialstaat solle nicht gleich das politische System über Bord geworfen werden. Bisher zeigt die historische Erfahrung allerdings, dass noch kein politisches System solche sozialen Umwälzungen unbeschadet überstanden hat.

Hinzu kommt: Sollte sich der Abbau von Kaufkraft nicht durch andere Formen der Wertschöpfung ausgleichen lassen und die Informationsgesellschaft eine wirtschaftliche Pleite werden, wären diese Umwälzungen selbst für ihre Protagonisten völlig absurd. Obwohl Global Marketing als die Herausforderung der Zukunft bezeichnet wird, sind viele Fragen ungeklärt:

- Wie soll der Warenverkehr eines globalen Konsum-Netzes ablaufen, wie sollen die Produkte zu ihren KäuferInnen gelangen?
- Wie wird Information als Ware verkauft und gesichert, wem nutzen und schaden Copyright und Urheberrecht?
- Welche Rechte haben KundInnen, wie sollen sie ihren GeschäftspartnerInnen vertrauen, welche Rechtsform haben elektronische Verträge zwischen PartnerInnen in den verschiedenen Rechtssystemen auf dem Globus?
- Wie soll das Geld bei diesem Warenverkehr fließen? Wie tragfähig ist die Idee vom elektronischen Geld?

Eine betriebswirtschaftliche Betrachtung mag für einzelne Firmen ausreichend sein, für die Entwicklung der Informationsgesellschaft als neuer Gesellschaftsform fehlt es bislang an volkswirtschaftlicher Analyse. Eine globale Informations-Infrastruktur macht Staaten zu lokalen Größen, deren Einflußmöglichkeiten Grenzen gesetzt sind. Als vor zwei Jahrzehnten Wirtschaftspolitik noch als staatliche Aufgabe begriffen wurde, galten unkontrollierbare multinationale Unternehmen als Gefahr für die staatliche Souveränität. Heute konkurrieren Staaten mit anderen im globalen Wettbewerb um die Gunst von Unternehmen. Vom Antagonisten sind Staaten zu Dienstleistern für Unternehmen geworden. Schon gilt Microsoft den US-Aufsichtsbehörden global gesehen als nicht groß genug für eine Klage wegen Kartellbildung. Statt kleine Unternehmen zu stützen, sollen Unternehmenskonglomerate gegen die Unwägbarkeiten der Entwicklung schützen. Auch dies ein Indiz tiefer politischer Ratlosigkeit.

Getreu der postindustriellen Theorie Bells mahnt auch der Innovationsrat den Wandel in eine Wissensgesellschaft an. In die Praxis von Forschung und Wissenschaft ist das nicht vorgedrungen. Die Informatik als Schlüsseltechnologie einer Informationsgesellschaft scheint eher ein Gegenbeispiel zu sein. Elektronische Netze und neue Produkte werden von InformatikerInnen entwickelt. Doch in der Bundesrepublik nehmen seit 1991 die StudentInnenzahlen im Fachbereich Informatik ab, die Schließung des ersten Informatikfachbereiches ist beschlossen, hochqualifizierte InformatikerInnen werden nach Asien und Nordamerika abgeworben. Alles dies gesunde Anzeichen einer globalen Wirtschaft, aber ist das auch ausreichend für ein prosperierendes nationales Wirtschaftssystem? Da die Bundesregierung pro Jahr weniger Geld in Informatik-Forschung und Entwicklung steckt als der japanische Elektronikkonzern Fujitsu, ist es nur folgerichtig, dass der Bereich mit der höchsten Wertschöpfung, die Softwaretechnik, mit gerade einmal 6 Millionen DM gefördert wird. Allerdings herrscht

dabei Einigkeit zwischen Bundesregierung und Unternehmen: Sie kaufen ihre Software lieber in Indien ein, statt sie selbst zu produzieren. Was machen diese Firmen aber, wenn auch ihre KundInnen direkt per Datennetz in Indien kaufen?

Drittes Argument: Die Ökologie

Beispielhaft für viele erklärt Minister Rüttgers die ökologischen Vorteile der Informationsgesellschaft damit, Telearbeit könne den Berufsverkehr ebenso merklich ausdünnen wie Videokonferenzen die Dienstreisen. Ökologische Zukunftsmusik, denn die Zahlen stehen dem bisher entgegen. Dabei werden auch hier die Nettoeffekte außer Acht gelassen.

Über Telearbeit heißt es heute wie vor zehn Jahren: Sie ist etwas für wenige. Doch ist hier neues zu beobachten. Der Lagerhaltung auf der Autobahn à la *Just-in-Time* entlehnt ist die Praxis sogenannter *Road Warriors* in den USA – Geschäftsreisende ohne Büro, die ihre Bürotätigkeit „auf dem Weg" erledigen und telekommunikativ an die Firma angebunden sind. Abgesehen davon, dass sich Bürotätigkeiten „auf dem Weg" nur in der Bahn oder im Stau erledigen lassen, geht es auch hierbei nicht um Ressourcenschonung, sondern um erhöhte Kundenpräsenz durch maximale Reisetätigkeit. Ökologische Effekte kann Telearbeit allenfalls – was eigentlicher Effekt sein wird – aus dem Export von Arbeitsplätzen in Niedriglohnländer aufweisen.

Gern vergessen wird auch, dass Multimedia ein Markt ist, der vom Absatz neuer Geräte lebt. Deren Herstellung verbraucht Ressourcen, die Altgeräte werden zu Elektronikschrott. Die von der Bundesregierung geförderte 100-Hertz-Technologie flimmerfreier Bildschirme macht alle Gewinne stromsparender PCs zunichte. Die Ökobilanz der Informationsgesellschaft beginnt daher mit einer erheblichen ökologischen Belastung, eine Entlastung ist dagegen nicht konkret greifbar.

Viertes Argument: Demokratie

Ein auch von NutzerInnen elektronischer Netze gern verwandtes Argument ist, dass neue Möglichkeiten von Information und Kommunikation gänzlich neue Formen der Mitsprache und Organisation von Basisinitiativen eröffnen. Politische Mitsprache ist jedoch mehr als politisches Gehör auf elektronischem Weg. Die Expertengremien der Bundesregierung und der EU-Kommission zur Gestaltung der Informationsgesellschaft sind kein Beispiel für demokratische Teilhabe. In den verabschiedeten Dokumenten wird die verstärkte Beteiligung der BürgerInnen nicht einmal erwähnt, der Innovationsrat sieht sie gar als mögliche Gefahr. Ohne den Zugang zu Dokumenten der politischen Entscheidungsfindung und ohne faktische Möglichkeiten der Mitentscheidung bieten elektronische Medien lediglich technische Erleichterungen bereits bekannter politischer Instrumente. Partizipation benötigt weniger die Technik, als den politischen Willen.

Die Informations- und Kommunikationstechnologie gefährdet auf der anderen Seite BürgerInnenrechte in hohem Maße. Eine ausgesprochen vielfältige Überwachungstechnologie ist kostengünstig verfügbar und findet breite Verwendung. Jede Nutzung von Computernetzen hinterlässt sensible Datenspuren. Welcher Dienst wie oft und in welcher Folge aufgerufen wurde, lässt sich ebenso leicht zusammenstellen, wie eine Liste aller Kommunikationspartner. Über KonsumentInnen werden Kundenprofile erstellt, die weit über das hinausgehen, was staatliche Stellen – bis auf Ausnahmen – über BürgerInnen erfassen dürfen. Behörden verkaufen zudem ihre Daten nicht.

Jede Weitergabe elektronischer Post wird standardmäßig protokolliert, elektronische Netze sind ungesichert gegen Manipulation und Kontrolle. Die Rechtslage ist verworren: Auf dem Weg einer elektronischen Nachricht zwischen zwei NutzerInnen in der Bundesrepublik kann diese mehrere Staaten und damit unterschiedlichste Rechtssysteme durchlaufen. Persönliche Briefe – Mails – zwischen Compuserve-Nutzern werden ausschließlich über den Zentralrechner in Ohio geleitet, wo es weder eine Regelung über die Nutzung von Kundendaten, noch ein Datenschutzgesetz, noch ein Fernmeldegeheimnis dafür gibt. Der effektive Schutz der Daten von BürgerInnen, ArbeitnehmerInnen und KonsumentInnen ist bisher beim Umbau der Gesellschaft außer Acht geblieben.

Ohne rechtlichen Rahmen und ohne Datenschutz gibt es auf elektronischen Netzen allein unter kommerziellen Gesichtspunkten keine Entwicklung zu vertrauensvollen Transaktionen, sondern ein Klima der Unsicherheit und des Mißtrauens, das die Akzeptanz behindert und die Marktentwicklung bremst. Eine Gesellschaft auf eine technische Basis zu stellen, die keinen verbindlichen Rechtsrahmen kennt und in der keine BürgerInnenrechte verankert sind, ist ein Rückschritt in vordemokratische Zeiten.

Trotz dieser demokratisch äußerst bedenklichen Tendenzen sahen es die G7-Staaten nicht als notwendig an, demokratische Grundprinzipien und Rechte in ihre Forderungen aufzunehmen. Bisher existiert nicht einmal der erklärte Wille zu einer vereinheitlichten elektronischen Straßenverkehrsordnung, geschweige denn einer notwendigen Angleichung von Rechtsnormen.

Ingo Ruhmann und Ute Bernhardt

Ingo Ruhmann ist Informatiker, wissenschaftlicher Referent und Lehrbeauftragter an der FH Brandenburg. Zum Zeitpunkt des Erscheinens des Beitrags 1995 war er wissenschaftlicher Mitarbeiter bei Dr. Manuel Kiper, MdB, in Bonn.

Ute Bernhardt ist Informatikerin, wissenschaftliche Referentin und Lehrbeauftragte. Zum Zeitpunkt des Erscheinens des Beitrags war sie Geschäftsführerin des FIfF in Bonn.

Beide sind ehemalige Vorstandsmitglieder im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. und arbeiten zu Datenschutz, IT-Sicherheit sowie Informatik und Militär.

Der Weg in die Informationsgesellschaft darf nicht zur Gefährdung des Rechtssystems und der Demokratie führen und kann nur in wohlüberlegten Schritten und unter Beteiligung der Betroffenen erfolgen. Die demokratischen Werte und Ziele unserer Gesellschaft müssen Leitbild der Entwicklung sein. Ohne eine solche politische Lösung wird die Informationsgesellschaft zum Schreckgespenst.

Ein Danaergeschenk

Bisher lässt sich nur erkennen, dass es den politisch Verantwortlichen am Verständnis für die Tiefe der von ihnen mit der Informationsgesellschaft heraufbeschworenen sozialen und gesellschaftlichen Umwälzung fehlt. Die Frage nach Alternativen wird nirgendwo gestellt. Die Tragfähigkeit des sozialen Modells namens Informationsgesellschaft aus den frühen 70er Jahren bleibt unhinterfragt. Es stellt sich bei noch nicht einmal allzu genauer Betrachtung als undurchdachtes Konzept heraus, dessen politische, soziale und ökonomische Tragfähigkeit zweifelhaft ist. Nachvollziehbar sollte sein, dass durch die unausgewogene Verteilung der Produktivitätsgewinne sozialer Sprengstoff angesammelt wird. Diese mit Technikgläubigkeit und sozialer Kaltblütigkeit verfolgte Idee einer Gesellschaft kann sich als ebenso unrealisierbar erweisen wie die Atomtechnik. Wenn sich das politische System nicht selbst gefährden, gar überflüssig machen will, liegt hierin dringender Handlungsbedarf.

Der Beitrag ist die überarbeitete Fassung von Ute Bernhardt; Ingo Ruhmann: Mit den Konzepten von gestern in die Gesellschaft von morgen; in: Frankfurter Rundschau, 15.11.95, S. 18 bzw. – in der Langfassung – als Ute Bernhardt und Ingo Ruhmann: Revolution von oben. Der Weg in die Informationsgesellschaft; in: FIfF-Kommunikation, Heft 2/1995, S. 8-14

Humanistische Union u. a.

Grundrechte-Report 2014

Schwerpunkte des alternativen Verfassungsschutzberichts sind die Folgen der NSA-Überwachungsaffäre, das demokratie- und rechtsstaatsfeindliche Agieren des bundesdeutschen Verfassungsschutzes sowie der Umgang mit MigrantInnen – von der Zurückweisung an den europäischen Grenzen bis hin zur mangelnden Aufnahme in den Kommunen.

Am 3. Juni 2014 wurde der Grundrechte-Report 2014 durch die frühere Bundesjustizministerin, Sabine Leutheusser-Schnarrenberger, in Karlsruhe präsentiert. Der von acht namhaften Bürgerrechtsorganisationen herausgegebene Report zieht für das Berichtsjahr 2013 eine kritische Bilanz zum Umgang mit den Bürger- und Menschenrechten in Deutschland.

Sabine Leutheusser-Schnarrenberger erklärte anlässlich der Präsentation des Berichts: „*Die Vorgänge um die NSA und den NSU zeigen, dass es im Kernbereich des Grundrechtsschutzes in Deutschland schlecht aussieht. Ein freiheitlicher Rechtsstaat kann es nicht dulden, dass die im Geheimen agierenden Dienste den einzelnen Menschen zum bloßen Objekt ihrer Informationsbegehrlichkeiten entwürdigen. Der Grundrechte-Report analysiert dies schonungslos.*"

Die im Zuge der NSA-Affäre bekannt gewordenen Geheimdienstaktivitäten sowie die bisherige Verweigerung jeglicher rechtspolitischer Konsequenzen und Schutzmaßnahmen durch Bundesregierung und Justiz bilden einen Schwerpunkt der aktuellen Ausgabe. Rolf Gössner beschreibt in seinem Einleitungsbeitrag die Folgen der ausufernden, grenzen- und verdachtslosen Massenüberwachung. Die geheimdienstlichen Datenexzesse übertreffen nicht nur alle bisherigen Vorstellungen, sondern befördern Selbstkontrolle und vorauseilenden Gehorsam. Gössner spricht von einem „*geheimen Informationskrieg*" und einem präventiven Ausnahmezustand, in dem demokratische und rechtsstaatliche Regeln praktisch außer Kraft gesetzt werden. Der Vizepräsident der Internationalen Liga für Menschenrechte stellt fest: „*Dieser Angriff auf Substanz und Selbstverständnis freiheitlicher Demokratien erfolgt nicht etwa von außen, von ‚extremistischen' oder terroristischen Kräften, sondern aus dem Inneren des Systems – wie eine aggressive, überschießende Reaktion des Immunabwehrsystems.*"

Till Müller-Heidelberg, Elke Steven, Marei Pelzer, Martin Heiming, Heiner Fechner, Rolf Gössner, Ulrich Engelfried und Sophie Rotino (Hg.) (2014) Grundrechte-Report 2014 – Zur Lage der Bürger- und Menschenrechte in Deutschland; Frankfurt am Main: Fischer-Taschenbuch-Verlag
ISBN 978-3-596-03018-7;
Preis € 10,99; 240 Seiten

Elke Steven vom Komitee für Grundrechte und Demokratie betonte anlässlich der Präsentation: „*Der Zustand der Verfassungswerte zeigt sich gerade am Umgang mit den Schwächsten in der Gesellschaft. Wie schlecht es darum bestellt ist, zeigen zahlreiche Fallbeispiele des aktuellen Reports.*"

Dazu gehören Obdachlose, die von öffentlichen Orten verdrängt werden; Kinder, Jugendliche sowie psychisch auffällige Menschen, die in geschlossene Einrichtungen abgeschoben werden; MigrantInnen und Flüchtlinge, die von der deutschen Politik und Gesetzgebung oft nur noch als Sicherheits- und Sozialrisiko wahrgenommen werden.

Der Grundrechte-Report 2014 enthält zahlreiche Beispiele für die zunehmende Perfektionierung der Ausgrenzung und Abschottung gegenüber Flüchtlingen: Das beginnt mit der Überwachung und dem Zurückdrängen von Flüchtlingsbooten in internationalen Gewässern beispielsweise vor Mauretanien und Senegal; reicht über die 340 Millionen Euro teure Aufrüstung

des neuen Grenzüberwachungssystems EUROSUR – und endet noch lange nicht in der wahllosen Inhaftierung von Flüchtlingen in Europa, für die sich niemand zuständig fühlt und denen selbst einfachste Unterkünfte verweigert werden. Daneben werden zunehmend europäische BürgerInnen diskriminiert, denen in Deutschland Leistungen der Existenzsicherung verwehrt werden. Das zwingt sie in die Billiglohnarbeit und führt sie in die Obdachlosigkeit. Martin Heiming vom Republikanischen Anwältinnen und Anwälteverein: „*Europa will gegenwärtig der Ukraine ‚die Demokratie' bringen, und muss doch selbst erst lernen, dass menschliche Solidarität darin eine tragende Säule ist. Europa ist eine Sozialunion – oder überflüssig.*"

Der jährliche Report zur Lage der Bürger- und Menschenrechte in Deutschland bilanziert in insgesamt 42 Beiträgen kritisch die Verfassungswirklichkeit Deutschlands. Als „*wichtiges Instrument des Menschenrechts-Monitorings in Deutschland*" (Beate Rudolf) behandelt er die gesamte Bandbreite von Einschränkungen der Grundrechte durch Gesetzgeber, Verwaltung und Justiz sowie durch private Unternehmen. Aktuelle Fälle zur unverhältnismäßigen Einschränkung der Privatsphäre, der Glaubensfreiheit oder des Streikrechts im Arbeitsleben sind ebenso vertreten wie die zahlreichen Beschränkungen politischer Freiheitsrechte beispielsweise von Demonstrierenden und JournalistInnen. Die 18. Ausgabe des alternativen Verfassungsschutzberichts bietet deshalb einen ebenso umfassenden wie ernüchternden Blick auf den Zustand der Bürger- und Menschenrechte in Deutschland.

Quelle: Pressemitteilung der Humanistischen Union.

W&F Wissenschaft und Frieden 3/2014 – Die Kraft der Künste

Die Kraft der Künste – dazu der guatemaltekische Künstler Plinio Villagráh Galindo in seinem Interview: „*Die Kunst, wenngleich sie häufig als elitär bezeichnet wird, ist doch das einzige Medium, welches die Werkzeuge für Reflexion zur Verfügung stellt. Sie ist das Schlachtfeld der Ideen, der Kreativität, der Sensibilität als Waffe gegen die Gewalt.*" Damit verweist Villagráh Galindo auf den inhaltlichen Zusammenhang der beiden großen Themenfelder in der neuen W&F-Ausgabe: die Verbindung von Kunst zu Krieg und Frieden.

Wie greift Kunst das Thema Krieg und Frieden auf? Mit welchen ästhetischen Mitteln wird das Unfassbare ausgedrückt? Wie positionieren KünstlerInnen sich selbst und ihr künstlerisches Werk in diesem Zusammenhang? Es schreiben Friederike Pannewick: *Subversion in arabischer Literatur*, Benjamin T. Hilger: *Krieg und Musik – Panorama eines Wechselverhältnisses*, Louisa Prause: *Y'en a marre – HipHop in Bewegung*, Gerd Büntzly und Ulrich Klan: *Lebenslaute – Gewaltfreier Widerstand mit Konzertblockaden*, Jürgen Nieth: *Liedermacher und die Friedensbewegung*, Steffen Bruendel: *Kunst und Krieg 1914-18*, Plinio Villagráh Galindo im Interview mit María Cárdenas: *Dass wir zivilisiert sind, ist eine Lüge*, Tim Holert im Interview mit Felix Koltermann: *Bilder im Zeitalter des Drohnenkriegs*, Michael Schulze von Glaßer: *Bundeswehr-Bilder – Die Darstellung der deutschen Armee in aktuellen Filmproduktionen*, Linda Ebbers: *Theater und zivile Konfliktbearbeitung*.

Die Artikel außerhalb des Schwerpunktes beschäftigen sich mit den PhysikerInnen im Ersten Weltkrieg und mit den PazifistInnen vor dem Ersten Weltkrieg, mit der Debatte um eine Änderung des Parlamentsbeteiligungsgesetzes sowie mit der Entwicklung im Nahen Osten nach den Massenprotesten vor drei Jahren.

W&F liegt ein Dossier bei, das sich mit der so genannten Schutzverantwortung befasst. Alleine während der vergangenen zwölf Monate kam es zu vielfachem Eingreifen auswärtiger Mächte in Konflikte in formal souveränen Ländern, im Südsudan, in Zentralafrika, in Mali, in der Ukraine und anderswo. Diese sehr unterschiedlichen Eingriffe in sehr unterschiedliche Konfliktsituationen werden sehr unterschiedlich bewertet, als Unterstützung in einer Krisensituation, als Prävention in einem sich abzeichnenden Völkermord oder als aggressive Einmischung in die inneren Angelegenheiten eines Staates. Wann und wie internationales Eingreifen gerechtfertigt oder gar geboten erscheint, darüber findet seit vielen Jahren eine kontroverse Diskussion unter dem Schlagwort „Schutzverantwortung" statt. Auf dieses Konzept werfen Lou Pingeot und Wolfgang Obenland im Dossier *In wessen Namen?* einen kritischen Blick.

Wissenschaft & Frieden, 3/2014 **Die Kraft der Künste**
€ 7,50 plus Porto.
W&F erscheint vierteljährlich. Jahresabo 30 €, ermäßigt 20 €, Ausland 35 €, ermäßigt 25 €. 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, *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-Accounts
@FIfF_de und
@FaireComputer
@FIfF_AK_RUIN

FIfF-Blog
http://blog.faire-computer.de/

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** (Dortmund); 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

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	Britta Schinzel, Sara Stadler und Stefan Hügel
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	Universal Automatic Computer Model 120 – Foto Department of Interior, Bureau of Mines, 1961 Rails Girls Leipzig Workshops 2013 – Foto: Natalie Sontopski (links)
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.

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

Aktuelle Ankündigungen

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

Freedom not Fear 2014
26. bis 29. September in Brüssel

FIfF-Jahrestagung
7. bis 9. November 2014 in Berlin
„Der Fall des Geheimen – Blick unter den eigenen Teppich"

FIfF-Vorstandssitzung
9. November 2014 im Anschluss an die Jahrestagung

FIfF-Kommunikation
4/2014 »30 Jahre FIfF«
Stefan Hügel u.a.
Redaktionsschluss: 7. November 2014

1/2015 »Der Fall des Geheimen – Blick unter den eigenen Teppich«
Rainer Rehak u.a.
Redaktionsschluss: 6. Februar 2015

W&F – Wissenschaft & Frieden
1/14 – Konfliktdynamik im »Globalen Norden«
2/14 – Gewalt(tät)ige Entwicklung
3/14 – Künste, Krieg und Frieden
4/14 – Soldat

vorgänge - Zeitschrift für Bürgerrechte und Gesellschaftspolitik
#203 (3/13) – Religiöse Sonderrechte auf dem Prüfstand
#204 (4/13) – Polizei
#205 (1/14) – Sicherungsverwahrung
#206 (2/14) – Überwachung

DANA – Datenschutz-Nachrichten
1/14 – Konzerndatenschutz
2/14 – Internet der Dinge
3/14 – Datenschutz an Flughäfen
4/14 – Big Data

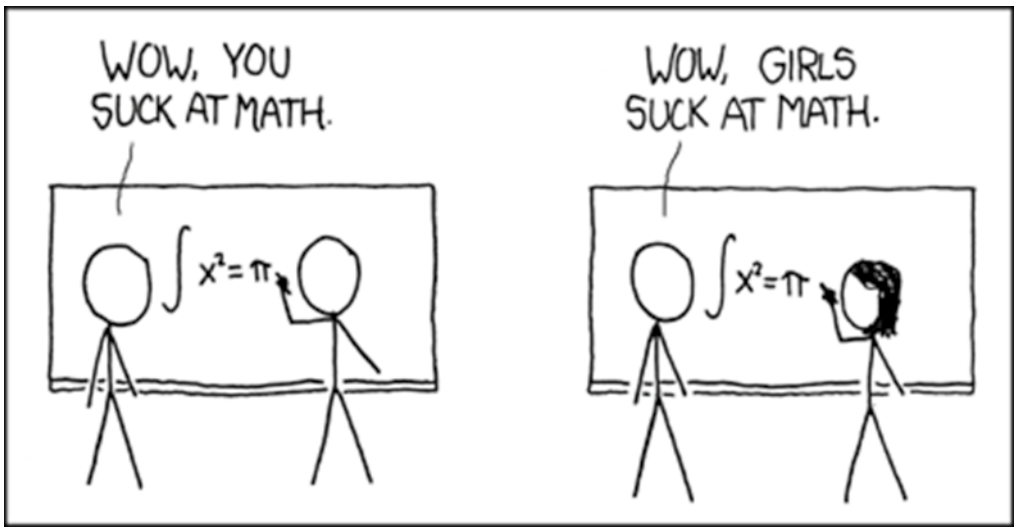
Das FIfF-Büro

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*

Bankverbindung
Sparda Bank Hannover eG
Spendenkonto: 800 927 929
IBAN: DE66 2509 0500 0800 9279 29
BIC: GENODEF1S09

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

Schluss FIfF



Quelle: xkcd.com, http://xkcd.com/385/
CC BY-NC 2.5, Randall Munroe, http://xkcd.com/about/

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