H 7625

FIfF-Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

29. Jahrgang 2012 Einzelpreis: 7 EUR **1/2012 – März 2012**

Dialektik der Informationssicherheit

Interessenskonflikte bei

Anonymität

ISSN 0938-3476

• Rüstung und Cyberwar • Informatik und Gesellschaft an Hochschulen •

FIfF Kommunikation

Titelbild: Deckblatt vom Flyer zur FIfF-Jahrestagung 2011
Flyer-Layout & -Design: Idealistik

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Inhalt

Ausgabe 1/2012

inhaltt

Schwerpunkt „Dialektik der Informationssicherheit“

09 Anonymität, Integrität und Vertraulichkeit vs. Strafverfolgung
- Phillip W. Brunst

16 Was ist eine Quellentelekommunikationsüberwachung?
- Felix Freiling

18 Schützenswerter Rohstoff Geist
- Interview mit Michael George

Berichte aus den Arbeitsgruppen

19 AG1: Killerroboter, Cyberwar & Co.
- Hans-Jörg Kreowski und Dietrich Meyer-Ebrecht

21 AG1: It's a Challenge – Militärische Roboterwettbewerbe
- Ralf E. Streibl

26 AG3: Faire Computer – Gibt's das?
- Sebastian Jekutsch

27 AG4: Facebook & Co. und meine Daten im WWW

27 AG5: Maltego – Data-Mining im Internet
- Iwan Gulenko

28 AG6: EU Sicherheitspolitik und -forschung
- Sylvia Johnigk

29 AG8: Europäische Vernetzung
- Stefan Hügel, Dietrich Meyer-Ebrecht und Jens Rinne

Retrospektive

71 Viren als Mittel des Cyberwar

71 Computerviren – ein Kampfmittel der Zukunft?
- FIfF e.V.

72 KGB-„khaker“ und CIA-Viren
- Ingo Ruhmann

Rubriken

69 Lesen – Neues für den Bücherwurm

75 Impressum/Aktuelle Ankündigungen

76 SchlussFIfF

03 Editorial
- Sylvia Johnigk, Kai Nothdurft und Stefan Hügel

Aktuelles

31 Log 1/2012
- Stefan Hügel

37 Hinter feindlichen Linien
- Kai Nothdurft

39 0. Spackeriade
- Stefan Hügel

41 Cyberwarfare
- Sylvia Johnigk und Kai Nothdurft

46 Bremer Universität bestätigt Zivilklausel
- Ralf E. Streibl

48 Interaktiver Rüstungsatlas
- Andreas Seifert

52 Für ein kontrollierbares Abkommen zur Abschaffung aller Atomwaffen
Appell aus Berlin!

53 Keine Panik
- Andrea Knaut, Jörg Pohle und Stefan Ullrich

55 Verlernen Informatik-Studierende Verantwortungnahme?
- Britta Schinzel, Monika Götsch, Yvonne Heine, Karin Kleinn und Michael Richter

64 „Scrum“ als Innovations- und Emanzipationsgenerator?
- Daniela Wühr und Stefan Sauer

68 Das „geistige Eigentum“ ad-ACTA
- Ulrich Klotz

69 Legt ACTA ad ACTA!
- FIfF e.V.

FIfF e.V.

04 Brief an das FIfF – Erinnern und Handeln
- Stefan Hügel

05 Ankündigung FIfF-Jahrestagung 2012 in Fulda

05 Ankündigung FIfF-Studienpreis 2012

06 Gemeinsame Erklärung zum sechsjährigen Bestehen der EU-Richtlinie zur Vorratsdatenspeicherung
- Arbeitskreis Vorratsdatenspeicherung

07 H.R. 3261, the Stop Online Piracy Act
- European Digital Rights – offener Brief

08 Aufruf zur Teilnahme an der SIGINT 2012

Editorial

Dialektik der Informationssicherheit – der Titel unserer letztjährigen Jahrestagung ist gleichzeitig das Schwerpunktthema dieses Hefts. Nahezu die gesamte Gesellschaft nutzt Informationen in digitaler Form. Die Computerisierung der Gesellschaft hat insbesondere durch die allgegenwärtige Nutzung des Internet im Privatbereich, im Geschäftsleben und in Behörden und ihren Verwaltungsprozessen die Sicherheit dieser Informationen zu einer zentralen gesellschaftlichen Herausforderung werden lassen. Da fast alle Lebensbereiche davon betroffen sind, fokussieren sich in den Sicherheitsinteressen auch die verschiedenen gesellschaftlichen Interessen, die Gemeinsamkeiten und Konflikte, Gestaltungsmöglichkeiten, Macht, Wirtschaftsinteressen und elementare Fragen des Zusammenlebens.

Dialektik zeigt sich dabei im Vorhandensein dieser verschiedenen Interessen, von Zielkonflikten, von Widersprüchlichkeiten, von allem innewohnenden Vor- und Nachteilen.

Einige der Gegensätze sind in der folgenden Tabelle beispielhaft dargestellt:

Beispiele	Staat	Bürger	Unternehmen
Staat	Spionage, Cyberwar, Sabotage	Vorratsdaten-speicherung, Überwachung, z. B. INDECT vs. Datenschutz, Recht auf freie Meinungsäußerung Bundestrojaner, ePA, DeMail, Geheimhaltung vs. Transparenz, Pressefreiheit z. B. Redaktionsdurchsuchung, Informantenschutz, Wikileaks, Geheimdienste vs. demokratische Kontrolle	Wirtschafts-spionage, Steuerfahndung, Geldwäsche, Aufsichtsbehörden (Datenschutz, Compliance, BAFIN, ...), SWIFT Datenabkommen, Einreisebestimmungen (Zoll schnüffelt am Laptop rum ...)
Bürger	Kriminalitäts-bekämpfung, Terrorabwehr, Datenschutz, Stalking, Cybermobbing	Recht auf Fassadenbilder (Google Streetview) vs. Datenschutz, Stalking, Cybermobbing vs. Anonymität im Internet	Verbraucherschutz, Herkunftsnachweise, Inhaltsstoffe, Umweltpolitik des Unternehmens, Anlegerinformationen
Unternehmen	Digitale Verwertungsrechte, Copyright/ACTA, Patentschutz, Strafverfolgung bei Betrug, Sabotage, Beratung, Schutz vor Cyberattacken, Kartellrecht (Schutz vor unlauterem Wettbewerb)	Anonymes Bezahlen, Werbung/Marketing, Nutzung von Diensten, Monopolen, Arbeitnehmerdatenschutz vs. Kontrolle von Unternehmensprozessen (Sicherheitspolicies), Kreditwürdigkeit	Wirtschafts-kriminalität, Kreditwürdigkeit, Schutz von elektronischen Geschäftsgeheimnissen, Verträge, Preise, Kundendaten bei Outsourcing und Kooperationen

Die Dialektik findet sich selbst in den Sicherheitswerkzeugen wieder. Ein Verschlüsselungsverfahren kann gegensätzlichen Interessen dienen. Zum Beispiel kann mit SSL-Verschlüsselung eine Internetverbindung geschützt werden. Sie kann aber auch von einem Angreifer genutzt werden, um die Verbindung eines Trojaners zu seinem *Command-and-Control*-Server zu verschleiern.

Vertraulichkeit und Privatsphäre stehen staatlichen Sicherheitsinteressen gegenüber. *Phillip Brunst* widmet sich diesem Aspekt in seinem Artikel *Anonymität, Integrität und Vertraulichkeit vs. Strafverfolgung*. *Felix Freiling* untersucht, unter welchen Bedingungen ein gesetzeskonfomer Einsatz von Onlinetrojanern möglich ist. Wie die Sicherheitsindustrie in geschlossenen Lobbygruppen die Sicherheitsstrategie und Politik vorantreibt, beschreibt *Sylvia Johnigk* in ihrem AG-Bericht. Wie sich auf der anderen Seite die Netzaktivisten auf europäischer Ebene organisieren, schildern *Stefan Hügel, Dietrich Meyer-Ebrecht* und *Jens Rinne* im Bericht zur Europa-AG.

Doch auch Marktforschung und Verwertungsinteressen haben wenig Interesse an Anonymität und Vertraulichkeit. In der AG *Maltego* zeigte *Iwan Gulenko*, wie leicht sich Daten aus öffentlichen Quellen verknüpfen lassen. *Michael George* beschäftigt sich im Interview *Schützenswerter Rohstoff Geist* mit dem Problem der Wirtschaftsspionage. Es mag auf den ersten Blick überraschen, in der FIfF-Kommunikation ein Interview zu lesen, das ursprünglich ein Vertreter des Verfassungsschutzes dem Bayernkurier gegeben hat. Wir dokumentieren es hier als Beitrag zur Diskussion.

Zusätzlich zu den Beiträgen zur Infomationssicherheit im engen Sinne berichten wir über zwei weitere Arbeitsgruppen, die sich thematisch im Fokus des FIfF befinden: in den Beiträgen von *Hans-Jörg Kreowski* und *Dietrich Meyer-Ebrecht* und von *Ralf E. Streibl* zu *Killerroboter, Cyberwar & Co.*, und in dem Beitrag von *Sebastian Jekutsch, Faire Computer – Gibt's das?*

Den aktuellen Teil bilden vor allem Beiträge zu zwei weiteren Schwerpunktthemen: Der Themenbereich *Rüstung und Cyberwar* beginnt mit einem Beitrag von *Sylvia Johnigk* und *Kai Nothdurft* zur Cyberwarfare. Der Beitrag schließt mit einer Reihe von Forderungen, zu deren Diskussion wir aufrufen, um sie zu einem Forderungskatalog des FIfF weiterzuentwickeln. *Ralf E. Streibl* kommentiert im Anschluss daran Erfreuliches: Die Universität Bremen hat die Weitergeltung der Zivilklausel bekräftigt – auch künftig lehnt sie die Beteiligung an Forschung mit militärischer Zielsetzung ab. *Andreas Seifert* von der *Informationsstelle Militarisierung* (IMI) beschreibt das Projekt *Interaktiver Rüstungsatlas*, und wir drucken den Appell aus Berlin zur Abschaffung aller Atomwaffen.

Im Themenkomplex *Informatik und Gesellschaft* an Hochschulen fordern *Andrea Knaut, Jörg Pohle und Stefan Ullrich* dazu auf, einen Masterstudiengang Informatik und Gesellschaft zu etablieren. Danach berichten *Britta Schinzel et al.* aus der DFG-Studie *Weltbilder der Informatik*, und fragen dabei: *Verlernen Informatik-Studierende Verantwortungnahme?*

Eine Untersuchung von *Daniela Wühr* und *Stefan Sauer* zur Entwicklungsmethodik *Scrum als Innovations- und Emanzipationsgenerator* und einige Gedanken von *Ulrich Klotz* anlässlich der weltweiten Demonstrationen gegen *ACTA* beschließen den aktuellen Teil.

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

Sylvia Johnigk, Kai Nothdurft, Stefan Hügel
für die Redaktion

Brief an das FIfF

Erinnern und Handeln

Liebe Mitglieder des FIfF, liebe Leserinnen und Leser,

am 27. Januar 2012 gedachte der Bundestag der Befreiung des Konzentrationslagers Auschwitz. In bewegenden Worten schilderte Marcel Reich-Ranicki den Tag, an dem die Deportation der Bürger jüdischen Glaubens aus dem Warschauer Ghetto begann. Wir dürfen nie vergessen, welche Verbrechen damals von Deutschen verübt wurden.

Doch sich zu erinnern, reicht nicht aus – wichtig sind die Handlungen, die wir daraus ableiten. Einer der Grundsteine der nationalsozialistischen Herrschaft wurde an gleicher Stelle gelegt: Am 24. März 1933 wurde im damaligen Deutschen Reichstag das „Gesetz zur Behebung der Not von Volk und Reich" beschlossen – das Ermächtigungsgesetz. Es fand eine große Mehrheit; auch bürgerliche Parteien stimmten dem Gesetz zu.

Wären die damaligen politischen Eliten ihrer Verantwortung besser gerecht geworden – vielleicht wäre dann die Gedenkstunde nicht notwendig gewesen.

Auch heute beobachten wir wie damals das Phänomen, dass rechter Terror verharmlost wird. Fast unter den Augen des Verfassungsschutzes konnten Neonazis zehn Menschen ermorden. „Rechts blind, links blöd", so schrieb der Politikberater Michael Spreng in seinem Blog – immerhin 2002 der Wahlkampfmanager des damaligen konservativen Kanzlerkandidaten Edmund Stoiber. Durch rechte Gewalt kamen seit der Wiedervereinigung nach Recherchen der linker Umtriebe wahrlich unverdächtigen Zeitung *Die Welt* 182 Menschen ums Leben. Dass der nun nicht mehr zu leugnende rechte Terror überraschend sein soll, befremdet unter diesen Umständen.

Man kann ihn aber auch einfach wegdefinieren: Die National*sozialistische* Deutsche *Arbeiter*partei sei ja wohl eine linke Partei gewesen, wurde unter dem Namen @SteinbachErika getwittert – eine bewusste „Provokation", wie später nachgeschoben wurde. Dass es sich dabei tatsächlich um die Frankfurter Bundestagsabgeordnete handelte, vermag man sich kaum vorzustellen. Bei einer derartigen Relativierung der Verbrechen des Dritten Reiches und dem Versuch, sie dem politischen Gegner in die Schuhe zu schieben, fehlen mir die Worte.

Aber der Verfassungsschutz hatte halt Wichtigeres zu tun. Spitzenpolitiker der Partei *Die Linke* werden seit Jahren beobachtet. Es handelt sich dabei nicht etwa um unbelehrbare SED-Kader, sondern um pragmatisch agierende Vertreter der Bundestagsfraktion. Sie fordern einen demokratischen Sozialismus – wie er keineswegs im Widerspruch zum Grundgesetz steht. Dabei fehlt den Verantwortlichen und Befürwortern der geheimdienstlichen Beobachtung jegliches Unrechtsbewusstsein – im Gegenteil, sie fordern sogar noch eine Ausweitung. Allen voran der CSU-Generalsekretär Dobrindt, der sogar fand, man müsse über ein Verbot der Partei nachdenken.

In Öffentlichkeit und Medien rührt sich vorsichtige Kritik: „Irgendwelche Rücktritte? – Nö. Nennenswerte personelle Konsequenzen? – Nö. Wurden Landesämter für Verfassungsschutz geschlossen oder reformiert? – Nö", kommentierte Isabel Schayani in den Tagesthemen. „Was passiert jetzt? Wir bekommen eine Neonazi-Datei."

Und doch noch die Vorratsdatenspeicherung? Bei jeder Gelegenheit gebetsmühlenartig gefordert, warte ich inzwischen nur noch darauf, dass sie mir mein Hausarzt als Mittel gegen Grippe verschreibt. Eine Studie des Max-Planck-Instituts ergab nun, dass die Vorratsdatenspeicherung keine Auswirkung auf die Aufklärung von Straftaten hat. Ein „Schutzlücke" nach dem Wegfall der Vorratsdatenspeicherung in Folge des Urteils des Bundesverfassungsgerichts vom 2. März 2010 existiert nicht. Bekannt wurde die Studie erst durch den Chaos Computer Club.

Auch von anderer Seite sollen wir überwacht werden. SOPA, PIPA, ACTA – hinter diesen Abkürzungen verbergen sich weit gehende Überwachungs- und Zensurbefugnisse; diesmal im Interesse großer Medienkonzerne, die glauben, ihre eigenen Kunden überwachen zu müssen. Am 18. Januar 2012 blieben viele Web-Portale schwarz, darunter die englischsprachige Wikipedia.

Auch auf den Straßen regt sich Widerstand. Fast 50.000 Menschen gingen am 11. Februar 2012 bei Eiseskälte in vielen deutschen Städten auf die Straße, um gegen ACTA zu protestieren. Demonstrationen fanden weltweit statt. Die „Netzgemeinde", die sich inzwischen gar nicht mehr so sehr vor der Gesamtbevölkerung unterscheidet, fordert ihre Rechte ein. Dennoch: „Ihr werdet den Kampf verlieren", so unverdrossen der CDU-Bundestagsabgeordnete Ansgar Heveling, Anhänger der repressiven Durchsetzung eines veralteten Verständnisses von Urheberrecht – und Mitglied der Enquête-Kommission *Internet und digitale Gesellschaft.*

Warten wir's ab.

Mit FIfFigen Grüßen

Stefan Hügel

bitte vormerken – bitte vormerken – bitte vormerken – bitte vormerken – bitte vormerken

FIfF-Jahrestagung 2012

gemeinsam mit dem 26. Fuldaer Informatik Kolloquium

Digitalisierte Gesellschaft – Wege und Irrwege

9. – 11. November 2012 in Fulda

in der Hochschule Fulda, Fachbereich Angewandte Informatik

Weitere Informationen und Anmeldung unter
www.fiff.de/2012 oder bei der
Hochschule Fulda FB AI/IfF JT
Marquardstr. 35, 36039 Fulda

bitte vormerken – bitte vormerken – bitte vormerken – bitte vormerken – bitte vormerken

Das FIfF verleiht 2012 wieder den

FIfF-Studienpreis

für herausragende Abschlussarbeiten aus dem Bereich Informatik und Gesellschaft.

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

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

Wir laden dazu ein, geeignete Arbeiten bis 31. Mai 2012 einzureichen.

Das Preisgeld beträgt:

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

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

FIfF-Geschäftsstelle – Studienpreis 2012 – Goetheplatz 4, 28203 Bremen
oder per E-Mail an *studienpreis@fiff.de*. Weitere Details unter *http://www.fiff.de/studienpreis.*

Der Preis wird in einer Feierstunde im Rahmen der FIfF-Jahrestagung am Samstag, 10. November 2012 in Fulda verliehen.

Gemeinsame Erklärung zum sechsjährigen Bestehen der EU-Richtlinie zur Vorratsdatenspeicherung

Die vom Europäischen Parlament am 14. Dezember 2005 beschlossene Richtlinie 2006/24 zur Vorratsdatenspeicherung verpflichtet jeden EU-Mitgliedsstaat, Telekommunikationsgesellschaften Informationen über die Verbindungen ihrer sämtlichen Kunden aufzeichnen zu lassen. Zur Erleichterung etwaiger strafrechtlicher Ermittlungen soll nachvollziehbar sein, wer mit wem in den letzten 6-24 Monaten per Telefon, Handy oder E-Mail in Verbindung gestanden hat. Bei Handy-Telefonaten, SMS und Smartphone-Nutzung muss auch der jeweilige Standort des Benutzers festgehalten werden. Die Vorratsspeicherung von Internetkennungen (IP-Adressen) soll in Verbindung mit anderen Informationen zudem nachvollziehbar machen, wer was im Internet gelesen, gesucht oder geschrieben hat.

Frans Jozef Valenta, Bonn (CC BY-NC-ND 3.0)

Eine derart weitreichende Registrierung des Verhaltens der Menschen in ganz Europa halten wir für inakzeptabel. Ohne jeden Verdacht einer Straftat sollen sensible Informationen über die sozialen Beziehungen (einschließlich Geschäftsbeziehungen), die Bewegungen und die individuelle Lebenssituation (z. B. Kontakte mit Ärzten, Rechtsanwälten, Psychologen, Beratungsstellen) von über 500 Millionen Bürgerinnen und Bürgern der EU gesammelt werden. Damit höhlt eine Vorratsdatenspeicherung Anwalts-, Arzt-, Seelsorge-, Beratungs- und andere Berufsgeheimnisse aus und begünstigt Datenpannen und -missbrauch. Sie untergräbt den Schutz journalistischer Quellen und beschädigt damit die Pressefreiheit im Kern. Sie beeinträchtigt insgesamt die Funktionsbedingungen unseres freiheitlichen demokratischen Gemeinwesens. Die enormen Kosten einer Vorratsdatenspeicherung sind ohne Erstattungsregelung von den europäischen Telekommunikationsunternehmen zu tragen. Dies zieht Preiserhöhungen nach sich, führt zur Einstellung von Angeboten und belastet mittelbar auch die Verbraucher.

Untersuchungen belegen, dass bereits die gegenwärtig verfügbaren Kommunikationsdaten ganz regelmäßig zur effektiven Aufklärung von Straftaten ausreichen. Es gibt keinen wissenschaftlichen Beleg dafür, dass eine Vorratsdatenspeicherung besser vor Kriminalität schützte. Dagegen kostet sie Millionen von Euro, gefährdet die Privatsphäre Unschuldiger, beeinträchtigt vertrauliche Kommunikation und ebnet den Weg in eine immer weiter reichende Massenansammlung von Informationen über die gesamte europäische Bevölkerung.

In Deutschland wurde die gesetzliche Regelung zur Vorratsdatenspeicherung im März 2010 vom Bundesverfassungsgericht für verfassungswidrig und nichtig erklärt, da sie unverhältnismäßig weit in das Grundrecht auf Schutz des Telekommunikationsgeheimnisses eingriff. Rechtsexperten erwarten, dass auch die europäische Richtlinie zur Vorratsdatenspeicherung vor dem Europäischen Gerichtshof keinen Bestand haben wird, weil sie gegen die europäischen Grund- und Menschenrechte verstößt. Nichtsdestotrotz will die EU-Kommission eine neuerliche Umsetzung dieser Richtlinie in Deutschland im Wege eines Vertragsverletzungsverfahrens erzwingen.

Als Vertreter der Bürgerinnen und Bürger, der Medien, der freien Berufe und der Wirtschaft lehnen wir eine flächendeckende und verdachtsunabhängige Vorratsdatenspeicherung geschlossen ab. Wir appellieren an die in Deutschland politisch Verantwortlichen,

1. keinerlei verdachtslose Vorratsspeicherung von Informationen über jedes Telefonat, jede SMS, jede E-Mail oder jede Internetverbindung wieder anzuordnen,

2. die Abweichung Deutschlands von der EU-Richtlinie 2006/24 zur Vorratsdatenspeicherung von der EU-Kommission genehmigen zu lassen und nötigenfalls die Genehmigung einzuklagen,

3. die EU-Richtlinie zur Vorratsdatenspeicherung bis zur Entscheidung des Europäischen Gerichtshofs über die Gültigkeit dieser Richtlinie und über den Genehmigungsantrag nicht umzusetzen, selbst wenn der Gerichtshof gegebenenfalls eine Geldbuße gegen Deutschland verhängen könnte,

4. sich für eine Aufhebung der EU-Richtlinie zur Vorratsdatenspeicherung und für ein europaweites Verbot jeder verdachtslosen Vorratsspeicherung von Verbindungsdaten einzusetzen.

Mitzeichner:

Aktionsbündnis Sozialproteste (ABSP), Arbeitskreis Vorratsdatenspeicherung, Arbeitskreis Zensur, Berufsverband Deutscher Psychologinnen und Psychologen e.V. (BDP), Bundesverband Deutscher Zeitungsverleger e.V. (BDZV), Bund demokratischer Wissenschaftlerinnen und Wissenschaftler e.V. (BdWi), Bürgerinitiative Umweltschutz e.V., Bürgerrechte & Polizei/ CILIP, Campact e.V., Chaos Computer Club e.V. (CCC), contrAtom, Dachverband Freier Weltanschauungsgemeinschaften, data:recollective, Deutscher Freidenker-Verband, Deutscher Journalisten-Verband (DJV), Digitale Gesellschaft e.V., Digital Unite e.V., FoeBuD e.V., Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF), Frauenverband Courage e.V., FREELENS e.V. (Verband der Fotojournalistinnen und Fotojournalisten), German Privacy Foundation, Gesellschaft zur Wahrung der Grundrechte e.V. (GWG), Institut für Sozialwissenschaftliche Praxis und Analyse e.V., Berlin, Katholische Junge Gemeinde, LabourNet Germany, Lesben- und Schwulenverband in Deutschland (LSVD), MOGiS e.V. – Eine Stimme der Vernunft, naiin – no abuse in internet e.V., Naturfreundejugend, Netzwerk Rauchen e.V., Republikanischer Anwältinnen- und Anwälteverein e.V. (RAV), Stuttgarter Bündnis für Versammlungsfreiheit, Verband der Freien Lektorinnen und Lektoren e.V., Verbraucherzentrale Bundesverband e.V. – vzbv, Vereinigung Demokratischer Juristinnen und Juristen e.V., Verein zur Förderung der Suchmaschinen-Technologie und des freien Wissenszugangs e.V. (SuMa-eV)

European Digital Rights – offener Brief

H.R. 3261, the Stop Online Piracy Act

Chairman Lamar Smith, Committee on the Judiciary
The Honorable John Conyers, Jr., Chairman, Committee on the Judiciary
Washington D.C.

November 15, 2011

Dear Chairman Smith and Ranking Member Conyers,

as press freedom and human rights advocates, we write to express our deep concern with H.R. 3261, the Stop Online Piracy Act (SOPA). While this is a domestic bill, there are several provisions within SOPA that would have serious implications for international civil and human rights which raise concerns about how the United States is approaching global internet governance. The United States has long been a strong advocate for the protection and promotion of an open Internet. However, by institutionalizing the use of internet censorship tools to enforce domestic law in the United States creates a paradox that undermines its moral authority to criticize repressive regimes.[1] We urge the United States to uphold its proclaimed responsibility as a leader in internet freedom and reject bills that will censor or fragment the web.

Through SOPA, the United States is attempting to dominate a shared global resource. Building a nationwide firewall and creating barriers for international website and service operators makes a powerful statement that the United States is not interested in participating in a global information infrastructure. Instead, the United States would be creating the very barriers that restrict the free flow of information that it has vigorously challenged abroad. By imposing technical changes to the open internet while eroding due process, SOPA introduces a deeply concerning degree of legal uncertainty into the internet economy, particularly for businesses and users internationally. Business cannot be conducted online when international users and businesses do not have faith that their access to payments, domain names, and advertising will be available, raising challenges to economic development and innovation. This is as unacceptable to the international community as it would be if a foreign country were to impose similar measures on the United States.

EUROPEAN DIGITAL RIGHTS

The provisions in SOPA on DNS filtering in particular will have severe consequences worldwide. In China, DNS filtering contributes to the Great Firewall that prevents citizens from accessing websites or services that have been censored by the Chinese government.[2] By instituting this practice in the United States, SOPA sends an unequivocal message to other nations that it is acceptable to censor speech on the global Internet. Additionally, Internet engineers have argued in response to the Protect IP Act, DNS filtering would break the internet into separate regional networks.[3] Worse still, the circumvention technology that can be used to access information under repressive Internet regimes would be outlawed under SOPA, the very same technology whose development is funded by the State Department.

SOPA puts the interests of rightsholders ahead of the rights of society. SOPA would require that web services, in order to avoid complaints and lawsuits, take "deliberate actions" to prevent the possibility of infringement from taking place on their site,

pressuring private companies to monitor the actions of innocent users. Not only will this effectively negate the safe harbor protection provided in the Digital Millennium Copyright Act (DMCA), but the proposed legislation would disproportionally affect small online communities who lack the capacity to represent their users in legal battles. Wrongly accused websites would suffer immediate losses as payment systems and ad networks would be required to comply with a demand to block or cease doing business with the site pending receipt of a legal counter-notice. Even then, it would still be at the discretion of these entities to reinstate service to the website regardless of the merits of an alleged rightsholder's claim, robbing online companies of a stable business environment and creating a climate where free speech is subject to the whims of private actors.

Censoring the internet is the wrong approach to protecting any sectoral interest in business. By adopting SOPA, the United States would lose its position as a global leader in supporting a free and open Internet for public good.

The international civil and human rights community urges Congress to reject the Stop Online Piracy Act.

Best regards,

Access, AGEIA DENSI (Argentina), ahumanright.org, Association for Progressive Communications (APC), Bits of Freedom (The Netherlands), Center for Media Justice, Center for Rural Strategies, Centre for Internet and Society (India), Church of Sweden, Communication Is Your Right!. Computer Professionals for Social Responsibility, Consumers International, Derechos Digitales (Chile), Digitale Gesellschaft e.V. (Germany), Digital Rights Ireland, Electronic Frontier Finland (Effi), European Digital Rights (EDRi) (Association of 27 digital rights groups from around Europe), Center for Technology and Society (CTS/FGV) (Brazil), Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF) (Germany), Free Network Foundation, Free Press, Free Software Foundation, Global Partners & Associates, GreenNet (England), The Julia Group (Sweden), Instituto Nupef (Brazil), Index on Censorship, Internet Democracy Project (India), Karisma (Colombia), La Quadrature du Net (France), May First/People Link, MobileActive.org, Net Users' Rights Protection Association (NURPA) (Belgium), Open Rights Group (ORG) (UK), Open Spectrum Alliance, Palante Technology Cooperative, The Public Sphere Project, Reporters Without Borders/Reporters sans Frontières, Virtual Activism, wlan slovenija (Slovenia), 10com (European Union)

Endnotes

1 *http://blogs.lse.ac.uk/mediapolicyproject/2011/11/02/freedom-abroad-repression-at-home-the-clinton-now-cameron-paradox/*

2 *http://opennet.net/research/profiles/china*

3 *Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf*

FIfF e.V.

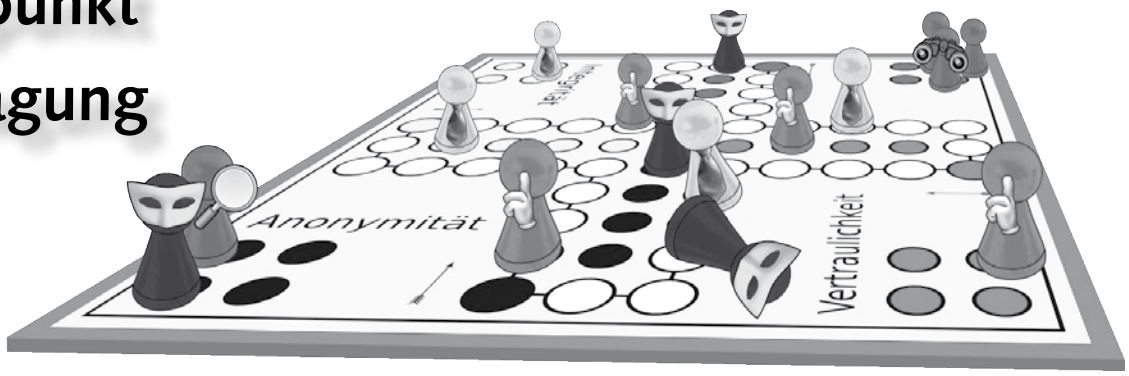
Aufruf zur Teilnahme an der SIGINT 2012

Vom 18. bis 20. Mai 2012 findet zum dritten Mal die SIGINT im Kölner Medienpark statt. Die Abkürzung SIGINT steht zum einen für *Signals Intelligence*, die nachrichtendienstliche Informationsgewinnung, zum anderen für *Signal Interrupt*, ein unter Unix-Systemen gesendetes Signal zur Benachrichtigung von Prozessen. Zwischen diesen Bedeutungspolen möchte sich die Konferenz verortet wissen (*http://sigint.ccc.de*). Veranstalter ist der Chaos Computer Club. Die SIGINT ist eine Konferenz für Hacker, Netzbewohner und Aktivisten. Schwerpunkt ist die Auseinandersetzung mit gesellschaftlichen Auswirkungen der Informationstechnik insbesondere im politischen Kontext – im Gegensatz zum alljährlich stattfindenden Chaos Computer Congress, der überwiegend eine Hackerkonferenz ist. Es wird dazu Vorträge und Workshops geben.

Das FIfF wird zum zweiten Mal einen Stand haben, um den Verein und unsere Arbeit einem großen Kreis von Aktivisten und Interessierten vorzustellen. **Wir suchen deshalb Mitstreiter, die uns bei der Vorbereitung und Standbetreuung helfen.**

Bitte meldet Euch zahlreich bei *fiff@fiff.de*.

Schwerpunkt Jahrestagung 2011



Phillip W. Brunst

Anonymität, Integrität und Vertraulichkeit vs. Strafverfolgung

Geht es um Gründe, das Recht auf Anonymität[1] im Internet oder etwa das vom Bundesverfassungsgericht herausgearbeitete neue Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme[2] gegenüber den Bürgerinnen und Bürgern einzuschränken, werden oftmals die Interessen der Strafverfolgung oder der Gefahrenabwehr ins Feld geführt. Im Vortrag des Autors auf der FIfF-Jahrestagung, dessen Kernthesen hier wiedergegeben werden, wurden wichtige Rahmenbedingungen dargestellt, die zwar einerseits die große Bedeutung von Computer- und Internetdaten für Ermittlungs- und Strafverfahren belegen, andererseits aber auch deutlich machen, dass bereits mit der gegenwärtigen Gesetzeslage weitreichende Eingriffe in das Recht auf Anonymität sowie in die Vertraulichkeit und Integrität informationstechnischer Systeme möglich sind.

Die Bedeutung von Computer- und Internetdaten bei der Bekämpfung klassischer IT-Straftaten ist unmittelbar ersichtlich. Ohne etwa Zugriff auf die IP-Adresse eines E-Bay-Betrügers oder eines Angreifers auf ein Computersystem zu haben, sind Ermittlungen – abgesehen von wenigen Ausnahmen[3] – von Beginn an zum Scheitern verdammt. Die Verkehrsdaten sind in diesem Fall die einzigen Spuren, die zum Täter führen können. Aber auch bei eher klassischen Straftaten ist die Bedeutung von (insb. Verkehrs-) Daten unübersehbar. So geben z. B. Telefon- und Internetverbindungen Aufschluss über Gruppen-, Kommunikations- und Kommandostrukturen im Bereich der organisierten Kriminalität und liefern damit einen wichtigen Baustein für erste Ermittlungsansätze. Bei anderen Straftaten, wie z. B. dem sog. „Enkeltrick"[4] sind sie womöglich die einzige Möglichkeit, verwertbare Hinweise auf die Identität der Täter zu erhalten.

Ob trotz dieser Bedeutung ein echter Reform-Bedarf im Sinne einer weiteren Einschränkung von Bürgerrechten besteht, erscheint zumindest auf den ersten Blick zweifelhaft, wenn man sich vor Augen führt, welche Eingriffe bereits nach der gegenwärtigen Rechtslage zulässig sind. Diese Eingriffe lassen sich für den Bereich der Internetstraftaten in drei große Bereiche unterteilen, nämlich den Zugriff auf Bestands-, Verkehrs- und Inhaltsdaten.

I. Zugriff auf Bestandsdaten

Bestandsdaten sind nach § 3 Nr. 3 TKG Informationen, die für die Begründung, die inhaltliche Ausgestaltung, die Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Vereinfacht ausgedrückt handelt es sich um identifizierende Informationen, die für die Vertragsabwicklung zwingend benötigt werden, etwa Name und Anschrift einer Person. Diese Daten sind jedoch insbesondere bei den über das Internet angebotenen kostenlosen Dienstleistungen, etwa bei Freemailern, nicht notwendig – diese Dienste werden gerade gegenüber jedermann erbracht, ohne dass die Identität des Nutzers eine Rolle spielen würde. Die Erhebung personenbezogener Daten ist daher nicht erforderlich und somit datenschutzrechtlich unzulässig. In § 13 Abs. 6 TMG wurde dieses Prinzip für den Bereich der Telemedien auch ausdrücklich festgehalten:

> *„Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren."*

In der Praxis wird dennoch häufig versucht, bei der Registrierung eine Vielzahl personenbezogener Daten zu erlangen, auch wenn diese für das eigentliche Angebot gar nicht erforderlich sind. Zum Teil setzen sich Nutzer hiergegen indirekt zur Wehr, indem frei erfundene oder aus dem Telefonbuch abgeschriebene Phantasiedaten verwendet werden.[5] Dass aber offenbar dennoch die hinterlassenen personenbezogenen Daten in vielen Fällen der Wahrheit entsprechen, zeigen die Abfragen nach §§ 112, 113 TKG. Nach diesen Vorschriften können verschiedene Behörden Bestandsdaten bestimmter TK-Anbieter über die Bundesnetzagentur abfragen lassen. Seit dem Jahr 2001 hat sich die Anzahl der auf diesem Weg generierten Bestandsdatenabfragen von zunächst 3,2 auf zuletzt 26,6 Millionen Abfragen pro Jahr gesteigert[6] – umgerechnet entspricht dies ca. 73.000 Abfragen von Bestandsdaten pro Tag. Angesichts der Bedeutung von Bestandsdaten zur Identifizierung von Internetnutzern verwundert es nicht, dass Gesetzgeber weltweit versuchen, verbleibende *Schlupflöcher* für eine anonyme Internetnutzung zu

schließen. So war in Italien von 2005 bis zum Ende des Jahres 2010 zum Beispiel keine anonyme Nutzung von Internet-Cafés mehr möglich, da gesetzlich eine vorherige Identifizierung festgeschrieben war.[7] Gleiches gilt in Deutschland für den Bereich der Prepaid-Telefone: Während ein sachlicher Zwang zur Identifizierung hier nicht erkennbar ist, da alle möglicherweise anfallenden Kosten bereits im Vorfeld entrichtet werden müssen, und eine solche Datenspeicherung auch gegen den Gedanken der Datensparsamkeit (§ 3a BDSG) verstößt, ist sie dennoch gesetzlich in § 111 TKG festgeschrieben worden. Danach müssen alle geschäftsmäßigen Anbieter von Telekommunikationsdiensten, die dabei Rufnummern oder andere Anschlusskennungen vergeben, u.a. den Namen und die Anschrift des Anschlussinhabers erheben, speichern und für Anfragen der Behörden abrufbar halten.[8]

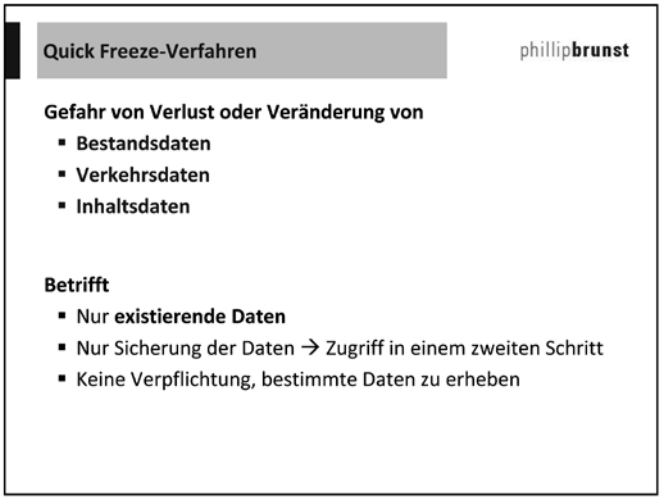
II. Zugriff auf Verkehrsdaten

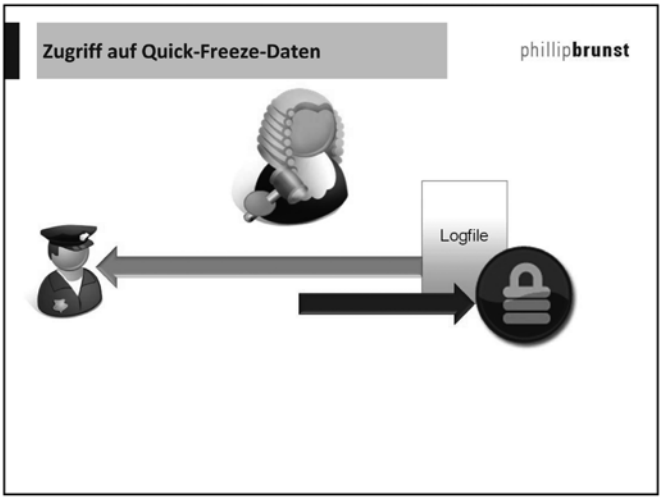
Während Bestandsdaten erforderlich sind, um eine konkrete Person zu identifizieren, erscheinen Verkehrsdaten zunächst *harmloser*. Sie geben „nur" Aufschluss über die näheren Umstände einer Kommunikation, d. h. Kommunikationsbeteiligte, -uhrzeiten, genutzte IP-Adressen oder aufgerufene URL, nicht jedoch über die eigentlichen Inhalte der Kommunikation oder – jedenfalls nicht unmittelbar – die Identität der Kommunikationsbeteiligten. Ein näherer Blick auf URI, bei denen Suchparameter mit Hilfe der GET-Methode übermittelt werden, zeigt jedoch, dass diese Aussage keine absolute Geltung beanspruchen kann. Auch bestimmte E-Mail-Adressen (aidsberatung@krankenhaus.de) oder Telefonnummern (0190-RUF-MICH-AN) geben möglicherweise Aufschluss über ausgetauschte Kommunikationsinhalte, auch wenn diese explizit nicht vorliegen. Erst recht können Standortdaten, die z. B. bei der Nutzung von Mobiltelefonen anfallen, umfassend Aufschluss über Lebensgewohnheiten geben.[9] Die Speicherung von und der Zugriff auf Verkehrsdaten haben daher eine außerordentlich große Praxisrelevanz – insbesondere wenn, wie oben dargestellt, sich eine Tat ausschließlich mit Hilfe von Verkehrsdaten aufklären lässt.

A. Datenspeicherung

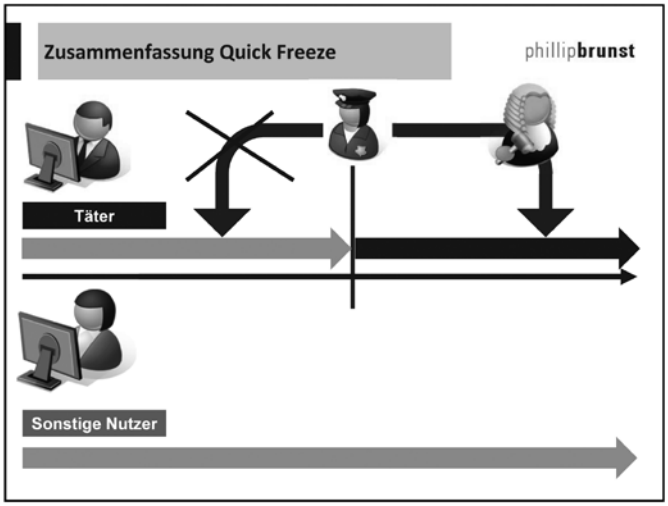
Nachdem das Bundesverfassungsgericht die Speicherung von Verkehrsdaten auf Vorrat in der gegenwärtigen Form für unzulässig erklärt hat,[10] gilt in Deutschland momentan § 96 TKG. Danach darf (d. h. er ist nicht dazu gezwungen, sondern nur berechtigt) ein Diensteanbieter bestimmte Verkehrsdaten erheben, wenn dies für bestimmte Zwecke, insb. zur Rechnungserstellung, erforderlich ist. Besonders die zunehmende Verbreitung von Flatrate-Tarifen hat auf die Anwendung dieser Vorschrift große Bedeutung: wenn bei Nutzung eines Flatrate-Tarifs keine Verkehrsdaten zu Abrechnungszwecken erforderlich sind, ist datenschutzrechtlich deren Erfassung weitgehend unzulässig.[11] Deutsche Ermittler beschweren sich daher, dass in Deutschland gegenwärtig die Verfolgung von Internetstraftaten oder anderen Delikten, deren Aufklärung auf derartige Daten angewiesen ist, weitgehend unmöglich ist. Ob dies lediglich ein subjektiver Eindruck ist oder fehlende Verkehrsdaten tatsächlich Auswirkungen auf die Aufklärungsraten haben, ist hoch umstritten.[12]

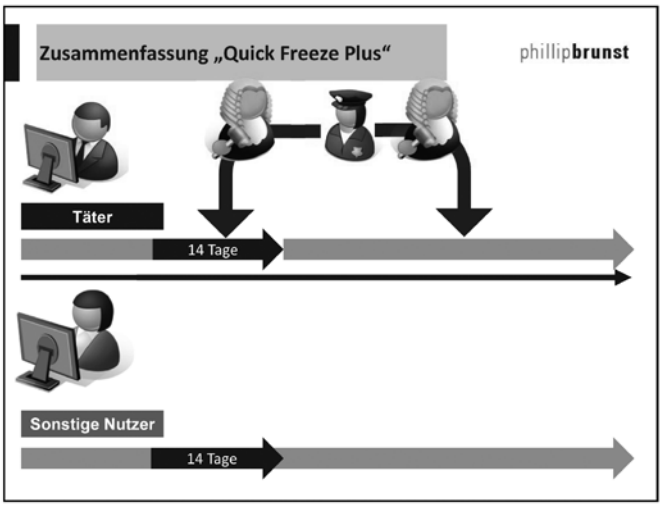
International werden vor dem Hintergrund des Problems zunehmend wichtiger werdender und dennoch seltener vorliegender Verkehrsdaten vor allem zwei Modelle diskutiert: das Quick-Freeze-Verfahren sowie die Vorratsdatenspeicherung.





Das Quick-Freeze-Verfahren ist in der Cybercrime-Konvention des Europarates angelegt[13] und sieht vor, dass Maßnahmen eingeführt werden, die eine „umgehende Sicherung bestimmter Computerdaten einschließlich Verkehrsdaten" erlauben. Das Quick-Freeze-Verfahren ist damit grundsätzlich auch auf Bestands- oder Inhaltsdaten anwendbar und ist insoweit weitergehend als das Vorratsdatenverfahren. Andererseits erlaubt es nur, bereits existierende Daten einzufrieren – die Erhebung von Daten, die nicht vom Provider benötigt werden und daher dort nicht gespeichert werden, sieht es nicht vor (anders wiederum die Vorratsdatenspeicherung, die den Provider dazu zwingt, bestimmte Daten zu erheben, auch wenn diese von ihm gar nicht benötigt werden). Quick-Freeze ist damit datenschutzfreundlicher als die Vorratsdatenspeicherung und bezieht sich zudem ausschließlich auf die Daten von Personen, die bereits in den Fokus der Strafverfolgungsbehörden gelangt sind. Gleichzeitig besteht der größte Vorwurf darin, dass mit Hilfe des Quick-Freeze-Verfahrens nur auf Daten zugegriffen werden kann, die bereits beim Provider vorliegen oder zukünftig anfallen. Länger zurückliegende Daten werden, wenn sie der Provider nicht aus anderen Gründen rechtmäßig aufbewahrt hat, regelmäßig auch mit Hilfe des Quick-Freeze-Verfahrens den Strafverfolgungsbehörden nicht zur Verfügung gestellt werden können.





In Abgrenzung zum Quick-Freeze-Ansatz ist das Verfahren der Vorratsdatenspeicherung zu sehen, das von der EU favorisiert wird und in der Richtlinie 2006/24/EG niedergelegt ist. Es sieht eine weitgehende Speicherung bestimmter Telefon- und Internetdaten (insb. von E-Mails, VoIP und IP-Zuordnungen) für einen Zeitraum von mindestens sechs Monaten und höchstens zwei Jahren vor. Anders als in der Öffentlichkeit dargestellt, bezieht sich die Vorratsdatenspeicherung nicht nur auf Verkehrsdaten: gerade die Identifizierungspflicht für Nutzer von Internetdiensten betrifft auch Bestandsdaten, die zwingend zu erfassen und auf Vorrat zu speichern sind. Gegen die Richtlinie bestehen international Bedenken; in mehreren europäischen Ländern wurden die Umsetzungen in nationales Recht als verfassungswidrig beurteilt und die Vorratsdatenspeicherung dort ausgesetzt (so auch in Deutschland). Vor dem EuGH ist indes bislang nur die Rechtsgrundlage der Vorratsdatenspeicherung (Rahmenbeschluss vs. Richtlinie) überprüft und für rechtmäßig befunden worden.[14] Die inhaltliche Vereinbarkeit mit europäischen Grundrechten ist ausdrücklich bisher nicht Gegenstand einer europäischen richterlichen Überprüfung geworden. Gleichwohl scheint sich auf der europäischen politischen Ebene angesichts der zunehmenden Anzahl kritischer nationaler Gerichtsentscheidungen und der öffentlichen Meinung eine kritischere Haltung gegenüber der Vorratsdatenspeicherung durchzusetzen.[15] Ob die Vorratsdatenspeicherung daher in der gegenwärtigen Form auch zukünftig Bestand haben wird, erscheint fraglich.

Als Kompromiss zwischen Vorratsdatenspeicherung und Quick-Freeze-Verfahren wurde vom deutschen Datenschutzbeauftragten *Schaar* das *Quick-Freeze-Plus*-Verfahren in die Diskussion eingebracht.[16] Dieses kombiniert eine *kleine Vorratsdatenspeicherung* von etwa zwei Wochen mit dem Quick-Freeze-Verfahren. Auf diese Weise soll es den Strafverfolgern ermöglicht werden, Zugriff auf retrograde Verkehrsdaten nehmen zu können (jedenfalls aus den vergangenen zwei Wochen) und über das Quick-Freeze-Verfahren eine Sicherung auch zukünftig anfallender Daten bewirken zu können. Dieses Verfahren ist in der Fachöffentlichkeit skeptisch aufgenommen worden: den Verfechtern der Vorratsdatenspeicherung ist die Zwei-Wochen-Frist zu kurz, die Gegner der Vorratsdatenspeicherung befürchten hingegen, dass jeglicher (Neu-) Einstieg in die Vorratsdatenspeicherung einen Dammbruch bedeuten könnte und lehnen daher das Verfahren aus grundsätzlichen Erwägungen heraus ab. Zu bedenken ist weiterhin, dass sowohl das Quick-Freeze-Verfahren an sich als auch Quick-Freeze Plus nicht ausreichend sind, um die verbindlichen Vorgaben der EU-Vorratsdatenspeicherungsrichtlinie umzusetzen.

B. Zugriff auf gespeicherte Daten

Während die oben geschilderte Frage das Problem betrifft, ob überhaupt, bzw. wenn ja, welche Daten von den Providern zwangsweise zu speichern sind, betrifft ein weiterer Problemkreis die Frage, wer auf diese Daten zu welchen Zwecken zugreifen darf. Hierfür ist in strafprozessualer Hinsicht vor allem die Vorschrift des § 100g StPO einschlägig. Dieser unterscheidet zwischen zwei Kategorien, die sich vor allem hinsichtlich der Schwere der Tat grundsätzlich unterscheiden.

Nach § 100g Abs. 1 Nr. 1 StPO darf auf gespeicherte Verkehrsdaten zugegriffen werden, wenn es sich um eine Straftat von auch im Einzelfall erheblicher Bedeutung handelt. Exemplarisch wird in diesem Zusammenhang auf den Katalog des § 100a Abs. 2 StPO verwiesen, der vor allem Straftaten der mittleren und höheren Kriminalität enthält, die ihrerseits auch zu einer Telekommunikationsüberwachung berechtigen würden. Bei derart gewichtigen Straftaten erscheint es nachvollziehbar, dass nicht nur Eingriffe in das Fernmeldegeheimnis durch ein Abhören der Kommunikation erfolgen, sondern auch ein Zugriff auf vorliegende oder entstehende Verkehrsdaten gerechtfertigt ist.

Mit Blick auf die eingangs bereits erwähnten Schwierigkeiten bzw. größtenteils Unmöglichkeiten, IT-Kriminalität ohne vorliegende Verkehrsdaten aufklären zu können, gewährt § 100g Abs. 1 Nr. 2 StPO jedoch auch den Zugriff auf Verkehrsdaten bei jeglichen Straftaten, die „mittels Telekommunikation“ begangen wurden. In diesen Fällen soll es also auf die Schwere der Straftat und ihre Bedeutung nicht mehr ankommen und ein Zugriff auf Verkehrsdaten grundsätzlich[17] möglich sein. Dieser Wertungswiderspruch wird zum Teil kritisiert, eine Änderung der Gesetzeslage ist gegenwärtig jedoch nicht zu erwarten.

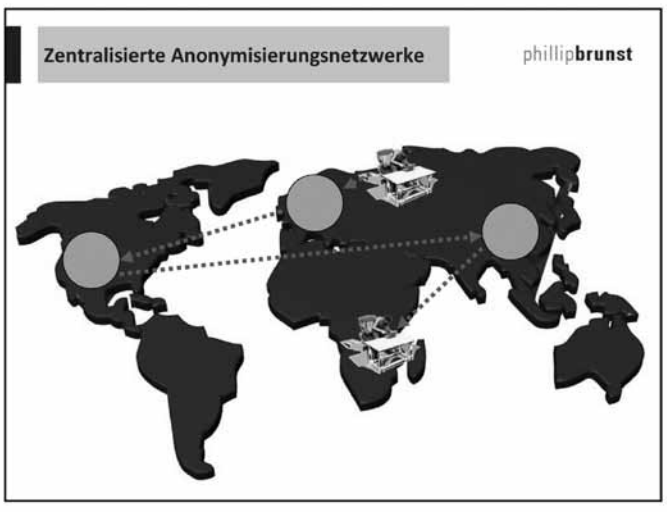
C. Weitere Entwicklung

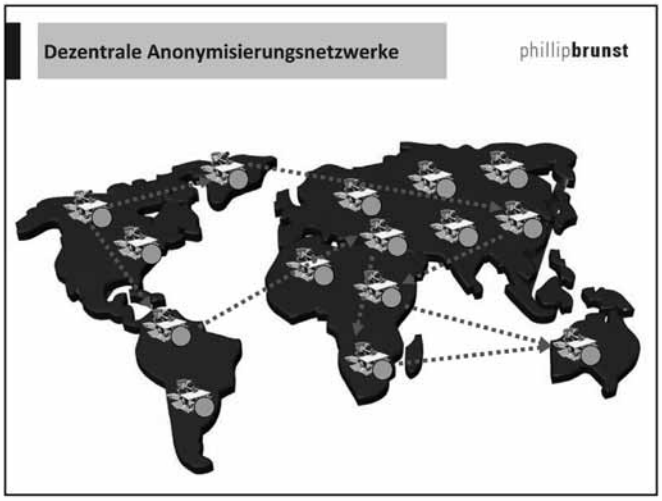
Als ein möglicher Ausweg aus den rechtlichen Beschränkungen werden zum Teil technische Handlungsoptionen gesehen. Dies

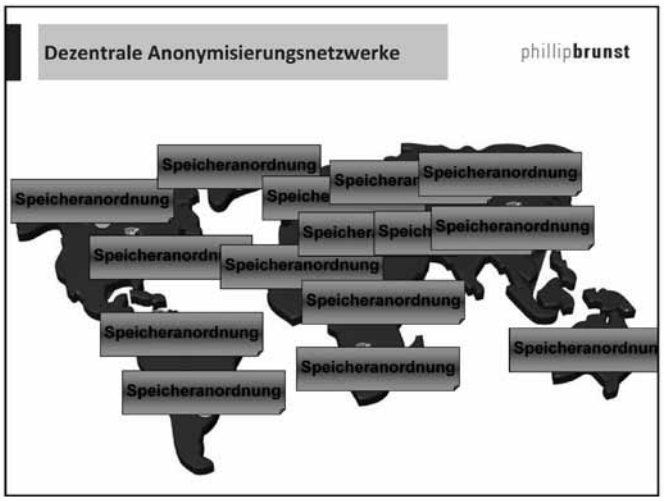
führt zu zum Teil absurden Wechselspielen zwischen Recht und Technik.

So würde beispielsweise die Nutzung von Proxy-Servern oder Anonymisierungsdiensten[18] dazu führen, dass zwar Verkehrsdaten über die Nutzung erfasst werden, diese jedoch ggf. nur auf den Proxy-Server bzw. den Exit-Knoten des Anonymisierungsdienstes verweisen würden. Die deutsche Umsetzung der Vorratsdatenspeicherung sah in § 113 Abs. 6 TKG a.F. daher vor, dass auch Anbieter, die zu speichernde Angaben verändert haben, zur Speicherung der ursprünglichen und der neuen Angaben verpflichtet waren. Damit waren sowohl die Anbieter von Anonymisierungsdiensten, Proxy-Servern als auch von NAT-Diensten (jedenfalls bei öffentlich zugänglichen Telekommunikationsdiensten) von der Speicherpflicht betroffen.[19] Nach Auffassung des Berliner Beauftragten für Datenschutz und Informationsfreiheit führte die Regelung des § 113 Abs. 6 TKG – die in der Vorratsdatenspeicherungsrichtlinie so auch gar nicht enthalten war – zu einer unverhältnismäßigen Einschränkung der Bürger, da diese sich nicht mehr mit Hilfe von Anonymisierungsdiensten im Internet unbeobachtet bewegen konnten.[20] Das Gericht ist dieser Auffassung nicht gefolgt, da durch die Speicherpflicht der Betrieb von Anonymisierungsdiensten nicht grundsätzlich unterbunden werde. Aufgehoben würde die Anonymität „nur gegenüber den staatlichen Behörden und dabei auch nur dann, wenn nach den engen Voraussetzungen für die unmittelbare Verwendung der nach § 113a TKG gespeicherten Verkehrsdaten ein Datenabruf ausnahmsweise erlaubt ist." Abgehalten würden damit allein Kunden, „deren Anonymisierungsinteresse sich gegen die in solchen besonders schwerwiegenden Fällen ermittelnden Behörden richtet."[21] Auf die Frage, ob Anonymisierungsdienste überhaupt Telekommunikationsdienste sind oder nicht vielmehr Telemediendienste, ist das Gericht leider nicht eingegangen.[22]

Selbst wenn diese Regelung bei einer Neufassung der Vorschriften wieder aufgenommen werden sollte, so bestehen doch gravierende Zweifel an ihrer Durchsetzbarkeit. Sinnvoll konstruierte Anonymisierungsdienste verteilen ihre Kaskaden über mehrere Länder. Es wäre daher notwendig, dass in allen Ländern einer Anonymisierungskaskade die erforderlichen Daten überhaupt gespeichert werden, diese zum Zeitpunkt einer rechtlichen Anfrage immer noch vorliegen, die beteiligten Länder bereit wären aufgrund der vorgetragenen Sachlage diese Daten gerichtlich sicherstellen zu lassen und sie schließlich an das anfragende Land zu übermitteln. Ob dies in der gerichtlichen Praxis tatsächlich ein gangbarer Weg wäre, darf angesichts der hohen Hürden und langen Laufzeiten von Rechtshilfeersuchen bei vielen Ländern getrost bezweifelt werden. Während bei zentralisiert aufgebauten Anonymisierungsdiensten (wie z. B. AN.ON/Jondonym) aber zumindest theoretisch eine Chance auf ein derartiges Vorgehen besteht, ist dies bei dezentral aufgebauten Diensten, bei denen Daten über die Rechner von zufällig ausgewählten Teilnehmern weitergeleitet werden (und diese Route zudem im Laufe einer Session regelmäßig geändert wird), nicht mehr denkbar.







Im US-amerikanischen Raum wird insb. gegen die Verschleierung von IP-Adressen ein gänzlich anderes Instrument eingesetzt: CIPAV (Computer and Internet Protocol Address Verifyer) wird vermutlich als Trojaner auf den Rechner des Verdächtigen geschleust und soll von dort – anders als bei Online-Durchsuchung oder Quellen-TKÜ – keine Inhalts-, sondern ausschließlich Verkehrsdaten und nähere Informationen über den Rechner des Verdächtigen liefern, z. B. seine IP-Adresse, die MAC-Adresse und ähnliche Informationen, die genutzt werden können, um den Rechner des Verdächtigen auch dann eindeutig lokalisieren zu können, wenn dieser versucht, mit Hilfe von Anonymisierungs- oder Proxy-Diensten seine Verkehrsdatenzuordnung zu verhindern. Über CIPAV selbst sowie seine Einsatzmodalitäten sind lediglich bruchstückhafte Informationen verfügbar.[23] Obwohl es scheinbar Interesse von deutscher Seite an diesem Programm gab,[24] liegen über den tatsächlichen Einsatz hier ebenfalls keine näheren Informationen vor.

III. Zugriff auf Inhaltsdaten

Die wahrscheinlich sensibelsten Zugriffe betreffen die eigentlichen Inhalte, die entweder lokal auf einem Rechner oder auch verteilt in der Cloud abgelegt sein können. Hierbei kann es sich z. B. um Finanzunterlagen, Tagebücher, Korrespondenz oder die letzten Urlaubsbilder handeln. Insbesondere bei gravierenden Straftaten stellen derartige Inhalte wichtige Informationsquellen für Ermittler dar. Gleichzeitig ist der Zugriff auf sie hohen rechtlichen und auch tatsächlichen Anforderungen vorbehalten, da sich – über die eigentlichen Inhalte hinaus – in vielen Fällen Einblick in intimste Situationen des Betroffenen geben können.

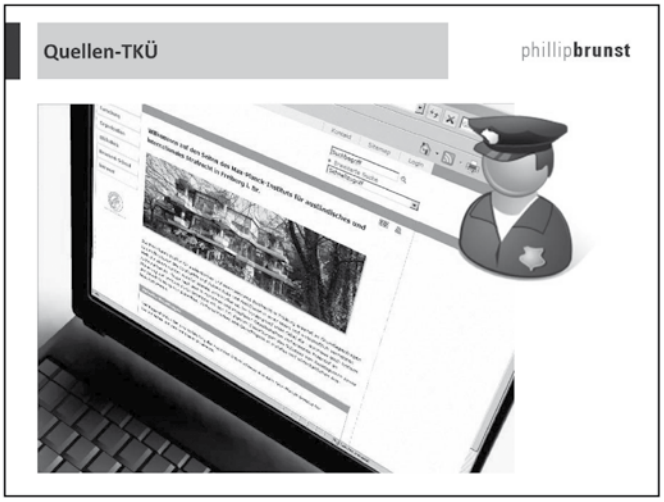
A. Öffentlich zugängliche Daten

Unproblematisch erscheint der Zugriff, wenn die Daten im Internet frei zugänglich sind, etwa wenn sie auf einer Webseite abrufbar oder in einem sozialen Netzwerk ohne größere Hürden für alle einsehbar sind. Per *virtueller Streife* ist die Polizei in diesem Bereich bereits seit vielen Jahren unterwegs und beobachtet öffentlich zugängliche Informationen auf Webseiten, in Blogs, einschlägigen Newsgroups oder Chat-Räumen.[25] Anders als die uniformierten Kollegen auf der Straße sind die *Cybercops* jedoch nicht unmittelbar erkennbar. Das BVerfG hat in diesem Zusammenhang bereits festgestellt,[26] dass eine Kenntnisnahme öffentlich zugänglicher Informationen dem Staat nicht verwehrt ist, selbst, wenn auf diesem Weg personenbezogene Informationen erhoben werden.

Spannender ist da schon die Frage, ob – da die Eigenschaft als Polizeibeamter wie erwähnt nicht zwingend erkennbar ist – auch das Auftreten unter einer virtuellen Legende zulässig ist. Während dies sonst an hohe Voraussetzungen geknüpft ist (vgl. §§ 110a ff. StPO), sieht das BVerfG bei derartigen Handlungen im Internet keinen Korrekturbedarf. Da die Kommunikationsdienste im Internet „in weitem Umfang den Aufbau von Kommunikationsbeziehungen [erlaubten], in deren Rahmen das Vertrauen eines Kommunikationsteilnehmers in die Identität und Wahrhaftigkeit seiner Kommunikationspartner nicht schutzwürdig ist“ und da hierfür „keinerlei Überprüfungsmechanismen bereitstehen“, sei kein Raum für ein Vertrauen im Internet. Dies gelte selbst bei lang aufgebauten Kommunikationsnetzen und „elektronischen Gemeinschaften“, da auch hier den Teilnehmern klar sei, dass die wahre Identität der Kommunikationspartner nicht bekannt sei und sich deren Angaben nicht überprüfen ließen. Das Vertrauen, dass der Kommunikationspartner gerade keine staatliche Stelle sei, sei in der Folge nicht schutzwürdig.[27] Diese Auffassung ist zu kritisieren: allein die *Möglichkeit*, dass im Internet leichter getäuscht werden kann, darf kein Argument dafür sein, dass hier – abweichend von den strengen Regelungen außerhalb des Internet – Bürger getäuscht werden *dürfen*. Im Gegenteil wäre die Leichtigkeit, mit der eine Täuschung möglich ist, gerade ein Argument dafür, dass ein besserer Schutz der Bürger gegen derartige Polizeiaktionen erforderlich wäre.

B. Verschlüsselte Kommunikation

Jenseits der öffentlich zugänglichen Inhalte ist für Strafverfahren vor allem der Zugriff auf Kommunikationsinhalte sowie auf sonstige Inhaltsdaten wichtig. Telekommunikationsüberwachungen sind nach §§ 100a, 100b StPO bereits seit langer Zeit möglich und ein wichtiges Instrument bei der Aufklärung schwerer Straftaten. Diese Vorschriften sind grundsätzlich auch zur Erfassung von VoIP oder anderen elektronischen Kommunikationsinhalten geeignet, gehen allerdings ins Leere, wenn die Inhalte verschlüsselt übertragen werden.



Um diese Schwierigkeit zu umgehen, wird vermehrt die Quellen-TKÜ eingesetzt, die unmittelbar auf dem Rechner eines Verdächtigen installiert wird und dann Kommunikationsinhalte erfasst bevor sie ver- bzw. nachdem sie entschlüsselt wurden. Die Zulässigkeit einer Quellen-TKÜ ist zwischen Literatur und Rechtsprechung umstritten, wird von der Praxis aber offenbar weitestgehend für rechtmäßig gehalten und auch eingesetzt.[28] Für die Gefahrenabwehr sind mit § 20l BKAG, § 15b HessSOG oder § 31 Abs. 3 Rh.-Pf. POG inzwischen spezialgesetzliche Normen geschaffen worden.

Phillip W. Brunst

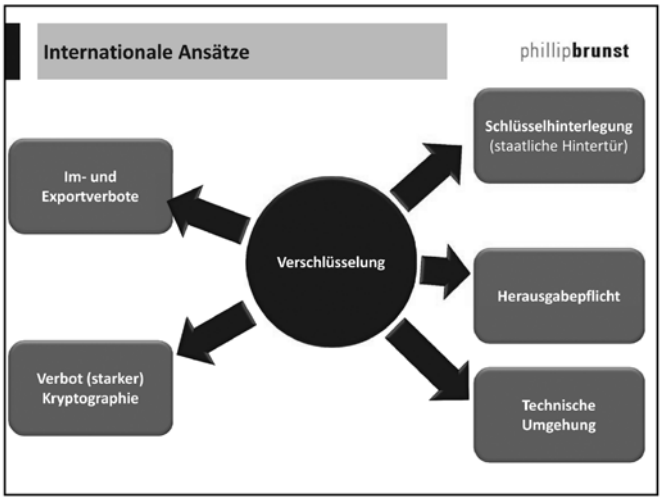
Dr. **Phillip W. Brunst** ist tätig für das Cybercrime Research Institute in Köln/Berlin. Er erstellt Gutachten und berät Unternehmen sowie nationale und internationale Organisationen zu aktuellen Fragen des Computer- und Internetstrafrechts. Seine wissenschaftlichen Schwerpunkte liegen insbesondere auf der komplexen Verbindung von technischen und juristischen Fragestellungen.
Kontakt: *brunst@cybercrime.de*

Das Bundesverfassungsgericht fordert, dass durch rechtliche und technische Maßnahmen sichergestellt wird, dass bei der Quellen-TKÜ ausschließlich Kommunikationsdaten erfasst werden.[29] Der bayerischen Interpretation, nach der dies auch die Anfertigung von Screenshots von Browser- und Skype-Fenstern umfasst, ist durch das LG Landshut eine deutliche Absage erteilt worden.[30] Welche weiteren Funktionen staatliche Software zur Kommunikationsüberwachung noch enthält, wird wohl erst die Zukunft zeigen.[31]

C. Sonstige verschlüsselte Inhalte

Während die Quellen-TKÜ *nur* Kommunikationsinhalte erfassen soll, besteht in der Praxis ein häufig auftretendes Problem darin, dass auf gespeicherte Inhalte eines Verdächtigen zugegriffen werden soll, die dieser entweder auf seinem eigenen Rechner oder auf Netzspeichern abgelegt hat. Daten auf dem Rechner können zumindest ausgewertet werden, wenn der Rechner, z. B. bei einer Wohnungsdurchsuchung, beschlagnahmt wird. Sind die darauf abgelegten Daten jedoch zuverlässig verschlüsselt, so ist eine Auswertung nicht möglich. Gleiches gilt, wenn die Daten z. B. per Cloud-Storage abgelegt wurden und eine forensische Analyse des Systems keine verwertbaren Informationen hierzu liefert oder die Daten dort ebenfalls verschlüsselt abgelegt sind.

Während in Ländern mit einem geringen Rechtsstaatsniveau der Betreffende z. B. körperlich gefoltert wird, um den notwendigen Schlüssel zu erhalten, haben sich in anderen Ländern alternative Strategien entwickelt, um dem Verschlüsselungsproblem Herr zu werden. In Vor-Internetzeiten war das Verbot oder eine umfassende Regulierung des Zugriffs auf starke (oder gleich sämtliche) Verschlüsselungsverfahren ein Weg, um Inhalte zu kontrollieren. Spätestens seitdem Software aber aus dem Internet heruntergeladen werden kann, lassen sich derartige Regelungen ebenso wie ausgefeilte Im- und Exportverbote nur noch unzureichend umsetzen, auch wenn die Regelungen in weiten Teilen immer noch rechtlichen Bestand haben.[32]



Größere Bedeutung haben heute hingegen gesetzliche Zwänge zur Schlüsselhinterlegung oder zum Einbau staatlicher *Hintertüren*, die eine spätere Entschlüsselung wieder erleichtern können. Auch derartige Pflichten lassen sich jedoch in vielen Fällen nur schwer umsetzen. Andere Länder setzen daher beim Inhaber der Schlüssel an und drohen ihm zwar keine Folter an, dafür aber eine unter Umständen mehrjährige Haftstrafe, wenn die benötigten Schlüssel im Einzelfall den Behörden nicht zur Verfügung gestellt werden.[33] Die ersten Anwendungsfälle haben das Vertrauen in den restriktiven Umgang mit derartigen Vorschriften nicht unbedingt gestärkt.[34]

In Deutschland ist hingegen die umstrittene Online-Durchsuchung das Mittel der Wahl, um heimlich auf Computer von Betroffenen zugreifen zu können, und auf diesem Weg Zugangsdaten zu Online-Speichern, benötigte Verschlüsselungsinformationen oder auch gespeicherte Inhalte erlangen zu können. Die vom Bundesverfassungsgericht für derartige Zugriffe aufgestellten hohen Hürden wurden schließlich in § 20k BKAG und z. B. § 31c Rh.-Pf. POG oder Art. 34d BayPAG umgesetzt. Die letztgenannte Vorschrift erlaubt sogar – weitergehend als die Bundesvorschrift – die Löschung von Daten auf dem Rechner des Betroffenen. Die ursprüngliche Fassung, nach der sogar die Veränderung von Daten erlaubt war, ist im Jahr 2009 wieder zurückgenommen worden.

IV. Ergebnis

Betrachtet man die hier vorgestellten Vorschriften, die der Polizei zur Verfügung stehen, so wird deutlich, dass sowohl die Anonymität des Betroffenen als auch die Integrität und Vertraulichkeit seiner informationstechnischen Systeme massiv gefährdet sein kann, wenn er in den Fokus der Ermittlungsbehörden gerät. Dabei ist zwar zu berücksichtigen, dass die Hürden für den heimlichen Zugriff auf Kommunikations- und Inhaltsdaten relativ hoch angesetzt sind. Die Ereignisse um den vom CCC aufgedeckten Staatstrojaner lassen jedoch den Eindruck aufkommen, dass in der Praxis diese hohen Hürden nicht immer beachtet bzw. rechtliche Grenzen nicht immer eingehalten werden. Zudem wird von politischer Seite zunehmend gefordert, Anonymität im Internet nicht nur im Bereich der Strafverfolgung und der Gefahrenabwehr einzuschränken, sondern ganz generell.[35] Hinzu kommen Möglichkeiten des nationalen sowie des internationalen Datenaustauschs, die in bestimmten Konstellationen nicht nur auf rechtlichen und ermittlungstaktischen Notwendigkeiten beruhen, sondern Ergebnis politischen Drucks sind. Nimmt man dann noch Angriffe durch fremde Nachrichtendienste und Cyberkriminelle hinzu, die an die hier vorgestellten rechtlichen Regeln von Beginn an gar nicht erst gebunden sind, so wird deutlich, dass sicherheitlich sensibilisierte Nutzer ihre Selbstschutzmaßnahmen noch konsequenter anwenden müssen und dass es Organisationen wie dem FIfF bedarf, um diese Erkenntnis auch auf breiter Ebene fachlich fundiert zu vermitteln.

Anmerkungen

1 *Vgl. hierzu näher Bäumler/v. Mutius, Anonymität im Internet. Wiesbaden 2003, Brunst, Anonymität im Internet. Rechtliche und tatsächliche Rahmenbedingungen. Berlin 2009.*

2 *Vgl. BVerfG vom 27.02.2008, http://bit.ly/atx5fr.*

3 *Denkbar ist es etwa, dass der Täter bei der Begehung seiner Tat personenbezogene Informationen hinterlässt, die Anlass für weitere – klassische – Ermittlungsmethoden bieten, z. B. eine Postanschrift, an die Waren geschickt werden sollen oder ähnliche Informationen, die Hinweise auf die Identität des Täters liefern können.*

4 *Beim sog. „Enkeltrick" werden vor allem ältere Menschen telefonisch davon überzeugt, dass sich Familienmitglieder (insb. ein Enkel) gerade in einer finanziellen Notsituation befinden, z. B. wegen eines Autounfalls im Ausland. Ein vermeintlich „guter Freund" wird daher geschickt, um kurzfristig größere Bargeldsummen vom Opfer abzuholen, um sie schnellstmöglich an das in Not geratene Familienmitglied weiterzuleiten. Abgesehen von einer – meist dürftigen – Personenbeschreibung lassen sich häufig nur mit Hilfe von Telekommunikationsanalysen erste Hinweise auf die Täter ermitteln.*

5 *Vgl. etwa Fox, Trust and privacy online: Why Americans want to rewrite the rules, S. 10, http://bit.ly/te8N5T.*

6 *Vgl. Bundesnetzagentur, Tätigkeitsbericht Telekommunikation 2008/2009, S. 246, http://bit.ly/uK33aF.*

7 *Vgl. Decreto legge no. 144 vom 27.07.2005, veröffentlicht in Gazzetta Ufficiale no. 177 vom 01.08.2005. Das Gesetz wurde durch Consiglio dei ministri no. 225 vom 29.12.2010 (sog. Dekret Milleproroghe) wieder aufgehoben.*

8 *Gegen dieses Verfahren ist bereits seit dem Jahr 2005 eine Verfassungsbeschwerde anhängig (Az. 1 BvR 1299/05), über die aber bis heute noch nicht abschließend entschieden worden ist.*

9 *Vgl. Gonzalez, et al., Nature 2008, Vol. 543, 779*

10 *BVerfG, Urt. vom 02.03.2010, http://bit.ly/bg9q3F.*

11 *Gerichtlich ist dies bereits seit dem Jahr 2003 geklärt, als der Netzaktivist Holger Voss erfolgreich gegen eine Datenerhebung trotz Flatrate vorging. Vgl. hierzu näher Brunst, Anonymität im Internet. Rechtliche und tatsächliche Rahmenbedingungen. Berlin 2009, S. 347 ff.*

12 *Vgl. hierzu näher Grafe, Die Auskunftserteilung über Verkehrsdaten nach §§ 100g, 100h StPO. Freiburg i. Br. 2007, Albrecht, et al., Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO. Freiburg i. Br. 2008, Müller, „Die Wirtschaft muss sich besser schützen" – Interview mit Jörg Ziercke, http://bit.ly/uH6Mdj.*

13 *Vgl. Art. 16 des Europarats Übereinkommen über Computerkriminalität, CETS Nr. 185. Vgl. hierzu näher Brunst, DuD 2011, 618*

14 *EuGH, Urt. vom 10.02.2009, Az. C-301/06, Irland ./. Parlament und Rat.*

15 *Vgl. etwa http://bit.ly/m2EWCc, http://fm4.orf.at/stories/1682829/, Der Standard, Oberster EU-Datenschützer erneuert Kritik an Vorratsdatenspeicherung, http://derstandard.at/1304554474239/.*

16 *Vgl. http://bit.ly/b7nlSy.*

17 *Zwar schränkt § 100g Abs. 1 StPO dies insoweit ein, als dass festgestellt werden muss, dass der Zugriff auf Verkehrsdaten nur zulässig sein soll, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist, weil eine Ermittlung auf andere Weise aussichtslos erscheint und wenn zudem der Zugriff auf die Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Diese gesetzlichen Voraussetzungen spielen in der Praxis jedoch offenbar keine Rolle, vgl. Albrecht, et al., Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO. Freiburg i. Br. 2008.*

18 *Zur Funktionsweise näher Brunst, Anonymität im Internet. Rechtliche und tatsächliche Rahmenbedingungen. Berlin 2009, S. 130 ff, Gercke/Brunst, Praxishandbuch Internetstrafrecht. Stuttgart 2009, S. 351 ff, Kubieziel, Anonym im Netz. Techniken der digitalen Bewegungsfreiheit. München 2007.*

19 *Vgl. Hoeren, JZ 2008, 668 (670). Bereits die Erfassung von NAT erscheint allerdings zweifelhaft, da die für eine Zuordnung erforderlichen Portnummern gar nicht von der Vorratsdatenspeicherungspflicht erfasst waren.*

20 *BVerfG, Urt. vom 02.03.2010, http://bit.ly/bg9q3F, Abs. 171.*

21 *BVerfG a.a.O, Abs. 295.*

22 *Hoeren a.a.O. hält die Einordnung als Telekommunikationsdienst für „anerkannt". Anders sehen dies z. B. Gitter/Schnabel, MMR 2007, 411 (415).*

23 *Vgl. http://bit.ly/mwpHjC sowie http://bit.ly/BUfqm. In der Literatur findet CIPAV Erwähnung etwa in Brunst, DuD 2011, 618 (620), Gercke/Brunst, Praxishandbuch Internetstrafrecht. Stuttgart 2009., Rn. 24, Fox, DuD 2007, 840.*

24 *Vgl. AG Hamburg, Beschl. v. 28.08.2009, Az. 160 Gs 301/09 und Besprechung in Spoenle, jurisPR-ITR 2010, Iss. 6/2010 Anm. 5.*

25 *Das Bayerische LKA ist bereits seit 1995, das BKA seit dem Jahr 1999 aktiv. Neben der Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD), das pro Jahr etwa 400 bis 800 Straftaten feststellt, existiert mit KaRIN, der Koordinierungsgruppe für anlassunabhängige Recherchen im Internet, auch eine Plattform, auf der einschlägige polizeiliche Informationen zwischen Bundes- und Landesbehörden ausgetauscht werden können.*

26 *BVerfG, Urt. vom 27.02.2008, http://bit.ly/atx5fr.*

27 *BVerfG, a.a.O., Abs. 311.*

28 *Vgl. etwa AG Bayreuth, MMR 2010, 266; LG Landshut, Beschl. v. 20.01.2011, Az. 4 Qs 346/10 m.w.N.; Gercke/Brunst, Praxishandbuch Internetstrafrecht. Stuttgart 2009., Rn. 884 ff.; a.A. Buermeyer/Bäcker, HRRS 2009, 433, Albrecht, JurPC 2011, Iss. Web-Dok. 59/2011. Vgl. auch OLG Hamburg NStZ 2008, 478.*

29 *BVerfG, a.a.O., Abs. 190.*

30 *LG Landshut, Beschl. v. 20.01.2011, Az. 4 Qs 346/10.*

31 *Einen ersten Einblick liefert die Analyse des CCC zum sog. „Staatstrojaner", vgl. http://0zapftis.info/, http://bit.ly/vC9Rup, http://bit.ly/rr8ALX.*

32 *Die bekannte Verschlüsselungssoftware PGP wurde z. B. zunächst mit Hilfe von Datennetzen illegal aus den USA exportiert. Ein legaler Export war anschließend jedoch auf dem Offline-Weg möglich: Der Source Code des Programms wurde ausgedruckt und als 12-bändiges Buch (ISBN 0-262-24039-4) nach Europa exportiert. Dort wurde das Printwerk mit Hilfe von OCR wieder in Software zurückgewandelt. Da das strenge Krypto-Export-Regime ausschließlich auf Software, nicht jedoch auf Druckwerke anwendbar war, konnte auf diesem Weg ein legaler Export bewerkstelligt werden. Vgl. hierzu näher http://bit.ly/4D4m54.*

33 *In Art. 49, 53 des englischen Regulation of Investigatory Powers Act (RIPA) werden zum Beispiel bis zu zwei Jahren Haft angedroht.*

34 *Vgl. etwa http://bit.ly/8LYyh0. Weitere Fälle finden sich bei http://bit.ly/t5i90d.*

35 *Vgl. etwa die Äußerungen von Bundesinnenminister Friedrich (http://bit.ly/qxvAlS), von BKA-Präsident Ziercke (http://bit.ly/t5wDvB, http://bit.ly/t1phma) sowie der Parlamentarier Fischer und Uhl (http://on.fb.me/aliXpn, http://bit.ly/oMroJJ). Zusammenfassend vgl. http://bit.ly/vPfmal.*

Felix Freiling

Was ist eine Quellentelekommunikationsüberwachung?

Im Verfahren des Bundesverfassungsgerichts zur Online-Durchsuchung im Jahr 2007 interessierten sich die Richter sehr für die tatsächlichen Möglichkeiten und Methoden, mit denen informationstechnische Systeme durch Ermittlungsbehörden infiltriert werden können. Die technischen Gutachter, zu denen auch der Autor zählte, waren damals gezwungen, allgemeine Erkenntnisse aus dem Bereich der Cyberkriminalität auf den Bereich staatlicher Eingriffe zu übertragen. Im vergangenen Jahr bot sich jedoch erstmals die Gelegenheit, die damaligen Annahmen anhand eines konkreten Falles staatlicher Infiltration zu überprüfen.

TKÜ und Quellen-TKÜ

Hoch entwickelte Gesellschaften sind sehr viel mehr auf sichere Informationstechnik angewiesen als die organisierte Kriminalität. Darum ist die Einführung von starker Kryptographie in allen Bereichen des Cyberspace aus gesellschaftlicher Sicht uneingeschränkt zu befürworten. Natürlich ergeben sich neue Probleme aus der zunehmenden Tendenz, Daten standardmäßig Ende-zu-Ende-verschlüsselt auszutauschen,

Ein bekanntes Problemfeld entsteht aus dem Wunsch staatlicher Ermittlungsbehörden, laufende Telekommunikation zu überwachen (TKÜ), da auch die Hilfe des Telekommunikationsdiensteanbieters bei entsprechender Verschlüsselung nicht mehr ausreicht. Ein möglicher Lösungsweg besteht im Einbringen einer Software an der *Quelle* der Verschlüsselung, also an der Stelle, wo beispielsweise die Sprachinformationen aufgenommen werden. Dies wird häufig mit dem Begriff *Quellentelekommunikationsüberwachung* (Quellen-TKÜ) bezeichnet. So sehr sich dieser Begriff an die *normale* Telekommunikationsüberwachung anlehnt, so unterschiedlich sind doch die Mechanismen, mit denen gearbeitet wird. Es stellt sich die Frage, unter welchen Bedingungen eine Quellen-TKÜ mit einer klassischen, netzbasierten TKÜ vergleichbar wäre.

Untersuchung von BckR2D2

Im Sommer 2011 wurde uns durch den Rechtsanwalt Patrick Schladt die Kopie der Festplatte eines seiner Mandanten zur Verfügung gestellt. Aus dem Kontext des Ermittlungsverfahrens heraus bestand die Vermutung, dass eine auf dem Rechner installierte Software Daten an die Polizeibehörden ausgeleitet hatte. Wir fanden auf dieser Festplatte ein Programm, das sich als Variante der Schadsoftware herausstellte, deren Analyse der Chaos Computer Club im Oktober 2011 medienwirksam veröffentlichte [2]. Die Umstände des Fundes und die öffentlichen Reaktionen der Behörden legen nahe, dass es sich in der Tat um eine Software handelt, die auch zur Durchführung einer Quellen-TKÜ in das System eingebracht wurde.

Uns liegen mittlerweile zwei Varianten dieser Software vor, die inzwischen meist als BckR2D2-I und II bezeichnet werden. Die Ergebnisse unserer Analysen [1] decken sich im Wesentlichen mit denen des CCC [2] und anderer. Bemerkenswert erscheinen uns dabei zwei Punkte.

Der erste Punkt bezieht sich auf die mangelhafte Qualität der durch die verschiedenen Varianten der Software implementierten Datensicherheitsmechanismen. So beruhten der Authentifikationsmechanismus und die Verschlüsselung auf fest codierten Werten, die leicht aus der Software extrahierbar waren. Außerdem wurden sämtliche Parameter, die an den aufgefundenen Kernel-Level-Treiber übermittelt wurden, nicht überprüft. Durch den unbeschränkten Zugriff auf das Dateisystem war es dadurch für Dritte sehr leicht, das System in beliebiger Weise auch ohne Administratorrechte zu manipulieren.

Der zweite Punkt bezieht sich auf die durch die Software implementierte Überwachungsfunktionalität. In der Variante BckR2D2-I wurde offenbar die Schadsoftware in alle startenden Prozesse injiziert und aktivierte sich, wenn der Prozessname in einer Applikations-Whitelist enthalten war. Diese enthielt in Version BckR2D2-I sechs Programmnamen, darunter die VoIP-Programme Skype und XLite. In Version II wurden jedoch bereits 14 Programme auf ähnliche Weise überwacht, darunter auch einige Instant-Messenger-Anwendungen. Zusätzlich erlaubte die Software, Bildschirmfotos sowohl aktiver Fenster von Internetbrowsern als auch des gesamten Desktops anzufertigen.

Was ist eine Quellen-TKÜ?

Im Lichte der Analyseergebnisse ist fraglich, ob die Überwachungsmöglichkeiten, die die untersuchte Software erlaubte, noch in irgendeiner Form mit einer klassischen Telekommunika-

Felix Freiling

Felix Freiling ist Inhaber des Lehrstuhls für IT-Sicherheitsinfrastrukturen an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Schwerpunkte seiner Arbeitsgruppe in Forschung und Lehre sind offensive Methoden der IT-Sicherheit, technische Aspekte der Cyberkriminalität sowie digitale Forensik (IT-Beweismittelsicherung und -analyse). In den Verfahren zur Online-Durchsuchung und zur Vorratsdatenspeicherung vor dem Bundesverfassungsgericht diente Felix Freiling als sachverständige Auskunftsperson.

tionsüberwachung vergleichbar sind. Es scheint deshalb geboten, die Anforderungen an eine Quellen-TKÜ sowohl technisch als auch juristisch präziser zu definieren und von einer klassischen netzbasierten TKÜ abzugrenzen.

Als erstes muss gefordert werden, dass Datensicherheitsstandards nach dem Stand der Technik eingehalten werden. Dies betrifft sowohl die Verschlüsselung und (individuelle) Authentifikation der Netzwerkkommunikation als auch die sichere Implementierung aller Softwarekomponenten. Die Risiken, die durch die Überwachungssoftware entstehen, müssen nach dem Stand der Technik minimiert werden. Im Vergleich zu BckR2D2 erscheinen aktuelle Banking-Trojaner als geradezu vorbildhaft.

Beschränkung auf „laufende Telekommunikation"

Nimmt man den Vergleich zur klassischen TKÜ ernst, so darf auch die Quellen-TKÜ ausschließlich „laufende Telekommunikation" ausleiten. Die Software ist aber gezwungen, Daten bereits vor der Ausleitung (nämlich vor der Verschlüsselung) abzufangen und zu speichern. Ausgeleitet werden dürfen sie jedoch nur, wenn das entsprechende Chiffrat über das Netz verschickt wird.

Technisch könnte man das wie folgt definieren: Wenn ein gegebenes Kommunikationssystem (etwa ein Computer mit VoIP-Software) keine Verschlüsselung benutzt, dann ist „laufende Telekommunikation" das, was über das Netz verschickt wird. Wenn wir allerdings ein Kommunikationssystem K1 haben, das Verschlüsselung benutzt, dann kann man sich gedanklich ein hypothetisches Kommunikationssystem K2 konstruieren, was genau das gleiche macht wie K1, ohne allerdings Verschlüsselung zu benutzen. (Technisch würde man einfach die Aufrufe der Verschlüsselung weglassen.) Was dann bei K1 mitgeschnitten werden darf, sind alle Daten, die K2 versenden oder empfangen würde.

Selbstverständlich muss die Verschlüsselung in unmittelbarem (funktionalem und auch zeitlichen) Zusammenhang mit dem Versand passieren. Andernfalls könnte man die Definition auf jede Art von Verschlüsselung anwenden. Die Definition passt also auf typische VoIP-Programme, SSL-verschlüsselten Datenverkehr und verschlüsselte E-Mails, die unmittelbar vom Mailprogramm chiffriert werden (beispielsweise via S/MIME). Die Definition träfe nicht zu auf Dateien, die zu einem Zeitpunkt händisch verschlüsselt und dann später als Anhang verschickt werden. Dies ist auch sinnvoll, denn bei einer weiter gefassten Definition wäre es möglich, beliebige Dateien (quasi prophylaktisch) beim Verschlüsseln abzufangen, auch wenn nicht klar ist, ob diese überhaupt jemals verschickt werden. Das wäre auch bei wohlwollender Interpretation des Begriffs keine Telekommunikationsüberwachung.

Fazit

Die Schwierigkeiten, eine Quellen-TKÜ im Sinne einer klassischen TKÜ zu definieren, zeigen auf, wie unterschiedlich diese beiden Konzepte eigentlich sind. Darauf hat auch das Bundesverfassungsgericht in seinem Urteil zur Online-Durchsuchung deutlich hingewiesen: Mit der Infiltration eines Systems sei „die entscheidende Hürde genommen, um das System insgesamt auszuspähen." [3, Absatz-Nr. 188] Diese Einsicht ist aber vielerorts noch nicht im Bewusstsein von Richtern und Gesetzgebern angekommen. Das neue BKA-Gesetz regelt beispielsweise in einem eigenen Paragraphen die Quellen-TKÜ (§20l, Absatz 2, BKAG), jedoch wird (1) der Begriff der „laufenden Telekommunikation" nicht näher definiert, und es werden (2) keine spezifischen Anforderungen an die eingesetzte Software formuliert. Im Lichte der Erkenntnisse über die Software BckR2D2 sollte jedoch klar sein, dass es neben präzisen technischen und juristischen Definitionen auch eine unabhängige Kontrolle der Überwachungssoftware geben muss, etwa in Form einer Zertifizierung durch das Bundesamt für die Sicherheit in der Informationstechnik [4, S. 144].

Danksagung

Der Autor dankt Matthias Bäcker für hilfreiche Diskussionen.

Anmerkungen

[1] Andreas Dewald, Felix C. Freiling, Thomas Schreck, Michael Spreitzenbarth, Johannes Stüttgen, Stefan Vömel, Carsten Willems: Analyse und Vergleich von BckR2D2-I und II. Friedrich-Alexander-Universität Erlangen-Nürnberg, Department Informatik, Technischer Bericht CS-2011-08, Dezember 2011.

[2] Chaos Computer Club: Analyse einer Regierungs-Malware. http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf, 8. Oktober 2011.

[3] BVerfG, 1 BvR 370/07 vom 27.2.2008.

[4] Dominik Brodowski, Felix C. Freiling: Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft. Forschungsforum öffentliche Sicherheit, Schriftenreihe Sicherheit Nr. 4, März 2011.

Foto: Dagmar Boedicker

Schützenswerter Rohstoff Geist

Wirtschaftsspionage betrifft zu 96 Prozent den Mittelstand

München – Das Thema Wirtschaftsspionage wird von vielen Unternehmen nach wie vor unterschätzt. Im Internet kursieren zum Beispiel leicht zugängliche Programme, mit denen man Gespräche über Handy mithören kann. Im Gespräch mit Bayernkurier-Mitarbeiter Frank Gundermann erläutert Michael George (43), Referent für Spionageabwehr und Wirtschaftsspionage beim Bayerischen Landesamt für Verfassungsschutz, wie man seine Betriebsgeheimnisse am besten vor Schnüfflern und Spionen schützen kann.

Sie halten regelmäßig Vorträge zum Thema Wirtschaftsspionage vor Geschäftsführern und Verantwortlichen von kleinen und mittleren Unternehmen. Worüber sind Ihre Zuhörer am meisten überrascht?

Michael George: Viele Leute fühlen sich nach den Vorträgen häufig betroffener als zuvor. Die meisten Unternehmer sind der Meinung, dass ihr Betrieb viel zu unwichtig ist, um zum Angriffsziel von Wirtschaftsspionage werden zu können. Spionage wird häufig als James-Bond-Thema angesehen, das Konzerne betrifft oder Staaten, aber eben nicht den Mittelstand. Dabei betrifft Wirtschaftsspionage zu 96 Prozent den Mittelstand und lediglich zu vier Prozent Konzerne. Das überrascht die Zuhörer sehr.

Im Gegensatz zur Industriespionage, bei der Privatpersonen oder Unternehmen andere Unternehmen ausspionieren, betrifft die Wirtschaftsspionage Unternehmen, die von ausländischen Nachrichtendiensten ausspioniert werden. Welche Branchen sind hierbei besonders gefährdet?

Michael George: In Deutschland gibt es nur wenige Rohstoffe. Unsere Rohstoffe sind vor allem Ideenreichtum, Ingenieurskunst und das entsprechende Know-how. Das weckt im Ausland natürlich Begehrlichkeiten. Deshalb sind hochtechnologisierte Bereiche besonders betroffen, beispielsweise Umwelttechnologien oder Global-Trend-Themen.

Was sollten Unternehmer tun, die sich bislang mit dem Thema noch nicht auseinandergesetzt haben? Was sind die wichtigsten Schritte?

Michael George: Unternehmer können sich gerne an uns wenden. Unsere Aufgabe ist es, Informationen zu verteilen, damit das Sicherheitsdenken gesteigert wird. In Gesprächen vertiefen wir dann das Thema mit den Unternehmen. Prinzipiell gilt: Die allerwichtigste Maßnahme ist, dass das Unternehmen definiert, was seine Kronjuwelen sind. Also die fünf Prozent an Unternehmens-Know-how, die wirklich schützenswert sind und deren Verlust das Unternehmen existenziell gefährden würde. Erst wenn diese schützenswerten Informationen definiert wurden, lassen sich passende Maßnahmen treffen. Ich sage immer: Die Konstruktionszeichnungen eines Unternehmens haben nicht den gleichen Schutzcharakter wie der Kantinenplan. Das bedeutet: Nur, wenn man den Unterschied kennt, kann man sein Know-how entsprechend schützen und dies auch seinen Mitarbeitern kommunizieren, damit sie wissen, wie sie mit diesen Informationen umgehen müssen.

Unternehmen ergreifen heutzutage vor allem Sicherheitsmaßen im IT-Bereich und fühlen sich sicher. Worauf sollte man zusätzlich achten?

Michael George: Viele Unternehmen stellen sich mittlerweile technisch gut auf und haben einen relativ hohen Grundschutz installiert. Allerdings bemerken wir, dass es oft bei den Mitarbeitern mangelt oder organisatorische Regelungen nicht umgesetzt werden. Das bedeutet, dass das Thema falsch adressiert wird. Wenn das Thema Informationssicherheit ausschließlich an die IT adressiert wird, kann das fatal sein, weil nur 20 Prozent der beobachtbaren Fälle wahrgenommen werden. Es gibt Situationen, in denen ungewünschter Transfer von Wissen stattfinden kann. Zum Beispiel der Verlust von USB-Sticks, im Papierkorb liegengebliebene Unterlagen, externe Mitarbeiter, Praktikanten, Diplomanden, die Gespräche mithören, Mitarbeiter, die das Unternehmen verlassen, ohne dass es vorher bekannt ist, soziale Netzwerke, Geschäftsreisen, Forschungsprojekte mit Universitäten usw. Das sind alles Situationen, in denen eventuell Wissen verloren gehen kann. Wenn das Thema Informationssicherheit nur an die IT adressiert wird, dann werden solche Bereiche wie Papierkörbe, liegengebliebene Unterlagen, externe Leute, etc. gar nicht mehr beobachtet. Wenn dann etwas passiert, ist das Kind meistens bereits in den Brunnen gefallen. Diese einseitige Adressierung von Informationssicherheit an die IT ist ein großes Problem. Man sollte immer auch die Mitarbeiter und organisatorische Regelungen einbeziehen.

Michael George

Michael George, Referent für Spionageabwehr und Wirtschaftsspionage beim Bayerischen Landesamt für Verfassungsschutz.
Foto: Wirtschaftsschutz (LfV)

Mehr als 80 Prozent aller Täter im Bereich Wirtschaftsspionage sind Mitarbeiter des betroffenen Unternehmens. Was bewegt Angestellte dazu, ihren Arbeitgeber auszuspionieren?

Michael George: Solche Täter werden als Innentäter bezeichnet. Es gibt drei Punkte, die den Mitarbeiter zum Innentäter werden lassen. Dies sind: Motivation, Gelegenheit und Rechtfertigung. Wenn diese Punkte erfüllt sind, dann wird eine Person zum Innentäter. Wenn ein Mitarbeiter beispielsweise nichts stehlen oder weitergeben will, dann wird er es nicht tun. Wenn er keine innerliche Rechtfertigung für seine Tat hat, die man aus psychologischer Sicht immer braucht, bspw. dass das Unternehmen versichert ist oder sich sowieso alle so verhalten, dann wird er es nicht tun. Und wenn er keinen Zutritt oder Zugang zu sensiblen Informationen hat, dann gibt es auch keine Gelegenheit für ihn. Loyalitätsbildende Maßnahmen, durch die sich der Mitarbeiter mit dem Unternehmen verbunden fühlt, sind definitiv ein aktiver Pluspunkt gegen Spionage und Innentäterschaft.

Weitere Informationen zum Thema Wirtschaftsspionage bietet das Bayerische Landesamt für Verfassungsschutz online in einem virtuell begehbaren Unternehmen unter *www.wirtschaftsschutz-bayern.de* an. Zudem bietet die Behörde kostenlose Informationsberatungen für Unternehmer sowie Vorträge an. Für Anfragen: Telefon 089/31 201 206 sowie per E-Mail an *wirtschaftsschutz@lfv.bayern.de.*

Zu diesem Beitrag

Michael George konnte leider keinen Text für die FIfF-Kommunikation schreiben, er hat zu viel zu tun. Deshalb hat er uns diesen Text überlassen, der einige Aspekte aus seinen Diskussionsbeiträgen auf dem Podium unserer Jahrestagung darstellt. Das Interview erschien am 5. November 2011 im Bayernkurier Report Nr. 44. Wir danken Frank Gundermann und dem Bayernkurier für die Genehmigung zum Nachdruck.

Hans-Jörg Kreowski und Dietrich Meyer-Ebrecht

AG1: Killerroboter, Cyberwar & Co.

Die digitale Aufrüstung geht weiter …

Seit der Gründung des FIfF ist die Verflechtung von Rüstung und Informatik ein bestimmendes Thema, das auch nicht an Bedeutung verliert, solange Informations- und Kommunikationstechnologie umfassend und maßgeblich eingesetzt werden, um Waffen effektiver zu machen und Kriege zu organisieren. Die Arbeitsgruppe 1 auf der FIfF-Jahrestagung 2011 hat sich mit dieser Problematik auseinandergesetzt.

Von den Anfängen der Computertechnik und Informatik bis heute werden deren Errungenschaften militärisch genutzt. Ihre vielfältige und umfassende Verwendung in der Rüstungstechnik einerseits und bei der Planung und Organisation von Kriegen andererseits hat völlig neue Formen der Kriegführung ermöglicht und die Bedrohung durch Kriege um einige perfide Komponenten erweitert. Ein Beispiel sind Killerroboter, die programmiert töten und dabei die Illusion nähren, die eigenen Soldaten könnten verschont bleiben. Ein anderes Beispiel ist das, was unter den verniedlichenden Begriff des *Cyberwar* fällt: Propaganda, Spionage, Sabotage mit Mitteln der Informations- und Kommunikationstechnik, um militärische und vor allem auch zivile Infrastruktur des Gegners lahmzulegen.

Die Arbeitsgruppe war mit 26 Teilnehmerinnen und Teilnehmern sehr gut besucht. Nach einer Vorstellungsrunde haben die Organisatoren der AG kurze Referate gehalten, an die sich jeweils eine Diskussion anschloss. Hans-Jörg Kreowski hat die Killerroboter thematisiert, Dietrich Meyer-Ebrecht hat sich mit dem Thema Cyberwar beschäftigt und Ralf E. Streibl ist auf die Militarisierung von Bildung und Wissenschaft eingegangen. Der erste Beitrag unter dem Titel *Gehören Killerroboter vor ein Kriegsgericht?* wurde bereits in der vorigen Ausgabe der FIfF-Kommunikation (4/2011) abgedruckt, die das Thema der Arbeitsgruppe als Schwerpunkt hatte. Der zweite Beitrag ist im Folgenden zusammengefasst. Der dritte Beitrag ist ab Seite 21 in diesem Heft nachzulesen.

Die „Neuen Kriege"

Mit informationstechnischen Mitteln und Methoden – oder zumindest mit ihrer Unterstützung – werden Auseinandersetzungen eines neuen Typs ausgefochten, für die sich der Begriff *Cyberwar* etabliert hat. Fällt dieser Begriff, reichen die Assoziationen von Science-Fiction bis zu beängstigenden Bedrohungsszenarien. Wenn nicht gerade brisante Meldungen punktuell von den Medien hochgespielt werden – Cyberangriff auf staatliche Infrastrukturen in Estland (2007), psychologische Kriegsführung im Internet gegen Georgien (2008), massive Datenspionage zurückverfolgbar ins chinesische Internet (2009), Einsatz des Sabotagevirus *Stuxnet* gegen iranische Atomtechnikanlagen (2010) –, wird das Thema jedoch in der Öffentlichkeit wenig wahrgenommen. Zum Krieg gehören Waffen, und mit dem Begriff Waffe verbinden wir etwas Anfassbares – die Mittel und Methoden des *Cyberwar* aber lassen sich nicht greifen, sie bleiben abstrakt.

In den Stabsstellen der Verteidigungsministerien ist *Cyberwarfare*, die Kriegführung mit informationstechnischen Mitteln und Methoden, jedoch mittlerweile fest in das militärische Kalkül eingebunden[1]. In der Militärdoktrin haben sich längst Vorstellungen vom IT-basierten Schlachtfeld, von den so genannten „Neuen Kriegen" etabliert. Sie sind mittlerweile ein relevantes Element der *Revolution of Military Affairs* (RMA). Wie real die Bedrohung eingeschätzt wird, beweist das Interesse der Friedens- und Konfliktforschung an dem Thema[2,3].

Ganz sicher darf auch das FIfF dieses Thema nicht ignorieren. Ute Bernhardt[4] und Ingo Ruhmann[5] widmeten ihm bereits zwei Beiträge in der letzten *FIfF–Kommunikation*. Der Entwurf eines Positionspapiers des FIfF ist in diesem Heft auf Seite 41 abgedruckt. Als Informationsbasis für die weitere Arbeit wird derzeit in unserem Wiki eine Sammlung von Quellen zum Thema *Cyberwarfare* angelegt[6]. Wenn wir auf unserer Jahrestagung 2011 mit der Ausrichtung der AG1 für eine Neubelebung unseres Arbeitskreises „Rüstung und Informatik" – kurz *RUIN* – warben, so auch weil wir die Bearbeitung des Themas *Cyberwarfare* zur Diskussion stellen wollten. Anmoderiert wurde die Diskussion mit Stichworten zu den verwirrend vielfältigen Facetten des Themas, die im Folgenden kurz zusammengefasst werden.

Cyberwar oder *Cyberwarfare, Cyberweapons, Information War* oder *Information Warfare*, … – allein schon die Begriffe, unter denen das Thema gehandelt wird, variieren. Vielschichtig sind die Szenarien und ‚Technologien': die Heterogenität der Akteure, die Vielfalt der Motive, die kontextbedingte Intransparenz und Beweisproblematik, schließlich die Berichterstattung der Medien, die zwischen Horrorszenarien und Abwiegelung pendelt.

Weit gespannt ist der Bereich der Eskalation von Aktionen im *Cyberspace*. Er beginnt bei feindlichen Manipulationen der Medien. Wie diese verursachen auch Industriespionage und Ausspähung strategischer Pläne zunächst nur indirekte Schäden. Aber schon bei der Verfolgung von Dissidenten und Aktivisten – wie effektiv moderne IT repressiven Machthabern in die Hände spielt, beschreibt Morozov[7] – kommen auch Menschen als Individuen in existenzielle Gefahr. Der Einsatz von Schadsoftware kann schließlich, wenn vitale Infrastrukturen gezielt gestört werden, weit reichende bis katastrophale Wirkungen auf die Zivilgesellschaft haben. Noch nachhaltiger kann die physische Zerstörung von IT-Infrastrukturen mit konventionellen Zerstörungsmethoden wirken. Gezielt und mit geringeren ‚Kollateralschäden' können hochenergetische elektromagnetische Impulse (EMP), erzeugt durch (nicht-atomare) EMP-Generatoren, IT-Einrichtungen von Mobiltelefonen bis zu Großrechenanlagen dauerhaft außer Funktion setzen – was ein *Nuclear electromagnetic pulse* (NEMP) als ‚Nebenwirkung' eines Atomwaffeneinsatzes flächendeckend in einem weiten Umkreis erreicht.

Trotz dieses Bedrohungspotenzials müssen wir eine schleichende Eskalation der Risiken konstatieren: Immer engmaschiger und weit greifender wird die Vernetzung der Infrastrukturen, immer stärker die Abhängigkeit der Zivilbevölkerung von der Unterstützung durch digitale Dienstleistungen, Datensammlungen und Kommunikationsnetze. Gleichzeitig steigt die Komplexität der vernetzten Systeme selbst. Damit steigt die Zahl der involvierten Akteure, und es steigt die Vielfalt der verwundbaren Stellen. Bedenklich ist die gleichzeitige Aufgabe strenger Systemisolation zugunsten vermeintlicher Optimierungsgewinne.

Unübersichtlich und schwer greifbar wird das Thema auch, weil zunehmend die Grenzen verschwimmen zwischen zivil und militärisch (Stichwort *Dual-Use*), zwischen Sicherheitsinteressen und staatlichen Eingriffen in die Privatsphäre oder kriminellen Absichten. Ob es sich um digitale ‚Kollateralschäden' handelt oder um gezielte Angriffe, kann oft nicht unterschieden werden. Auch ob Cyber-Angriffe noch ‚Kriegsspiel' sind oder schon als reale Kampfhandlungen gelten müssen, zeigt sich erst in der Entwicklung der Situation: Wann werden aus virtuellen Aktionen ‚kinetische' Wirkungen, d. h. physische Zerstörungen? Wann schlägt ein noch als Frieden geltender Zustand in Krieg um, insbesondere wenn die Konstellation in einen asymmetrischen Krieg mündet? Das Attributierbarkeitsproblem, das sich aus den vielen Unsicherheiten der Einschätzung von Ereignissen und Situationen ergibt, führt zur *„Strategic Ambiguity"*, zu dem hochgefährlichen Entscheidungsproblem, wie, wo und gegen wen zu reagieren ist.

Noch wirft das Thema viel mehr Fragen auf, als Antworten gegeben werden können. Unklar ist die Definition von „Waffen", was unter anderem Auswirkungen auf die Richtlinien für Exportbeschränkungen hat. Ist eine Kontrolle des *Cyberspace* gegen einen Missbrauch als Kriegsschauplatz möglich, und wenn ja, durch welche Instanzen? Welche ‚Kollateralschäden' muss die Gesellschaft für mehr Sicherheit hinnehmen (Eingriffe in die Privatsphäre etc.)? Ist eine ‚digitale' Abrüstung möglich?

Leider wird die Beantwortung der aufgeworfenen Fragen nicht einfacher, wenn das Thema durch *Buzzwords* vernebelt wird. Für das FIfF stellt sich deshalb als vordringliche Aufgabe, Fakten zu sammeln und zu bewerten, die Entwicklung zu beobachten, Zusammenhänge zu analysieren und allgemeinverständlich aufzuklären. Und ‚Aktive' zu finden, die an diesen Aufgaben mit Kompetenz und Engagement mitarbeiten wollen …

Die Arbeitsgruppe endete mit einer kurzen Diskussion, ob, und wenn ja, in welcher Form der bundesweite FIfF-Arbeitskreis RUIN (Rüstung und Informatik) wiederbelebt werden soll. Vorschläge dazu sollen demnächst folgen. Wer daran interessiert ist, möge uns eine E-Mail schicken an *dme@fiff.de* oder *kreo@informatik.uni-bremen.de*.

Anmerkungen

1 *Gaycken S: „Cyberwar: Das Internet als Kriegsschauplatz", Open Source Press, 2010 (siehe auch die Rezension des Buches in der FIfF-Kommunikation 4/2011)*
2 *„Wettrüsten im Cyberspace", gemeinsamer Workshop des IFSH und des FONAS, Hamburg, 24.06.2011*
3 *„Challenges in Cybersecurity: Risks, Strategies, and Confidence–Building", International Conference gemeinsam ausgerichtet vom Auswärtigen Amt, der FU Berlin, dem IFSH und dem UNIDIR; Berlin, 13./14.12.2011*
4 *Bernhardt U: „Mahnen und Aufklären – Information Warefare und FIfF", FIfF-Kommunikation 4/2011, 26-27*
5 *Ruhmann I: „Cyber-Krieg oder Cyber-Sicherheit – wächst aus Abhängigkeit auch die Einsicht?", FIfF-Kommunikation 4/2011, 38-43*
6 *http://wiki.fiff.de/LinklisteCyberwar*
7 *Morozov E: „The Net Delusion – How Not to Liberate The World", Allen Lane, London, 2011 (siehe auch die Rezension des Buches in der FIfF-Kommunikation 2/2011)*

Ralf E. Streibl

AG1: It's a Challenge – Militärische Roboterwettbewerbe

Oder: Von reizvollen Wettbewerben, schleichenden Vereinnahmungen und der Notwendigkeit von Diskursen[1]

»Am Anfang, in der Mitte und am Ende der Angewandten Informatik stehen Entscheidungen: Informatik ist eine Entscheidungswissenschaft.«
(Steinmüller 1992, S.103)

Verschwimmende Grenzen

2005 unternahm Wolfgang Liebert von der Darmstädter Forschungsgruppe *IANUS* (Interdisziplinäre Arbeitsgruppe Naturwissenschaft, Technik und Sicherheit) den wichtigen Versuch, das Verhältnis von Forschung und Militär einige Jahre nach dem Fall der Mauer und den Veränderungen in Osteuropa etwas genauer zu analysieren. Er kam dabei zu einem desillusionierenden Ergebnis: *„Nach der Implosion des mit dem Westen konkurrierenden Systems sah es für kurze Zeit so aus, als ob in Wissenschaft und Technik die Konzentration auf den zivilen Sektor Dominanz bekommen würde, doch heute ist die Verzahnung von militärischer und ziviler Forschung unübersichtlicher als jemals zuvor"* (Liebert 2005, S.26).

Es mag in früheren Zeiten vergleichsweise einfacher gewesen sein, militärische von ziviler Forschung zu unterscheiden und vielleicht auch zu trennen. Verschiedene parallel laufende Entwicklungen führten jedoch dazu, dass die Grenzen heutzutage wesentlich unschärfer sind bzw. sich in manchen Bereichen immer mehr auflösen.

Motive für Dual-Use

Forschung und Entwicklung (FuE) hinsichtlich von Technologien, die direkt auf militärische Anwendungen zugeschnitten sind und für die es keinen kommerziellen Markt gibt, sind zu unterscheiden von ziviler Forschung und Entwicklung, deren Ergebnisse auch militärisch genutzt oder nutzbar gemacht werden. Dieser letztgenannte Bereich gewann in der Vergangenheit gegenüber der rein militärischen FuE zunehmend an Bedeutung – eine Entwicklung, die durch mehrere Faktoren befördert wurde und wird (vgl. hierzu u.a. Gummett & Reppy 1988, Domke 1991, Liebert 2005, Neuneck 2010):

- **Wachsende Militärausgaben:** Innerhalb des Militärs wuchs zunehmend die Besorgnis über die stetig steigenden Ausgaben, die insb. auch der technisch immer aufwändigeren Ausstattung geschuldet waren: *„Each generation of equipments costs more than its predecessor (in part because of greater complexity and sophistication), and in consequence is purchased in smaller numbers"* (Gummet & Reppy 1988, S.2). Die steigenden Rüstungshaushalte gingen dabei immer mehr zu Lasten des Gesamthaushalts, die Hoffnung auf einen wirtschaftlich interessanten »Spin-off« aus der Militärforschung bestätigte sich kaum.

- **Wirtschaftliche Konkurrenzfähigkeit:** Die rüstungsbezogenen Ausgaben wurden dabei nicht nur aufgrund ihrer absoluten Höhe, sondern auch im relativen Vergleich zu Ausgaben für zivile Forschung und Entwicklung betrachtet. Dabei wurde in den westlichen Kernwaffenstaaten hinterfragt, ob durch den Fokus auf rüstungsrelevante Forschung zu viele Mittel und in der Folge natürlich auch die Kompetenz der beteiligten Wissenschaftlerinnen und Wissenschaftler gebunden und somit vom zivilen Fortschritt abgezogen würde, was dann eine Schwächung im wirtschaftlichen Wettbewerb nach sich zöge – beispielsweise im Vergleich zum technologiestarken Japan mit seinen vergleichsweise geringen Rüstungsausgaben.

- **Relevanz generischer Technologien:** In manchen Anwendungen – nicht zuletzt im Bereich der Elektronik, Informations- und Kommunikationstechnik – zeigen sich beim Einsatz grundlegender Technologien und Materialien bei der konkreten Betrachtung von Sub- oder Sub-Sub-Systemen kaum oder gar keine Unterschiede zwischen militärischem und zivilem Einsatz und Gebrauch. Hier finden teilweise identische Komponenten und Algorithmen Einsatz – erst im Kontext des Gesamtsystems wird der militärische Zweck deutlich.

- **Friedenspolitische Argumente:** Insbesondere in Deutschland besteht eine gewisse gesellschaftliche Aufmerksamkeit und eine latente Diskussion hinsichtlich der Rolle des Militärs (vgl. Meyer 2004). Dies ist insb. vor dem Hintergrund der beiden Weltkriege und verschiedener größerer gesellschaftlicher Debatten zu Fragen der Militär- und Friedenspolitik (Wiederbewaffnung, Wehrpflicht, „Nachrüstung"/NATO-Doppelbeschluss, humanitäre Interventionen, Out-of-Area-Einsätze, neue Rolle der Bundeswehr etc.) zu verstehen. Dadurch existiert auch ein friedenspolitisch verortbares, gesellschaftliches Unbehagen hinsichtlich Rüstungsforschung. In Reaktion hierauf wurden und werden militärrelevante Forschungsaktivitäten und Fördermaßnahmen seitens der beteiligten Akteure in Politik, Wirtschaft und Wissenschaft in der Öffentlichkeit gerne in einen zivilen Rahmen eingebettet (oder auch nur mit zivilem Deckmäntelchen kaschiert). Ein – dann dem Augenschein nach nicht intendierter – Rüstungsbezug tritt somit erst später ans Licht. *„Mit*

1 Der vorliegende Beitrag ist die erweiterte Fassung eines Vortrages im Rahmen der Arbeitsgruppe »Killerroboter, Cyberwar & Co. – die digitale Aufrüstung geht weiter« bei der 27. FIfF-Jahrestagung, November 2011 in München.

»Dual-Use« wird abgelenkt von der Einflußnahme der Sicherheitspolitik auf die Forschungs- Technologie- und Wirtschaftspolitik sowie vom Einsatz ziviler Ressourcen bei der Entwicklung von Technologien für das Militär. »Dual-Use« suggeriert Neutralität, Wert- und Zweckfreiheit von Wissenschaft und Technologie" (Domke 1991, S.173).

„Zivilitärische" Forschung

Die geschilderten Trends und Einflussfaktoren trugen zu einer Verschiebung in Richtung auf zivile Forschung unter Berücksichtigung militärischer Nutzung bei – mit unterschiedlichen Ausprägungen, wie Manfred Domke bereits 1991 hervorhob. Er unterschied dabei insbesondere *„Technologien des zivilen Marktes, die auch militärisch genutzt werden"* sowie *„Technologien, die im Interesse des Militärs und für das Militär zivil gefördert, zivil erforscht und entwickelt werden und aus Kostengründen auch zivil genutzt werden sollen"* (Domke 1991, S.172).

Welche Bedeutung gerade dem letztgenannten Bereich zukommt, verdeutlicht der einleitende Beitrag von Wolfgang Liebert, Rainer Rilling und Jürgen Scheffran zu der Tagungsdokumentation *Die Janusköpfigkeit von Forschung und Technik* (1994). Darin werden anhand verschiedener Quellen aus dem Kontext der Deutschen Bundesregierung frühzeitige Absprachen zwischen dem Verteidigungs- und dem Forschungsministerium sichtbar, die das Ziel verfolgten, zivile Programme und Projekte durch militärische Wünsche zu beeinflussen. Die Indizien veranlassen die Autoren zu folgender Schlussfolgerung: *„Die scheinbar unvermeidbare Ambivalenz erweist sich bei genauerem Hinsehen als nüchtern geplante Strategie, die hinter einem Schleier der Intransparenz verborgen wird"* (Liebert, Rilling, Scheffran 1994, S.27).

Entsprechende Zusammenhänge sind auch auf europäischer Ebene erkennbar. Zivil-militärische Kooperation innerhalb von Konzernen wird durch zunehmende Firmenzusammenschlüsse realisiert und ausgebaut. Die Politik sekundiert dabei, wie Wolfgang Liebert u.a. mit Verweis auf das im November 2003 vorgelegte EU-Weißbuch zur Raumfahrtpolitik belegt:

»Darin wird ganz selbstverständlich und selbstbewusst das Raumfahrtinstrumentarium als ein Mittel für die Verwirklichung der Gemeinsamen Außen- und Sicherheitspolitik (GASP) sowie für die Europäische Sicherheits- und Verteidigungspolitik (ESVP) angepriesen. Betont wird: Raumfahrtsysteme wie die ehrgeizigen europäischen Satellitenprogramme „unterstützen nicht nur eine breite Palette ziviler Politikbereiche, sondern können auch einen unmittelbaren Beitrag zur GASP und ESVP leisten" (Liebert 2005, S.28).

Ambivalenz

Dual-Use steht für die Nutzung von Forschungsergebnissen für zivile und militärische Zwecke. Diese kann sich aufgrund strukturell ähnlicher Bedürfnisse des Militärs mehr oder weniger einfach „ergeben", oftmals wird sie jedoch von Beginn an intendiert sein. In diesem Fall sind konkrete Einflüsse auf die konkrete Planung und auf Entscheidungen im FuE-Prozess zu erwarten – unter dem Primat des Militärischen.

Der Begriff der *Ambivalenz* hebt hingegen stärker auf die Anwendungs*möglichkeiten* ab und betont damit die grundsätzliche Problematik der Zweischneidigkeit von Forschung und Technologieentwicklung. Neben der Frage eines militärischen Gebrauchs ziviler Forschungsergebnisse können unter diesem Begriff auch andere Ambivalenzen betrachtet werden (z. B. Auswirkungen in ökologischer oder sozialer Hinsicht). Der Begriff geht – wie Wolfgang Liebert berichtet – zurück auf Carl Friedrich von Weizsäcker: *„Ambivalenz nennen wir die Erfahrung, dass wir, gerade wenn wir etwas Angestrebtes erreicht haben oder verwirklicht haben, entdecken müssen, dass es eigentlich nicht das Angestrebte, sondern vielleicht sogar dessen Verhinderung war"* (zit. n. Liebert 1997, S.247).

Mit dem Ambivalenzbegriff kommt *„die Möglichkeit der Bearbeitung dieser Problematik bereits auf der Ebene von Forschung und Technologieentwicklung selbst"* in den Blick, stellt Liebert (2005, S.28) heraus. Insofern nimmt der Ambivalenzbegriff die Akteurinnen und Akteure auf Seiten der Wissenschaft stärker in die Pflicht, sich nicht als fremdbestimmte Handelnde zu sehen, sondern sich aktiv mit ihrer eigenen Verantwortung zu befassen. *Ambivalenz* beinhaltet die Notwendigkeit einer wertebasierten Auseinandersetzung und Entscheidungsfindung – hierzu mehr am Ende des Beitrages.

Herausforderungen

Vor dem Hintergrund dieser eher allgemeinen Überlegungen zum Verhältnis von Militär und Wissenschaft soll nun das Augenmerk auf ein spezifisches Beispiel gelenkt werden: Wettbewerbe im Bereich Robotik.

DARPA Challenge

2004 fand in Kalifornien die erste *DARPA Grand Challenge* statt, ein Wettbewerb für fahrerlose Landfahrzeuge, die eine Strecke von über 200 Kilometer Länge autonom fahren sollten. Während in jenem Jahr kein Team erfolgreich war, schafften es im darauf folgenden Jahr fünf Fahrzeuge – das Gewinnerteam kam von der Stanford University. 2007 gab es erneut ein Rennen, diesmal als *DARPA Urban Challenge* in bebautem Gebiet. Die *DARPA* (Technologiebehörde des US-Verteidigungsministeriums) stellte für diesen Wettbewerb ein Budget von 20,5 Millionen US-Dollar bereit, davon 3,5 Millionen Preisgelder. Das Format des Team-Wettbewerbs bietet zum einen durch die ausgelobten Preisgelder und zum anderen durch die *Herausforderung* selbst einen hohen Anreiz, der insb. auch universitäre Teams lockte. Es sei erklärtes Ziel, so eine DARPA-Sprecherin, gerade auch solche Forscher zu gewinnen, die ansonsten nicht für das Militär arbeiten würden (Walker, zit. n. Mariske 2007). Hintergrund des Wettbewerbs war eine Forderung des US-Congress, bis 2015 ein Drittel der US-Militärfahrzeuge unbemannt fahren zu lassen.

ELROB

In Europa existieren entsprechende Wettbewerbe. Seit 2006 gibt es *ELROB (European Land-Robot Trial)* – jährlich wechselnd

Abb. 1: Plakat zu ELROB 2010, Quelle: www.elrob.org

in einer militärischen und in einer zivilen Variante. Die Aufgaben der zivilen Variante betreffen beispielsweise Szenarien hinsichtlich Überwachung, Zivil- und Katastrophenschutz.

Auch bei *ELROB* liegt ein erklärtes Ziel in der Vernetzung von Universitäten und Forschungseinrichtungen mit Militär und Rüstungsindustrie. So heißt es beispielsweise im Informations-Flyer für *ELROB 2010*:

> *„(...) The participation of universities, institutes, companies and capability developers not only of European armed forces allows users, developers as well as representatives of trade and industry to congregate as a community. ELROB is not a »battle of competitors« with high-tech visions but rather a forum to show what is feasible in robotics, to support technological developments in Europe, and to find solutions for the current military challenges." (ELROB 2010)*

UAV-Forge

Inzwischen hat die US-Regierung Wettbewerbe und Crowdsourcing offenkundig als systematisch einzusetzende Methode für sich entdeckt. So schrieb beispielsweise das *US Department of Defense (DoD)* im vergangenen Jahr auf der Website *challenge.gov*, mit der die US-Regierung diverse Wettbewerbe (unterschiedlich in Art, Umfang und Thema) auslobt, die Entwicklung kleiner, unbemannten Flugobjekte aus:

Verantwortlicher Umgang mit Forschungsfreiheit und Forschungsrisiken

(...) Denn auch als hochspezialisierter Forscher bleiben Sie ein zoon politicon. Und deshalb ist Wissenschaft heute nicht nur – wie Carl-Friedrich von Weizsäcker gesagt hat, »sozial organisierte Erkenntnissuche« – sondern Wissenschaft ist zugleich eine zur sozialen Verantwortung verpflichtete Erkenntnissuche!"

Helmut Schmidt (2011):
Rede bei der Max-Planck-Gesellschaft

Am 19. März 2010 beschloss der Senat der Max-Planck-Gesellschaft Hinweise und Regeln zum verantwortlichen Umgang mit Forschungsfreiheit und Forschungsrisiken (MPG 2010). Diese sollen als ethische Leitlinie im Sinne der Selbstregulierung Missbrauch der Forschung verhindern und Risiken vermeiden. Bereits im Einleitungsteil wird dabei auch auf die Problematik von Rüstungsforschung eingegangen:

> *„(...) Mit den Erfolgen einer freien und transparenten Forschung gehen jedoch auch Risiken einher. Diese resultieren nicht nur unmittelbar aus eigenem fahrlässigen oder vorsätzlichem Fehlverhalten von Wissenschaftlern. Daneben besteht bei einzelnen Forschungen die mittelbare Gefahr, dass – für sich genommen neutrale oder nützliche – Ergebnisse durch andere Personen zu schädlichen Zwecken missbraucht werden. Diese Möglichkeit des »Dual-Use« erschwert oder verhindert heute in vielen Bereichen eine klare Unterscheidung von »guter« und »böser« Forschung, von Zivil- und Rüstungsforschung, von Verteidigungs- und Angriffsforschung sowie von Forschung für »friedliche« und für »terroristische« Anwendungen. Die »Dual-Use«-Problematik muss auch in der wissensgetriebenen Grundlagenforschung beachtet werden, deren Resultate oft nicht vorhersehbar sind und deren Ergebnisse deswegen per se nicht gut oder schlecht sind. (...)" (S.4)*

Im weiteren Verlauf des Textes wird deutlich herausgestellt, dass rechtliche Normen die Freiheit der Wissenschaft beschränken. Sie können beispielsweise Forschungsziele ausschließen, Methoden reglementieren, den Export von Wissen, Dienstleistungen und Produkten in bestimmte Regionen untersagen. Jedoch können nicht alle Risiken und Missbrauchsmöglichkeiten vollständig und effektiv normiert und dadurch verhindert werden. Insofern dürfen sich Wissenschaftler aber auch nicht nur mit der Einhaltung dieser gesetzlichen Regelungen begnügen, sondern es sind weitergehende ethische Grundsätze zu berücksichtigen:

> *„Der einzelne Wissenschaftler (...) soll dabei sein Wissen, seine Erfahrung und seine Fähigkeiten einsetzen, um die einschlägigen Risiken einer Schädigung von Mensch und Umwelt zu erkennen und abzuschätzen. In kritischen Fällen muss er eine persönliche Entscheidung über die Grenzen seiner Arbeit treffen, die er im Rahmen seiner Forschungsfreiheit selbst verantwortet. Dies kann dazu führen, dass Vorhaben, auch wenn sie gesetzlich nicht verboten sind, im Einzelfall nur in modifizierter Form oder überhaupt nicht durchgeführt werden." (S.5)*

„UAVForge is a Defense Advanced Research Projects Agency (DARPA) and Space and Naval Warfare Systems Center Atlantic (SSC Atlantic) collaborative initiative to design, build and manufacture advanced small unmanned air vehicle (UAV) systems. Our goal is to facilitate the exchange of ideas among a loosely connected international community united through common interests and inspired by innovation and creative thought. (...) A top manufacturing company will also be selected to participate to provide you and your fellow designers with insight and expertise throughout the competition. (...) Top teams will be invited to a competition fly-off where the winning team will receive a $100,000 prize, a subcontract with a manufacturer to produce a limited number of systems, and an invitation to demonstrate the winning UAV design solution in an exclusive operational military demonstration.“ (UAVForge.net 2011 → ... [Just the Basics])

Das zu entwickelnde System soll dabei – lt. Einsatzszenario – im Rucksack eines Mitglieds einer fiktiven Kampfeinheit transportiert und auch von einer einzelnen Person gesteuert werden können. In einem städtischen Gebiet soll damit dann außerhalb direkter Sichtweite bis zu drei Stunden lang die Beobachtung verdächtiger Aktivitäten erfolgen (UAVForge 2011 → ... [Mission Scenario]).

Abb. 2: Crowdsourcing mit challenges.gov – „Federal agencies can use challenges and prizes to find innovative or cost–effective submissions or improvements to ideas, products and processes.“

SAUC-E

Ein weiterer europäischer Wettbewerb (seit 2006) ist *SAUC-E (Students Autonomous Underwater Challenge – Europe)*. Er wird vom britischen und französischen Verteidigungsministerium veranstaltet, zunächst an wechselnden Orten. Seit 2010 wird der Wettbewerb bei NURC (NATO Undersea Research Center) in Italien durchgeführt.

Ziel ist die Entwicklung eines autonomen Unterwasser-Fahrzeugs, welches einige im Vorfeld spezifizierte Missionen erfüllen können soll, wie z. B. eine Pipeline oder ein sich bewegendes Schiff finden und verfolgen. Neben der technischen Zielsetzung soll den angehenden Ingenieuren und Wissenschaftlern auch das Arbeitsfeld schmackhaft gemacht werden:

„The event is designed to encourage students to think about underwater technology and related applications while fostering innovation and technology. It also aims at getting young engineers and scientists to consider careers in the field.“ (SAUC-E 2012 → [home])

Fortschritt und Vernetzung

Zusammenfassend lässt sich vermuten, dass diese und ähnliche Wettbewerbe wohl mehreren Zwecken dienen sollen:

- Beschleunigung der (militär)technischen Entwicklung
- Erweiterung der kreativen Basis und Abschöpfen innovativer Ideen
- Aufbrechen einseitiger Abhängigkeit von Rüstungskonzernen
- Kostenersparnis im Bereich militärischer FuE
- Engere Vernetzung mit Universitäten und Forschungsinstitutionen
- Abbau von Vorbehalten hinsichtlich Kooperationen mit dem Militär
- Nachwuchswerbung
- Allgemeine Imagewirksamkeit

Dabei – so zeigt bereits der obige, ausschnitthafte Blick auf einige Wettbewerbe – ist der Grad des offenkundigen, direkten Militärbezugs durchaus skalierbar. Dies wiederum mag es manchen Teilnehmenden erleichtern, Überlegungen hinsichtlich der späteren Einsetzbarkeit und Anwendung ihrer Forschungsergebnisse und Entwicklungen eher auszublenden.

Fragen

Wolfgang Liebert, Rainer Rilling und Jürgen Scheffran benennen in ihrem Problemaufriss zur Janusköpfigkeit der Wissenschaft vier Aspekte, deren Betrachtung im Kontext von Ambivalenzanalysen als erste Orientierung hilfreich sein kann. Selbstverständlich handelt es sich dabei aber nicht um eine abschließende Kriterienliste. Betrachtet man beispielsweise die oben genannten Wettbewerbe in diesem Sinne, so tritt ihre hohe militärische Relevanz trotz teilweise nicht direkt militärischer Aufgabenstellungen offen zu Tage.

- *„Die Natur der auftraggebenden und/oder finanzierenden Einrichtung (also etwa ein Verteidigungsministerium) und/oder ihre Nutzungsabsichten.*
- *Der Status der durchführenden Institution oder Person (also etwa ein staatliches Rüstungslabor).*
- *Die Natur des wissenschaftlich/technischen Projekts (z. B. seine Anwendungsnähe zu militärischen Nutzungen).*
- *Die tatsächliche Nutzungsmöglichkeit des erbrachten Ergebnisses bzw. seine Verwendungsweise (z. B. Beschränkung seiner Verbreitung durch Geheimhaltung).“* (Liebert, Rilling, Scheffran 1997, S.15)

Ambivalenz ist im Bereich wissenschaftlicher Forschung und technischer Entwicklung grundsätzlich nicht vermeidbar. Dennoch darf man nicht dem Fehlschluss verfallen, deswegen sämtliche wissenschaftliche Entwicklungen stoppen zu wollen. Vielmehr ist eine

Erhöhung der Transparenz und Auseinandersetzung auf gesellschaftlicher, fachlicher, institutioneller und subjektiver Ebene erforderlich, um die Ambivalenzproblematik produktiv anzugehen:

- Auf der Ebene von Wissenschaft und Gesellschaft ist eine *„frühzeitige antizipative Analyse von Forschung und Entwicklung"* erforderlich, *„die Fragen stellt nach Intentionen, wissenschaftlich-technischen Potenzialen, normativen Rand- und Vorbedingungen, ambivalenten Entwicklungslinien, gewollten Wirkungen, nicht-intendierten Folgen und sichtbaren Entwicklungsrisiken"* (Liebert 2009, S448).

- In der Bildung und insbesondere an den Hochschulen muss kontinuierlich eine intensive, aktive Auseinandersetzung mit direkten oder indirekten gesellschaftlichen Auswirkungen der Fachgebiete erfolgen (vgl. auch Streibl 2011).

- Auf institutioneller Ebene sind sowohl Regularien notwendig (z. B. Herstellung von Transparenz durch eine Verpflichtung zur Bekanntgabe von Forschungsthemen, Kooperationen und Herkunft von Fördermitteln sowie die Verpflichtung zur Veröffentlichung von Forschungsergebnissen). Darüberhinaussollteninnerhalbvon Forschungseinrichtungen Diskurse hinsichtlich Ambivalenz angeregt und unterstützt werden – dazu sind beispielsweise Zivilklauseln wünschenswert und hilfreich: als Appell, Selbstverpflichtung und Orientierung (vgl. auch Streibl 2012 – in diesem Heft).

- Nicht zuletzt ist die persönliche Ebene zentral: Erforderlich ist sowohl die Bereitschaft, sich entsprechende Fragen zu stellen, als auch die Bereitschaft, sich diesen Fragen dann tatsächlich zu stellen. Hilfreich mag hier auch der Austausch und die Diskussion mit anderen sein, um weitere Perspektiven und Ansichten mit in die eigenen Überlegungen einbeziehen zu können. Am Ende steht dann die eigene, persönlich zu verantwortende Entscheidung.

Quellen

Altmann, J.; Bernhardt, U.; Nixdorff, K.; Ruhmann, I.; Wöhrle, D. (2007): Naturwissenschaft – Rüstung – Frieden. Basiswissen für die Friedensforschung. Wiesbaden: vs.

ELROB (2010): 5th European Land Robot Trials – 3rd Military Elrob. Flyer. http://www.elrob.org/fileadmin/melrob2010/flyer.pdf

Gummett, Ph.; Reppy, J. (eds) (1988): The Relations between Defence and Civil Technologies. NATO ASI Series. Dordrecht: Kluwer.

Liebert, W. (1997): Ambivalenz und Janusköpfigkeit in der Wissenschaft. Bemerkungen zur Analyse und zu wissenschaftstheoretischen Hintergründen. In: Liebert, W.; Rilling, R.; Scheffran, J. (Hrsg.): Die Janusköpfigkeit von Forschung und Technik. Zum Problem der zivil-militärischen Ambivalenz. Marburg: BdWi, S.242-258.

Liebert, W. (2005): Dual-use revisited. Die Ambivalenz von Forschung und Technik. In: Wissenschaft und Frieden, 23 (1), S.26-29.

Liebert, W.; Rilling, R.; Scheffran, J. (1994): Die Ambivalenz von Forschung und Technik und Dual-use Konzeptionen in der Bundesrepublik Deutschland – Ein Problemaufriß. In: Liebert, W.; Rilling, R.; Scheffran, J. (Hrsg.): Die Janusköpfigkeit von Forschung und Technik. Zum Problem der zivil-militärischen Ambivalenz. Marburg: BdWi, S.12-30.

Liebert, W. (2009): Umgang mit Dual-Use von Technologien und Ambivalenz in der Forschung. In: Albrecht, S.; Bieber, H.-J.; Braun, R.; Croll, P.; Ehringhaus, H.; Finckh, M.; Graßl, H.; von Weizsäcker, E.U. (Hrsg.): Wissenschaft – Verantwortung – Frieden: 50 Jahre VDW. Berlin: Berliner Wissenschafts-Verlag, S.445-450.

Mariske, H.-A. (2007): Das große Roboter-Rennen. In: Telepolis, 27.10.2007. http://www.heise.de/tp/druck/mb/artikel/26/26497/1.html

Meyer, B. (2004): Meinungsentwicklung zu Bundeswehr und Sicherheitspolitik. In: Fuchs, A.; Sommer, A. (Hrsg.): Krieg und Frieden. Handbuch der Konflikt- und Friedenspsychologie. Weinheim: Beltz, S.250-262.

MPG (2010): Hinweise und Regeln der Max-Planck-Gesellschaft zum verantwortlichen Umgang mit Forschungsfreiheit und Forschungsrisiken. http://www.mpg.de/200127/Regeln_Forschungsfreiheit.pdf

Neuneck, G. (2010): Rüstungsforschung und Raumfahrt: Wie dünn ist die Unterscheidung zwischen zivilem Nutzen und militärischer Verwendung? Vortrag vor dem Akademischen Senat der Universität Bremen, 27.10.2010.

SAUC-E: Students Autonomous Underwater Challenge – Europe. http://www.sauc-europe.org/

Schmidt, H. (2011): Forschung heißt, Verantwortung für die Zukunft zu tragen. Festansprache am 11.1.2011 bei der Max-Planck-Gesellschaft aus Anlass des 100-jährigen Gründungsjubiläums der Kaiser-Wilhelm-Gesellschaft. http://pdf.zeit.de/2011/03/100-Jahre-KWG-Rede.pdf

Steinmüller, W. (1992): Informationstechnologie und Gesellschaft. Einführung in die Angewandte Informatik. Darmstadt: Wissenschaftliche Buchgesellschaft.

Streibl, R.E. (2011): Für eine zivilisierte Bildung und Wissenschaft. In: FIfF-Kommunikation, 28 (4), S.44-50.

Streibl, R.E. (2012): Bremer Universität bestätigt Zivilklausel. Wichtiges Signal für Verantwortung in der Wissenschaft. In: FIfF-Kommunikation, 29 (1), S.46-48

UAVForge.net (2011): Design...Compete...Build Your UAV – How It Works. www.uavforge.net → [How It Works] → ...

(Alle Internetquellen Stand 17.2.2012)

Rainer W. Gerling in der Diskussion mit den TeilnehmerInnen der AG2: Wenn Daten das Unternehmen verlassen – Wie können mobile Daten abgesichert werden?

Sebastian Jekutsch

AG3: Faire Computer – Gibt's das?

Nein, gibt's nicht. Deshalb sollte die Arbeitsgruppe vor allem ausloten, wie wir dahin kommen können.

Videostill aus dem Film „Behind the Screen – Das Leben meines Computers" (http://www.behindthescreen.at/), der im Rahmen der Jahrestagung gezeigt wurde.

Warum unsere Geräte nicht fair (d. h. sozial verträglich) hergestellt werden, warum wir sogar weit davon weg sind und wie sich das aber ändern könnte, war Thema der AG 3 „Faire Computer – Gibt's das?" Wir begannen ganz am Anfang der Wertschöpfung, bei der Gewinnung der Rohstoffe. Ein Video zeigte den Abbau von Zinnerz, geprägt durch Kinderarbeit, Militärkontrolle und einsturzgefährdete Minen. Es begann eine Diskussion darüber, was „unfair" bedeutet, ob so genannter ethischer Konsum etwas ändert und warum es so wenig Nachfrage gibt.

Inhaltlich wurde nachgelegt mit reichlich bebilderten Berichten über die Arbeitsbedingungen in chinesischen Computerfabriken. Sie bedeuten 12-Stunden-Schichten im Stehen, Basislöhne unter dem Existenzminimum und respektlose Unterkünfte. Die Diskussion fokussierte sich auf die Initiativen zur Herstellung fairer IT-Produkte *(www.fairphone.org, www.phefe.de)* und die Chancen öffentlicher Beschaffung nach ökologischen und sozialen Kriterien, zum Beispiel an Universitäten.

Mit dem letzten Schritt im „Leben meines Computers" (so der Untertitel des am Abend gezeigten Films zum gleichen Thema), der Entsorgung der Altgeräte unter teilweise haarsträubenden Bedingungen, konnten wir uns nicht mehr befassen. Statt dessen haben wir uns festgelegt auf ein sinnvolles, uns interessierendes Maßnahmenpaket:

- Es ist wichtig, das Thema bekannt zu machen und den Unterschied zwischen fair und unfair zu definieren. Die Domain *faire-computer.de* ist bereits reserviert.

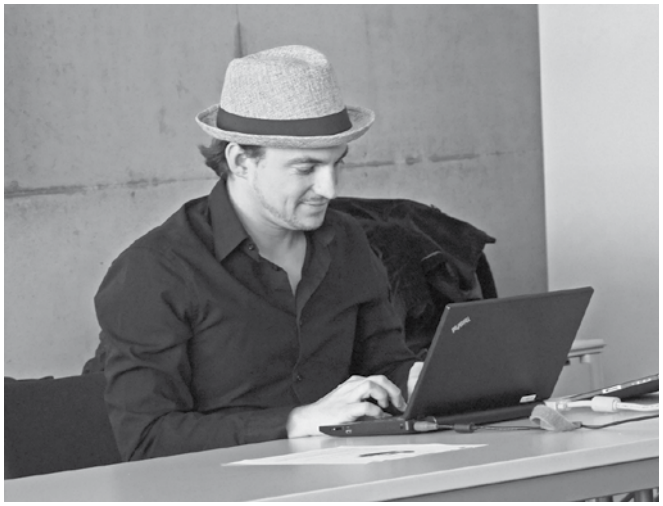
- Wir wollen verstehen, wie an Universitäten der Einkauf von Computern vonstattengeht. Ein Musterbrief soll entwickelt werden, der uns oder besser den Fachschaften und Initiativen hilft, dies an den Unis festzustellen, und um die Chancen einer ökologisch-fairen Beschaffung auszuloten. Wichtig wären persönliche Ansprechpartner in den Verwaltungen.

- In Zusammenarbeit mit dem Fachbereich 8 der GI ist denkbar, Module für Lerneinheiten an Schulen zum Thema auszuarbeiten. Zum Beispiel könnte man durch eigenhändiges Zusammenbauen von Computermäusen sowohl die Arbeits- als auch die Rohstoffthematik motivieren.

Wer hier auf dem Laufenden bleiben möchte, kann sich auch der passenden FIfF-Mailingliste anschließen:
http://lists.fiff.de/mailman/listinfo/fiff-fairit

Sebastian Jekutsch ist FIfF-Mitglied aus Hamburg.
Kontakt: *sj@fiff.de.*

AG4: Facebook & Co. und meine Daten im WWW



Tom von der Isar während seines Vortrages zu Facebook & Co: Seiner These „Ich bin der Herr meiner Daten, ich entscheide, was ich von mir angebe“ konnten die TeilnehmerInnen so nicht zustimmen. Das Problem, „was andere über mich ins Netz stellen“ ist nach wie vor offen, Lösungen sind nicht mal in Ansätzen sichtbar. Nur wenige TeilnehmerInnen hatten eigene Erfahrungen mit Facebook & Co. Trotz großem Interesse scheuen es die meisten, mit ihrer wahren Identität an sozialen Netzwerken teilzunehmen, aber nur so wäre es möglich, den „Geheimnissen“ von Facebook auf die Schliche zu kommen. Ein „bisschen“ Facebook ergibt keinen Sinn.

Jungen Menschen und Schülern gibt Tom von der Isar – z. B. im Rahmen der Aktion *Datenschutz geht zur Schule* – sinngemäß folgenden Rat: Bei allem, was sie im Netz als Text, Bild oder Film von sich mitteilen, sollten sie sich vorher die Frage stellen, ob ihre Eltern dies auch so sehen dürften. (Zusammenfassung B. Schroeder)

Iwan Gulenko

AG5: Maltego – Data-Mining im Internet

Bei *Open Source Intelligence* (OSINT) ist das Ziel, Informationen aus frei verfügbaren Quellen zu sammeln und Erkenntnisse zu gewinnen. Das Programm *Maltego*, das in der Community-Version kostenfrei erhältlich ist, demonstriert diese Möglichkeiten insbesondere in Zeiten des Web 2.0. Ohne viel Vorwissen lassen sich mit sogenannten *Transforms*-Abfragen über Suchmaschinen, die Twitter- oder Facebook-API starten. Dabei arbeitet Maltego als Client-Server-Architektur. Bei der kostenfreien Version wird mit einem öffentlichen Server unverschlüsselt kommuniziert, während die Vollversion, die etwa 700,- Euro kostet, verschlüsselt Abfragen mit dem Server austauschen kann.

Im Workshop wurde vorgestellt, wie sich in Twitter oder Facebook mit der Community-Version nach Begriffen wie „Paypal Probleme“ suchen lässt. Daraufhin werden Nutzer gefiltert, die Entsprechendes auf den Plattformen veröffentlichten. Bei einer Teilmenge ließ sich über das öffentliche Profil die E-Mail Adresse ermitteln, wodurch gezieltes Phishing möglich wird („Sie hatten letztens Probleme mit Paypal …“).

Weiterhin wurde im Workshop die vom Vortragenden entwickelte Facebook-App *(http://apps.facebook.com/can_you_be_googled/)* präsentiert. Damit lässt sich der eigene Freundeskreis auf verdächtige Inhalte durchleuchten. Zum einen zeigt die Applikation, wer die öffentliche Suche, eine Privatsphäre-Option in Facebook, nicht abgestellt hat und somit aus Sicht der Privatsphäre gefährdet sein könnte, zum anderen wird angezeigt, wer Opfer von Clickjacking geworden ist, indem die *Gefällt-Mir* Objekte der Freunde analysiert werden. Die Freunde werden aufgelistet und es ist per Link möglich, die Namen der Freunde in den gängigen Suchmaschinen zu suchen, um zu erfahren, was das Internet über sie weiß. Dadurch können Problemfälle im Freundeskreis aufgedeckt und die Freunde z. B. per Pinnwand-Post oder besser auf vertraulichem Weg gewarnt werden.

Fotos aus den AGs: Dagmar Boedicker

Als Fazit lässt sich festhalten, dass OSINT in Zeiten von Web 2.0 immer mehr Bedeutung gewinnen wird. Das neu gegründete *Open Source Center* der CIA beobachtet beispielsweise Facebook und Twitter, um Entwicklungen in der Welt schnellstmöglich mitzubekommen *(http://intelnews.org/2011/11/08/01-861/)*.

Iwan Gulenko studierte Bachelor Wirtschaftsinformatik und spezialisiert sich in seinem Informatik-Master an der TU München auf den Bereich IT-Sicherheit. Schwerpunkt seiner Abschlussarbeit waren soziale Netzwerke und die davon ausgehenden Gefahren für die IT-Sicherheit.

Sylvia Johnigk

AG6: EU Sicherheitspolitik und -forschung

Die AG 6 der Jahrestagung – EU Sicherheitspolitik und -forschung – befasste sich inhaltlich mit folgenden Themen: EU-Sicherheitsforschung, EU- und insbesondere deutsche „Sicherheitsgesetze", mit der German European Security Association e.V. und Handlungsmöglichkeiten.

Das Thema EU-Sicherheitsforschung, insbesondere das 7. Frameworkprogramm (FP7), wurde inhaltlich bereits in der FIfF-Kommunikation 3/2011[1] behandelt und diente dem AK als Grundlage. Zusätzlich zum FP7 wurden Forschungsprojekte identifiziert, die exclusiv in Deutschland gefördert werden sowie EU-Sicherheitsprojekte, die von anderen EU-behördlichen Geldgebern finanziert werden.

Vergleicht man die aktuelle Forschung mit dem vorherigen FP6[2] und PASR *Preparatory Action in the field of Security Research*[3] zeigt sich ein eindeutiger Trend in die Richtung, dass Überwachung- und Militärprojekte bei der Vergabe von Forschungsgeldern gegenüber Menschenrechtsthemen dominieren. Zur Erinnerung, im 7. Frameworkprogramm stehen 1,3 Milliarden EURO zur Verfügung, von denen gerade mal knapp 1 % für Datenschutz und Freiheit vergeben wurden.

Das Thema EU und insbesondere Deutsche „Sicherheits- und Strafgesetze" war geprägt durch ein Ergebnispapier des *Gödelitzer Kreises*. Der *Gödelitzer Kreis e.V. – Für Demokratie und Rechtsstaat* ist ein Zusammenschluss von Menschen, die sich kritisch unter anderem mit der Gesetzgebung und Strafverfolgung auseinandersetzen.[4] Im Oktober 2009 gaben sie ein Thesenpapier unter dem Titel *Freiheit und Sicherheit* heraus. Sie stellen darin fest, dass es wo es Menschen gibt schon immer Verbrechen und den Kampf gegen das Verbrechen gibt. Es ist ein Kampf, der nicht gewonnen werden kann. Das Verbrechen kann nur eingedämmt werden. Die Kernfrage lautet: Welchen Preis ist eine Gesellschaft bereit zu zahlen, um das Verbrechen einzudämmen? In ihrem Thesenpapier stellen sie zum eigenen Erschrecken fest, dass seit 9/11 die Strafgesetze sowohl auf nationaler als auch auf EU Ebene geradezu inflationär verschärft worden sind. Der Trend setzt sich fort. Vor allem werden Gesetze mit der Begründung „die Gesetze reichen nicht aus" weiter verschärft, ohne das ihre Auswirkungen in der Praxis überhaupt evaluiert werden konnten.

Bemerkenswert ist, dass ursprünglich die Strafgesetze, wie zum Beispiel das StGB, dazu gedacht waren, Bürger vor allzu viel Willkür durch die Strafverfolgungsbehörden zu schützen, indem sie die möglichen Ermittlungsinstrumente auf bestimmte Straftaten einschränkten und die Erlaubnis, sie einzusetzen einer unabhängigen Kontrolle unterwarfen. Dies hat sich drastisch verändert. So stellen sie insbesondere fest, dass eine Vielzahl von bislang weniger schweren Straftaten in den Katalog schwerer Straftaten geschoben wurden. Präventive Strafvereitelung und insbesondere Ermittlung tritt immer weiter in den Vordergrund. Die ausführenden Strafverfolgungsbehörden haben mehr Kompetenzen erlangt. Gleichzeitig wurden Kontrollinstanzen entmachtet, sodass Strafverfolger mittlerweile weitestgehend ohne unabhängige Evaluierung durch einen Richter und unabhängige Kontrolle durch das Parlament präventive und aufklärerische Ermittlungen führen können. Auskunftsrechte der Bürger, eines Anwalts und des Parlaments oder andere auskunftsberechtigter Stellen wurden drastisch eingeschränkt.

Wenn sich zeitgleich Gesetze soweit ändern, dass gegen immer mehr auch ehemals nicht schwere Straftaten unkontrolliert jedesmal die ganze Pallette von Ermittlungsinstrumenten eingesetzt werden kann und sich fast die gesamte (IT-)Sicherheitsforschung darauf fokussiert, diese Instrumente zu erforschen oder besser zu entwickeln, ist dies mehr als bedenklich.

Foto: Dagmar Boedicker

Spätestens seit Bekanntwerden eines Vereins names GESA e.V.[5] könnte es zumindest eine mögliche Erklärung geben, warum das „Ganze" so hervorragend zusammenpasst.

GESA steht für *German European Security Association*[6]. Sie hatte (während der AK stattfand) ihren Sitz am Platz der Republik 1, 11011 Berlin. Es ist die Adresse des Deutschen Bundestags.[7] Die Mitglieder des Vereins: Hans-Peter Uhl, CSU-Bundestagsabgeordneter und Innenpolitiker, ist nicht nur Mitglied, sondern sitzt im Vorstand des Vereins. Die anderen Mitglieder des Vorstands sitzen ebenfalls im deutschen oder europäischen Parlament, bekleiden Posten in Ausschüssen, die über die Vergabe von Forschungsgeldern (einschließlich der zu fördernen Themen) entscheiden. Ebenfalls Mitglied des Vorstands ist der CEO von Bosch Sicherheitssysteme Gert von Iperen und der Leiter des Fraunhofer Instituts EMI Prof. Dr. Klaus Thoma[8]. Ein weiteres prominentes Mitglied ist Prof. Dr. Stock, der stellvertretende Leiter des BKA. Auf ihrer Internetseite geben sie unverblümt zu, dass in diesem Verein Bedarfsträger, Industrien, Entscheider zusammenarbeiten, um eine Sicherheitsstrategie zu entwerfen. Dies tun sie selbstverständlich, so schreiben sie es, „selbstlos und ohne eigene Gewinnerzielungsabsicht."[9] Es sitzen Bedarfsträger (BKA), zusammen mit Parlamentariern, die sie eigentlich kontrollieren sollen, ebenso Entscheider über Forschungs- und Entwicklungsgelder zusammen mit Industrien, die die Gelder über die geförderten Projekte zusammen mit Universitäten und halb staatlichen Forschungsinstituten erhalten.

Praktischerweise bringen sie (zumindest die Mitglieder aus den Parlamenten) auch die nötigen Gesetzesänderungen auf den Weg. Profiteure sind militärische und überwachungstechnische Industrien und eine Politik, der eine äußerst fragwürdige Haltung zu unserer noch freiheitlich demokratischen Verfassung zugrunde liegt.

Sehr schnell waren sich die Teilnehmer einig, dass dem Einhalt geboten werden muss. Leider ist die Thematik sehr komplex und Auswirkungen derartigen Handelns werden erst in den nächsten Jahren sichtbar. Es ist an der Zeit, dass den Bürgern ein Gefühl vermittelt werden soll, dass unsere Gesellschaft nicht durch Terroristen, Hooligans und Pädophile gefährdet ist. sondern durch eine Politik, die durch Angstmacherei Demokratie und Freiheit drastisch einschränkt.

Möglichkeiten, eine breite Masse zu erreichen ist das Internet oder das Fernsehen/der Film. Deshalb soll nach Filmemachern gesucht werden, die daran interessiert sind, die Thematik (Verschärfung der Gesetze gekoppelt mit neuen Überwachungstechnologien) in einem halbdokumentarischen Film umzusetzen, der entweder im Fernsehen oder zumindest über Youtube verbreitet werden soll.

Eine etwas andere Idee ist, an Hochschulen Workshops zu machen, mit dem Ziel, diese Thematik als Theaterstück umzusetzen und aufzuführen.

Unterstützung, Tipps wen wir ansprechen können um ein Filmprojekt zu starten, etc. werden gerne gesehen.

Anmerkungen

1 *FIfF-Kommunikation 3/2011, Seite 56ff: Bewertung der Sicherheitsmaßnahmen im Forschungs-Rahmenprogramm*
2 *http://cordis.europa.eu/fp6/dc/index.cfm?fuseaction=UserSite.FP6HomePage*
3 *ftp://ftp.cordis.europa.eu/pub/security/docs/vademecum_en.pdf*
4 *„Der Gödelitzer Kreis ist ein Zusammenschluss von Rechts- und Innenpolitikern verschiedener Parteien, von Richtern, Wissenschaftlern und Journalisten, die in diesem für unser Gemeinwesen so wichtigen Politikfeld die Entwicklung begleiten und Denkanstöße zur Bewahrung von Rechtsstaat und Demokratie in Deutschland geben wollen." [GÖD2009] http://www.ost-west-forum.de/files/Freiheit%20und%20Sicherheit.pdf*
5 *Bekannt geworden durch einen Artikel von Jörg Tauss http://www.gulli.com/news/17409-die-strippenzieher-wenn-zusammen-kommt-was-nicht-zusammen-gehoert-update-2011-11-24*
6 *Webseite des Vereins: www.gesa-network.de*
7 *Mittlerweile ist der Verein umgezogen, die postalische Adresse ist jetzt das Büro des CDU-Europaabgeordneten Dr. Christian Ehler in Potsdam. Nachzulesen http://www.gulli.com/news/17757-die-strippenzieher-lobbyverein-gesa-nach-gulli-anfrage-aus-bundestag-ausgezogen-2011-12-22*
8 *It. der Web-Seiten des Vereins: „Prof. Thomas' Forschungsschwerpunkte liegen im Bereich der Sicherheit und Verteidigung. Er ist Sprecher des Fraunhofer-Verbunds für Verteidigungs- und Sicherheitsforschung."*
9 *https://gesa-network.de/ziele.html*

Stefan Hügel, Dietrich Meyer-Ebrecht, Jens Rinne

AG8: Europäische Vernetzung

Wie kommt das FIfF nach Europa?

Auch wenn sich die politische Berichterstattung immer noch stark auf die nationale Sicht konzentriert – wesentliche Beschlüsse, auch in der Netzpolitik, werden seit längerer Zeit in Brüssel und Straßburg gefasst. Wenn aber die wesentlichen Entscheidungen auf europäischer Ebene getroffen werden, ist es entscheidend für netzpolitische Initiativen, dass sie europaweit aktiv werden und sich vernetzen.

Das war die Ausgangslage für diesen Workshop. Sein Ziel war, Möglichkeiten zur Mitwirkung auf europäischer Ebene zu identifizieren, und Personen zu finden, die sich dabei engagieren möchten.

Zum Einstieg führten drei Impulsreferate in die Thematik ein:

- *EDRi – European Digital Rights*, eine Institution, in der das FIfF seit 2004 Mitglied ist, hat sich als europäischer Dachverband für Organisationen etabliert, die sich um digitale Rechte kümmern. Einen Überblick über EDRi gab zunächst *Dietrich Meyer-Ebrecht* (vgl. dazu auch Lönnies (2011)). Neben einer kurzen Vorstellung der Organisation gab er einen Überblick über die inzwischen fast 30 Mitgliedsorganisationen und einer Reihe von individuellen Beobachtern. Diese decken eine große Bandbreite ab; gleichzeitig findet eine zunehmende Professionalisierung von EDRi als Lobbyverband statt.
- Wichtige netzpolitische Themen werden heute auf europäischer Ebene entschieden – dies stellte *Stefan Hügel* anschließend in seinem Überblick dar. Dort wird über Richtlinien entschieden, die anschließend in den Mitgliedsstaaten in nationales Recht umzusetzen sind. Die Erfahrung zeigt, dass dabei zivilgesellschaftliche Initiativen meist zu spät kommen: Die Zivilgesellschaft reagiert erst auf die nationale Umsetzung – dann sind aber die Weichen längst gestellt; die Initiativen kommen zu spät, um Korrekturen vorzunehmen und Fehlentwicklungen zu verhindern. Hauptursache ist das Fehlen einer europäischen Öffentlichkeit, in der Entwicklungen frühzeitig thematisiert werden (können). Das Spektrum der Themen ist dabei sehr breit: Vorratsdatenspeicherung, Fluggastdatenabkommen, Europäische Datenschutzrichtlinie, INDECT sind nur einige der Themen, die in Brüssel diskutiert und vorangetrieben werden (vgl. auch Hügel (2010)).

- Eine Darstellung von EDRi gab zuletzt *Jens Rinne*: EDRi hat seinen Sitz in Brüssel, wo es mittlerweile ein mit drei Personen besetztes Büro gibt. Dieses Büro ermöglicht eine sehr professionelle Lobbyarbeit für digitale Rechte. Neben ständigem Kontakt mit Parlamentariern und Eingaben an die politischen Institutionen gibt EDRi auch Veröffentlichungen heraus: Unter dem Titel *EDRi-Papers* (*www.edri.org/papers*) werden Broschüren zu aktuellen Themen der Netzpolitik herausgegeben. Geführt wird der Verein durch einen dreiköpfigen Vorstand mit Andreas Krisch (Wien) als Präsident. Jährlich tritt die Generalversammlung der EDRi-Mitglieder zusammen, um grundsätzliche, organisatorische und strategische Entscheidungen für die Organisation zu treffen.

Möglichkeiten der verstärkten Mitarbeit des FIfF können entlang folgender Leitfragen diskutiert werden:

- Welche Möglichkeiten hat das FIfF, auf europäischer Ebene mitzuwirken?
- Wie können wir dieses Potenzial besser nutzen, um europäische Initiativen zu unterstützen?
- Welche Informationen benötigen wir dafür?
- Brauchen wir andere Strukturen?
- Und nicht zuletzt: Wer im FIfF kann dabei mitarbeiten und ihre oder seine Kompetenz einbringen?

Kritisch ist dabei – das zeigte auch diese eher mäßig besuchte Arbeitsgruppe – der letzte Punkt. Die Kapazität, intensiv an den Themen mitzuarbeiten, ist in einer ehrenamtlichen Organisation nicht gerade im Überfluss vorhanden. Damit stellt sich die Frage nach einer Professionalisierung: Bei EDRi ist das bereit erfolgt; ob das FIfF das ebenfalls will – und kann – wäre weiter zu diskutieren. Denkbar wäre eine Person, die die Positionen des FIfF nach Europa trägt, und der die ehrenamtlichen Mitglieder inhaltlich zuarbeiten – jeweils im Rahmen dessen was sie oder er zu leisten bereit und imstande ist.

alle Fotos: Dagmar Boedicker

Eines ist klar: Wenn wir auf Entwicklungen erst reagieren, wenn sie auf der nationalen Ebene angekommen sind, ist es in der Regel zu spät, noch etwas zu bewegen. Deswegen ist ein stärkeres europäisches Engagement für das FIfF dringend notwendig. Also auf nach Brüssel!

Referenzen

Stefan Hügel (2011): IT- und Bürgerrechtspolitik in Europa, FIfF-Kommunikation 3/2011, 26-30

Tobias Lönnies (2011): Digitale Bürgerrechtsorganisationen in Europa, FIfF-Kommunikation 3/2011, 33-39

Stefan Hügel

Log 1/2012

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.

November 2011

6. November 2011: Berichten zufolge wird bei der Überwachung Oppositioneller in Syrien möglicherweise westliche IT eingesetzt, die von italienischen, französischen und deutschen Firmen geliefert wird. In dem Projekt eines italienischen Unternehmens geht es um die Verfolgung des Aufenthaltsorts von Personen; weitere europäische Firmen lieferten dabei Software und Speichertechnik zu (Quelle: Businessweek, Spiegel, Heise).

8. November 2011: Zu einer Datenpanne ist es bei der Piratenfraktion im Berliner Abgeordnetenhaus gekommen. Bei einer E-Mail an Bewerber für Stellen der Fraktion waren die Adressen der Empfänger für alle sichtbar. Der Parlamentarische Geschäftsführer räumt den Fehler ein; die Adressen seien versehentlich im cc- anstatt im bcc-Feld des E-Mail-Clients eingetragen worden (Quelle: Heise).

9. November 2011: Der oberste Gerichtshof der USA beurteilt die Überwachung Verdächtiger mit GPS kritisch. Besonders kritisieren die Richter des Supreme Court, dass Autos ohne richterliche Anordnung monatelang mit einem Satellitenpeilsender verfolgt werden sollen. Ein Vertreter des Justizministeriums bezeichnete dies auf die kritische Nachfrage der Richter als verfassungsgemäß (Quelle: Heise).

10. November 2011: Die deutsche Verbraucherschutzministerin Ilse Aigner und EU-Justizkommissarin Viviane Reding fordern, dass Unternehmen, die in Europa Dienste anbieten, dem europäischen Datenschutzrecht unterliegen sollen. Die heutige Praxis, dass in der EU tätige US-Unternehmen nach dem Patriot Act dortigen Behörden auch Zugriff auf Daten von EU-Unternehmen und -Bürgern gewähren, solle beendet werden. Andernfalls sollten solche Unternehmen keine Geschäfte im europäischen Binnenmarkt machen dürfen (Quelle: europa.eu, Heise).

10. November 2011: Der Hamburgische Datenschutzbeauftragte Johannes Caspar hat rechtliche Schritte wegen der Gesichtserkennung bei Facebook angekündigt. Facebook unterhält eine Datenbank mit biometrischen Daten seiner Nutzer und führt beim Upload eine automatische Gesichtserkennung durch. Caspar sieht darin einen Verstoß gegen europäisches und deutsches Datenschutzrecht. Von jedem Nutzer müsse explizit die Genehmigung dazu eingeholt werden (Quelle: Hamburgischer Datenschutzbeauftragter, Heise).

10. November 2011: Beim Fluggastdatentransfer ist es offenbar zu einer Einigung zwischen den USA und der EU-Kommission gekommen. Innenkommissarin Cecilia Malmström erklärte, der Datenschutz für EU-Bürger sei dabei erheblich verbessert worden. Nach sechs Monaten sollen die gespeicherten Daten für Standardabfragen verschleiert werden; in Sonderfällen bleibt der Zugriff auf die vollständigen Daten aber erhalten. Die Speicherfrist solle von 15 Jahren auf 10 Jahre verkürzt werden. In der Folge gibt es an den geplanten Regelungen scharfe Kritik (Quelle: Frankfurter Allgemeine, Heise).

11. November 2011: Hacker haben sich Zugriff auf die Anwenderdatenbank der Spieleplattform *Steam* verschafft. Die Angreifer haben nach Angaben des Unternehmens Zugriff auf Namen, Hashes von Passwörtern, Kaufbestätigungen, Rechnungsadressen und verschlüsselte Kreditkarteninformationen gehabt. Für die Nutzung dieser Daten gebe es keine Beweise; die Ermittlungen dauerten aber noch an (Quelle: Heise).

11. November 2011: Der Kurznachrichtendienst Twitter muss nach einem Urteil des Bezirksgerichts Alexandria im Bundesstaat Virginia im Berufungsverfahren Daten von Wikileaks-Helfern – darunter die isländische Parlamentsabgeordnete Birgitta Jonsdottir – herausgeben. Durch das freiwillige Hinterlassen der IP-Adresse bei der Anmeldung hätten die Nutzer bereits ihr Einverständnis für die weitere Nutzung der Daten gegeben; dies schließe die Weitergabe an Strafverfolgungsbehörden ein. Die Electronic Frontier Foundation spricht von einem schwarzen Tag für die Bürgerrechte. „Mit dieser Entscheidung sagt das Gericht allen Nutzern von Online-Diensten mit Sitz in den USA, dass die US-Regierung einen geheimen Zugang zu ihren Daten hat“, erklärte Jonsdottir (Quelle: Electronic Frontier Foundation, Heise).

11. November 2011: Nach Angaben des Projekts *Citizen Lab* der Universität Toronto wird US-Technik sowohl in Syrien als auch in Burma zur Filterung des Internet eingesetzt. Das Unternehmen Blue Coat hat die Verwendung seiner Technik in Syrien bereits eingeräumt, aber bestritten, dass es selbst Geschäftsbeziehungen dorthin unterhalte (Quelle: Heise).

14. November 2011: Das Bundeskriminalamt (BKA) hat nach Angaben von Staatssekretär Ole Schröder die internationale Arbeitsgruppe für den Erfahrungsaustausch zu Staatstrojanern initiiert. Die heutige „Remote Forensic Software Group“ hieß zu Beginn „DigiTask User Group“. Das BKA hatte zuvor noch behauptet, keine Software der Firma DigiTask zu nutzen (Quelle: Heise).

15. November 2011: Für den Einsatz von Nacktscannern an Flughäfen hat die EU-Kommission einen Vorschlag für Regelungen vorgelegt. Unberechtigter Zugang müsse verhindert, Bilder dürften nicht gespeichert, kopiert, ausgedruckt oder empfangen werden können. Eine Kontrolle mit den Geräten müsse freiwillig sein (Quelle: europa.eu, Heise).

16. November 2011: Neonazis sollen nach der Vorstellung von Bundesinnenminister Hans-Peter Friedrich in einem zentralen Register erfasst werden. Es sollen „Daten über gewaltbereite Rechtsextremisten und politisch rechts motivierte Gewalttaten zusammengeführt werden", sagte er der Süddeutschen Zeitung. Bundesdatenschutzbeauftrager Peter Schaar warnte vor dem übereilten Aufbau neuer Strukturen bei den Sicherheitsbehörden (Quelle: Süddeutsche Zeitung, Heise).

16. November 2011: Gegen den bayerischen Innenminister Joachim Herrmann wird nicht wegen des Einsatzes des Bayerntrojaners ermittelt. Der Rechtanwalt Thomas Stadler hatte im Namen der Piratenpartei in Bayern gegen ihn und weitere Beteiligte Anzeige nach §§202a und 202c StGB – unbefugtes Ausspähen von Daten – erstattet. Begründet wurde die Ablehnung damit, dass ein gerichtlicher Beschluss nach §100a StPO vorgelegen habe, durch den der Trojanereinsatz gerechtfertigt gewesen sei (Quelle: internet-law.de, Heise).

16. November 2011: Gegen den Stop Online Piracy Act (SOPA) gibt es in den USA erheblichen Widerstand. Das Gesetz richtet sich aus Sicht seiner Befürworter gegen Urheberrechtsverletzungen; Gegner sprechen von einem Zensurgesetz. Provider und Netzbetreiber können danach angewiesen werden, den Zugang zu Web-Seiten zu sperren; die Seiten müssten aus den Indizes von Suchmaschinen entfernt werden. Zahlungen an die Betreiber sollen unterbunden werden. Den Anbietern würden damit erhebliche Pflichten zur Prüfung und zur Überwachung der Kunden auferlegt werden (Quelle: Heise).

16. November 2011: Die bayerische Justizministerin Beate Merk (CSU) und der Innenexperte der CDU/CSU-Bunestagsfraktion fordern die Einführung der Vorratsdatenspeicherung; diesmal wegen der Neonazis der *Zwickauer Zelle*. Mittäter und Hintermänner könnten nur mit Hilfe der Vorratsdatenspeicherung ermittelt werden, so Merk (Quelle: Heise).

21. November 2011: Bundesinnenminister Hans-Peter Friedrich fordert die Verlängerung der Speicherfristen von Daten über Verdächtige. Die bisherige Frist von fünf Jahre sei zu kurz; außerdem solle die Unterscheidung zwischen gewalttätigen und anderen Extremisten entfallen (Quelle: Spiegel, Heise).

23. November 2011: Laut der Antwort des Innenministers Ralf Jäger auf eine kleine Anfrage der Abgeordneten Anna Conrads wurden durch den Versand *stiller SMS* in Nordrhein-Westfalen 2010 „insgesamt 5.276 Mobilfunkanschlüsse überwacht. An 2.644 dieser Mobilfunkanschlüsse wurden auch Ortungsimpulse versandt. Je nach Ermittlungsziel und -verlauf können auf einen einzelnen überwachten Mobilfunkanschluss eines bis zu mehreren hundert dieser Ortungssignale versandt worden sein. Insgesamt wurden im Jahr 2010 in NRW 255.784 Ortungsimpulse versandt" (Quelle: netzpolitik.org).

24. November 2011: Es hat bisher sieben Fälle von verdeckten Zugriffen auf IT-Systeme (Online-Durchsuchung) durch das BKA gegeben, so das Bundesinnenministerium auf eine parlamentarische Anfrage der Fraktion Die Linke. Bisher wurde von weniger solchen Zugriffen ausgegangen. Durch die selbst entwickelte Software seien Kosten in Höhe von 682.581 Euro entstanden (Quelle: Heise).

24. November 2011: Der bayerische Datenschutzbeauftrage Thomas Petri hat angekündigt, alle 22 Trojanereinsätze in Bayern überprüfen zu wollen. Dabei soll der Quellcode aus datenschutzrechtlicher Sicht geprüft werden. Die Überprüfung erfolge auf Ersuchen des bayerischen Innenministers (Quelle: Bayerische Landtagsfraktion der Grünen, Heise).

25. November 2011: Der Bundesdatenschutzbeauftragte Peter Schaar wirft der Bundesregierung vor, wichtige Weichenstellungen beim Datenschutz im Internet zu versäumen. Durch Unternehmen werde eine Realität geschaffen, mit der sich der Gesetzgeber schwer tue; Selbstregulierung reiche nicht aus. Innen-Staatsekretärin Rogall-Grothe setzt dagegen auf Selbstverpflichtungen (Quelle: Heise).

25. November 2011: Der Bundesrat segnet die Änderung des Verfassungsschutzgesetzes ab. Mit der umstrittenen Änderung werden Kompetenzen aus dem Terrorismusbekämpfungsergänzungsgesetz fortgeschrieben und teilweise erweitert. Das betrifft Informationen, die die Geheimdienste bei Banken, Fluggesellschaften, Reisebüros, Postdienstleistern sowie den Anbietern von Telekommunikations- und Telediensten über Terrorverdächtige einholen können (Quelle: Heise).

26. November 2011: Bundesinnenminister Hans-Peter Friedrich will die Kompetenzen des Verfassungsschutzes ausweiten. Er will die Erweiterung von Speicherbefugnissen und die Verlängerung von Löschfristen durchsetzen. Die Zusammenarbeit mit dem Bundeskriminalamt soll durch ein gemeinsames Abwehrzentrum intensiviert und Datenbestände verknüpft werden. Die Überwachung von Nazi-Homepages soll erweitert werden (Quelle: tagesschau.de, Heise).

27. November 2011: Bundesinnenminister Hans-Peter Friedrich fordert die Einführung der Vorratsdatenspeicherung (Quelle: Welt am Sonntag, Heise).

29. November 2011: Eine Hackergruppe, die sich selbst *Teampoison* nennt, veröffentlicht die Zugangsdaten und E-Mail-Adressen von einigen hundert UN-Mitarbeitern. Viele der Adressen gehören Mitarbeitern des United Nations Development Program (UNDP). Die Passwörter waren offenbar nicht verschlüsselt; einige Accounts scheinbar überhaupt nicht durch ein Passwort gesichert. Später erklärt eine Sprecherin des UNDP, die Daten seien veraltet und nicht mehr gültig (Quelle: Heise).

30. November 2011: Der Innenausschuss hat mit den Stimmen der Koalition dem Gesetzentwurf zum Aufbau einer Visa-Warndatei zugestimmt. Sie soll Antragsteller und weitere Personen erfassen, die die Antragsteller auf ein Visum eingeladen haben, sofern sie als Einzelperson mehr als drei Einladungen pro Jahr aussprechen. Die Daten werden automatisch mit der Antiterror-Datei abgeglichen. Die Grünen und die Linke sprechen von einer überzogenen generellen Terrorverdächtigung und stimmten gegen den Entwurf (Quelle: Heise).

Dezember 2011

1. Dezember 2011: Offenbar werden Personen-Suchmaschinen (yasni.de, 123people.com) verstärkt von Behörden und Unter-

nehmen genutzt. Dies ergab eine Auswertung der nach IP-Adressen aufgeschlüsselten Zugriffe. Seit 2010 gebe es eine erhebliche Steigerung, so ein Sprecher von Yasni. Spitzenreiter seien die niedersächsischen Landebehörden (Quelle: Heise).

2. Dezember 2011: Der Deutsche Bundestag hat das „Zugangserschwerungs-Gesetz" zur Einrichtung von Websperren mit den Stimmen aller Fraktionen aufgehoben. Das Gesetz wurde von der damaligen Bundesfamilienministerin Ursula von der Leyen initiiert, war sofort heftig umstritten und führt zur bisher erfolgreichsten Internet-Petition mit ca. 134.000 Petenten. Obwohl beschlossen, kam es nie zur Anwendung; nach späteren Aussagen eines Regierungsmitglieds in Interviews spielten bei dem Gesetz auch Überlegungen zum Wahlkampf eine Rolle (Quelle: Deutscher Bundestag, Heise).

2. Dezember 2011: In einem Gutachten hat der schleswig-holsteinische Landtag den Standpunkt des Unabhängigen Landeszentrums für Datenschutz (ULD) zu Facebooks „Like"-Button kritisiert. Nach Ansicht des ULD verstößt der Button gegen Datenschutzbestimmungen. Dies ist unter Juristen umstritten; Frage ist dabei, ob dynamische IP-Adressen personenbezogene Daten sind und damit unter den Datenschutz fallen (Quelle: Schleswig-Holsteinischer Landtag, Heise).

4. Dezember 2011: Mangelndes Vertrauen in die Datensicherheit bei Cloud-Diensten verschlechtert die wirtschaftlichen Aussichten bei den Anbietern dieser Dienste, so Philip Verveer vom US-Außenministerium. Kristallisationspunkt für solche Bedenken ist der Patriot Act in den USA, der es Behörden erlaubt, auf Daten in Clouds zuzugreifen. Bereits zuvor hatten sich die deutsche Verbraucherschutzministerin Aigner und EU-Justizkommissarin Reding dafür ausgesprochen, alle in der EU tätigen Unternehmen unter europäisches Datenschutzrecht zu stellen (Quelle: Heise).

5. Dezember 2011: Der geplante Einsatz des Überwachungssystems INDECT bei der Europameisterschaft im Männerfußball 2012 wird von dem FDP-Europaabgeordneten Alexander Alvaro kritisiert. Das geplante Vorgehen widerspreche allen Datenschutzbestimmungen und sei in Deutschland eindeutig verfassungswidrig. Stephan Urbach von der Piratenpartei sprach im Zusammenhang mit INDECT von „Gedankenpolizei" (Quelle: Süddeutsche Zeitung, derwesten.de, Heise).

5. Dezember 2011: Trotz formeller Beanstandung durch den sächsischen Landesdatenschutzbeauftragten Andreas Schurig und trotz heftiger Kritik in der Öffentlichkeit hat das sächsische Landeskriminalamt die im Rahmen einer Anti-Nazi-Demonstration abgefragten Daten nicht reduziert. Dies hatte Schurig in seiner Untersuchung gefordert; er bezeichnete die flächendeckende Datenerfassung als unverhältnismäßig und rechtswidrig. Dennoch werden die Daten weiterhin genutzt und zusätzlich neue Daten erfasst (Quelle: Heise).

6. Dezember 2011: Bei ihrem Bundesparteitag in Berlin hat die SPD einen Antrag zur Vorratsdatenspeicherung beschlossen. Obwohl die Vorratsdatenspeicherung als gravierender Eingriff in die informationelle Selbstbestimmung bezeichnet wird, wird die Bundestagsfraktion in dem Beschluss aufgefordert, anhand festgelegter Eckpunkte einen Gesetzentwurf zu erarbeiten (Quelle: netzpolitik.org, Heise).

6. Dezember 2011: Die Piratenfraktion im Braunschweiger Rathaus wendet sich gegen die Überwachung der Internetnutzung durch die Stadtverwaltung. „Die Stadtverwaltung behält sich das Recht vor, die Internet-Nutzung Einzelner im Rathaus stichprobenartig zu überprüfen. Auch die Grünen haben das Thema nach einer entsprechenden Anfrage der Piraten im Rat nun für sich entdeckt. Man habe das ‚Kleingedruckte' zunächst wohl nicht richtig gelesen, gibt der stellvertretende Fraktionsvorsitzende Gerald Heere zu", so ein Bericht des NDR (Quelle: NDR, netzpolitik.org).

7. Dezember 2011: Durch einen Fehler bei Facebook war es zeitweise möglich, auf Privatbilder anderer Nutzer zuzugreifen. Auch Privatbilder von Facebook-Chef Mark Zuckerberg waren dadurch frei im Internet verfügbar (Quelle: netzpolitik.org, Heise).

7. Dezember 2011: Bei Facebook wird die zuvor angekündigte Timeline eingeführt, bei der alle Facebook bekannten Ereignisse des eigenen Lebens auf einem Zeitstrahl angeordnet sind. Dadurch entsteht ein Lebenstagebuch des Nutzers (Quelle: Heise).

8. Dezember 2011: Durch Löschung des Datenbank-Hauptschlüssels und Vernichtung der entsprechenden Chipkarten sind die erhobenen Daten des Elektronischen Entgeltnachweises (ELENA) nach Angaben des Bundesdatenschutzbeauftragten Peter Schaar nicht mehr zugänglich. Das unter anderem wegen Datenschutzbedenken heftig kritisierte Projekt war zuvor gestoppt worden. Laut Schaar ist dies der erste Schritt zur vollständigen Löschung der ca. 700.000.000 Datensätze (Quelle: Heise).

8. Dezember 2011: Die deutsche Bundesregierung sieht keinen Handlungsbedarf beim Export von Überwachungs-Software an diktatorische Regimes. Es werde derzeit nicht geprüft, inwiefern solche Produkte zur Unterdrückung genutzt werden, teilte das Bundeswirtschaftsministerium mit. Der netzpolitische Sprecher der Grünen im Bundestag, Konstantin von Notz, erklärte, es wäre „moralisch höchst verwerflich, wenn Unrechtsregime von Deutschland aus proaktiv mit solcher Überwachungssoftware versorgt würden" (Quelle: Heise).

8. Dezember 2011: Niederländischen Medien zufolge wurde der Webserver des niederländischen Zertifikatsherausgebers *Gemnet* kompromittiert. Dadurch habe sich der Hacker Zugang zur Datenbank verschafft. Laut dem Bericht sei die Datenbank nicht passwortgeschützt gewesen (Quelle: Heise).

9. Dezember 2011: Google+ führt die Funktion „Find my Face" zur automatischen Gesichtserkennung ein. Damit können Nutzer Kontakte im eigenen Fotoalbum leicher markieren können. Eine Erfassung biometrischer Daten erfolge nur mit Zustimmung der Nutzer; dies bewertete der hamburgische Datenschutzbeauftragte Johannes Caspar positiv. Bei Facebook hatte er das Fehlen der obligatorischen Zustimmung bei einer vergleichbaren Funktion kritisiert (Quelle: Heise).

9. Dezember 2011: Nach Plänen der Innenminister von Bund und Ländern soll ein Kompetenzzentrum zur Bekämpfung der Internet-Kriminalität eingerichtet werden. Dort solle u.a. eine Leistungsbeschreibung für eine Software zur Quellen-TKÜ erstellt werden (Quelle: Heise).

12. Dezember 2011: Der umstrittene frühere Bundesminister Karl-Theodor zu Guttenberg soll EU-Kommissarin Neelie Kroes bei der Umsetzung der neuen „No disconnect"-Strategie helfen und Netzaktivisten unterstützen. Sie schätze zu Guttenberg vor allem für seine internationale Weitsicht und seine Erfahrung in auswärtigen Angelegenheiten. Zu Guttenberg gehörte während seiner Amts zu den entschiedenen Befürwortern von Netzsperren, die vor allem seine Frau zum Schutz vor Kindesmissbrauch propagierte (Quelle: netzpolitik.org, Heise).

12. Dezember 2011: Bei einem Angriff auf das Immobilienportal Immobilienscout24 haben sich Angreifer Zugang zu Namen, Kontaktdaten und internen Registrierungsnummern von Anbietern verschafft. Es soll sich dabei aber um Daten handeln, die ohnehin in den Exposés der Web-Seite veröffentlicht sind (Quelle: Heise).

13. Dezember 2011: Laut einer Antwort des Bundesinnenministeriums an den Bundestagsabgeordneten Andrej Hunko (Die Linke) verschickten Zollkriminalamt und weitere Fahndungsämter der Grenzkontrolleure, das Bundeskriminalamt (BKA) und das Bundesamt für Verfassungsschutz 2010 insgesamt 440.783 sogenannte *stille SMS* zur Ortung von Mobiltelefonen (Quelle: Heise).

14. Dezember 2011: Das EU-Parlament hat mit knapper Mehrheit eine Resolution von Sozialdemokraten, Liberalen und Grünen zur europäischen Antiterror-Politik der vergangenen zehn Jahre angenommen. Die EU-Kommission wird darin aufgefordert, alle seit dem 11. September 2001 beschlossenen Maßnahmen zu überprüfen. Die einzelnen Instrumente sollen auf Effektivität, Kosten, Grundrechtseingriffe und ihre demokratische Kontrolle hin untersucht werden (Quelle: Heise).

15. Dezember 2011: Bradley Manning, der mutmaßliche Informant von Wikileaks steht vor einem US-amerikanischen Militärgericht; ihm droht lebenslange Haft. Bei einer Anhörung soll geklärt werden, ob es tatsächlich zum Prozess gegen Manning kommt. Manning selbst gibt sich kaum Mühe, seine Taten zu verbergen. „Wenn Du freien Zugang zu Geheimdokumenten hast, und du unglaubliche, schreckliche Dinge siehst … Dinge, die an die Öffentlichkeit gehören … was würdest du tun?" wird er zitiert (Quelle: Heise).

16. Dezember 2011: Das umstrittene *Anti-Counterfeiting Trade Agreement (ACTA)* wird durch die Landwirtschaftsminister in Brüssel im Agrar- und Fischereirat abgenickt. Für die Bundesregierung nahm Ministerin Ilse Aigner (CSU) an dem Treffen teil. Die vor allem von führenden Industriestaaten weitgehend hinter verschlossenen Türen ausgehandelte Vereinbarung gilt als nicht-legislative Maßnahme, sodass sie bei einer beliebigen Sitzung des Ministergremiums abgesegnet werden konnte (Quelle: Heise).

20. Dezember 2011: Die *Artikel 29*-Gruppe der europäischen Datenschutzbeauftragten formuliert in einem Schreiben an das IATA-Verbindungsbüro in Brüssel Bedenken gegen das Projekt „Checkpoint of the Future" zur Fluggastkontrolle an Flughäfen. Sie fordert weitere Aufklärung über die Funktionsweise der geplanten Hightech-Kontrollpunkte an Flughäfen sowie die rechtliche Basis für die damit verbundene Datenverarbeitung. Passagiere sollen mit ihrem Handgepäck beim Durchgang durch die Sicherheitsschleusen von Sensoren und Scannern durchleuchtet werden. Das Vorhaben dürfte sich stark auf die Privatsphäre der Passagiere auswirken, so die Datenschützer. Das System setze auf biometrische Identifizierung, Verhaltensanalyse, Zufall und ein Vorzugsprogramm für *bekannte Reisende* (Quelle: ec.europa.eu, Heise).

26. Dezember 2011: Die *Go Daddy Group*, eigenen Angaben zufolge der größte Domain-Registrar weltweit, will das umstrittene Anti-Piraterie-Abkommen *SOPA (Stop Online Piracy Act)* in den USA entgegen vorherigen Absichten nicht mehr unterstützen. Die derzeitige Ausgestaltung des Gesetzes sei unzureichend; die Go Daddy Group werde ihre SOPA-Unterstützung deshalb zurückziehen, erklärte CEO Warren Adelman in einer Stellungnahme. Auch weitere bisherige Befürworter von SOPA ziehen sich angesichts der heftigen öffentlichen Kritik zurück (Quelle: Heise).

29. Dezember 2011: Die Polizei prüft einer Umfrage von dpa zufolge bundesweit, beim sozialen Netzwerk Facebook aktiv zu werden. Vorreiter ist seit März die Polizei Hannover, die jetzt erstmals in einem Mordfall über die Internet-Plattform nach dem Täter sucht (Quelle: Deutsche Presse-Agentur, Heise).

Januar 2012

1. Januar 2012: Der bayerische Ministerpräsident Horst Seehofer fordert Bundesjustizminsterin Sabine Leutheusser-Schnarrenberger auf, die Vorratsdatenspeicherung umzusetzen (Quelle: Heise).

1. Januar 2012: Die Hackergruppe *Anonymous* veröffentlicht nach ihrem Angriff auf das Sicherheitsberatungsunternehmen *Stratfor* dessen Kundendaten. Es handelt sich dabei um ca. 75.000 Datensätze mit Adressen, Kreditkartennummern und Passwörtern sowie weitere 860.000 Benutzernemn und E-Mail-Adressen. Hintergrund der Attacke ist offenbar der Prozess gegen Bradley Manning, dem mutmaßlichen Wikileaks-Informanten (Quelle: Heise).

3. Januar 2012: Die neue, konservative, spanische Regierung will das umstrittene *Sinde*-Gesetz umsetzen, das Web-Sperren gegen illegale Downloads vorsieht. Der Gesetzentwurf sieht vor, in einem zweistufigen Verfahren über die Blockade von Angeboten mit Copyright-Verstößen zu entscheiden. Das Gesetz orientiert sich an Plänen, die bereits die sozialistische Vorgängerregierung gefasst hatte (Quelle: Heise).

3. Januar 2012: In Weißrussland soll die Internetnutzung stärker reglementiert werden. Ein neues Gesetz sieht Strafen vor, wenn Seiten für E-Mails oder Finanztransaktionen verwendet werden, die nicht in Weißrussland registriert sind. Unternehmen müssen ihre Server ins Inland verlegen und registrieren lassen; ausländische Dienste dürfen für den Vertrieb nicht mehr genutzt werden. Zur Kontrolle müssen Verbindungsdaten aufgezeichnet und illegales Nutzungsverhalten unverzüglich durch den Anschlussinhaber angezeigt werden (Quelle: Heise).

4. Januar 2012: Unbekannte haben nach Medienberichten Namen, Adressen und Kreditkarteninformationen von rund 14.000 Israelis veröffentlicht (Quelle: Heise).

4. Januar 2012: Der Europäische Rat hat einen ersten Entwurf für eine Richtlinie zur Regelung einer neuen europäischen Ermittlungsanordnung fertig gestellt. Das Abhören von Telefonaten und E-Mails in Echtzeit sowie der Zugriff auf Verbindungs- und Standortdaten in anderen Mitgliedsstaaten soll dadurch erleichtert werden. Damit könnten Maßnahmen zur Telekommunikationsüberwachung bald grenzüberschreitend erfolgen (Quelle: Statewatch, Heise).

5. Januar 2012: Aus Sicht der EU-Kommission fehlt es in Sachen Vorratsdatenpeicherung an Unterstützung durch die Mitgliedsstaaten. Nur 11 von 27 EU-Ländern hätten Daten geliefert, die einen Nutzen der umstrittenen Maßnahme für die öffentliche Sicherheit und die Strafverfolgung nahelegten. Dadurch sei in der Öffentlichkeit die Wahrnehmung entstanden, dass die Vorratsdatenspeicherung wenig bringe (Quelle: quintessenz, Heise).

5. Januar 2012: Das Verfassungsgericht der Tschechischen Republik spricht erneut ein Urteil gegen die Vorratsdatenspeicherung. Das erneute Urteil wendet sich gegen die zu allgemeinen, nicht verhältnismäßigen Regelungen zur Übermittlung und Verwendung der Daten. Bereits im März letzten Jahres hat das oberste Gericht das dortige Umsetzungs-Gesetz der EU-Richtlinie annulliert und damit die Verpflichtung der Provider zur sechsmonatigen Speicherung der Daten aufgehoben (Quelle: netzpolitik.org).

7. Januar 2012: Die schwedische Filesharing-Bewegung „Kirche der Kopimisten" hat die Anerkennung als Religion erreicht. Damit ist Schweden das erste Land, dass Kopimismus als Religionsgemeinschaft einstuft. Zentraler Glaube der Kopimisten ist, dass sich der Wert von Informationen durch das Kopieren vervielfältigt. Die Religion wird durch „Kopyacts" zum Kopieren und Remixen von Informationen ausgeübt (Quelle: Heise).

10. Januar 2012: Nach Ansicht von Verfassungsrichter Johannes Masing sind mit der geplanten Neuregelung des Datenschutzes auf EU-Ebene nationale Grundrechte nicht mehr anwendbar. Damit müsse das Bundesverfassungsgericht seine Kontrollfunktion in wesentlichen Bereichen aufgeben, in denen es „weit über die Grenzen hinaus als vorbildlich geltende freiheitliche Strukturen geschaffen hat" (Quelle: Süddeutsche Zeitung, netzpolitik.org, Heise).

11. Januar 2012: Der FoeBuD führt eine Aktion zum Datenschutz-Risiko durch Funketiketten in Kleidungsstücken in der Bielefelder Innenstadt durch. Vor dem Gerry-Weber-Damenmodehaus demonstrierten die Aktivisten ahnungslosen Kundinnen, dass man ihre frisch erstandene Garderobe – und damit auch die Trägerin – unbemerkt aus mehreren Metern Entfernung identifizieren kann (Quelle: netzpolitik.org, Heise).

13. Januar 2012: Rund 29.000 Österreicher haben auf der Website des Parlaments für die Initiative gegen die Einführung der Vorratsdatenpeicherung unterschrieben. Dies setzt eine neue Höchstmarke bei den seit Oktober 2011 möglichen Online-Initiativen (Quelle: Heise).

16. Januar 2012: Bei einem Hackereinbruch in ein Tochterunternehmen von Amazon haben sich nach Angaben des Unternehmens die Angreifer Zugriff auf die persönlichen Daten der rund 24 Millionen registrierten US-Kunden verschafft. Betroffen sind Namen, Mailadressen, Rechnungs- und Lieferadressen, Telefonnummern sowie die letzten vier Ziffern der Kreditkartennummern. Außerdem hatten die Täter offenbar Zugriff auf die Passwort-Hashes (Quelle: Heise).

16. Januar 2012: Nach einer Antwort der Bundesregierung auf die Anfrage des Abgeordneten Herbert Behrens von der Linken sollen beim Bundeskriminalamt (BKA) 30 Planstellen für ein „Kompetenzzentrum Informationstechnische Überwachung" (CC ITÜ) geschaffen werden. Dort soll ein eigenes Trojanerprogramm zur sogenannten „Quellen-Telekommunikationsüberwachung" entwickelt werden. Zusätzlich werden Sachmittel in Höhe von 2,2 Millionen Euro bereitgestellt (Quelle: Heise).

16. Januar 2012: Nach Medienberichten wird der umstrittene Gesetzesvorschlag für den Stop Online Piracy Act (SOPA) im US-Repräsentantenhaus auf Eis gelegt. Laut Mehrheitsführer Eric Cantor werde das Gesetz vorerst nicht zur Abstimmung vorgelegt. Erst solle eine Einigung in den strittigen Fragen gefunden werden (Quelle: Heise).

18. Januar 2012: Die englischsprachige Version von Wikipedia präsentiert für einen Tag eine schwarze Protestseite. Damit soll gegen das geplantes US-Gesetz Stop Online Piracy Act (SOPA) protestiert werden, das zum Schutz der Urheberrechte auch Netzsperren vorsieht. Durch das Gesetz würde eine Zensur-Infrastruktur geschaffen, die auch für andere Zwecke einsetzbar wäre. Google platzierte unter seinem Suchfenster den Link zu einer Online-Petition gegen das Gesetz (Quelle: netzpolitik.org, Heise).

18. Januar 2012: Der vom Bundesinnenministerium (BMI) vorgelegte Gesetzentwurf zur Verbesserung der Bekämpfung des Rechtsextremismus wird vom Bundeskabinett verabschiedet. Dadurch wird die rechtliche Grundlage zum Aufbau einer „Verbunddatei Rechtsextremismus" geschaffen. Die Polizeigewerkschaften kritisieren die Maßnahme als ungenügend (Quelle: Heise).

19. Januar 2012: Die von den Netzbetreibern routinemäßig erfassten Verkehrsdaten von Mobiltelefonen werden offenbar immer öfter abgefragt und ausgewertet. Wegen der versuchten Brandstiftung an einem Fahrzeug erfassten Ende 2009 Polizei und Staatsanwaltschaft in Berlin sämtliche Verkehrs- und Verbindungsdaten in einem mehrere Quadratkilometer großen Gebiet (Quelle: netzpolitik.org, Heise).

Stefan Hügel

Stefan Hügel ist Vorsitzender des FIfF, arbeitet als IT-Berater und lebt in Frankfurt am Main

23. Januar 2012: Nach Aussagen der Vizepräsidentin der Berliner Polizei Margarete Koppers im Innenausschuss des Abgeordnetenhauses, sind bei der Funkzellenabfrage zu Fahndungszwecken in 357 Fällen rund 4,2 Millionen Verbindungsdaten ausgewertet worden. Rund 1,7 Millionen Datensätze würden noch aufbewahrt. Die Betroffenen seien nicht informiert worden. Damit gehen die Maßnahmen weit über die flächendeckende Erfassung von Mobilfunkdaten anlässlich einer Anti-Nazi-Demonstration in Dresden im Februar 2011 hinaus. Ermittlungserfolge ergaben sich aus der Abfrage offenbar nicht (Quelle: netzpolitik.org, Heise).

25. Januar 2012: Google hat angekündigt, ab dem 1. März 2012 eine geänderte Datenschutzrichtlinie und AGB zu verwenden. Im Kern besagen die neuen Richtlinien, dass Nutzerdaten der verschiedenen Google-Dienste verknüpft und aufgezeichnet werden (Quelle: netzpolitik.org).

26. Januar 2012: In einer Stellungnahme, die durch den stellvertretenden Vorsitzenden der Bundestagsfraktion, Dr. Günter Krings, und den Berichterstatter für das Urheberrecht im Rechtsausschuss und im Ausschuss für Kultur und Medien, Ansgar Heveling, verfasst wurde, begrüßt die Bundestagsfraktion der CDU/CSU die Gesetzesvorschläge *Stop Online Piracy Act (SOPA)* und *Protect IP Act (PIPA)* gegen Urheberrechtsverstöße. Gleichzeitig wird die Verschiebung der Abstimmung im US-Senat aufgrund von Protesten bedauert. Der Fall *Megaupload* zeige, dass man im Internet einen „klaren Rechtsrahmen" benötige (Quelle: netzpolitik.org, Heise).

26. Januar 2012: Das umstrittene Anti-Counterfeiting Trade Agreement (ACTA) wird durch die Europäische Union unterzeichnet. Das Abkommen sieht unter anderem vor, dass Internet-Anbieter für Urheberrechtsverletzungen von Kunden haftbar gemacht werden können. ACTA zielt in gleiche Richtung wie die US-Gesetzesinitiativen SOPA und PIPA, deren Abstimmungen nach Protesten gerade auf unbestimmte Zeit verschoben wurden. Der Vertrag wurde durch 22 EU-Mitgliedsstaaten und die Europäische Union in Japan unterzeichnet, wo die Dokumente von ACTA aufbewahrt werden. Die Ratifizierung des Vertrags steht noch aus (Quelle: netzpolitik.org, Heise).

26. Januar 2012: Nach Erkenntnissen des Grünen-Politikers Malte Spitz wird nach dem Urteil des Bundesverfassungsgerichts gegen die Vorratsdatenspeicherung von einzelnen Mobilfunkanbietern der gleiche Datenumfang gespeichert, wie zuvor. Lediglich die Speicherdauer sei zurückgegangen. Im untersuchten Fall T-Mobile werden offenbar 29 Einzelinformationen gespeichert (Quelle: netzpolitik.org).

27. Januar 2012: Nach einer vom Bundesjustizministerium beim Freiburger Max-Planck-Institut für Strafrecht in Auftrag gegebene Untersuchung gibt es keine Beweise für die essenzielle Bedeutung der verdachtsunabhängigen Protokollierung von Nutzerspuren für die Strafverfolgung. Basis der Untersuchung sind Übersichten über die Erhebung der Verkehrsdaten für die Jahre 2008 und 2009, Angaben der Bundesregierung sowie Interviews mit überwiegend polizeilichen Ermittlern. Sie untersuchten zudem die Aufklärungsquoten für den Zeitraum 1987 bis 2010. Demnach war die Aufhebung der Bestimmungen zur Vorratsdatenspeicherung durch das Bundesverfassungsgericht im März 2010 nicht Ursache für statistische Veränderungen der Aufklärungsquote (Quelle: netzpolitik.org, Heise).

27. Januar 2012: Der Präsident des Bundeskriminalamts (BKA), Jörg Ziercke, kritisiert in Berlin die Ergebnisse der Studie des Max-Planck-Instituts zur Vorratsdatenspeicherung. „Aufklärungsquoten als Maßstab herzunehmen, ist der gröbste Hobel, den man ansetzen kann", so Ziercke. Die Polizei nutze auf Vorrat gespeicherte Daten, um Ermittlungen zu beginnen, eine Aufklärungsquote stehe erst ganz am Ende (Quelle: Heise).

27. Januar 2012: Das Land Berlin hat bei der Software-Firma *Syborg* eine Überwachungssoftware in Auftrag gegeben, die zur Überwachung des Rechners eines Verdächtigen dort ohne dessen Wissen installiert wird und prinzipiell alle Aktivitäten aufzeichnen kann. Bei der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) können Ermittler auch verschlüsselte Kommunikationsdienste wie Skype kontrollieren. Aus Sicht von Mitgliedern der Piratenpartei und Der Linken überschreitet die Software die Grenzen, die das Bundesverfassungsgericht für Quellen-TKÜ und Online-Durchsuchung gesetzt hat (Quelle: Spiegel, Heise).

28. Januar 2012: Der Bundestag beschließt einen Entwurf zur Änderung des Luftverkehrsgesetzes, mit dem erstmals „unbemannte Luftfahrtsysteme" als neue Kategorie aufgenommen werden. Solche Drohnen mit einem Startgewicht bis zu 150 Kilo sollen neben bemannten Flugzeugen „gleichberechtigt am Luftverkehr teilnehmen" können. Für das Vorhaben votierte neben den Regierungsfraktionen von CDU/CSU und FDP die SPD. Die Grünen enthielten sich, die Linke stimmte dagegen (Quelle: Heise).

28. Januar 2012: Der irische High Court ruft den Europäischen Gerichtshof (EuGH) wegen der Brüsseler Vorgaben zur Vorratsdatenspeicherung an. Laut irischen Medienberichten sollen die Richter prüfen, ob die EU-Richtlinie Grundrechte der Nutzer respektiert, wie sie in der europäischen Grundrechtecharta verbrieft sind. Außerdem soll geprüft werden, ob eine nationale Umsetzung der Bestimmungen auch die Datenschutzartikel der Europäischen Menschenrechtskonvention beachten muss (Quelle: Heise).

29. Januar 2012: In über 80 polnischen Städten sind ACTA-Gegner auf die Straße gegangen, um gegen das umstrittene Anti-Counterfeiting Trade Agreement zu demonstrieren. Zuvor hatte Polen zusammen mit 21 weiteren EU-Mitgliedstaaten und der Europäische Union das Abkommen unterzeichnet (Quelle: Telepolis, Heise).

30. Januar 2012: In einem Gastkommentar im Handelsblatt veröffentlicht CDU-Politiker und Mitglied der Enquête-Kommission *Internet und digitale Gesellschaft*, Ansgar Heveling, eine Kampfansage an die „liebe Netzgemeinde". „Ihr werdet den Kampf verlieren," scheibt er, und bezeichnet die Protagonisten eines freien Netzes als „digitale Maoisten". Heveling befürwortet die US-Gesetzesinitiativen SOPA und PIPA, die eine weitgehende Überwachung des Netzes vorsehen, um Immaterialgüterrechte durchzusetzen. Auffällig bei Hevelings Einlassungen ist die militaristische Sprache mit Begriffen wie „Kampf" und „digitalem Blut". Der Kommentar wird im Netz kritisch aufge-

nommen, eine Reihe von Twitterern machen sich über Heveling lustig und verspotten seine Ansichten als veraltet (Quelle: Handelsblatt).

Februar 2012

3. Februar 2012: In Mecklenburg-Vorpommern wird die Einrichtung einer Zentralstelle zur Bekämpfung der Internetkriminalität geprüft. „In Kombination mit der Einrichtung einer Schwerpunkt-Staatsanwaltschaft wäre dies eine in Deutschland einmalige organisatorische Maßnahme zur Bündelung der Kapazitäten auf diesem Gebiet", sagte Justizministerin Uta-Maria Kuder (Quelle: Heise).

3. Februar 2012: Die polnische Regierung hat die Ratifizierung des Vertragswerks ACTA ausgesetzt. „Ich teile die Ansicht derjenigen, die von unvollständigen Beratungen sprechen", so Ministerpräsident Donald Tusk. Die Argumente der Netzgemeinde seien berechtigt. Auch in Tschechien und Lettland wird die Ratifizierung von ACTA ausgesetzt (Quelle: Heise).

6. Februar 2012: Rund zwei Wochen, nachdem die Polizeidirektion Hannover ihre Facebook-Fahndungen aufgrund von Datenschutzbedenken gestoppt hatte, hat das Innenministerium offenbar einen Weg gefunden, US-amerikanische Server zu umgehen und trotzdem Fahndungsaufrufe bei Facebook einzustellen. Die Fahndung per Facebook ist umstritten, da personenbezogene Daten außerhalb der Kontrolle deutscher Behörden auf Servern in den USA gespeichert werden (Quelle: Hannoversche Allgemeine Zeitung, Heise).

7. Februar 2012: Von Juli an sollen sämtliche internationalen Flugplätze in Australien mit Nacktscannern ausgerüstet werden. Laut dem Vorhaben sollen Reisende auf Anweisung durch die Scanner gehen müssen. Ausnahmen gibt es nur für Passagiere mit ernsthaften Gesundheitsbeschwerden (Quelle: Herald Sun, Heise).

10. Februar 2012: Auch Deutschland wird das internationale Urheberrechtsabkommen ACTA vorerst nicht unterzeichnen. Das Auswärtige Amt habe die bereits erteilte Weisung zur Signierung des umstrittenen Vertragswerks wieder zurückgezogen (Quelle: Deutsche Presse-Agentur, Heise).

11. Februar 2012: In rund 60 deutschen Städten finden Proteste gegen das Anti-Counterfeiting Trade Agreement (ACTA) statt. Veranstaltungen, zu denen u.a. der Chaos Computer Club und die Piratenpartei eingeladen hat, gibt es z. B. in Berlin, Frankfurt, Hamburg, Köln, München oder Stuttgart (Quelle: Heise).

Kai Nothdurft

Hinter feindlichen Linien

der 28. Chaos Communication Congress (28C3) vom 27. bis 30. Dezember 2011 in Berlin

Dieses Jahr fand das Jahrestreffen des Chaos Computer Club unter dem Motto „Behind Enemy Lines" statt.

The congress – sold out!

Der Congress war wie schon in den letzten Jahren mit 4.500 Teilnehmern an der Belastungsgrenze des Berliner Congress Centers (bcc) am Alexanderplatz. Seit Jahren sucht der Club vergeblich einen alternativen geeigneten Veranstaltungsort.

Maximal zwei Dauerkarten konnte man an drei angekündigten November-Terminen im Vorverkauf ausschließlich über das Online Presale System erwerben. Das erste Kontingent mit der Hälfte der 4.500 Karten war innerhalb von fünf Minuten ausverkauft. Die anderen beiden Kontingente gingen ähnlich schnell weg. Einige wenige Tagestickets konnte man noch vor Ort erstehen. Ehemalige Vortragende konnten sich über ein Golden Token ein Ticket reservieren. Ohne Ticket kamen nur noch geladene Gäste, Vortragende und ausgewählte Pressevertreter in das bcc.

Tickets für FIfF-Standbetreuung

Die Limitierung der Eintrittskarten ist auch für das FIfF eine Herausforderung, denn wir waren dieses Jahr wieder mit einem Infostand vor Ort. Doch selbst die Engagierten, die den Stand betreuen, bekommen keine extra Tickets. Wir wollen für nächstes Jahr eine Aktion starten, bei der FIfF-Mitglieder, die hinfahren, das zweite Ticket für die Standbetreuung reservieren können. So können wir die raren Tickets Menschen anbieten, die mithelfen, den Stand zu betreuen.

Der FIfF-Stand war wieder günstig zwischen dem AK Vorrat und dem FoeBuD platziert und etwa die Hälfte der Zeit besetzt. Neben den Verkaufserlösen und Spenden sammelten wir auch Spenden für Zwiebelfreunde e.V. – *Friends of the Onion*[1], die

den Aufbau und Betrieb des TOR-Anonymisierungsnetzwerks fördern und die nicht mit einem eigenen Stand vor Ort waren.

Die englische Version unseres aktuellen FIfF-Flyers[2] war gerade noch rechtzeitig fertig geworden. Das internationale Publikum nahm ihn gut an. Wir wollen die internationale Vernetzung des FIfF mit Partnerinitiativen und Organisationen weiter ausbauen. Die 28C3 Veranstaltung bietet viele Möglichkeiten, persönliche Kontakte zu knüpfen und zu pflegen.

Seit zwei Jahren steht den Teilnehmern neben Internet und LAN auch ein vor Ort selbst betriebenes Mobilfunk-Netz zur Verfügung, das sogar Roaming ins öffentliche Telefonnetz erlaubt.

Das Programm

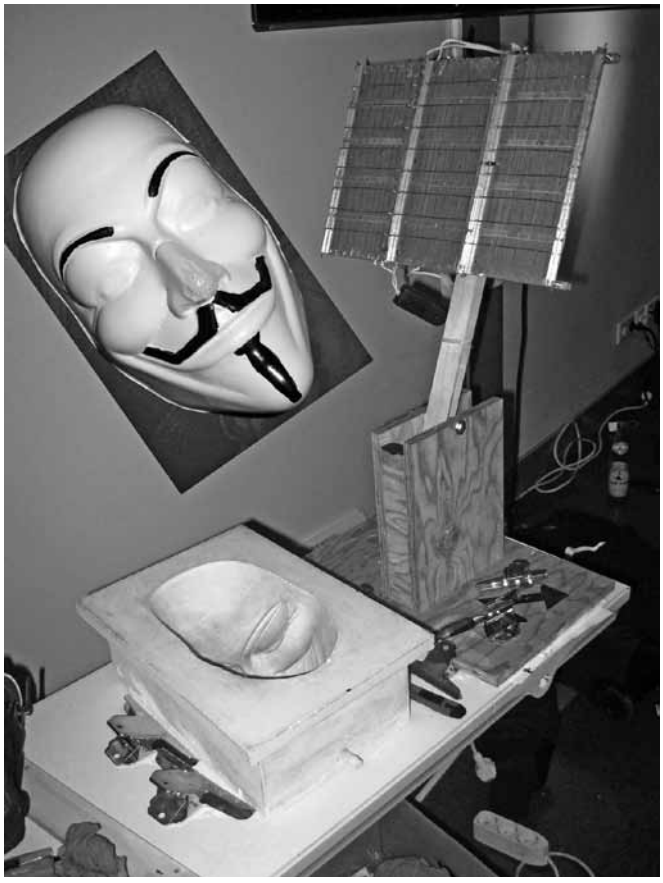
Wir waren aber hauptsächlich wegen des Programms[3] zum Congress gefahren und diesbezüglich wurde wieder einiges geboten. Die Vorträge[4] fanden, wie schon in den letzten Jahren, in drei randvollen Sälen parallel statt und wurden live ins lokale Congress-LAN, WLAN und ins Internet gestreamt. Auf den Fluren konnten diejenigen, die keinen Platz mehr fanden, noch auf Flatscreens zuschauen. Zusätzlich war Audio-Übertragung via DECT verfügbar.

Neben zahlreichen Hacker-Vorträgen zu Sicherheitslücken gab es auch wieder zahlreiche Vorträge zu gesellschaftspolitischen Themen mit Bezug zur Informationstechnik.

Anne Roth beschrieb in ihrem Vortrag *Sachsen dreht frei – On- und Offline-Überwachung: Weil sie es können*[5] wie Menschen, die sich gegen Rechtsradikale engagieren, von den sächsischen Sicherheitsorganen drangsaliert werden. Dabei war die Funkzellenauswertung im Zusammenhang mit der Demonstration gegen den Neonaziaufmarsch in Dresden im Februar 2011 nur ein bekannterer Fall von vielen. Anne Roth zeichnete ein Bild, wonach die Einschüchterung von politisch gegen Rechtsradikale Aktiven im „Frei"Staat Sachsen systematisch erfolgt.

Im Vortrag *Der Staatstrojaner. Vom braunen Briefumschlag bis zur Publikation*[6] feierte der CCC seine publicityträchtige Analyse der staatlichen Schnüffelsoftware. Constanze Kurz, Frank Rieger, Ulf Buermeyer und der Forensiker *0zapfths* erläuterten ausführlich, wie der Club die Trojaner erhalten und untersucht hat. Für den Abtransport der vom Trojaner gesammelten Informationen wurde in verschiedenen Versionen des Trojaners immer wieder der gleiche Schlüssel verwendet. Süffisant schilderten sie auch ihre vergebliche Suche nach einem zweiten Kryptoschlüssel, weil sie gar nicht nicht glauben konnten, dass die Software beim Nachladen keine Authentisierung erforderte und damit überhaupt nicht gegen Manipulationen beim Nachladen von Code geschützt war.

Karsten Nohl und Luca Meletta beschrieben in ihrem Talk *Defending mobile phones*[7] ein konkretes Szenario, wie bereits länger bekannte Schwächen in der Verschlüsselung des Mobilfunkprotokolls GSM für betrügerische Abbuchung von kostenpflichtigen Dienstleistungen ausgenutzt werden könnten. Schwerpunkt des Vortrags waren aber Vorschläge zur Absicherung oder Risikoreduzierung. Mit einem Crowdsourcing-Projekt



Kreativität auf dem 28C3:
Anlage zum Eigenbau von Guy Fawkes Masken

bieten sie eine Möglichkeit an, zu testen, welche Maßnahmen von einem Provider, bei dem man mit einem speziell dafür konfigurierten Handy eingebucht ist, aktuell implementiert sind.[8] Diese Informationen sollen so gesammelt und direkt auf einer Webseite publiziert werden. Dies dient dazu, Druck auf die Anbieter auszuüben, die auch kurzfristig möglichen Verbesserungen einzuführen.

Roger Dingledine und Jacob Appelbaum, zwei Hauptentwickler des Anonymisierungsdienstes TOR, hielten den Vortrag *How governments have tried to block Tor*[9]. Dingeldine leitet das TOR-Projekt, Appelbaum ist ein bekannter Hacker, Menschenrechtler und Netzaktivist. Im Rahmen des *US Patriot Act* wurde Twitter gezwungen, Informationen zu Appelbaums *Followern* herauszugeben, weil er Wikileaks öffentlich unterstützt hatte.

Die beiden schilderten engagiert und lebhaft, wie staatliche Behörden unter anderem in China, Syrien und dem Iran immer wieder versuchen, und es zeitweise leider auch schaffen, den Zugang ihrer Bürger zum TOR-Netzwerk zu blockieren. Es hat in den letzten Jahren ein regelrechtes Wettrüsten zwischen staatlichen Zensurbehörden und dem TOR-Projekt stattgefunden. Zuerst sperrten einige Staaten öffentlich bekannte Torserver. Dingeldine rief bereits auf dem 26C3 die Benutzer-Community dazu auf, möglichst viele dezentrale TOR-Installationen als Bridges zum TOR-Netzwerk zur Verfügung zu stellen und so ein indirektes Erreichen der bekannten Torserver zu ermöglichen.[10]

Überwachungs- und Analyse-Tools wie *Deep-Packet-Inspection-Systeme* können aber inzwischen TOR-Netzwerkverkehr erken-

nen und damit an wichtigen Internetknoten, etwa bei staatlichen Providern, blocken. Das TOR-Projekt hat reagiert und arbeitet daran, die SSL-verschlüsselten TOR-Verbindungen immer mehr wie normale Firefox-Apache-SSL-Verbindungen aussehen zu lassen, um diese Filterung zu erschweren.

In einem flammenden Appell forderten Dingledine und Appelbaum die Zuhörer auf, politisch gegen die Verbreitung von Überwachungs- und Filtertechnologien vorzugehen und insbesondere deren Export in repressive Staaten zu erschweren. Auch ein Boykott des Kaufs wurde ins Spiel gebracht. Leider gibt es noch keine alternativen Produkte von Unternehmen, die sich *politically correct* verhalten. Die beiden Vortragenden wurden mit *Standing Ovations* vom Publikum bedacht.

Eric Filiol und Seun Omosowon versuchten in ihrem Vortrag *Taking control over the Tor network*[11] nachzuweisen, dass es möglich sei, TOR-Benutzer gezielt auf von einem Angreifer kontrollierte Server zu leiten. Dies wurde in einer Testumgebung durch Kompromittierung von schlecht gepatchten Torservern in Kombination mit Denial-of-Service-Attacken auf weitere Server simuliert. Die beiden im Auditorium anwesenden TOR-Key-Developer Appelbaum und Dingledine kritisierten, dass die genannten Schwächen grundsätzlich bekannt seien und dass das Testszenario nur bedingt auf die Realität übertragbar sei, der Vortrag also keine substantiell neuen Erkenntnisse lieferte. Im Anschluss diskutierten die vier aber noch mindestens 30 Minuten direkt vor unserem FIfF-Stand weiter und unterhielten sich konstruktiver über grundsätzliche Möglichkeiten, die skizzierten Risiken zu begrenzen.

Der Sprachwissenschaftler Martin Haase (*maha*) sezierte in seinem Vortrag *Die Koalition setzt sich aber aktiv und ernsthaft dafür ein – sprachlicher Nebel in der Politik*[12] einmal mehr den entlarvenden Sprachgebrauch von Spitzenpolitikern.

Ein Highlight jedes Kongresses ist der *Fnord-Jahresrückblick* von „Fefe" Felix von Leitner und Frank Rieger, dieses Jahr mit dem Untertitel *von Atomendlager bis Zensus*. Darin werden Meldungen mit versteckten Botschaften auf sehr erheiternde Weise präsentiert, welche durch das Lesen zwischen den Zeilen oder ihre Zweideutigkeit bei genauem Hinsehen oder Nachdenken auflachen oder aufhorchen lassen.

Den Abschluss bildeten schon zum 15. Mal die *Security Nightmares*[14] von Frank Rieger und Ron, in denen sowohl ein Rückblick als auch ein Ausblick auf kommende Sicherheitsrisiken, Schwachstellen und deren Ausnutzung gegeben wurde.

Wir haben vor, auch dieses Jahr wieder mit einem FIfF-Stand auf dem Jahrestreffen Präsenz zu zeigen. Vom 18.-20. Mai 2012 findet zuvor in Köln erneut die noch stärker netz- und gesellschaftspolitisch ausgerichtete SIGINT-Konferenz des CCC statt (näheres dazu im Aufruf zur Teilnahme auf Seite 8 in dieser Ausgabe). Für den FIfF-Stand suchen wir noch Aktive als Betreuende, wenn Ihr Interesse habt, meldet euch unter *fiff@fiff.de*.

Anmerkungen

1 *http://www.torservers.net/wiki/verein/index*
2 *http://fiff.de/about/FIfF_Info-Flyer_small.pdf/view*
3 *http://events.ccc.de/congress/2011/wiki/Schedule*
4 *Videoaufzeichnungen der Vorträge: http://events.ccc.de/congress/2011/wiki/Documentation*
5 *http://events.ccc.de/congress/2011/Fahrplan/events/4876.en.html*
6 *http://events.ccc.de/congress/2011/Fahrplan/events/4901.en.html*
7 *http://events.ccc.de/congress/2011/Fahrplan/events/4736.en.html*
8 *gsmmap.org*
9 *http://events.ccc.de/congress/2011/Fahrplan/events/4800.en.html*
10 *http://mirror.fem-net.de/CCC/26C3/mp4/26c3-3554-de-tor_and_censorship_lessons_learned.mp4.torrent*
11 *http://events.ccc.de/congress/2011/Fahrplan/events/4581.en.html*
12 *http://events.ccc.de/congress/2011/Fahrplan/events/4675.en.html*
13 *http://events.ccc.de/congress/2011/Fahrplan/events/4866.en.html*
14 *http://ftp.halifax.rwth-aachen.de/ccc/28C3/mp4-h264-HQ/28c3-4898-de-security_nightmares_h264.mp4*
15 *http://sigint.ccc.de/Main_Page*

Stefan Hügel

0. Spackeriade

Bericht von der Tagung der datenschutzkritischen Spackeria am 29. Dezember 2011 in Berlin

Netzpolitisch Aktive setzen sich grundsätzlich für den Datenschutz ein – so könnte man meinen, wenn man Publikationen des Chaos Computer Club, der Digitalen Gesellschaft e.V., der Mehrheit der Piratenpartei und nicht zuletzt auch des FIfF verfolgt. Weit gefehlt – die Datenschutzkritische Spackeria *propagiert* Post-Privacy *– das Leben nach dem Datenschutz.*

Wir befinden uns in der *Post-Privacy*-Ära, so der Ausgangspunkt dieser Vereinigung von Datenschutzkritikern (*spackeria.org*), deren Name auf den von *Constanze Kurz* auf dem 27c3 salopp dahingeworfenen Begriff der *Post-Privacy-Spacken* zurückgeht. Die Spackeria geht von der Annahme aus, dass *erstens* Privatheit heute überhaupt nicht mehr möglich ist, da durch Verknüpfung auch scheinbar harmloser Daten und Informationen bereits ein relativ genaues Bild von den Eigenschaften und Vorlieben eines Menschen entsteht. Sie ist aber *zweitens* auch nicht mehr unbedingt wünschenswert: Wir geben Informationen von

uns an das Netz und erhalten eine Vielfalt von Informationen zurück. Dadurch bereichern wir unser Leben – und sind dadurch gleichzeitig freier, da wir nicht mehr ständig darauf bedacht sein müssen, Informationen über uns selbst zu verheimlichen.

Dabei gehen die Datenschutzkritiker auch davon aus, dass Datenschutz das eigentliche Problem überhaupt nicht löst: Heute brauchen wir den Datenschutz, weil wir beispielsweise darauf achten müssen, dass beispielsweise unser Arbeitgeber bestimmte Dinge über uns nicht erfährt. Die Lösung dafür könnte ein bedingungsloses Grundeinkommen sein, das helfen würde, wirtschaftliche Abhängigkeit zu reduzieren.

Man kann diese Position als naiv kritisieren, da sie tatsächlich gesellschaftliche Machtverhältnisse unterschätzt, die uns zwingen, nicht alles über uns preiszugeben. Zu einfach darf man es sich dabei aber nicht machen, wie das in diesem Heft (Seite 69) rezensierte, durchaus fundierte Buch von Christian Heller – *Post-Privacy. Prima leben ohne Privatsphäre* – zeigt.

Die *0. Spackeriade* fand am 29. Dezember 2011 parallel zum *Chaos Communication Congress 28c3* in Berlin statt. Im Gegensatz zu diesem war es eine überschaubare Veranstaltung, in der Post-Privacy unter verschiedenen Aspekten beleuchtet wurde.

Nach der Eröffnung erläuterten *Bastian Greshake* und *Philipp Bayer*, *was die Post-Genomics-Ära für die Privatsphäre bedeutet*. Dargestellt wurden Möglichkeiten, Konsequenzen und Motive der Analyse – und Veröffentlichung – des eigenen Genoms in einer Zeit, in der solche Analysen immer preisgünstiger werden und immer mehr Informationen daraus abgeleitet werden können.

Program or be programmed – Postprivacy als Ideologie der Ausgrenzung? – damit befasste sich *Jürgen Geuter* (aka *tante*) in seinem Vortrag. Der Umgang mit und die Nutzung von Daten und Informationen erfordern besondere Qualifikationen und Fähigkeiten – damit kann die angestrebte Gleichheit in eine andere Form der Ungleichheit umschlagen, die aus den ungleich verteilten Möglichkeiten resultiert, mit der Informationsvielfalt umzugehen und sie zu nutzen. Diese Ungleichheit muss minimiert werden.

Heide Hagen behandelte in ihrem Vortrag *Zwei Seelen wohnen, ach! in meiner Brust… Plädoyer für die Einheit des politischen und des privaten Ichs* Fragen der Individualisierung der Gesellschaft, von Verantwortung, von Rechten und Pflichten und den Konsequenzen daraus. Hier entbrannte eine Diskussion vor allem an der These der Referentin, *Liquid-Democracy*-Abstimmungen und Anonymität seien nicht miteinander vereinbar. Viele Teilnehmer der Tagung stimmten damit nicht überein.

Kritik an der Öffentlichkeitsarbeit der Datenschutzkritiker übte *Ole Reißmann*. *Dabei sein ist nicht alles: Ein paar Leute kamen ins Fernsehen und machten nichts draus. Zehn Thesen zur Spackeria*. Die öffentliche Aufmerksamkeit sei nicht genutzt worden, um die Ziele umzusetzen.

Datenschutz im Spannungsfeld Opferschutz und Vertraulichkeit medizinischer Informationen hieß der Vortrag von *Christian Bahls*, Gründer der Vereinigung MOGIS. Darin und in einer ausführlichen anschließenden Diskussion ging es um die Konsequenzen für Missbrauchsopfer, wenn sie den Missbrauch offenlegen?

Mit der These der Datenschutzkritiker, Offenheit würde Diskriminierung entgegenwirken, setzte sich *Helga Hansen*, Mitautorin des feministischen Blogs *Mädchenmannschaft* auseinander. *Alles offen, alles gut? Wie gefährlich Kontrollverlust und Post-Privacy wirklich sind*, so ihr Beitrag. Offenheit wird hier überschätzt, und kann Diskriminierung nicht beseitigen, wenn ganz andere Ursachen der Auslöser dafür sind.

Provozieren wollten *Fiona* und *erlehmann* mit ihrem Vortrag *Fickileaks – Post Privacy X-Treme*, der Post-Privacy auf die Spitze trieb. Die Idee, (Vermutungen über) sexuelle Beziehungen in einem Graphen aufzubereiten, führte offenbar zu sehr grundsätzlichen Diskussionen – bis hin zur Aufkündigung von Freundschaften.

Dass soziale Privilegien bei der Nutzung der aus der Informationsfreiheit entstehenden Möglichkeiten durchaus eine Rolle spielen, betonte *Daniel Schweighöfer* in seinem Referat *Kampf für die Informationsfreiheit ist ein sozialer Kampf*. Er beschrieb die Mechanismen und skizzierte Lösungsmöglichkeiten für gesellschaftliche Benachteiligungen.

Den Abschluss bildete eine Rückschau auf die Organisation der Spackeriade. Hier sorgte vor allem die ursprüngliche Absicht, *Rainer Langhans* als Keynote-Speaker einzuladen, für Irritiationen. Kritik entzündete sich dabei vor allem an den rechtslastigen Thesen, die Langhans vor einiger Zeit geäußert hatte.

Man kann sicherlich die Annahmen der Post-Privacy kritisieren, vor allem, wenn sie die Bedeutung gesellschaftlicher Machtverhältnisse für allzu freien Umgang mit den eigenen Daten unterschätzen. Doch eines hat die Tagung – und auch das erwähnte Buch – gezeigt: Wir müssen uns mit ihnen auseinandersetzen.

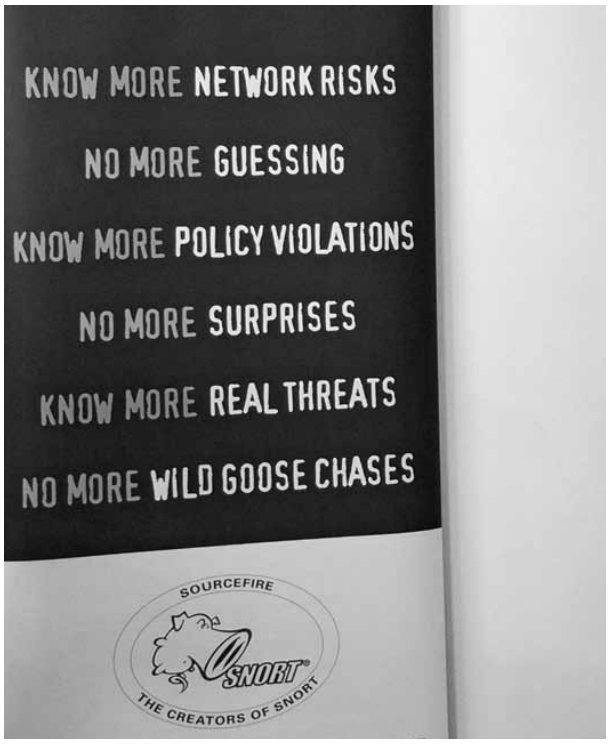


Foto: Dagmar Boedicker

gesehen auf der it-sa 2010

Sylvia Johnigk, Kai Nothdurft

Cyberwarfare

Aufrüstung im Cyberspace als Herausforderung für die Friedensarbeit des FIfF

Dieser Artikel basiert auf einer Gedankensammlung im FIfF-Mitglieder-Wiki[1], an der sich noch mehrere Personen beteiligt haben. Wir wollen die Position des FIfF zum Thema Cyberwar dort weiterentwickeln. Ihr seid alle herzlich eingeladen, Euch daran zu beteiligen.

Wie wird der Begriff Cyberwar verwendet?

Unter *Cyberwarfare* verstehen wir die Kriegsführung mit Computern als Waffen. Computer werden dabei dazu genutzt, militärisch motivierte Angriffe auf andere IT-Systeme durchzuführen (offensive Strategie) oder solche Angriffe mit IT-technischen Mitteln zu erkennen und abzuwehren (defensive Strategie). Da in der politischen und teilweise auch fachlichen Debatte eine verbale Aufrüstung stattfindet, ist es uns wichtig, *Cyberwar* von den Begriffen *Cybercrime* und *Hacktivismus* abzugrenzen, die in der IT-Sicherheit häufig ebenfalls im Zusammenhang mit Angriffen genannt und dabei unter Cyberwar subsummiert werden, denen aus unserer Sicht aber keine militärische Motivation zu Grunde liegt.[2]

Cybercrime umfasst die Begehung von Straftaten, in der Regel mit der Motivation der kriminellen Bereicherung. Unter Hacktivismus verstehen wir das Attackieren von IT-Systemen im Rahmen von politischen Kampagnen z. B. durch zeitweises Lahmlegen mittels *Denial-of-Service*-Attacken oder das Eindringen in Systeme, um geheim gehaltene Informationen der Öffentlichkeit zugänglich zu machen (*Leaken*).

Unter *Cyberespionage* verstehen wir Informationsbeschaffung aus geheimen Quellen mittels Eindringen in IT-Systeme. Diese kann sowohl kriminell-wirtschaftlich (Wirtschaftsspionage) als auch militärisch motiviert sein (Zugang zu militärischen Geheimnissen). Damit kann Cyberespionage, je nach Motivation und Art der ausspionierten Information, zur Cyberwarfare gezählt werden, etwa wenn sie der Vorbereitung eines Angriffs dient.

Cyberwar ist ein sehr wichtiges Thema für das FIfF, das sich kritisch mit den gesellschaftlichen Auswirkungen der IT und insbesondere der Verflechtung von IT und ihrer militärischen Nutzung beschäftigt. Das FIfF wurde vor 27 Jahren von InformatikerInnen gegründet, die die Steuerung von Raketen durch Computer als Bedrohung für die Menschheit identifizierten. Man befürchtete u.a. die Auslösung eines Atomkriegs durch Computerfehler. Inzwischen steuern Computer nicht nur Waffen sondern werden immer mehr selbst zur Waffe. Die Entwicklung von autonomen Kampfrobotern und Drohnen lässt die Grenze zwischen der Waffe und der Technik, die sie steuert, bereits verschmelzen, aber im Cyberwar wird der Computer selbst zur Waffe und dient zur Bekämpfung anderer IT-Systeme, indem Sabotagehandlungen von Angreifern ausgeführt werden. Zum Beispiel können Schadprogramme in die Ziele eingeschleust werden oder Exploits direkt zum Absturz der angegriffenen Systeme führen.

Viele Staaten haben bereits für den Cyberwar spezialisierte militärische Einheiten aufgebaut oder zumindest damit begonnen. Die Einheiten, bestehend aus IT-Spezialisten in Uniform, haben nicht rein defensiven Charakter sondern sind zumindest teilweise auch für Cyber-Angriffe vorgesehen. Neben Russland und China sind vor allem die USA eine treibende Kraft in der digitalen Aufrüstung.

Im Februar 2009 berichtete der SPIEGEL, dass auch die Bundeswehr eine 76 Mann umfassende geheime Cyberwar-Einheit aufbaue, die sowohl defensive als auch offensive Aufgaben habe.[3]

In Deutschland wurde außerdem am 23. Februar 2011 das nationale Cyber-Abwehrzentrum NCAZ gegründet. Hauptzweck des NCAZ soll ein verbesserter Informationsaustausch unter den Strafverfolgern, Militär, Geheimdiensten und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sein.

Die Bundesregierung hielt es formal nicht für nötig, ein Errichtungsgesetz verabschieden zu lassen, weil es sich nach ihrer Auffassung beim NCAZ nicht um eine eigenständige Behörde handele. „Dabei sollen alle Mitarbeiter im Abwehrzentrum, unter Wahrung der Zuständigkeit der einzelnen Behörden wie unter Berücksichtigung des Trennungsgebotes zwischen Nachrichtendiensten und Polizei, in ihre jeweiligen Behörden eingebunden bleiben.“[4] Durch die gemeinsame Arbeit wird jedoch aus unserer Sicht eine Vermischung von Strafverfolgung und Geheimdienstaufgaben und zusätzlich noch dem militärischen Bereich gefördert, die de facto das Trennungsprinzip aufweicht und in der Folge zu gefährlichen Machtkonzentrationen führen kann.

US-amerikanische Cyberspace-Strategie

Am 14. Juli 2011 veröffentlichte das amerikanische *Verteidigungs*ministerium eine neue Militärstrategie für das Operieren im Cyberspace.[5] Dieser veröffentlichte Teil der Strategie war entgegen früheren Ankündigungen und Erwartungen[6] zunächst rein defensiv ausgerichtet. Noch im Mai war in Medienberichten diskutiert worden, dass Cyber-Attacken zukünftig von den USA als Kriegsgrund gewertet würden, der auch mit konventionellen Waffen beantwortet werden könnte. Neuere Meldungen und die Tatsache, dass nur Teile der Strategie veröffentlicht wurden, deuten jedoch darauf hin, dass es auch in den USA weiter gehende Überlegungen gibt, die sich sehr wohl mit offensiven Cyberwar-Strategien beschäftigen. So soll das US-Militär bei der Planung des Libyen-Einsatzes im Frühjahr erwogen haben, „in die libyschen Kommunikationsnetze einzudringen,“ um „die daran angeschlossenen Radaranlagen und so die Raketenflugabwehr“ zu stören. Auch für die gezielte Tötung Bin Ladens war erwogen worden, das pakistanische Radar mit einer Cyber-Attacke auszuschalten. „Laut James Andrew Lewis vom *Center for Strategic and International Studies* wollten die USA nicht die

ersten sein, die offiziell Cyberwar-Instrumente einsetzen und damit einen Dammbruch herbeiführen."[7]

Ein Grund dürfte dabei auch die eigene Verletzlichkeit der USA gegenüber Cyber-Angriffen sein, auf die im Strategiepapier vom Juli 2011 mehrfach hingewiesen wird. Diese defensive Schwäche gegen Cyber-Angriffe, die nicht nur die USA sondern alle hochtechnisierten Gesellschaften betrifft, gründet in einer jahrzehntelangen Vernachlässigung der IT-Sicherheit in Architekturen, Design und Implementierung von Netzwerken, Betriebssystemen und Anwendungsprogrammen und setzt sich in Embedded Systems und Steuerungsanlagen fort. Sicherheitsmaßnahmen und Basisschutz müssten für alle mit dem Internet verbundenen Systeme existieren. Stattdessen strotzen die allermeisten Web-Anwendungen vor Sicherheitslücken. Versäumnisse in der Software-Entwicklung wie schlechte Codequalität und fehlendes Testen gegen Sicherheitslücken aufgrund enger Release-Termine und das Sparen an qualifiziertem Personal im Systembetrieb führen zu diesen Sicherheitsrisiken.[8] Die Zentralisierung, Vernetzung (insbesondere über das Internet), Cloud-Computing und der Zugriff über völlig ungesicherte mobile Endgeräte wie Smartphones oder Tablets erhöhen zudem stetig das Risikopotenzial der IT-Systeme und damit die Verletzlichkeit der Betreiber und der gesamten Gesellschaft, in der sie eingesetzt werden.

Das Sicherheitsniveau der meisten Systeme ist für die potenziellen Schäden, die bei einer Manipulation, Sabotage oder Kompromittierung entstehen können, viel zu gering, da in der Vergangenheit IT-Sicherheit häufig hinter anderen Kriterien wie erweiterter Funktionalität, Kosten oder Bequemlichkeit zurückgestellt wurde. Eine der fünf im Strategiepapier genannten Initiativen soll das Sicherheitsniveau der militärischen wie zivilen IT-Systeme verbessern – ein Ziel, das sicherlich nicht kurzfristig zu erreichen ist.

Was wird als Angriff gewertet?

Das DoD (*Department of Defense*) betrachtet in seinem Strategiepapier sehr unterschiedliche Formen von Bedrohungen im Cyberspace, unterscheidet aber aus unserer Sicht zu wenig zwischen durch Cyberwar, Cybercrime und Hacktivism motivierten Angriffen. Neben *Denial-of-Service*-Attacken auf die militärischen Netzwerke und angeschlossenen Systeme oder Angriffen auf zivile Einrichtungen mit Sabotagecharakter – Infrastrukturen wie Energieversorgung, Verkehrsinfrastrukturen – werden auch Manipulationen oder der Diebstahl von Informationen als Bedrohung der nationalen Sicherheit angesehen. Der Diebstahl von geistigem Eigentum schwäche demnach die technologische Vormachtstellung. Aber auch sonstige Wirtschaftsspionage wird als Bedrohung angesehen, weil dadurch die ökonomische Stärke der USA beeinträchtigt und damit die USA insgesamt geschwächt wird.

In den Monaten, bevor die Strategie veröffentlicht wurde, kam es vermehrt zu spektakulären Hacking-Aktivitäten und Cyber-Attacken, die für die USA eine Herausforderung darstellten und auch allgemein als Eskalation der Bedrohungen der IT-Sicherheit wahrgenommen werden können:

1. Im Juni 2010 wird der *Stuxnet-Wurm* entdeckt, bei dem es sich um eine völlig neue Klasse von Schadsoftware handelt. Da der Wurm seine Schadroutinen nur bei einer sehr speziellen Art von Steuerungssystemen ausführt (*Simatic S7* von Siemens) und dabei sehr gezielte Veränderungen in der Steuerung vornimmt, und weil Iran von Infektionen besonders stark betroffen war, wird angenommen, dass der Wurm speziell für die Sabotage von Zentrifugen in der iranischen Urananreicherungsanlage in Natanz entwickelt wurde.[9] Die Entwicklungskosten liegen im 7-stelligen Dollarbereich. Die Urheberschaft ist bisher unbekannt, wird aber wegen des Ziels und der Höhe der eingesetzten Mittel bei israelischen und/oder US-amerikanischen staatlichen Stellen vermutet.

2. In 2010 werden von Wikileaks mehrere für die US Regierung problematische Dokumente enthüllt: am 5. April ein Video zu Luftangriffen von US-Kampfhubschraubern in Bagdad, bei denen gezielt Zivilisten – u.a. auch Reporter – getötet wurden, im Juli die *Afghan War Diaries*, 76.911 Dokumente über den Krieg in Afghanistan, und am 28. November 250.000 US Botschaftsdepeschen (*Cables*).

3. Als Solidaritätsmaßnahme für Wikileaks wurde ab Ende 2010 von den lose organisierten Netzaktivisten von Anonymous die *Operation Payback* gestartet. Es handelte sich dabei um zeitlich begrenzte, aber erfolgreiche DDoS Attacken mit einem Tool namens *Ionenkanone*. Die Attacken richteten sich u.a. gegen Visa, Mastercard und Paypal, weil diese keine Zahlungen an Wikileaks mehr transferierten. Die Web-Dienste der betroffenen Unternehmen waren dadurch zeitweise nicht mehr erreichbar.

4. Die Hackergruppe *Lulzsec* drang in mehrere Server (u. a. Sony, Nintendo, die US Fernsehsender Fox und PBS, die Website des US-Senats) ein und stellte kopierte Daten demonstrativ ins Internet, darunter auch sensible personenbezogenene Informationen.[10]

5. Im März 2011 wurden durch eine Hacking-Attacke, hinter der ein ausländischer Geheimdienst vermutet wurde, 24.000 geheime Dateien des Pentagon entwendet.[11]

6. Unbekannte aus dem Umfeld von Anonymous erlangten im Juli Zugriff auf fünft GB Daten der NATO.[12]

7. Am 18. März 2011 gab die Sicherheitsfirma RSA bekannt, Opfer einer APT-(*Advanced Persistance Threat*) Attacke geworden zu sein. Dabei wurden Firmengeheimnisse über das Produkt *Secure ID Token*, das zur 2-Faktor Authentisierung genutzt wird, entwendet.[13] Am 21. Mai 2011 wurde in Server des US-Rüstungskonzerns Lockheed Martin eingebrochen, wobei Informationen aus dem vorangegangenen RSA-Hack genutzt wurden.[14]

Alle genannten Vorfälle würden nach der Doktrin als Cyber-Bedrohungen gewertet, die die nationale Sicherheit der USA gefährden.

Mit der sehr weiten Definition von Bedrohungen geht aber eine gewisse Beliebigkeit einher, was alles als militärischer Angriff gewertet werden kann, aus dem möglicherweise auch militärische Gegenaktionen legitimiert werden sollen.

Der IT-Sicherheitsexperte Bruce Schneier warnt zu Recht vor verbaler Hochrüstung und davor, zu schnell Angriffe auf die IT-Sicherheit als Cyberwar-Aktivität zu werten:

> *„And just as every shooting is not necessarily an act of war, every successful Internet attack, no matter how deadly, is not necessarily an act of cyberwar."*[15]

Die breite Definition von Bedrohungen, unabhängig von der Motivation und Organisation des Angreifers, lässt mit ihrer Beliebigkeit theoretisch auch die Taten einer Einzelperson, etwa eines pubertierenden *Scriptkiddies*, das eine Malware ausprobiert, als Kriegsgrund zu. Sie könnte sogar als ungesetzlicher Kombattant eingestuft werden. Bei den Bedrohungen wird nicht unterschieden, ob militärische oder zivile Systeme angegriffen werden. Wenn Gleiches auch für die Offensive gilt, entsteht ein großes, neues Risiko für die Zivilbevölkerung der angegriffenen Länder. Im Cyberwar verschwimmen die Grenzen zwischen militärischen und zivilen Zielen weiter, und die Schwere und Häufigkeit von Kollateralschäden bei der Zivilbevölkerung wächst.

Besonders kriminell motivierte Angriffe kommen sehr häufig vor. Wenn davon auch nur ein Bruchteil als kriegerischer Akt eingestuft wird, herrscht Dauerkrieg. Die Subsummierung kann auch durch eine Konkurrenz zwischen Strafverfolgungsbehörden und Militär motiviert sein, wer für Cyber-Attacken zuständig ist, wer zu deren Bekämpfung finanzielle Mittel bekommt, wessen Methodiken der Gegenmaßnahmen angewendet werden. Schon beim *Krieg gegen den Terror* wurde vergeblich versucht, Kriminalität militärisch zu bezwingen.

Es gibt durch die Beliebigkeit von Bedrohungen in der Strategie auch keine erkennbaren Maßstäbe, ob es sich um eine völkerrechtlich legitimierbare Verteidigung nach einem tatsächlich erfolgten Angriff handelt. Im Zweifelsfall werden technische Details als Geheimsache unter Verschluss gehalten (werden müssen), womit sie sich jeglicher Prüfung durch unabhängige Instanzen entziehen, ob ein militärische Gegenschläge rechtfertigender Angriff überhaupt stattgefunden hat.

Jeder Cyber-Angriff könnte damit sogar den Vorwand für das Ausrufen eines militärischen Bündnisfalls liefern.

Birgt schon die militärische Bewertung aus der Defensive erhebliche Risiken, so ist die offensive Cyberwar-Kriegsführung aus mehreren weiteren Gründen äußerst kritisch zu sehen.

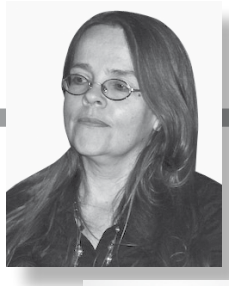
Wer ist der Angreifer?

Schon das korrekte Identifizieren des Gegners wird im Cyberwar zum Problem, wie auch das DoD erkannt hat (Problem der *Non-Attribution*):

> *„Cyber is also an attractive weapon to our adversaries because it is hard to identify the origin of an attack and even more difficult to deter one. A keystroke travels twice around the world in 300 milliseconds. But the forensics necessary to identify an attacker may take months. Without establishing the identity of the attacker in near real time, our paradigm of deterrence breaks down. Missiles come with a return address. Cyber attacks, for the most part, do not." (William Lynn, Deputy Secretary of Defense*[16]*)*

Halbwegs versierte Angreifer nutzen für Cyber-Attacken nicht den eigenen Computer sondern infizieren den PC eines (bis dahin unbeteiligten) Dritten mit Malware und übernehmen dadurch die Kontrolle darüber. Der so übernommene PC wird ab diesem Zeitpunkt bei Bedarf durch den Angreifer ferngesteuert. Der kompromittierte PC wird zu einem *Zombie* als Ausgangspunkt für den eigentlichen Angriff. Dieses Verstecken des Angreifers hinter einem kompromittierten PC lässt sich noch mehrfach iterieren, indem der erste befallene PC einen weiteren befallen PC fernsteuert usw.

Oft werden solche Zombie-PCs mit anderen infiltrierten PCs zu einem Bot-Netz zusammengeschaltet, in dem mehrere befallene Rechner von einem Controlserver gemeinsam gesteuert werden. Dadurch können dann auch *Distributed-Denial-of-Service*-Angriffe (DDoS-Attacken) ausgeführt werden. Der Angreifer steu-



Sylvia Johnigk und Kai Nothdurft

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.

Kai Nothdurft studierte Informatik an der Uni Bremen und beschäftigte sich schwerpunktmäßig mit Datenschutz und IT-Sicherheit. Nach dem Studium arbeitete er fünf Jahre als Freiberufler im Schulungs- und Consultingbereich. Seit 1999 arbeitet er als IT-Sicherheitsbeauftragter für ein großes deutsches Versicherungsunternehmen.

ert dabei eine große Menge an Zombie-PCs, was es zum Beispiel ermöglicht, angegriffene Systeme durch Überlastung zusammenbrechen zu lassen.

Will man aber die Quelle solcher Angriffe identifizieren und sucht in Logfiles nach der Quell-IP, so stößt man zunächst nur auf die Zombie-PCs und muss in deren Logfiles nach weiteren Spuren suchen, von wo aus diese kontrolliert wurden – ein zeitaufwendiges und oft auch erfolgloses Unterfangen. Damit wird es aber sehr schwer, die eigentliche Quelle des Angriffs zu ermitteln. Ein militärischer Gegenschlag kann, wenn überhaupt, nicht zeitnah erfolgen oder man riskiert dabei, den „Falschen" zu erwischen.

Auf der Angreiferseite ist durch das geringe Entdeckungs- und Vergeltungsrisiko die Hemmschwelle zum Ausführen eines Cyber-Angriffs geringer als für einen konventionellen Angriff.

Da die Identifizierung des Angreifers so problematisch ist, kommen bei Sicherheitspolitikern bestimmt auch bald wieder Wünsche nach einer zwangsweisen Identifizierung und Vorratsdatenspeicherung als einfache politische Antworten auf dieses Problem auf. Dem muss entgegengesetzt werden, dass sich Cyber-Soldaten oder gewiefte Kriminelle eben fremder, gestohlener Identitäten oder in letzter Instanz dann doch Anonymisierern bedienen.[17]

Verstärkung der Tendenz zur asymmetrischen Kriegsführung

Die Cyber-Strategie der USA erwähnt auch, dass das Land sich in einer technologischen Führungsposition befindet. Wird aber ein offensiver Cyber-Krieg gegen technologisch weniger entwickelte Gegner geführt, werden diese womöglich mit einfachen Guerilla-Aktionen reagieren. Durch die Aufrüstung im Cyberspace wird so die Tendenz zur asymmetrischen Kriegsführung verstärkt. Wenn das gegnerische Militär technologisch überlegen ist, werden primitive Gegenmaßnahmen in Form von bspw. Sprengstoffattentaten auf zivile Einrichtungen attraktiver.

Militärische Geheimhaltung schadet auch der eigenen Zivilgesellschaft

IT-Sicherheit ist bisher noch ein Sicherheitsbereich, der nicht staatlich kontrolliert und nur wenig reglementiert wird. Versuche der USA in der Vergangenheit, z. B. Kryptografie-Exporte zu beschränken, scheiterten, da sich dies als negativ für die eigene Wirtschaft herausstellte.

Wissen über Sicherheitslücken (*less than Zero day exploits*) geheim zu halten, um sie im Cyberwar zum Angriff nutzen zu können, ist gefährlich, da es auch die eigene Wirtschaft gefährdet, die die gleichen Betriebssysteme und Anwendungen einsetzt wie der Gegner, den man angreifen möchte. Dieses Dilemma wurde von der NSA als *Equity Issue* identifiziert. Es handelt sich um ein *Dual-Use*-Problem, dass man Sicherheitslücken als militärischen Vorteil geheim halten kann, dann aber auch die eigenen Unternehmen und Zivilisten gefährdet, oder sie veröffentlicht und damit auch dem „Gegner" hilft, seine IT-Sicherheit und damit Cyber-Verteidigungsfähigkeit zu verbessern.[18] In ein vergleichbares Dilemma laufen staatliche Institutionen auch, wenn sie im Rahmen der Strafverfolgung Sicherheitslücken geheim halten, um damit PCs von Verdächtigen mit einem Staatstrojaner kompromittieren zu können.

Kriminelle erlangen Wissen schneller als die Öffentlichkeit, daher entstehen sehr schnell auch volkswirtschaftliche Schäden. Da sich viel Geld damit verdienen lässt, wird solches Wissen nicht nur an offizielle Stellen verkauft, ganz davon abgesehen davon, dass es auch in staatlichen Institutionen Kriminelle gibt. Es gibt viel zu viele Lücken und daher Möglichkeiten, diese zu entdecken, als das man das Problem kurz- oder mittelfristig unter Kontrolle bringen könnte.

Cyber-Demonstrationsrecht – Digitale Aktionsformen und Hacktivismus

Die in der Medienberichterstattung viel beachtete Aktivistengruppe Anonymous würde nach der US-Strategie als nationale Bedrohung eingestuft. Im Gegensatz zu von staatlichen Institutionen durchgeführten Angriffen machen sie ihre Aktivitäten publik und kündigen sie sogar an. Bei den Aktionen von Anonymous handelt es sich auch weniger um Hacking zur Sabotage oder Spionage als vielmehr um einen Online-Protest im Rang zivilen Ungehorsams, der in die kriminelle Ecke gedrängt und als Terrorismus diffamiert werden soll. Bei der Nutzung des DDoS-Tools *Ionenkanone* wurden die betroffenen Server nur vorübergehend für einen kurzen Zeitraum lahmgelegt. Die Aktionen wurden zum Teil sogar vom eigenen PC aus vorgenommen, waren also nicht einmal vollständig anonym und einige Aktivisten bekamen in der Folge entsprechende Repressalien zu spüren. Solche Aktionen gleichen politische Sit-Ins oder Blockaden zu Demonstrationszwecken. Sie müssten eher als ziviler Ungehorsam eingeordnet werden denn als Terror oder gar Angriff in einem Cyberwar. Da inzwischen viele Organisationen sehr stark, einige sogar ausschließlich im virtuellen Raum in Erscheinung treten und agieren, muss auch die Kritik und Auseinandersetzung bis hin zum gewaltfreien Widerstand im Cyber-Raum legitim werden.

An ethische Grenzen stoßen solche Aktionen allerdings, wenn dabei wichtige Grundrechte verletzt oder gar Menschenleben gefährdet werden. So hat die Hackergruppe Lulzsec mehrfach sensible personenbezogene Daten von Servern, in die sie eingedrungen waren, kopiert und im Internet veröffentlicht, etwa die Kundendaten von Sony.

Conclusio

Für das potenzielle Schlachtfeld im Cyberspace wurde eine neue gefährliche Rüstungsspirale in Gang gesetzt. Sie zieht ihre Motivation aus dem Auf- und Ausbau von militärischen Cyberwar-Einheiten, der hohen Verletzlichkeit der *digitalen* Gesellschaften mit ihren global vernetzten IT-Systemen und dem vermeintlich geringen Risiko für den Angreifer, identifiziert und für sein Tun sanktioniert zu werden. Es ist höchste Zeit, dass die in Gang gesetzte Rüstungsmaschinerie wieder gestoppt wird. Das FIfF als Teil der Friedensbewegung ist in besonderer Weise gefordert, seine fachliche Expertise dafür zu nutzen. Die folgenden Forderungen sollen zu einer Deeskalation und Vermeidung von Cyber-Kriegen beitragen:

Forderungen des FIfF

1. **Verzicht auf Erstschlag und Offensive im Cyberspace: Staaten sollen öffentlich darauf verzichten, Cyber-Waffen präventiv oder zum Angriff einzusetzen.**
2. **Reine defensive Sicherheitsstrategie: Staaten sollen sich verpflichten, keine Offensivwaffen für den Cyberwar zu entwickeln oder gar einzusetzen.**
3. **Digitale *Genfer Konvention*: Für die Zivilbevölkerung lebenswichtige Infrastrukturen wie Wasserversorgung, Gesundheitsversorgung, etc. dürfen nicht angegriffen werden. Eine Verletzung dieses Grundsatzes soll als Kriegsverbrechen gelten.**
4. **Anerkennung eines Grundrechts auf zivilen Ungehorsam und Online-Protestformen im Internet: Derartige Aktionen dürfen nicht kriminalisiert werden geschweige denn als Kriegsgrund herhalten.**
5. **Wirtschaftliche Interessen, wie ein Verstoß gegen *Intellectual Properties*, sind kein legitimer Kriegsgrund.**
6. **Konventionelle Waffen dürfen nicht als Antwort auf eine Cyber-Attacke eingesetzt werden.**
7. **Staatliche Stellen müssen zur Offenlegung von Schwachstellen verpflichtet werden (ableitbar aus dem Grundrecht für Integrität, das der Staat schützen muss).**
8. **Betreiber kritischer Infrastrukturen müssen verpflichtet werden, sich selbst zu schützen, bzw. IT-Systeme sicher zu gestalten, zu implementieren und zu betreiben, anstatt nach dem Staat oder gar Militär zu rufen. Kompetente, transparente Prüfungen und Tests müssen Voraussetzung für eine Betriebserlaubnis sein. Wir fordern Entnetzung und Dezentralisierung kritischer Infrastrukturen (wie z. B. DE-CIX).**
9. **Abrüstung der politische Sprache: Klare Trennung von Cyberwar, Cyberterror, Cybercrime, ethical Hacking, politischen Protestformen.**
10. **Demokratische Kontrolle, Gewaltenteilung, Parlamentsvorbehalt für Cyber-Sicherheitsstrategien und deren Umsetzung.**
11. **Transparenz beim Aufbau jeglicher „Cyber-Zentren".**
12. **Klare friedenspolitische Ausrichtung der Cyber-Zentren.**
13. **Die Trennung von Polizei und Geheimdiensten und Militär in Cyber-Abwehrzentren muss gewährleistet werden.**
14. **Cyberpeace-Initiative: Verpflichtung zur Förderung von Friedensforschung zur Entwicklung von Strategien zur Befriedung des Cyberspace.**

Anmerkungen

1 *http://wiki.fiff.de/CategoryCyberwarfare. Login-Daten erhaltet Ihr über die Geschäftsstelle.*
2 *Eine gefährliche Analogie wäre auch, IT-Sicherheitstools mit Waffen gleichzusetzen. In dieser Logik wäre ein Programmierer, der solche Tools herstellt, ein Rüstungsbetrieb, befänden sich Massenvernichtungswaffen (Botnetze) in den Händen von kriminellen Zivilisten.*
3 *http://www.spiegel.de/netzwelt/tech/0,1518,606096,00.html*
4 *http://de.wikipedia.org/wiki/Cyberabwehrzentrum*
5 *http://www.defense.gov/news/d20110714cyber.pdf – Department of Defense: Strategy for operating in Cyberspace*
6 *http://www.heise.de/security/meldung/Bericht-USA-wollen-Hacker-angriffe-zum-Kriegsgrund-erklaeren-1253088.html*
7 *http://www.heise.de/newsticker/meldung/Bericht-US-Regierung-erwog-Cyberwar-gegen-Libyen-1362698.html*
8 *Schlecht konfigurierte und nicht gehärtete Betriebssysteme, unzureichend gesicherte Netze, keine oder fehlerhaft konfigurierte Intrusion Detection Systeme, mangelnde Überwachung dieser Systeme sind nur eine kleine Auswahl von Sicherheitslücken, mit denen sich die Liste erweitern lässt.*
9 *Ein Foto auf der Webseite des iranischen Präsidenten Ahmadinedschad von einem Besuch in Natanz zeigt ein Steuerungs-Panel für die gleiche Anzahl von Zentrifugen, die mit Stuxnet manipuliert werden.*
10 *http://www.heise.de/security/artikel/LulzSec-ausser-Rand-und-Band-1261669.html*
11 *http://www.spiegel.de/politik/ausland/0,1518,774553,00.html*
12 *http://www.spiegel.de/netzwelt/web/0,1518,775811,00.html*
13 *http://www.heise.de/security/meldung/RSA-Hack-koennte-Sicherheit-von-SecurID-Tokens-gefaehrden-1210245.html*
14 *http://www.heise.de/security/meldung/Hacker-steigen-bei-Lockheed-Martin-ein-1251902.html*
15 *http://www.schneier.com/blog/archives/2007/06/cyberwar.html*
16 *Remarks at Stratcom Cyber Symposium William J. Lynn http://www.defense.gov/speeches/speech.aspx?speechid=1477*
17 *Auch das DoD fördert das TOR-Projekt und Sicherheitsbehörden und Militärs nutzen TOR selbst.*
18 *http://www.softsecurity.com/news/blog-posts/dual-use-technologies-and-the-equities-issue.html*

Ralf E. Streibl

Bremer Universität bestätigt Zivilklausel

Wichtiges Signal für Verantwortung in der Wissenschaft

„(...) But there are other areas of scientific research that may directly or indirectly lead to harm to society. This calls for constant vigilance. (...)"
(J. Rotblat 1995)

In seiner Sitzung vom 25. Januar 2012 hat der Akademische Senat als höchstes beschlussfassendes Gremium der Universität Bremen in Bestätigung der Grundsätze früherer Beschlüsse mit sehr großer Mehrheit für eine Zivilklausel votiert und die Leitziele der Universität dahingehend präzisiert (Wortlaut siehe unten).

Vorangegangen waren Monate mit Diskussionen im akademischen Senat, in der Universität und in der Öffentlichkeit. Mehrere Informations- und Diskussionsveranstaltungen sowie diverse Presseberichte bildeten den Rahmen. In den Debatten vermengten sich dabei viele verschiedene Diskussionsstränge, u.a. über Sinn und Gefahren fremdfinanzierter (Stiftungs)Professuren, über konkrete Firmen-Kooperationen, über die veränderte politische Lage nach dem Ende des kalten Krieges, über „neue Sicherheitspolitik", über Pazifismus, über Bildung für den Frieden, über Wissenschaftsfreiheit, über Dual-Use, über Zivilklauseln an Hochschulen allgemein sowie ihre Operationalisierbarkeit im Besonderen und – nicht zuletzt – über Verantwortung in der Wissenschaft. All diese Themen haben inhaltlich miteinander zu tun, jedoch wurde die Diskussion durch die Verquickung sachlicher, politischer und emotionaler Aspekte zeitweise stark erschwert.

Vor dem Hintergrund der langen, durchaus kontrovers geführten Debatte mag es dann verwundern, dass am Ende ein solch klarer, deutlicher Beschluss für die Zivilklausel erfolgte. Zu seinem Zustandekommen mag auch ein wachsendes Verständnis für die zwei Ebenen der rechtlichen Dimension und der moralischen Bedeutung einer Zivilklausel beigetragen haben.

Wissenschaftsfreiheit

Die Freiheit der Wissenschaft ist sowohl im Grundgesetz als auch in der Verfassung des Landes Bremen garantiert (Einschränkungen ergeben sich nur durch andere in der Verfassung garantierte Grundrechte):

> *GG Art. 5: „(3) Kunst und Wissenschaft, Forschung und Lehre sind frei. Die Freiheit der Lehre entbindet nicht von der Treue zur Verfassung."*
>
> *BremVerf Art. 11: „(1) Die Kunst, die Wissenschaft und ihre Lehre sind frei."*

Das Bremische Hochschulgesetz wird dazu etwas ausführlicher. Im § 7 *„Freiheit von Wissenschaft und Kunst, Forschung, Lehre und Studium"* heißt es u.a., dass das Land und die Hochschulen im Rahmen ihres Haushalts sicherzustellen haben, dass die Mitglieder der Hochschulen diese verfassungsrechtlich verbürgten Grundrechte wahrnehmen können. Entscheidungsbefugnis der Hochschulorgane in Fragen der Forschung ist nur hinsichtlich der Organisation des Forschungsbetriebes, der Förderung und Abstimmung von Forschungsvorhaben sowie bei der Bildung von Forschungsschwerpunkten gegeben.

Im BremHG ist ferner geregelt, dass Forschungsergebnisse aus Drittmittelprojekten innerhalb eines absehbaren Zeitraums veröffentlicht werden müssen (§ 75 (5)).

Rechtliche Reichweite einer Zivilklausel

Eine Universität kann selbstverständlich keine Beschlüsse fassen, die verfassungsgemäße Rechte außer Kraft setzen würden. Insofern trifft die seitens des Rektors der Bremer Universität zu Beginn der Akademischen Senatssitzung getroffene Feststellung natürlich zu, dass einem Professor oder einer Professorin im Falle eines Verstoßes gegen die Zivilklausel keine dienstrechtlichen Folgen drohen würden.

Gerade da *kein grundsätzliches Verbot* einer Beteiligung von Wissenschaft an einer Forschung mit militärischer Nutzung ausgesprochen wurde, ist die Zivilklausel der Universität Bremen *vereinbar* mit Art. 5 Abs. 3 GG und den entsprechenden anderen gesetzlichen Regelungen. Ein Vorwurf, die Existenz der Zivilklausel gefährde die Wissenschaftsfreiheit, geht somit ins Leere.

Völlig ohne dienstrechtliche Relevanz ist die Zivilklausel dennoch nicht. Sollte beispielsweise ein Hochschullehrer sich entscheiden, rüstungsrelevante Forschung zu beginnen, und Mitglieder seiner Arbeitsgruppe würden die Mitarbeit daran unter Verweis auf die im Akademischen Senat beschlossene Zivilklausel verweigern, so wäre die Universitätsleitung gefordert, sich schützend vor diese Mitarbeiterinnen und Mitarbeiter zu stellen, wenn ihnen seitens des Hochschullehrers dienstrechtliche Schritte angedroht würden.

Auf organisatorischer Ebene kann die Universität ferner beschließen, dem entsprechenden Hochschullehrer angesichts solcher Projekte keine weiteren, über die garantierte Grundausstattung hinausgehenden Forschungsgelder, Fördermaßnahmen o.ä. zur Verfügung zu stellen.

Moralischer Appell – gesellschaftliche Verantwortung

Die universitäre Zivilklausel – so die Rechtsstelle der Universität Bremen in einer Stellungnahme im Vorfeld der Sitzung des aka-

demischen Senats (Banik 2011) – beinhalte einen *„grundsätzlich sanktionslosen moralischen Appell"*. Dennoch könne die Zivilklausel *„mittelbar Wirkungen auf das Verhalten der Forscherinnen und Forscher"* entfalten, z. B. durch den möglichen moralischen Druck der akademischen Gemeinschaft im Falle einer Missachtung.

Dies ist – was mögliche Wirkungen angeht – selbstverständlich richtig, greift jedoch m.E. in der Gesamtbetrachtung zu kurz. Aus dem Fokus gerät dabei zum einen der *Signalcharakter* solch einer Selbstverpflichtung: Wenn eine große Institution solch einen Beschluss fasst, hat dies eine andere Außenwirkung, als wenn einzelne Wissenschaftlerinnen und Wissenschaftler – so erfreulich dies ist – für sich individuelle Entscheidungen treffen. Die Existenz solch einer Selbstverpflichtung kann beispielsweise im Rahmen von Berufungsverfahren thematisiert werden und ebenso bei Kontaktgesprächen mit möglichen Kooperationspartnern (beides geschieht übrigens in Teilen der Universität Bremen seit Jahren). Zum anderen muss dringend das Augenmerk auf den eigentlichen Hintergrund solch einer Selbstverpflichtung gerichtet werden: Es geht dabei um praktizierte gesellschaftliche Verantwortung für Auswirkungen und Folgen eigenen wissenschaftlichen Handelns.

Im Bremischen Hochschulgesetz ist dieser Verantwortungsaspekt erfreulicherweise bereits direkt in den bereits genannten Paragraphen zur Wissenschaftsfreiheit eingewoben:

> *BremHG § 7: „(1) ... Alle an Forschung und Lehre Beteiligten haben die gesellschaftlichen Folgen wissenschaftlicher Erkenntnisse mitzubedenken. Werden ihnen im Rahmen ihrer Tätigkeit an der Hochschule Forschungsmethoden oder -ergebnisse bekannt, die die Menschenwürde, die freie Entfaltung der Persönlichkeit, das friedliche Zusammenleben der Menschen oder die natürlichen Lebensgrundlagen bedrohen können, soll dies öffentlich gemacht und in der Hochschule erörtert werden."*

Vor diesem Hintergrund greift auch der seitens eines Kritikers der bisherigen Zivilklausel in den Diskussionen der letzten Monate mehrfach geäußerte Vorwurf nicht, dass eine Zivilklausel ohne klare Kriterien dazu führen könne, dass alle möglichen Forschungsprojekte „skandalisiert" werden könnten. Der Begriff der „Skandalisierung" enthält hier bereits eine Negativ-Wertung, die die zentrale Frage nach Einschätzung und (Selbst)Reflexion der Forschung beschädigt. Unabhängig davon, ob es an einer Hochschule des Landes Bremen eine Zivilklausel gibt oder nicht, sind bereits durch das Hochschulgesetz ohnehin alle Mitarbeiterinnen und Mitarbeiter direkt aufgefordert, ein Augenmerk auf Forschungen und ihre möglichen Folgen zu haben und mögliche Bedenken oder Probleme publik zu machen und zur Diskussion aufzufordern.

Bildung

Häufig wird als Argument gegen Zivilklauseln die Schwierigkeit ihrer Operationalisierung angeführt: A-priori-Definitionsversuche, welche Forschungsprojekte unbedenklich seien und welche nicht, sind zum Scheitern verurteilt. Hinzu kommen unzählige „zivil-militärische Grauzonen", die Wolfgang Liebert anschaulich beschreibt: *„Was früher noch eindeutig »schwarz« erschien und nur militärischen Interessen dienlich war, hat auch Einzug in zivile Zusammenhänge gehalten. Umgekehrt werden ehemals für »weiß« gehaltene Forschungsbereiche mit dem (oft unzutreffenden) Argument, ökonomisch günstiger auch militärische Zielvorgaben erfüllen zu können, in die Grauzone hineingeführt"* (Liebert 2009, S. 445). Würde dadurch eine Zivilklausel nicht obsolet?

Ganz im Gegenteil: Gerade vor dem Hintergrund der geschilderten Problematik und Notwendigkeit des Umgangs mit Ambivalenz in der Forschung gewinnt die Reflexion enorm an Bedeutung – nicht zuletzt auch im Sektor der Lehre. Die Wissenschaftlerinnen und Wissenschaftler sind in der Pflicht, hinsichtlich ihrer Forschungen und Entwicklungen frühzeitig mit antizipativen Analysen zu beginnen, *„die Fragen stellt nach Intentionen, wissenschaftlich-technischen Potenzialen, normativen Rand- und Vorbedingungen, ambivalenten Entwicklungslinien, gewollten Wirkungen, nicht-intendierten Folgen und sichtbaren Entwicklungsrisiken"* (Liebert 2009, S.448).

Die Existenz einer Zivilklausel fordert zum einen alle Beteiligten in Forschung und Lehre dazu auf, sich selbst – und anderen – in der Institution entsprechende Fragen zu stellen und damit in einen stetigen und öffentlichen Diskurs zu treten (vgl. Streibl 2011).

Ralf E. Streibl

Ralf E. Streibl, Diplom-Psychologe; seit 1993 Lehrtätigkeit an der Universität Bremen (Schwerpunkt u.a. „Informatik und Gesellschaft"), zusätzlich wissenschaftlicher Angestellter im Studienzentrum Informatik; in der o.g. Sitzung des Akademischen Senats an der Formulierung und Beschlussfassung der aktuellen Zivilklausel aktiv beteiligt.

Mitglied der Gewerkschaft Erziehung und Wissenschaft (GEW), Sprecher der GEW-Gruppe an der Universität Bremen; Mitglied im Forum Friedenspsychologie (FFP); Mitglied im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF).

Insofern steht weder zu erwarten – noch wäre dies wünschenswert –, dass mit dem nun gefassten Beschluss die inhaltlichen Debatten an der Universität Bremen enden werden. Hierfür ist das aktuelle Bekenntnis zu ziviler Forschung eine gute gemeinsame Basis und eine konkrete Ausgangsposition.

Beschluss und Wortlaut

Ausgesprochen erfreulich – und erkennbar für viele überraschend – hat nach monatelanger, intensiver und oft kontroverser Diskussion der akademische Senat der Universität Bremen am 25. Januar 2012 dem nachstehenden Beschluss mit überwältigender Mehrheit in allen Gruppen zugestimmt – bei nur drei (professoralen) Enthaltungen und einer (studentischen/RCDS) Gegenstimme:

> *„Der Akademische Senat steht weiterhin zu den Grundsätzen des Beschlusses Nr. 5113 (X/24. Sitzung v. 14. Mai 1986, insbesondere zur Ablehnung jeder Beteiligung von Wissenschaft und Forschung mit militärischer Nutzung bzw. Zielsetzung: Forschungsthemen und -mittel, die Rüstungsforschung dienen könnten, sind öffentlich zu diskutieren und sind ggfls. zurückzuweisen) und des Beschlusses Nr. 5757 (XIII/6. Sitzung vom 26.06.1991; Verpflichtung der Universität Bremen auf zivile Forschung). Der Akademische Senat stellt fest: Die Universität Bremen ist dem Frieden verpflichtet und verfolgt nur zivile Zwecke. Dies ist Bestandteil der Leitziele der Universität."*

Referenzen

Banik, P. / Rechtsstelle Universität Bremen (20.07.2011): Vereinbarkeit der Zivilklausel mit dem geltenden Recht. (Vermerk für die LRK-Sitzung am 25.07.2011).

Liebert, W. (2009): Umgang mit Dual-Use von Technologien und Ambivalenz in der Forschung. In: Albrecht, S.; Bieber, H.-J.; Braun, R.; Croll, P.; Ehringhaus, H.; Finckh, M.; Graßl, H.; von Weizsäcker, E.U. (Hrsg.): Wissenschaft – Verantwortung – Frieden: 50 Jahre VDW. Berlin: Berliner Wissenschafts-Verlag, S.445-450.

Rotblat, J. (1995): Remember your Humanity. Rede zur Verleihung des Friedensnobelpreises. http://www.pugwash.org/award/Rotblatnobel.htm

Streibl, R.E. (2011): Für eine zivilisierte Bildung und Wissenschaft. In: FIfF-Kommunikation, 28 (4), S.44-50.

Die Erstveröffentlichung dieses Beitrages erfolgte 2012 in der Zeitschrift »Wissenschaft und Frieden«.

Andreas Seifert

Interaktiver Rüstungsatlas

– eine Projektinitiative der IMI –

Am 9. Dezember 2011 veranstaltete die Informationsstelle Militarisierung (IMI) *e.V. in Tübingen ein Treffen, auf dem bisherige Überlegungen zur Schaffung eines überregionalen Web-basierten Rüstungsatlas dargestellt und mit den an einer Kooperation interessierten TeilnehmerInnen diskutiert wurden. Interessant ist ein Rüstungsatlas als Arbeitsmittel für die Friedensarbeit. Mit Hilfe der heute verfügbaren Werkzeuge für die Gestaltung und den Betrieb interaktiver Websites könnte ein hoher Nutzungskomfort geboten und eine dynamische Aktualisierung ermöglicht werden. Wir stellen die Ergebnisse des Workshops im Folgenden zusammengefasst dar, um eine Grundlage für weitere Diskussionen und einen Anreiz für weitere Interessierte zu bilden mit dem Ziel, ein konkretes Projekt zu formulieren und Fördermittel für seine Realisierung einzuwerben.*

Was ist ein Rüstungsatlas?

Rüstungsatlanten sind bisher für mehrere Bundesländer erschienen (z. B. Hessen, Niedersachsen) – sie variieren in Aufbau und Stoßrichtung. Gemein ist allen, dass sie Informationen zu Rüstungsunternehmen und Militärstandorten enthalten und deutlich machen, dass Militär- und Kriegsmaschinerien bis in die letzten Zipfel der Republik verteilt sind. Im engeren Sinne sind sie allerdings kaum Atlanten, da sie selten mehr als eine einzige Karte enthalten. So könnte der jüngst erschienene Band zu Bremen als Rüstungsstandort durchaus auch das Label „Atlas" für sich in Anspruch nehmen. Ein „Rüstungsatlas", wie er hier verstanden werden soll, hat das Ziel, mit Hilfe von Karten, Grafiken und Texten über Rüstung und Militär zu informieren.

Als Beispiel beschreiben wir unser derzeitiges Projekt „Rüstungsatlas Baden-Württemberg". Während dieses Projekt noch auf eine Veröffentlichung in Broschürenform zielt, wird mit der anschließend dargestellten Initiative „Interaktiver Rüstungsatlas" die Entwicklung einer dynamischen Internetplattform zur überregionalen Sammlung und Darstellung aller in diesem Zusammenhang relevanten Information angestrebt. Ist der erste Teil vor allem ein Sachstandbericht mit konkreten Angeboten zur Beteiligung, so ist der zweite Teil vor allem als Anregung für die weitere Diskussion gedacht.

Die Vorgeschichte, ein Rüstungsatlas Baden-Württemberg

Die seit Jahren schwelende Idee, einen Rüstungsatlas mit den relevanten Informationen zu Militär und Rüstung in Baden-Württemberg aufzubauen, wurde von der IMI aufgegriffen. Sie soll in einer Printpublikation umgesetzt werden. Ziel einer solchen Publikation ist es, den Friedensinitiativen und interessierten Menschen einen Überblick über die Themen Rüstung und Militär in

Baden-Württemberg zu vermitteln. Der Atlas soll anregen, sich für den Frieden zu engagieren, und soll dem Protest Argumente und Hintergrundwissen vermitteln.

Kernpunkte des Atlas werden in vier Kapitel behandelt: Militär und Militäreinrichtungen in Baden-Württemberg, Rüstungsindustrie in Baden-Württemberg, Forschung für den Krieg und Forschung für die Sicherheit, Friedliche Alternativen und Möglichkeiten zum Protest. Jeder der Bereiche wird mit Karten und Grafiken versehen, die die vorgesehenen kurzen Texte begleiten und veranschaulichen. Jeder der Bereiche soll zudem mit einem Verzeichnis ergänzt werden, das Adressen und weitere Daten enthält.

Die Broschüre wird ca. 60 A4-Seiten umfassen. Höhe der Auflage und des Preises werden ermittelt, sobald wir den Umfang sicher abschätzen können. Redaktion und Herausgeber der Broschüre wird die Informationsstelle Militarisierung (IMI) e.V. sein. Autoren sollen aus allen Spektren und Zusammenhängen kommen – viele sind bereits angefragt, einige Themen sind noch offen. Bei Interesse an aktiver Mitarbeit bitten wir, uns anzusprechen und sich von uns über offene Themen oder Punkte informieren zu lassen. IMI ist offen für weitere Partner (-Organisationen), die als Mitherausgeber fungieren wollen. Denkbar ist auch das Modell, dass eine Organisation oder eine Einzelperson Herausgeber wird, indem sie die Abnahme einer bestimmten Anzahl an Broschüren zusagt und dann auch im Impressum geführt wird. Bei Interesse bitten wir, uns anzusprechen.

Ein interaktiver, zur Mitarbeit aktivierender Rüstungsatlas

Im Zuge der Überlegungen zur Print-Publikation entstand der Plan, eine zeitgemäße Form zu finden, die auch jüngere Leute über deren Informationsgewohnheiten anspricht. Dabei ist die Idee eines Web-basierten Rüstungsatlas keineswegs neu. Sie wurde bereits an anderer Stelle (z. B. im FIfF) geäußert. In Teilen wurde sie sogar schon in einzelnen Institutionen (z. B. BICC oder Linkspartei, Inge Höger) umgesetzt. Kernpunkt der Idee ist es, einen visuellen, an einer Landkarte orientierten Zugang zu relevanten Daten über das Internet zu bekommen. Die Informationen sollen über einen intuitiv zu bedienenden Mechanismus zugänglich sein. Benutzer und Benutzerinnen sollen sich mit wenigen Klicks zu den für sie interessanten Punkten durchfinden.

Ausgehend von der Frage, wer als der potenzielle Benutzer angesehen wird, ergeben sich Struktur und aufzunehmende Inhalte. Zentral ist dabei die Frage nach dem Nutzen einer solchen Website für ihre Benutzer. In der Diskussion wurden mehrere Modelle angesprochen und verschiedene Nutzergruppen in den Fokus genommen. Ausgehend von der oben genannten Print-Publikation könnte man sich zunächst auf das Anbieten von Information beschränken, d. h. eine letztlich relativ statische (und vergleichsweise einfach zu administrierende) Website schaffen, die im Internet, in diesbezüglichen Datenbanken etc. verfügbaren Informationen aufgreift und auf einer – z. B. Deutschland-weiten – Landkarte präsentiert. Will man hingegen aktivierend in die Friedensbewegung hinein wirken, muss eine viel größere Vielfalt der Interaktion angeboten werden. Ergebnis wäre dann eine Website, auf der autorisierte Nutzer selbst Inhalte in die Karte einfügen und sie somit als Plattform für die Vernetzung der Akteure und des Protestes nutzen können.

Mögliche Nutzergruppen, thematische Schwerpunkte

Setzt man den Schwerpunkt auf das im Titel genannte Feld der Rüstung – Rüstungsproduktion, Rüstungsforschung, Rüstungshandel –, dann folgt daraus ein Bedarf an konkreter Information zu einzelnen Firmen bzw. Institutionen, zu ihren Standorten, zu Personen in ihren Schlüsselpositionen, zu Produkten, deren Käufern und Verwendung (und, wo bekannt, den durch sie verursachten Schäden), zu politischen Verflechtungen auf bundes-, landes- oder lokalpolitischer Ebene. Nutzer können sich in eine bestimmte Stadt „hineinzoomen" und erhalten mittels Klick auf einzelne Fähnchen (Buttons, Pfeile, Marker oder ähnliches) konkrete Informationen zu einzelnen in dieser Hinsicht relevanten Firmen. Man kann hier z. B. auch Informationen zu den gesellschaftlichen oder politischen Aktivitäten entsprechender Firmen aufnehmen (z. B. Schulpartnerschaften, Sponsoring) bzw. Forschungsaktivitäten und Querverbindungen zu Hochschulen aufzeigen, so sie verfügbar sind. Sind spezielle Recherchen erforderlich, ergeben sich neue Probleme.

Eine solche Website bedient das Bedürfnis nach Information nur bis zu dem Grad, der sich aus den erreichbaren Informationsquellen (z. B. Datenbanken) ergibt. Nutzer, die umfassende Informationen und Fakten zu übergeordneten Zusammenhängen erwarten, werden sich einer solchermaßen statischen Website nur eingeschränkt bedienen. Der Fokus allein auf Rüstung und Rüstungsindustrie schränkt den Nutzerkreis auf Friedensinitiativen mit entsprechenden Aktivitäten und Lokaljournalisten ein.

Bedacht werden muss auch, dass speziell Rüstungsaktivitäten kein nationales, sondern ein transnationales Feld sind. Der geografische Rahmen Deutschland würde sicherlich nur beschränkt aussagefähig sein. Er müsste zumindest auf Europa erweitert werden.

Erweitert man den Fokus um weitere (immer noch statische) Elemente, wie z. B. Standorte der Bundeswehr, wichtige Militäreinrichtungen, so wird dies zwar den Nutzerkreis erweitern, aber nichts am grundsätzlich eingeschränkten Umfang der Nutzungsmöglichkeiten ändern.

Eine essenzielle Erweiterung seiner Nutzungsmöglichkeiten erfährt ein Rüstungsatlas, wenn z. B. dem Protest gegen bestimmte Firmen oder Standorte sowie den Friedensinitiativen vor Ort ebenfalls Platz eingeräumt wird. Adressen von Initiativen vor Ort, von involvierten Gruppen, Zusammenschlüssen, Verbänden wie DFG-VK, ORL sind öffentlich zugänglich und ließen sich problemlos einfügen. Mit diesem Schritt würde ein erster Schritt zur unmittelbaren Aktivierung von Nutzern der Website geleistet.

Bis zu diesem Punkt wären alle Informationen mit einem eher geringen Aufwand aktuell zu halten. Je detailreicher die Infor-

mationen sind, desto aufwändiger wird dies jedoch. So müssten beispielsweise übergreifende Texte, die über Schaltflächen neben der Landkarte aufgerufen werden können und eine Einordnung der präsentierten Daten erlauben, mindestens in größeren zeitlichen Abständen überarbeitet und aktualisiert werden.

Die Einbeziehung der Nutzer und ihres speziellen Wissens

Erweitert man den Fokus der Website, wie oben schon erwähnt, um das gesellschaftliche Engagement von Rüstungsfirmen – z. B. um die Diskussion über „Schule und Bundeswehr" oder um den Komplex Rüstungsforschung – so ergeben sich grundsätzliche erweiterte und andersartige Nutzungsmöglichkeiten, die natürlich auch andere Interaktionsmöglichkeiten bieten oder sogar erfordern. Für einen fiktiven pazifistisch eingestellten Nutzer vor Ort mag es von Interesse sein, zu erfahren, dass die Schule, auf die er seine Kinder schickt, von einem Rüstungsunternehmen gesponsert wird – eine Information, die meist nur lokal bekannt ist. Sie kann aber auf der Website nur eingetragen werden, wenn der Administrator davon erfährt. Das ist für eine bundesweite Seite nicht zu leisten, wenn auch diese nur für lokale Nutzer interessierenden Informationen zentral eingepflegt werden müssen. Man kann den Nutzen für lokale Initiativen über einen bestimmten Punkt hinaus nur erhöhen, wenn man diese aktiv in die Arbeit mit einbezieht und ihnen die Möglichkeit einräumt, selbst Informationen einzupflegen.

Am Beispiel der Rüstungs- und Sicherheitsforschung an Hochschulen lässt sich ein solcher Ansatz und sein Potenzial verdeutlichen. Die Informationen über konkrete Forschungsprojekte und deren Inhalte sind nur denen bekannt, die sich mit dem Komplex auseinander setzen, bzw. Zugang zu solchen Informationen an ihrer Hochschule haben. Solche Infos auf einer Website zu präsentieren ist neu. Es würde die Arbeit derjenigen unterstützen, die bundesweit kritisch an diesem Thema arbeiten, da erstmals umfassende Fakten dazu zusammengetragen werden würden. Zum anderen würde es die örtlichen Gruppen unterstützen, die meistens kaum einen direkten Kontakt in die entsprechenden Fachbereiche haben. Es ließen sich dann nicht nur Infos zu den Projekten, sondern auch solche zu dem Protest dagegen, zu den jeweiligen Hintergründen und zu den involvierten Initiativen unterbringen. Der Vernetzung der Akteure würde wirkungsvoll Vorschub geleistet. Kombiniert mit den Informationen über Firmen, die als Partner der Rüstungs- oder Sicherheitsforschungsprojekte auftreten, ergäben sich schnell ein Überblick über die Zusammenhänge und damit konkrete Anknüpfungspunkte für Kritik und Protest.

Gleiches gilt im Übrigen auch für die *klassische* Friedensbewegung. Wäre es möglich, die lokalen Proteste mittels einer solchen Website virtuell sichtbar zu machen, kann ein überregionaler Austausch effektiver gestaltet werden. Aktionen anderer Gruppen, konkrete Erfahrungen mit bestimmten Protestformen sowie schlagkräftige Argumente lassen sich austauschen. Dazu ist es nicht einmal notwendig, alle Informationen unmittelbar zu integrieren. Sie müssen nur zusammengeführt werden *können*. So kann ein Fähnchen, das einen Protest anzeigt, auf einen ausführlichen Bericht auf den Web-Seiten der jeweiligen Initiative verweisen. Thematische Blogs mit ihren diesbezüglichen Beiträgen können auf dieselbe Weise eingebunden werden, sodass sich auch ihnen damit ein neues Potenzial erschließt.

Nehmen wir als Beispiel die Aktion *Aufschrei*. Sie würde mit ihren vielen Events an Sichtbarkeit gewinnen, wenn jede Aktion mit einem kleinen Fähnchen verzeichnet wäre. Dabei würde es nicht nur darum gehen, auf Ereignisse hinzuweisen (und damit ein im besten Fall neues Publikum zu erreichen), sondern auch das Potenzial für weitere Veranstaltungen auszuloten. Andererseits würde das Potenzial der Website, Detailinformationen über die Produktion einzelner Waffen bereitzustellen, für Kampagnen der Aktion hilfreich sein. Sich alle Standorte der Zulieferer und Komponentenhersteller einer Waffe wie dem *Leopard II* mit einigen Klicks anzeigen zu lassen, böte die Möglichkeit, örtliche Initiativen zu lokalisieren und zur Vernetzung zu motivieren und die Kampagne damit schlagkräftiger zu machen. Gleiches gilt für andere laufende Projekte wie z. B. das Bundeswehr-Monitoring.

Technisch sollte sich die Komplexität jedoch in Grenzen halten lassen, indem die Website konsequent in verschiedene Layer strukturiert wird. Eine möglichst weitgehende Dekomposition der Layer und Entflechtung der jeweils spezifischen Information, entkoppelt einerseits die Entwicklungsarbeit. Andererseits trägt eine solche Architektur dazu bei, dass die Nutzer nicht mit Informationen überschwemmt werden, sondern eine Auswahl nach vorgegebenen thematischen, geografischen oder zeitlichen Gesichtspunkten erhalten.

Die Kernforderung an eine Erweiterung der prospektierten Website in der dargestellten Weise ist es also, dass den Nutzern der Website Raum für eigene Beiträge und Informationen eingeräumt wird und Funktionen angeboten werden, diese sachgerecht einzubinden und strukturiert darzustellen. Der primäre Zweck wäre es, damit mehr Menschen zu motivieren, sich bestehenden Aktionen anzuschließen oder neue zu initiieren. Das Ergebnis wäre in jedem Fall die Stärkung der Bewegung durch die neue interaktive Plattform. Das enorme Potenzial eines Ansatzes, der in der Aktivierung vieler Einzelpersonen für Informationsbeschaffung und Aktionismus liegt, ist unübersehbar.

Folgerungen für ein *aktivierendes* Konzept

Ein hoher Grad an Interaktion zieht fast zwangsläufig eine große Gruppe von aktiven Beitragenden nach sich. Die ist zwar einerseits gerade das Ziel dieses Ansatzes. Es erfordert jedoch neue Mechanismen der Administration, die den neue Möglichkeiten der Vernetzung Rechnung tragen und die neue Wissensbestände, die über die grafische Aufbereitung vorhandener Datenbanken hinaus gehen, angemessen verwalten können. Zu lösen bzw. zu bearbeiten sind

- die Methode, wie Nutzer ihre Beiträge einstellen – in technischer, administrativer, inhaltlicher, gestalterischer Hinsicht,
- welcher Art die aufzunehmenden Inhalte sein sollen,
- ihre Aufbereitung (Darstellung, Layer-Einbettung),
- die inhaltlichen Betreuung der Einträge (Redaktion oder Community),

- die Aufrechterhaltung der Aktualität, die Gewährleistung einer zeitlichen Überprüfung der Einträge,
- rechtliche Fragen bezüglich Haftung,
- die Einwerbung einer dauerhaften finanziellen Absicherung der Website,
- die Festlegung des geografischen Bereichs (z. B. ganz Deutschland) mit Andockfähigkeit für Initiativen in anderen Ländern,
- das Konzept der technischen Umsetzung und
- Wege, wie Initiativen und Einzelpersonen zur Mitarbeit motiviert werden können.

Jeder dieser Punkte ließe sich weiter ausdifferenzieren.

Klar sollte sein, dass ein solches Konzept das Potenzial hat, eine Eigendynamik zu gewinnen, und man jetzt kaum abschätzen kann, wie weit das mit der prospektierten Website zu schaffende Potenzial genutzt werden kann und genutzt werden wird, wie weit es die hohen Erwartungen erfüllen können wird. Deutlich ist aber auch, dass es sich nicht um ein Projekt handelt, dass nebenher gestaltet werden kann, sondern um eines, dass den vollen Einsatz mindestens einer (bezahlten) Person erfordert.

Umsetzung

Abhängig vom Umfang der prospektierten Website variieren die Kosten und der nachfolgende Administrationsbedarf erheblich. Je größer die Site sein soll, desto breiter sollte deshalb auch ihre Trägerschaft aufgestellt sein. Auch wenn man sich nicht für das umfassendste Modell entscheidet, so wird es ohne eine beträchtliche Anschubfinanzierung nicht umsetzbar sein. Zudem sollte man sich bewusst werden, dass, wie immer das Projekt aussieht, eine mittelfristige Perspektive (drei Jahre Betrieb) unumgänglich ist. Entscheidet man sich für das umfassendere Modell – die Funktionalität der Website bietet dem Nutzer die Möglichkeit, *seine* Information einzubringen –, muss man sich auch über die Strategien Gedanken machen, wie man Initiativen vor Ort zur Mitarbeit motiviert.

Auf dem Treffen wurden verschiedene Vorschläge unterbreitet, wie eine Finanzierung aussehen könnte, Modelle wurden diskutiert und potenzielle Geldgeber (z. B. Stiftungen) vorgeschlagen. Allen Antragsideen ist gemein, dass es einen Kreis der Beantragenden geben soll, der als Gruppe von Institutionen und/oder Einzelpersonen einen Antrag formuliert. Dieser Trägerkreis übernimmt die Verantwortung und beschäftigt die für den Aufbau benötigten Entwickler, sowie später die für den Inhalt verantwortlichen Redakteure. Ihre konkreten Aufgaben werden sich nach der zu beschließenden Ausgestaltung des Projektes richten.

Das Maximalprojekt, ein *aktivierender* Web-basierter „Friedensatlas" – der vorläufige Titel –, würde für eine Laufzeit von drei Jahren beantragt werden, nach deren Ablauf sich der Trägerkreis um eine Anschlussfinanzierung bemühen müsste. Das Maximalprojekt besteht dabei aus den folgenden Positionen:

- Ressourcen für die Programmierung der Website und aller Module zur Interaktion mit den Nutzern und deren technischer Betreuung.
- Ressourcen für eine Redaktion, d. h. für eine Person, die die Nutzereinträge inhaltlich und rechtlich prüft und selbst welche verfasst und einstellt sowie weitere Personen dazu motiviert, relevante Daten bereitzustellen. Sie übernimmt die Pflege der Daten und organisiert Öffentlichkeit (z. B. Workshops und Präsentationen auf den Events der Friedensbewegung). Sie bearbeitet das Feedback der Nutzer.
- Ressourcen für Betriebs- und Nebenkosten (Serverplatz, Reisekosten, Kommunikationskosten).
- Eine Geschäftstelle, die vom Trägerkreis gestellt werden würde.

Eine vorläufige Schätzung des erforderliche Aufwandes ergab ein Antragsvolumen von knapp 70.000 €, zu verteilen über eine Projektlaufzeit von drei Jahren. Darin enthalten sind einmalige Kosten vornehmlich für die Programmierung und die Einrichtung des Arbeitsplatzes (ca. 6.000 €) sowie laufende Kosten für die Redaktion, Kommunikation, Reisen und Serverbetrieb (ca. 21.000 € p.a.). Bei der Frage möglicher Förderer wurden verschiedene Vorschläge geäußert, u.a. gewerkschaftliche, kirchliche und politische Stiftungen, aber auch die Bewegungsstiftung. Zur Antragsstellung sollten jedoch alle konzeptionellen und inhaltlichen Fragen wie Art und Umfang der aufzunehmenden Inhalte sowie deren Verknüpfung und Präsentation geklärt sein.

Andreas Seifert

Andreas Seifert ist Vorstandsmitglied der Informationsstelle Militarisierung (IMI) e.V. in Tübingen. Die IMI erarbeitet Analysen und Studien zum Komplex Krieg und Frieden.
Mehr Informationen auf unserer Homepage *http://imi-online.de*

Schlusswort

Die hier skizzierte Idee sollte als Ansatzpunkt für weitere Diskussionen verstanden werden, nicht als fertiges Konzept. Wir halten es für notwendig, die vorhandenen Kompetenzen aus den unterschiedlichsten Bereichen zusammenzubringen und ein gemeinsames Projekt auf die Beine zu stellen, das am Ende auch von allen genutzt werden kann. Bei Interesse am Mitmachen oder auch mit Kommentaren kann man sich gerne an den Autor wenden: *ruestungsatlas@imi-online.de*.

Anmerkungen

1 Alex Klein: „Der Rüstungsatlas – ein interaktives Informationsportal zu Rüstungs- und Militärstandorten in Deutschland". AG4 auf der FIfF-Jahrestagung 2008 „Krieg und Frieden – digital", Aachen, 7.–8.11.2008, http://kufd.de/arbeitsgruppen

2 http://bicc.de/our-work/gmi.html

3 http://ruestungsatlas.de

Appell aus Berlin!

Für ein kontrollierbares Abkommen zur Abschaffung aller Atomwaffen

Wir Teilnehmer an der Abschlusssitzung der Konferenz „Vom atomaren Patt zu einer von Atomwaffen freien Welt – Zum Gedenken an Klaus Fuchs", veranstaltet von der Leibniz-Sozietät der Wissenschaften und dem Russischen Haus der Wissenschaft und Kultur, unterstützt durch die Deutsche Gesellschaft für Kybernetik, rufen alle in der Forschung und Entwicklung Tätigen, alle Politikerinnen und Politiker, alle friedliebenden Menschen dazu auf, sich für ein kontrollierbares Abkommen zum Verbot und zur Vernichtung aller Kernwaffen – als ein Gebot der Vernunft – einzusetzen.

Die Atombombenabwürfe am 6. und 9. August 1945 auf Hiroshima und Nagasaki forderten hunderttausende Opfer. Auch bei den Kernwaffenversuchen der nachfolgenden Jahre waren zahlreiche Opfer zu beklagen.

Der Kalte Krieg war von der realen Gefahr einer nuklearen Katastrophe geprägt.

Der Internationale Gerichtshof entschied 1996, dass Kernwaffen keine Waffen im Sinne des Kriegsrechts sind. Ihr Einsatz ist in keiner Weise zu rechtfertigen. Frieden in Freiheit ist nicht durch das Vorhandensein von Massenvernichtungswaffen zu erreichen.

Eine Reihe von Staaten erkennt das Urteil des Internationalen Gerichtshofs nicht an. Die Anzahl der Atomwaffen besitzenden Staaten hat sich erhöht und es besteht die reale Gefahr, dass sie sich weiter erhöhen wird. Riesige Kernwaffenlager existieren. Ihre Existenz wird mit immer neuen Argumenten gerechtfertigt. Eine Modernisierung von Atomwaffen wird angestrebt. Die Gefahr der Selbstvernichtung der Menschheit und ihrer Lebensbedingungen wächst weiter.

Wir fordern die national und international wirkenden Politikerinnen und Politiker auf, das Ziel der Abschaffung aller Atomwaffen unmittelbar und mit Nachdruck zu verfolgen. Es ist im Atomzeitalter wider die Vernunft, Krieg als geeignetes Mittel zur Wiederherstellung verletzter Rechte zu betrachten. Angesichts der Gefahr einer völligen Vernichtung der Menschheit gibt es keinen gerechten Krieg und auch keine gerechte Revolution, die den Einsatz solcher Waffen rechtfertigen würden. Soziale Ungerechtigkeiten sollten auf friedlichem Wege überwunden werden.

Wir sind der festen Überzeugung, dass alle Kernwaffen verboten und vernichtet werden müssen, damit die Gefahr einer völligen Vernichtung der Menschheit gebannt wird. Dieses Ziel zu erreichen ist nicht leicht! Es ist dazu unbedingt erforderlich, ein überprüfbares Abkommen zu erarbeiten, abzuschließen und alle Nationen daran zu beteiligen!

Alle Wissenschaftlerinnen und Wissenschaftler, besonders die in der Atomforschung und Waffenentwicklung wirkenden, sind aufgerufen, gemeinsam mit allen humanistischen friedliebenden Kräften auf dieses Ziel hinzuarbeiten.

Wichtige Schritte in diese Richtung wären der Abzug der taktischen Kernwaffen von deutschem Boden und die Schaffung einer kernwaffenfreien Zone in Mitteleuropa.

Berlin, den 26. November 2011

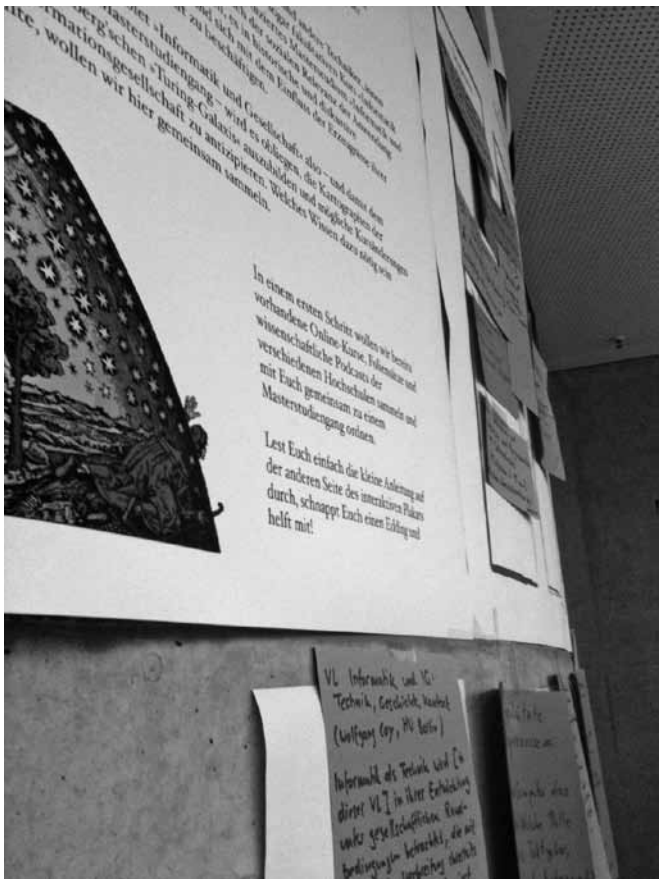
Andrea Knaut, Jörg Pohle, Stefan Ullrich

Keine Panik

Subject: subscribe Master-Studiengang „Informatik & Gesellschaft“

Wer im Rahmen eines Informatikstudiums ahnt, dass viele informationstechnische Innovationen nicht immer nur Spaß machen, die Welt retten oder Geld bringen; wer ahnt, dass sich informatische Theorie nicht allein um Effektivitäts- und Effizienzsteigerungen oder mathematische Optimierungsprobleme dreht, dass IT und ihre Nutzung insgesamt politische und soziale Sphären widerspiegeln und Teil dieser sind; dass mit Hilfe von IT-Systemen auch getötet wird und Menschen ersetzt werden; wer Softwarefehler ernst nimmt und das Verständnis von Elektrotechnik, formaler Sprachen, Datenbanksystemen und Software-Entwicklung als Teil digitaler Mündigkeit betrachtet und es entkoppeln kann und will von Geek- und Guruwissen, der oder die fand an deutschen Universitäten hin und wieder Lichtblicke im sogenannten Gebiet der *Informatik und Gesellschaft* (I&G) – hin und wieder eben. Für akademisch qualifizierte Informatikerinnen gehört gesellschaftlich verantwortungsvolles Handeln nicht zu den Kernkompetenzen, was angesichts des Lehrplans auch nicht verwunderlich ist.

Wieso also nicht endlich einen eigenen Master-Studiengang Informatik und Gesellschaft etablieren? Diese Idee haben drei Anhalterinnen der Turing-Galaxis auf der FIfF-Jahrestagung in München als Mitmach-Plakat ins Spiel gebracht. Und tatsächlich: Die Tagungsbesucherinnen haben mitgemacht. Viele von ihnen verweilten vor dem Plakat und es gab interessiertes und durchweg positives Feedback. Wo der Studiengang denn angeboten würde, fragten einige; doch so weit sind die Anhalterinnen noch nicht, sie sind zunächst noch auf archivarischer Suche nach den vielen Skripten, Video- und Audiomitschnitten, die in den letzten Dekaden der I&G dezentral an verschiedenen Hochschulen und Fachhochschulen oder in Netzwerken von Wissenschaftlerinnen an den Schnittstellen verschiedener Disziplinen, bei Bürgerrechtsaktivistinnen oder „Hobbyhackerinnen“ entstanden sind. Bisher – und das fiel auch in den Gesprächen auf der Konferenz auf – war I&G stark personengebunden und die Nachhaltigkeit und Kanonisierung ihrer Erkenntnisse war dementsprechend eingeschränkt. Viele bereits vorhandene Materialien sind schwer zugänglich oder gar verschwunden.



Das Mitmach-Plakat auf der FIfF-Jahrestagung in München

Es zeigte sich etwa, dass ein Bedarf nach einer methodologischen Fundierung des I&G-Forschungsgebietes besteht. In einem Propädeutikum im ersten Semester sollte demnach in diskursanalytische, systemtheoretische, dialektische oder andere fortgeschrittene Praktiken wissenschaftlicher Arbeitsweisen eingeführt werden. Klassische, eigentlich zum Grundrepertoire der I&G gehörende, Vorlesungen zur Geschichte der Informatik, der Arbeitsweise des Computers als Digitalmedium und technikphilosophischer Grundlagen bieten sich ebenfalls für die erste Hälfte des (Master-)Studiums an. Des Weiteren wurden diverse Veranstaltungen für Themen an den Schnittstellen zur Kunst, zu Medien-, Film-, Kunst-, Kultur- oder Theaterwissenschaften angeregt.

Einige Konferenzteilnehmerinnen konnten bereits Ressourcen für das Selbststudium oder zumindest Hinweise auf durchgeführte Lehrveranstaltungen anbieten, und sie halfen auch bei ersten Ansätzen für eine Strukturierung des viersemestrigen Studienganges. So gibt es etwa an der Humboldt-Universität seit Jahren die Vorlesungsreihe *Digitale Medien* (Coy)[1] mit zugehörigen Praktika, Teile davon stehen als Podcasts[2] zur Verfügung und können als Materialien für den Studiengang dienen. Die Uni Hamburg stellt in ihrem Videocast-Portal *Lecture2Go* neben klassischen Informatikthemen auch eine Vorlesung zu Informatik im Kontext (Rolf)[3] bereit. Auch außeruniversitäre Einrichtungen bieten sinnvolle Ressourcen zum Selbststudium an. So präsentiert das Unabhängige Landeszentrum für Datenschutz (ULD) Schleswig-Holstein etwa Interviews zur Geschichte und Programmatik des Datenschutzes in Deutschland (Rost)[4].

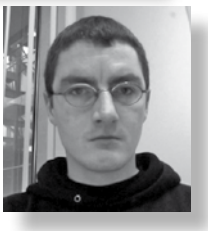
Zu vielen bereits durchgeführten Veranstaltungen liegen jedoch keine Materialien (mehr) vor, hier würden sich die Anhalterinnen über sachdienliche Hinweise der Leserinnenschaft freuen. Während der Tagung erzählten einige Teilnehmerinnen beispielsweise innerhalb der Workshops über verschiedene Projekte, deren Materialien ebenfalls sehr gut für das Studienprogramm in Semester III und IV geeignet sind. So werden auf

dem Theater-Campus der HTWG Konstanz Berufssituationen von Informatikerinnen im sogenannten Business-Theater nachgestellt – szenische Drehbücher für Rollenspiele in Bezug auf ethische Dilemmata oder aber auch vielleicht im Sinne des epischen Theaters Brechts können als aufklärerische Stücke hinsichtlich diverser Überwachungsszenarien des Alltags aufbereitet und bereitgestellt werden. Die vielen bereits vorhandenen Beiträge zur Rolle der Informatik in Rüstung und Militär, zur Kritik falscher Bilder der psychologischen Bedeutung des Computers in der Sozialisation und zum Umgang mit selbigem im Alter, zu umfassenden Materialien zur Geschlechterforschung in der Informatik, zu denen an den Universitäten in Freiburg, Bremen oder Berlin geforscht wurde und wird, sind willkommen. Auch die Seminare zu TOR und anderen Anonymisierungsdiensten, wie sie an der TU Dresden angeboten werden, oder Seminare zur Computerisierung der Arbeitswelt (bspw. Uni Bremen) reihen sich in die gesuchten Veranstaltungen ein. Ein weiterer wichtiger Bereich, der durch den Workshop zu FAIR IT auf der Tagung und den dort gezeigten Film *Behind the Screen* thematisiert wurde, ist die Erstellung von Handreichungen für Lehrerinnen zu diesem Thema. Das wirft auch die Frage eines allgemeinen Angebots lehrer- und schülergerechter Materialien aus der I&G für die Didaktik der Informatik auf. Ansätze dafür gibt es bereits im Projekt *Informatik im Kontext* (IniK)[5], eine bundesweite Initiative Bildungsverantwortlicher aus Hochschule und Schule.

Dies sind nun viele, bei weitem nicht alle auf der Konferenz angeregten Inhalte, teilweise noch immer gesucht, teilweise sogar schon zumindest in Form von Ansprechpartnerinnen gefunden. Es dürfte klar sein, dass die Anhalterinnen noch weiter suchen und gern mal hier und da eine Weile mitfahren, um mehr zu hören und zu lernen. Das Ziel der Reise ist bewusst offen gehalten. Die I&G-Wissenschaft hat es schwer, tritt sie doch als Mahnerin, Bremserin und Kritikerin innerhalb der fortschrittsgetriebenen Informatik auf. Der Wunsch nach Institutionalisierung eines Masterstudiengangs steht im Spannungsfeld einer drittmittelgestützten Universitätslandschaft mit von Projekten auf Zeit enttäuschten Visionärinnen und der Notwendigkeit, eine dem Menschen dienende Informatik zu professionalisieren und in ihrem Bestand abzusichern. Die Anhalterinnen halten daher zunächst alles, was sie von den erfahreneren Köpfen lernen können in ihrem Buch turing-galaxis.de/iundg[6] fest, das jeder Reisenden der Turing-Galaxis zugänglich und auf dessen Umschlag in freundlichen Buchstaben eingeprägt »KEINE PANIK« zu lesen ist. Der von vielen auf der Tagung geteilte Wunsch nach der weiteren Institutionalisierung der I&G im Rahmen eines solchen Studiengangs ist schließlich ohne Inhalte nicht realisierbar. Für Unterstützung bei weiteren Schritten zur Dokumentation und Zugänglichkeit des bereits Erkannten und Erreichten, sei es als Angebote oder Gesuche, Fragen oder Kritik, bedanken sich die *anhalterinnen@turing-galaxis.de*.

Anmerkungen

1 *http://waste.informatik.hu-berlin.de/Lehre/ws1011/VL_DigitaleMedien/mitschnitte.html*
2 *http://waste.informatik.hu-berlin.de/Lehre/ws1011/VL_DigitaleMedien/mitschnitte.html*
3 *http://lecture2go.uni-hamburg.de/veranstaltungen?p_p_id=gastVeranstaltungen_WAR_lecture2gogastspringportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1*
4 *https://www.datenschutzzentrum.de/interviews/*
5 *http://www.informatik-im-kontext.de/*
6 *http://www.turing-galaxis.de/iundg*



Andrea Knaut, Jörg Pohle, Stefan Ullrich

Andrea Knaut, ist Diplom-Informatikerin und arbeitet derzeit als wissenschaftliche Mitarbeiterin in der Arbeitsgruppe für Informatik und Gesellschaft an der Humboldt-Universität zu Berlin.

Jörg Pohle hat Rechts- und Politikwissenschaft sowie Informatik studiert, letzteres mit Diplom abgeschlossen, arbeitet als wissenschaftlicher Mitarbeiter in der Arbeitsgruppe für Informatik in Bildung und Gesellschaft an der Humboldt-Universität zu Berlin und promoviert zum Thema Datenschutz und Technik.

Stefan Alexander Ullrich, 1979 in Stuttgart-Bad Cannstatt geboren, ist seit 12 Jahren Wahlberliner und studierte Informatik und Philosophie an der Humboldt-Universität zu Berlin. Er arbeitet dort in der Arbeitsgruppe »Internet in Bildung und Gesellschaft« bei Prof. Wolfgang Coy. Seine Forschung zum Thema »Verantwortung des Informatikers« führte ihn zur Fachgruppe »Informatik und Ethik« der GI, deren Sprecher er seit nunmehr einem Jahr ist.

Britta Schinzel, Monika Götsch, Yvonne Heine, Karin Kleinn, Michael Richter

Verlernen Informatik-Studierende Verantwortungnahme?

Aus der DFG-Studie „Weltbilder in der Informatik“[1]

1. Die DFG-Studie „Weltbilder in der Informatik“

Die Durchdringung unseres Alltags mit Informationstechnologie ist umfassend und wird in Zukunft noch stärker werden, da in der Hoffnung auf wirtschaftliche Vorteile im globalen Konkurrenzkampf die Entwicklung der Informationstechnologie stark vorangetrieben wird. So wird durch die technische Architektur der Informationssysteme ein neues Problemfeld der Regulierung menschlichen Handelns geschaffen: Neben die traditionellen sozialen Regulierungsinstitutionen – Recht, Markt und soziale Normen – tritt der Code als weiterer Regulierungsmechanismus (Lessig 1999). Die herkömmlichen Regulatoren werden durch den Code nicht nur ergänzt, sondern auch gestaltet, umgeformt, kanalisiert oder sogar außer Kraft gesetzt.

Verschiedene Faktoren fließen in die Gestaltung des Codes/der Software mit ein. Zum einen sind die Anforderungen des Marktes bzw. der KundInnen zu nennen, welche meist diffuse, interpretationsbedürftige Anforderungen sind. Daneben fließen ebenso Technikleitbilder und die Arbeitskulturen mit ein. Diese Faktoren sind in unterschiedlichem Maße unscharf und werden im Verlauf der Anforderungsanalyse von den SoftwareentwicklerInnen interpretiert. Hier wirken die Weltbilder der EntwicklerInnen stark auf die Gestaltung der Software ein. Aber auch in späteren Phasen der Softwareentwicklung fließen Denkweisen, Einstellungen und Werte der SoftwareentwicklerInnen in die Entwicklung ein, denn SoftwareentwicklerInnen treffen alltäglich Entscheidungen, die für sich genommen oft belanglos erscheinen, aber die Richtung der weiteren Entwicklung bestimmen, indem sie manche Wege für den weiteren Verlauf der Entwicklung öffnen, andere aber verbauen. So wirken sich die Entscheidungen der EntwicklerInnen, die bei der Modellierung und Architektur, bei der Modularisierung und Schnittstellenbestimmung, beim Design der Benutzung – und dies in jeder Programmzeile – gefällt werden, auf die Ausgestaltung des Produktes aus. Diese Entscheidungen werden oft nicht aufgrund von formalen Methoden oder Qualitätsstandards getroffen, einmal, weil es sie nicht für jede Programmzeile gibt/geben kann, zum anderen weil Qualitätsstandards oft auch nicht explizit gemacht werden (Allhutter/Hanappi-Egger 2006). Das begünstigt die I-Methodology (oder Ego-Approach), d. h. diese Entscheidungen werden geleitet von den Einstellungen und Werten der Menschen, von ihren mentalen Konzepten getroffen, also von ihren Weltbildern beeinflusst. Doch obgleich InformatikerInnen und SoftwareentwicklerInnen die Welt derzeit mit am aktivsten verändern, indem sie den Code entwickeln, haben sie selten das Gefühl, die GestalterInnen der Zukunft zu sein.[2] Das hat mehrere Ursachen. Zum einen sind die meisten EntwicklerInnen nicht an vorderster Front tätig, wo es um neue Trends geht; so sehen sie sich nicht in der Position, große Veränderungen zu bewirken. Zweitens sind sie meist in große Entwicklungsteams eingebettet, deren Arbeitskulturen mit definierend sind (Bittner/Hornecker 2005), indem sie nicht nur Habitus, sondern auch Arbeitsabläufe bestimmen; und schließlich drittens sind die EntwicklerInnen selbst NutzerInnen bestehender Software, in die neu entwickelte Software und Vernetzung eingebettet wird und deren Protokolle und Eigenarten mit definierend sind, oder um die herum Anpassungen oder Anwendungen entwickelt werden. Auch sind bei größeren Projekten die EntwicklerInnen oft nur für Einzelteile der Software verantwortlich. Daher sieht sich „der kleine Informatiker am Endgerät“ oft einflusslos. Doch das zu Unrecht, denn alle InformatikerInnen haben Anteil an der „IT-schaffenden Kultur“, die das Verhältnis zwischen der IT-Profession, den NutzerInnen und den indirekt Betroffenen formt.

Auf die Weltbilder von InformatikerInnen und ihre (Um-)Prägungen durch das Studium der Informatik richtete sich das Forschungsinteresse dieser Studie. Dabei sollte auch auf die unterschiedlichen Fachkulturen an verschiedenen Universitäten und dabei unterschiedliche Weltbilder eingegangen werden. Daher befragten wir Informatikstudierende an fünf deutschen Universitäten, die in vielerlei Hinsicht eine möglichst breite Diversität abbilden sollten: die geografische Lage (Nord, Süd, Ost, West), Größe und Schwerpunkte der jeweiligen Fakultät und Universität (technische oder Humboldt´sche), Zusammenarbeit mit anderen Fachbereichen (z. B. geisteswissenschaftliche Wahlpflichtfächer), Universitätsranking sowie Traditionsuniversität vs. Reformuniversität. Als geeignet wählten wir die TU Dresden, die BTU Cottbus, die Universität Oldenburg, die TU Karlsruhe und die Universität Freiburg und fanden dort jeweils freundliche Kooperationspartner, die uns zum qualitativen Interview und zu Gruppendiskussionen bereite Studierende vermittelten.

Trotz der Vielfalt an Zugangsmöglichkeiten zu Berufen der IT-Entwicklung beschränkten wir uns in unserer Untersuchung auf Informatikstudierende an Universitäten, da die Universität der Ort ist, an dem die Zukunftsorientierung und die Weichen für die noch in Entwicklung befindliche Professionalisierung der Informatik gestellt werden. Die universitäre Informatik muss als wichtiger Ansatzpunkt für Veränderungen gesehen werden: Denn einmal werden zunehmend mehr SoftwareentwicklerInnen dort ausgebildet, zum anderen werden hier auch die zukünftigen HochschullehrerInnen – sowohl für die Universitäten als auch für die Fachhochschulen – herangezogen.

Mittels qualitativer Methoden wurden die Wahrnehmungs-, Bewertungs- und Handlungsmuster von Informatikstudierenden erfasst und analysiert. Weltbilder sind von weitreichender gesellschaftlicher Relevanz, da sie die Arbeit und so auch die Produkte der InformatikerInnen beeinflussen. Betroffen sind aufgrund der weiten Verbreitung der IuK-Technologien so gut wie alle Lebensbereiche mit sehr vielfältigen Anforderungen. Dieser Diversität auf der Anwendungsseite sollte eine ebensolche auf der Entwicklungsseite gegenüber stehen, um 1. der Vielfalt der Anwendungen gerecht zu werden und 2. wichtige Markterschließungs- und Wachstumspotenziale nicht zu verschenken. Diversität besteht in der Informatik nicht in ausreichendem Maße, weder bezüglich der Auswahl der Studierenden, was v.a.

(aber nicht nur) Frauen benachteiligt, noch – so unsere Hypothese – bezüglich der Weltbilder der Studierenden. Dazu tragen die Universitäten mit ihren jeweiligen Fachkulturen in unterschiedlichem Maße bei.

Wir gingen davon aus, dass Zusammenhänge zwischen den Fachkulturen und den individuellen Orientierungen schon vor Beginn des Studiums bestehen (aufgrund der impliziten Studierendennorm, vgl. Hauch/Horvath 2007), dass aber dennoch die Studierenden zu Beginn vergleichsweise wenig über Informatik wissen,[3] dass also das Studium nicht nur informatisches Wissen generiert, sondern auch Wissen um Informatik und ihre Weltbilder. Daher wurden Studierende am Beginn des ersten Semesters und solche in höheren Semestern interviewt. Am Ende wurden 20 Einzelinterviews mit Studierenden höherer Semester (davon 6 Frauen), 5 Gruppendiskussionen (mit insgesamt 18 Studenten und 2 Studentinnen höherer Semester), 20 Einzelinterviews mit Erstsemestern (davon 6 Frauen) für die Auswertung herangezogen. Das heißt es handelt sich um 60 Studierende (davon 13 Frauen, sowie 7 ausländische Studierende). Durchschnittlich (Median) waren die Studierenden der höheren Semester im 9. Semester und 25 Jahre alt, das Durchschnittsalter der Erstsemester lag bei 21 Jahren.

Ziel der Untersuchung war es, den Einfluss der verschiedenen informatischen Fachkulturen auf Weltbilder der Studierenden zu ermitteln, um Hinweise darauf zu erlangen, wie die Ausbildung der InformatikerInnen so gestaltet werden kann, dass die dringend nötige Diversität in der Informatik ermöglicht wird. Damit versteht sich die Studie als ein Beitrag sowohl zur Professionalisierung der Informatik als auch zu mehr Geschlechtergerechtigkeit. Im vorliegenden Beitrag beschränken wir uns auf jene Aspekte der Untersuchung, die im Zusammenhang mit der Übernahme bzw. Abweisung von Verantwortung stehen. Diese sind in komplexer Weise mit Technikbildern und Geschlechterbildern, aber auch mit allen anderen von uns erfragten Kategorien von Weltbildern verknüpft.

In unserer Studie wurden in einem zweistufigen Auswertungsprozess die am Ende von 2. genannten Weltbilder der Studierenden, die sich nicht direkt erfragen lassen, sondern vielmehr implizit als Deutungsmuster und in Alltagstheorien offenbaren, mittels qualitativer Methoden der Sozialforschung eruiert. Um die sozialisatorischen Effekte des Informatikstudiums und die Veränderungen der Weltbilder, die durch das Informatikstudium angestoßen wurden, zu erfassen, wurden die persönlichen Erfahrungen und Plausibilisierungen wie auch die gemeinsamen Deutungsmuster der Studierenden im Vergleich von StudienanfängerInnen mit Studierenden der höheren Semester analysiert. Im zweiten Phase wurden die Interviews und Gruppendiskussionen daraufhin ausgewertet, warum die Studierenden Informatik als Studienfach gewählt haben, welches Bild sie von Informatik sowie von Geschlecht in Zusammenhang mit Informatik haben und schließlich, wie sie durch das Studium kommen, kritische Situationen im Studium bewältigen. Dabei wurden subjektive Erklärungsmuster des eigenen Studienverlaufs, individuelles und kollektives (auch latentes) Sinnwissen der Studierenden sowie Sagbares und Nicht-Sagbares herausgearbeitet, um die Exklusions- und Inklusionsmechanismen im Informatikstudium zu erfahren.

Entgegen unseren Hypothesen waren die Unterschiede zwischen den Universitäten eher gering, auch Männer und Frauen unterschieden sich nicht so deutlich. Prägnanter dagegen war in einigen Fragen die Differenz zwischen Erstsemestern und höheren Semestern.

2. Zusammenhang zwischen Fachkultur und Weltbild

Der Kulturbegriff der akademischen Disziplinen (Fachkulturen) wird in der Regel im ethnologischen Sinne verstanden, der auf den gemeinsamen Lebensstil einer Gruppe und die damit verbundenen Werte, Konventionen, Verhaltensweisen und Beziehungen abhebt. Wichtig erscheint dabei der Zusammenhang

Auswahl der Universitäten und InterviewpartnerInnen

Universität	**Einzelinterviews** höhere Semester	**Gruppen-diskussionen** höhere Semester	Befragte **Frauen** und **Männer** höhere Semester	**Einzelinterviews** Erstsemester	Befragte **Frauen** und **Männer** Erstsemester
Albert-Ludwigs-Universität **Freiburg**	4	1 mit 5 Studierenden	1 ♀ 8 ♂	4	1 ♀ 3 ♂
Universität **Karlsruhe** (TH)	4	1 mit 4 Studierenden	1 ♀ 7 ♂	4	1 ♀ 3 ♂
TU **Dresden**	5	1 mit 3 Studierenden	2 ♀ 6 ♂	4	1 ♀ 3 ♂
BTU **Cottbus**	4	1 mit 4 Studierenden	1 ♀ 8 ♂	4	1 ♀ 3 ♂
Carl von Ossietzky Universität **Oldenburg**	5	1 mit 4 Studierenden	2 ♀ 7 ♂	4	1 ♀ 3 ♂

sozialer Praxen untereinander und ihre Fundierung in sozialen Strukturen, gleichzeitig aber auch, dass individuelle Stile und kollektive Muster (Habitus) durch Kultur ermöglicht werden, also nicht schon durch die Strukturen determiniert und auch nicht einfach manipulierbar sind.

Der Begriff des Weltbildes hat eher eine umgangssprachliche Bedeutung und bezieht sich jeweils auf einen Ausschnitt der Wirklichkeit, sodass jeder Mensch mehrere Weltbilder hat, die im Kontext einer bestimmten Kultur ausgeprägt werden. Weltbilder lassen sich als Gefüge von Wahrnehmungs-, Denk-, Bewertungs- und Handlungsmustern beschreiben, die sich durch sozialisatorische Praxis entwickeln, wobei sich spezifische individuelle Praxisstile (Praktiken, Werke, Rituale) und Denkstile (Konzeptionen, Bilder, Sprache) ausbilden.

Kultur und Weltbild stehen in Wechselwirkung zueinander, sodass je fachspezifisch geprägte Weltbilder innerhalb der unterschiedlichen Fachkulturen der Universität entstehen, die über das Denken und die Werte in das Handeln der FachvertreterInnen einfließen und damit Einfluss auf die Produkte ihrer beruflichen Tätigkeit haben. Die Fachkulturen manifestieren sich in anerkannten Mustern der Problemstellung und -bearbeitung, in geltenden Gütekriterien und Werten. Das wenigste davon wird explizit thematisiert, das meiste implizit durch die Ausbildungspraxis vermittelt und angeeignet. Der „heimliche Lehrplan" der Universitäten enthält aber nicht nur so genannte Sekundärtugenden wie Disziplin, Leistungskonkurrenz oder hierarchisches Denken, sondern auch inhaltliche Aspekte wie unthematisierte Prämissen und Verfahrenstraditionen der Fächer. Für Juristen zeigte Schütte (1982) eindrucksvoll, dass im Studium eine bestimmte Form der Zurechtlegung der Probleme eingeübt wird, sodass die Probleme juristisch behandelbar werden. Damit wird ein Zugriff auf die Wirklichkeit vermittelt, mit dem (nicht juristisch behandelbare) Teile der Wirklichkeit dezidiert ausgeklammert werden. Eine solche Untersuchung für die Informatik steht noch aus.

Die Frage nach dem Verhältnis zwischen Fachkultur und Weltbild kann unterschiedlich beantwortet werden: einmal erscheint der Fachhabitus als Sozialisationsergebnis in ein Fach, zum anderen kann davon ausgegangen werden, dass schon vor Studienbeginn eine Korrelation zwischen dem Weltbild der StudienanfängerInnen und der Fachkultur besteht. In jedem Fall begeben sie sich mit dem Eintritt in die Hochschule in den Einflussbereich einer neuen Kultur, die von ihrer Herkunftskultur mehr oder weniger verschieden ist, und sie bewegen sich in mehreren Kulturkreisen: der Herkunftskultur, der studentischen Kultur und der antizipierten Berufskultur. Diese Kulturen prägen das Individuum, das Weltbild ist Ausdruck dieser Kulturen auf der individuellen Ebene. Eine Entsprechung von subjektiver Erfahrungsgeschichte (erworbene Interessen, Gewohnheiten und Ziele) und disziplinärer Kultur aber trägt entscheidend zum Studienerfolg bei. Dass aber jedenfalls bei einem Teil der StudienanfängerInnen schon die Studienfachwahl auf der Affinität von individuellen Orientierungen mit Werten und Normen den Fachkulturen korrelieren, zeigen die Ergebnisse von Hauch/Horvath (2007) in Österreich, und sie legen nahe, dass schon vor Beginn des Studiums eine – scheinbar freiwillige – Auswahl an StudienanfängerInnen der Informatik stattfindet. In ihrer Studie identifizierten sie eine implizite „Studierendennorm", die sowohl im Vorfeld als auch während der ersten Semester des Studiums selegierend wirkt: Sowohl das Image der Informatik als auch die Organisation des Studiums sind ausgerichtet auf StudienanfängerInnen, die ihre Hochschulzugangsberechtigung an einer technisch ausgerichteten Schule erworben haben, Computer-Vorerfahrungen haben und die direkt nach der Schule oder nach dem auch überproportional häufig abgeleisteten Militär-/Ersatzdienst an die Universität kommen. Folglich handelt es sich in der Regel um Männer.

Das Weltbild eines Menschen ist sehr umfassend: Es enthält Konzepte über alle Lebensfragen der Menschen, wie über die Natur der Wirklichkeit, über den Menschen an sich, über das Verhältnis Mensch-Natur, Mensch und Gesellschaft, über Religion, den Sinn des Lebens, etc. Im Rahmen unserer Untersuchung erschien es sinnvoll, vor allem jene Aspekte des Weltbildes zu erfassen, die die zukünftige „Berufsfähigkeit" der InformatikerInnen bzw. die „Berufsangemessenheit" der Informatikausbildung im Hintergrund des Weltbildes betreffen. Daher lagen unsere Schwerpunkte auf dem Technikbild, der Wirklichkeitsauffassung, der Relation Realität – informatische Rekonstruktion derselben, dem Menschenbild einschließlich Geschlechterbild, der Relation Mensch-Maschine, der Relation EntwicklerInnen-NutzerInnen und dem Berufsbild Informatik einschließlich ethischer Fragen. Alle diese Weltbild-Komponenten sind für Fragen der Verantwortung in der Informatik von Bedeutung.

3. Informatik Fachkultur

Ein Motiv für die Untersuchung war auch das geringe Interesse am Informatikstudium und die zu hohen Abbruchquoten, welche zu dem allseits beklagten Mangel an InformatikerInnen auf dem Arbeitsmarkt führen. Als Ursachen werden u. a. das schlechte Bild der Informatik in der Öffentlichkeit und die ungenügenden Informationen über das Studium bei Studierwilligen verantwortlich gemacht, die schon vor Beginn des Studiums als Exklusionsmechanismen wirken (Broy u. a. 2008). Zugleich ist der Frauenanteil in der Informatik nach wie vor gering, obwohl „vom Technikinteresse her ein weit größeres Potenzial an Studentinnen, die für ein Ingenieurstudium gewonnen werden könnten" (BMBF 2005, 38), besteht. Als Ursachen für die außerordentlich hohen Abbruchquoten werden vor allem „fachkulturelle Mentalitäten und Verhaltensweisen" (Heublein u.a. 2008: 33; Derboven/ Winker 2010, Ihsen 2009) vermutet.

Mit fachkulturellen Denk-, Kommunikations- und Vorstellungsmustern werden fachliche Einstellungen, Wertvorstellungen und Ziele, aber auch ein bestimmter Habitus transportiert. In der westlichen Informatik, wie in den technischen Fächern überhaupt, entspricht dieser Habitus weitgehend einem weißen westlichen männlichen Persönlichkeitsprofil mit einem solchem Auftreten und Selbstinszenierung. Daher werden Frauen in MINT-Fächern mit widersprüchlichen Habitusanforderungen konfrontiert, solchen der Weiblichkeit und solchen der Technikaffinität. In vielen ingenieurwissenschaftlichen Geschlechterstudien (Janshen/Rudolph 1987, Ihsen 2009, Derboven/Winker 2010) fiel auf, dass wesentlich häufiger Anforderungen an das Persönlichkeitsprofil einer Ingenieurin gestellt werden als etwa an ihre Leistungsfähigkeit. Auch heute noch besteht eine Diskrepanz zwischen den Habitus-Anforderungen an eine vorwiegend männ-

liche Umgebung und solchen an Weiblichkeit, wie sie in der Weltbilderstudie von den Studierenden denn auch expliziert wurde und die von Frauen ausgehalten werden muss. Die Lehrenden präsentieren mit der Kommunikation von Werten implizite Selbstdefinitionen der Wissenschaften und der wissenschaftlichen Communities, und sie leben mit ihrem gesamten Verhalten den Habitus der Fachkultur vor. Studierende passen, um sich erfolgreich zu behaupten, ihre eigenen Wertorientierungen und habituellen Muster jeweils mehr oder weniger diesen Normen an. Die Aneignung vorherrschender Verhaltensweisen im technischen Studium und im Hochschulbetrieb wird von Frauen häufig als Prozess der „Akkulturation" (Schinzel 2007) erlebt, der im Widerspruch zu der geschlechtstypischen Sozialisation in Kindheit und Jugend steht. Dies gilt insbesondere für Konkurrenzverhalten und Profilierungsstreben.

Die Fachkultur der Informatik wird allgemein (Schinzel et al. 1999) als ein wesentlicher Grund dafür angesehen, dass viele junge Frauen (und Männer) das Studium zumeist noch im Grundstudium wieder verlassen. Die stark eingrenzende und disziplinierende Fachkultur ingenieurwissenschaftlicher Studiengänge hat negative Auswirkungen auf die Studierhaltung, die Motivation und das Selbstvertrauen insbesondere von Studentinnen. Diese Fachkultur wird weniger als sachliche Notwendigkeit angesehen denn als spezifisch historisch gewachsen. Für eine nachhaltige, erfolgreiche Veränderung in den Strukturen der Hochschulen und Fachbereiche zugunsten einer Zielgruppenerweiterung sei eine Umgestaltung der Institutions- und Fachkultur notwendig (Ihsen et al. 2009). Um das Feld für vielseitig interessierte junge Menschen zu öffnen, wäre es notwendig, das Selbstverständnis der ingenieurwissenschaftlichen Fachkultur wie auch das Selbstverständnis technischer Professionen durch gezielte Interventionen nachhaltig zu erschüttern (Derboven/Winker 2012).

Eine Fachkultur, die durch Kooperation und Synergien statt durch Konkurrenz gute Ergebnisse erzielen will, wird Frauen und diverse Studierendengruppen eher anziehen (Schinzel 2007).

4. Objektivismus und Technikdeterminismus

Das Technikbild der Befragten interessierte uns dahingehend, inwieweit es von der Metapher der (determinierten) technischen Evolution geprägt ist bzw. wie weit die Studierenden ihre Gestaltungsmacht erkennen. Dass Technikentwicklung ein sozialer Prozess ist, das Ergebnis einer Reihe spezifischer Entscheidungen, die von einer bestimmten Gruppe von Menschen an bestimmten Orten zu bestimmten Zeitpunkten zu ihren eigenen Zwecken getroffen werden, kollidiert mit der Vorstellung, dass die Entwicklung der Technik deterministisch vorgegeben und unbeeinflussbar sei. Dies führt zu der absurden Tatsache, dass gerade diejenigen, die die Welt aktiv und tief greifend verändern, glauben, auf diese Veränderung keinen Einfluss zu haben (Schinzel 2006).

Das ingenieurwissenschaftlich-mathematische Verständnis der Informatik integriert zwei ursprünglich nebeneinander bestehende Sichtweisen. Aus der Mathematik kommt die von Dijkstra geprägte Unterscheidung zwischen dem „Pleasantness"- und dem „Correctness"-Problem, wobei sich InformatikerInnen nur mit letzterem, also mit dem formalisierbaren Teil der Softwareentwicklung befassen sollten[4] bzw. mit dem, was mit mathematischen und logischen Methoden bearbeitbar ist. Damit wird die Aufgabe aus dem Ganzen herausgelöst. Hinzu kommt, dass der informatische Methodenhintergrund mit den Paradigmen Rationalität und Effektivität eine tayloristische Vorgehensweise mit sich bringt, in der das Paradigma „teile und herrsche" der rationalen Methode nicht nur den hierarchischen Zugangsprozess zu Wissen und Aufgaben prägt, sondern auch das wichtigste Mittel zur Komplexitätsreduktion im algorithmischen Vorgehen darstellt.[5] Sowohl aus den Ingenieurwissenschaften wie auch aus der Mathematik kommt die Ausrichtung auf Optimalität, aus der sich der für Informatik-Anwendungen unangemessene Glauben an einen „one-best-way" der Ingenieurwissenschaften ableitet.[6]

Vielfach tritt heute die Bedeutung der Mathematik in der Informatikausbildung hinter die der Ingenieurwissenschaften zurück, was zum Teil auf den Wechsel von strukturierter Softwareentwicklung mit geschlossenen Problemlösungen zum Paradigma der evolutionären Entwicklung offener Systeme zurückzuführen ist, zum Teil aber auch ökonomische Gründe hat.

Vorstellungen wie Objektivismus, Optimalitätsziele und one-best-way-Denken sowie Technikdeterminismus leiten auch die Informatik – zu ihrem eigenen Schaden. Denn keine Technik ist gestaltbarer und kontingenter als die die Diversifizierung der Aufgaben durch keine Materialeigenschaften einengende universalistische Methode der Formalisierung. Sind Software-Entwickelnde sich dessen nicht bewusst, so erhöht sich die ohnedies bestehende Gefahr der software-medialen Objektivierung von in Wahrheit Kontingentem, Kontextabhängigem, von Auslassungen und blinden Flecken. Hinzu kommen die professionellen Ideale der Informatik: Flexibilität und Geschwindigkeit, rasche Ideenproduktion, Karriereorientierung; die Bevorzugung von stets Neuem anstelle der Verbesserung des Alten, ein zu großer Anspruch an Universalismus und das ‚Selbstmachen', etwa durch Introspektion, das im so genannten „Ego-Approach" die von den Gender Studies kritisierte I-methodology generiert (Allhutter et al. 2008) und sich so hermeneutischen Erkenntnisproblemen bei der Wissensakquisition nicht stellt.

Für manche der von uns befragten Studierenden erweitert sich der Objektivismus auch auf das Menschenbild und vermindert so die imaginierte Distanz zwischen Mensch und Maschine. Während ein großer Teil der Studierenden im ersten Semester die Emotionalität des Menschen im Vergleich zum Computer hervorhebt, steht dieser Aspekt für die Studierenden in den fortgeschrittenen Semestern nicht so sehr im Vordergrund. Ein objektivistisches Menschenbild haben sowohl einige StudienanfängerInnen wie auch einige Studierende in höheren Semestern der Universitäten Freiburg, Dresden und Karlsruhe. Sie verstehen den Menschen als ein ausschließlich auf naturwissenschaftliche Prozesse zurückführbares Wesen, das vollständig nachbildbar wäre, gäbe es dafür ausreichende technische Möglichkeiten und Wissen über den Menschen. Gerade diejenigen, die z. B. den Menschen als „einen Haufen Zellen" beschreiben, beschreiben solche Sichtweise auf den Menschen und die Möglichkeiten der maschinellen Nachbildung oder deren Abweisung als Ansichtssache, „Weltanschauung" oder „Glaube". Insgesamt argumentieren die höheren Semester meist differenzierter, und viele be-

werten sowohl den Menschen als auch den Computer in dem für ihn spezifischen Bereich (Computer: Berechnung und Präzision, Mensch: Kreativität, Entscheidungsfähigkeit und Sozialität) als eindeutig besser. Insbesondere die Erstsemester können einen Vergleich von Mensch und Computer nicht nachvollziehen.

5. Kontingenzen und Diversität

Der deutsche Begriff Diversität leitet sich aus dem amerikanischen Konzept des Diversity Management ab, das den Umgang mit einer vielfältigen MitarbeiterInnenschaft in Organisationen gestalten will. In unserer Studie haben wir zwischen fachlicher und sozialer Diversität unterschieden.

Fachliche Diversität äußert sich in der Informatik auf vielfache und komplexe Weise: Die Computer- und Netzentwicklung hat aufgrund ihrer Dynamik und Unvorhergesehbarkeit enorm kontingente Verläufe genommen und diverse Selbstbeschreibungen der Informatik generiert: Beispielsweise hat niemand die Durchsetzung von PCs und damit einer individualisierten Nutzung anstelle von Mainframes antizipiert; niemand konnte die Entwicklungen des Internet vorhersehen, und seine jetzige Ausgestaltung zeugt von einem äußerst kontingenten impliziten Aushandlungsprozess (Hellige 2004). Neben dieser auf der Zeitskala sich als kontingente Entwicklungswege verzweigenden Diversität zeigt sich zu jedem Zeitpunkt die Diversität in der Vielfalt an unterschiedlichen Theorien und Modellen in der Informatik. Mit der Universalität des Computers und der Vielfalt der Nutzungsmöglichkeiten kommt eine weitere Kategorie von fachlicher Diversität und Freiheit zu diversifizierter Gestaltung ins Spiel, die sich, anders als in klassischer Technik, wo Aufgabe und Material die Gestaltung oft bis zum „one-best-way“ beschränken, in Hard- und Softwarevarietäten, Anwendungskontexten und somit auch sozialer Diversität der AnwenderInnen äußert. Aber auch die EntwicklerInnen mit ihren unterschiedlichen Herkünften, Kulturen, Vorerfahrungen und impliziten Annahmen, also ihrer sozialen Diversität, prägen die

Die Autorinnen

Britta Schinzel stieg nach ihrem Studium der Mathematik und Physik in die Compilerentwicklung in der deutschen Computerindustrie ein. Von dort wechselte sie in die Theoretische Informatik an der TH Darmstadt und habilitierte sich dort. Im Rahmen ihrer Professur für Theoretische Informatik an der RWTH Aachen arbeitete sie in verschiedenen Gebieten der Künstlichen Intelligenz, initiierte eine Reihe interdisziplinärer Projekte mit Soziologie, Linguistik, Biologie und Medizin und begann sich, zunächst nur in der Lehre, später auch in der Forschung, mit Informatik und Gesellschaft zu beschäftigen.
Seit ihrer Berufung (Denomination: Wirkungen der Informationstechnik in der Gesellschaft und Gender Studies Informatik) an das Institut für Informatik und Gesellschaft an der Universität Freiburg befasst sie sich mit verschiedenen Themen von Informatik und Gesellschaft, der Theorie der Informatik, Grundlagen, Rechtsinformatik, Informatik und Geschlecht, den Neuen Medien in der Hochschullehre in Forschung, Entwicklung und Anwendung oder mit den durch IT ermöglichten und verfestigten Normen und Normalisierungen durch Bild gebende Verfahren in der Biomedizin.

Monika Götsch studierte Soziale Arbeit, Soziologie, Politik und Gender Studies, promoviert in Soziologie. Zuletzt Mitarbeiterin am Institut für Informatik und Gesellschaft in Freiburg, im Projekt „Weltbilder in der Informatik“. Schwerpunkte: Gender und Wissensformationen.

Yvonne Heine (Dipl. Soz.Päd./Soz.Arb. (FH)) forscht zu den Themen Gender und Wissen. Wissenschaftliche Mitarbeiterin im Projekt „Weltbilder in der Informatik“ am Institut für Informatik und Gesellschaft in Freiburg.

Karin Kleinn studierte Soziologie und Erziehungswissenschaft, ist eine langjährige Mitarbeiterin am Institut für Informatik und Gesellschaft in Freiburg, zuletzt im Projekt „Weltbilder in der Informatik“. Schwerpunkt Genderforschung in Informatik und Naturwissenschaften.

Michael M. Richter received his Doctoral Degree in Mathematics in 1968 from the University of Freiburg, Germany. He was Professor of Mathematics at University of Texas at Austin, the RWTH Aachen from 1975 to 1986 and Professor of Computer Science at the University of Kaiserslautern from 1986 to 2003. He was president of the German Association for Mathematical Logic from 1981 to 1985 and served as Scientific Director at the German Research Center for Artificial Intelligence (where he was a cofounder) from 1989 to 1993. He was several times visiting the Unversidade de Santa Catarina, Brazil. Presently he is Adjunct Professor at the University of Calgary.

Diversität der Artefakte. Damit gelangen auch die in ihre kontingenten Herstellungsprozesse eingehenden Strukturen, Vorannahmen und Blindheiten bezüglich Ordnung, Strukturen und Repräsentation der Benutzung und des Wissens in die Anwendungswelt.

Es ist daher wichtig, sich all dieser Freiheiten mit der enormen Gestaltungsmacht bei Spezifikation, Modellierung und Problemlösung wie auch die jeweiligen Einengungen und Einschränkungen, die die dabei konkret verwendeten Modellbildungen den modellierten Realitäten aufzwingen, bewusst zu sein.

Unsere Studie befasste sich auch mit der Frage, über welche Konzepte von Diversität die befragten Informatikstudierenden verfügen und welche Bedeutung diesen ihrer Meinung nach in der Informatik bzw. der Softwareentwicklung zukommen soll. Die von uns befragten Studierenden verfügen über unterschiedliches ‚Diversity-Wissen', das mit dem Wissen über Informatik und Softwareentwicklung verbunden ist, wobei sie Einflüsse von fachlicher Diversität aufgrund ihrer expliziten Form eher anerkennen als Einflüsse sozialer Diversität, die in der Informatik noch immer wenig thematisiert werden und daher implizit bleiben.

Fachliche Diversität im Sinne von Zusammenarbeit unterschiedlicher Disziplinen mit der Informatik oder von interdisziplinärer Fachlichkeit der Informatik wird von den Studierenden sehr unterschiedlich bewertet, je nachdem ob die Informatik als „rein" formal-mathematische oder technische Disziplin, die als solche abgegrenzt und erhalten werden muss, oder als genuin interdisziplinäres Fach angesehen wird, das als Hilfswissenschaft von den Anwendungen in anderen Gebieten lebt. Die Freiburger Studierenden sehen mit dem Nebenfach (z. B. Kognitionswissenschaft) ausreichend Interdisziplinarität und die Brücke in andere Fächer gegeben, wobei diese sich auf den informatischen Blick von außen in eine andere Disziplin beschränken sollte, weniger geht es dabei um Zusammenarbeit oder fachlichen Austausch. Manche sehen auch die Notwendigkeit zu einem Minimum an Interdisziplinarität im Bereich der Anwendungen sowie zur Berücksichtigung der Bedürfnisse von NutzerInnen. Wieder andere halten Interdisziplinarität als der Informatik inhärent, da sie die Wünsche, Bedürfnisse und Denkweisen von Nicht-Informatikern nachvollziehen müssen, mit ihnen kommunizieren und zudem Technikfolgen abschätzen können müssen.

Der Einfluss sozialer Diversität auf Informatik-Produkte hingegen wird einerseits geleugnet oder als nicht oder nur dort wünschenswert erachtet, wo kleine spezifische Gruppenbedürfnisse erfüllt werden müssten.

Einige Besonderheiten ergeben sich in Bezug auf den Einfluss des Geschlechts. Hierzu wurden die Studierenden (unter anderem) gefragt, inwiefern ein höherer Anteil an Frauen die Informatik (also nicht nur die Softwareentwicklung) verändern würde. Manche berufen sich auf eine ominöse Unterschiedlichkeit von Frau und Mann, wobei Frauen die „andere" Herangehensweise haben, beispielsweise indem sie strukturierter an Aufgaben herangehen oder neue Sichtweisen auf Probleme einbringen. Auch der Wunsch nach Unberührtheit von sozialer Diversität findet sich hier wieder und verknüpft sich mit der von den Studierenden zugeschriebenen mangelnden Begabung von Frauen für die Informatik. Weitere argumentieren, dass soziale Diversität lediglich auf einige Bereiche der Informatik einen Einfluss habe. Hier erhält die Einteilung in einerseits die „reine" Informatik und andererseits alles andere, was darum herum angesiedelt wird, eine neue, abwertende Dimension: Ein höherer Anteil von Frauen bewirkt „keine richtige" oder „keine wirkliche" Veränderung, denn der Kern der Informatik wird davon nicht berührt. Nur dieser Kern also, die reine Informatik, ist das, was wirklich zählt und dieser ist und bleibt unveränderbar. Damit werden sowohl die Informatik, die sich mit dem ‚Drumherum' befasst, als auch die Frauen, die nur auf dieses ‚Drumherum' Einfluss nehmen können, als unbedeutend für die Informatik erklärt.

Es zeigt sich also, dass fachliche und soziale Diversität nicht vom Selbstverständnis der Informatik bzw. der Softwareentwicklung zu trennen sind. Wird Informatik als eine inhärent interdisziplinäre Disziplin und die Entwicklung von Software als umfassender Prozess gesehen, so ist Vielfalt in den Anwendungsbereichen eine Selbstverständlichkeit und bei der Softwareentwicklung unerlässlich. Das Verständnis von Informatik als einer streng formalen Disziplin, die sich auf einen eindeutig abgegrenzten Bereich bezieht und alles andere als nicht informatisch betrachtet, verortet Diversität dagegen außerhalb der Informatik und somit als unrelevant in der Softwareentwicklung.

6. Die gesellschaftliche Bedeutung und Verantwortung der Informatik und ihre individuelle Wahrnehmung

Die Studierenden messen der Informatik große Bedeutung und große Wirkmächtigkeit bei: Durch ihre Universalität und Allgegenwärtigkeit im Leben der Menschen hat Informatik großen gesellschaftlichen Einfluss. Manche definieren Informatik über Begriffe wie Fortschritt und Innovation, die ihre gesellschaftliche Bedeutung in den Blick nehmen, oft mit großer Fortschrittsbegeisterung. Sie sehen die Informatik als eine Institution mit großem Einfluss auf technologische Entwicklung, Gesellschaft und Individuen, da sie große Veränderungen hervorgerufen hat und weiterhin hervorrufen wird. Dies gilt sowohl für die AnfängerInnen als auch für die Fortgeschrittenen. Informatik bewirkt Veränderungen im Alltag, besonders in der Kommunikation, aber auch in Denken, Kultur und Gesellschaft. Die (informatische) Technik hat für die meisten Studierenden die Funktion, das Leben der Menschen zu verbessern und zu vereinfachen. Direkt nach dem Nutzen gefragt, nennen die Studierenden interessanterweise mehrheitlich fast ausschließlich Vorteile, die sich auf die Vernetzung der Welt durch neue Medien beziehen. Dies hängt sicher damit zusammen, dass die veränderte Kommunikation durch Computertechnik den augenfälligsten Wandel darstellt. Bei den StudienanfängerInnen findet sich Kommunikation als große Veränderung ausschließlich, bei den Studierenden der höheren Semester werden zusätzlich Auswirkungen auf die alltäglichen Routinen durch die Menge an neuen Gebrauchsgegenständen wie PC, Handy etc. genannt.

Bei so großem Einfluss stellt sich die Frage nach gesellschaftlicher Verantwortung. Die Bandbreite der Einstellungen hierzu ist sehr groß. Dennoch weisen die Welt-, Menschen-, Wissen-

schafts-, Technik-, Verantwortungs, Geschlechter- sowie Nutzer- und Nutzerinnenbilder der Informatik-Studierenden eine eingeschränkte Sicht auf, wie im folgenden expliziert wird.

Veränderungen durch die Computertechnik werden nicht ausschließlich positiv gesehen, auch Probleme werden genannt: zunehmende Abhängigkeit von informatischer Technik, zunehmende Arbeitslosigkeit in der Folge des technologischen Fortschritts, hoher Energieverbrauch von Rechenzentren und immer wieder die Veränderungen in der Kommunikation und im Umgang der Menschen miteinander. Interessant ist, dass von den StudienanfängerInnen insgesamt mehr negative Technikfolgen thematisiert werden als von Studierenden der höheren Semester. Vor allem zu den Themen Computerspielen, virtuelle Welten oder Internet, nach denen speziell die StudienanfängerInnen gefragt wurden, nannten sie viele Gefahren: Übertragung von Erfahrungen auf die reale Welt, Internetmobbing, Suchtgefahr, Fluchtgefahr, Verlust der Kommunikationsfähigkeit, nicht mehr unterscheiden können zwischen realer und virtueller Wirklichkeit. Aber auch bei Fragen, die allen Studierenden gestellt wurden (also Studierenden im ersten und in höheren Semestern) zeigten die StudienanfängerInnen ein stärkeres Bewusstsein für die negativen Auswirkungen vor allem von Internet und den veränderten Kommunikationsmöglichkeiten durch Informatik. Dass die StudienanfängerInnen das Internet und Computerspiele stark reflektieren, liegt nicht nur an der speziellen Fragestellung, sondern auch daran, dass dies die Bereiche sind, in denen sie die meiste Erfahrung mit Computern und (nach ihrer Meinung) Informatik gemacht haben. In ihren Überlegungen sind sie eindeutig durch ihre Sicht als AnwenderInnen geprägt: sie nutzen Software, Spiele und das Internet und sehen andere, die ebenfalls diese Anwendungen nutzen, und sie sehen auch, wozu das führen kann.

Die Frage nach der Verantwortung wird relativ unterschiedlich beantwortet. Unter den ErstsemesterInnen gibt es die Einstellung, dass Ethik den Fortschritt behindert und daher in der Informatik keine Rolle spielen sollte. Denn Informatik heißt „Innovation", „Fortschritt", „die Wissenschaft der Zukunft", „Voranbringung der digitalen Gesellschaft", die „Auslotung technischer Möglichkeiten", was oft mit großer Fortschrittsbegeisterung einhergeht und im Falle eines Studenten mit der Auffassung, dass ethische Überlegungen den Fortschritt nicht einschränken sollten („Ethik bringt die Menschen nicht weiter").

Andere möchten sich nicht selbst um ethische Fragen kümmern müssen und sie von anderen Disziplinen behandeln lassen, die sie eher dazu befähigt sehen, sich mit solch schwierigen Fragen zu befassen.

Zugleich gibt es die Haltung, dass Ethik für die Informatik bzw. für InformatikerInnen durchaus wichtig ist. Dabei gibt es Unterschiede wie weit die Verantwortung der InformatikerInnen geht: Manche beziehen sie nur auf ein Berufsethos, das zu korrektem Arbeiten und anständigem Verhalten gegenüber KundInnen und KollegInnen anhält, andere beziehen sich auch auf die Produkte der Informatik und deren Sinn und Nutzen. Am weitesten geht die Auffassung, dass auch nicht intendierte Folgen des eigenen Tuns in eine gewünschte Ethik der Informatik mit einbezogen werden müssen.

Neben dieser Bandbreite zu Auffassungen über Ethik in der Informatik gibt es aber auch diejenigen, die sich noch nie Gedanken darüber gemacht haben und auch im Verlauf des Interviews keine Überlegungen dazu entwickeln. Insgesamt sehen sich die ErstsemesterInnen noch weitgehend als Informatik-Nutzende und fordern entsprechend den Einbezug verantwortlichen Handelns, von welcher Berufsgruppe auch immer, im Zusammenhang mit Informatik.

Diese Sicht auf die Anwendungen scheint im Studium der Informatik zu einem gewissen Maße verloren zu gehen, da die Studierenden quasi „die Seite wechseln" und damit auch den Blickwinkel. Das ist interessant und zugleich auch erschreckend. Denn durch das Studium erlangen die Studierenden einen größeren Einblick, was mit Informatik alles möglich ist bzw. sein kann. Dass viele dabei auch die Fragen nach gesellschaftlichen Folgen aus dem Blick verlieren, scheint darauf hinzuweisen, dass die Professionalität, die an den Universitäten vermittelt wird, den Umgang mit Technikfolgen nicht im Zuständigkeitsbereich der InformatikerInnen sieht.

Bei den fortgeschrittenen Studierenden wurde im Zusammenhang mit dem Verständnis und dem Selbstverständnis von Informatik danach gefragt, inwieweit ethische Belange in die Zuständigkeit der Informatik fallen, und zwar auf zwei Ebenen: Zum einen wurde gefragt, ob „die Informatik" ganz allgemein sich mit ethischen Fragen auseinandersetzen muss; zum anderen wurde – konkreter – danach gefragt, wem InformatikerInnen verpflichtet seien. Entsprechend sind die Aussagen der Studierenden zum Teil auf eine irgendwie abstrakte Informatik bezogen, zum Teil auf die individuellen InformatikerInnen.

Wurde nach Ethik für die Informatik gefragt, so zeigte sich eine große Bandbreite an Einstellungen: Auf der einen Seite wird Informatik als ethikfrei gesehen, denn „Algorithmen kennen keine Ethik". Informatik ist damit objektiv und unterliegt keinen abwägenden Überlegungen. Zum Teil wird der Informatik als Institution dennoch die Beschäftigung mit ethischen Fragen nahe gelegt, wegen der industriellen und ökonomischen Interessen. Hier wird das Bild der Informatik scheinbar nicht erweitert, da ja die Informatik als objektive Disziplin selbst ethikfrei ist.

Auf die (weniger abstrakte) Frage nach der Verantwortung von InformatikerInnen wurden insgesamt mehr Aussagen gemacht. Manche Studierende sehen die Verantwortung der InformatikerInnen nur an der Stelle, wo sie sich ihren Arbeitsplatz suchen bzw. sich um einen Auftrag bewerben. Danach jedoch, wenn sie sich für eine Arbeitsstelle oder einen Auftrag entschieden haben, sind ethische Fragen bezüglich des Inhaltes der Arbeit nicht mehr relevant, diese Fragen scheinen mit der ersten Entscheidung abschließend geklärt zu sein. Im Bereich des Berufsethos anerkennen manche dennoch die Wichtigkeit einer moralischen Haltung, die zu korrektem Arbeiten und anständigem Verhalten gegenüber KundInnen und KollegInnen führen soll, oder wenn es um professionelles Arbeiten geht: Die Loyalität gegenüber ArbeitgeberIn und/oder AuftraggeberIn wird als wichtig erachtet. Das beinhaltet zum Beispiel, auftauchende Probleme weiterzugeben oder fachlich auf dem neuesten Stand zu sein und diesen Stand in die Arbeit einzubringen. Dann gibt es auch noch die Verpflichtung gegenüber den NutzerInnen, die manche nur indirekt über den Auftrag bzw. AuftraggeberIn sehen, andere

beziehen sich auch auf die Produkte ihrer Arbeit. Andere geben ganz konkrete Bereiche an, in denen ethische Verantwortung der Informatik relevant sind: Datenschutz, Waffenproduktion, ganz allgemein Anwendungen oder das Bild, das die Informatik in der Öffentlichkeit vermittelt. Mit der Beschränkung der Ethik auf einzelne Bereiche wird deutlich gemacht, dass es auch andere, ethisch nicht relevante Bereiche gibt, v.a. die Forschung und der Kern der Informatik werden hier genannt. Aber zum Teil wird es auch normativ formuliert: Computerspiele sollen nicht aufgrund von ethischen Überlegungen zu stark eingeschränkt werden. Am anderen Ende des breiten Spektrums findet sich die Auffassung, dass die Informatik immer bedenken muss, was sie macht, ethische Überlegungen also in ihre Arbeit einbeziehen muss. Viele begründen dies mit einer allgemeinen Verpflichtung für alle Menschen, die in jedem Beruf gilt; oder es wird eine hohe (nicht näher ausgeführte) Verantwortung besonders der Informatik genannt von einer Studentin, die bereits ein Seminar zu ethischen Aspekten der Informatik besucht hat. Hier zeigt sich, dass die Lehrveranstaltungen der Universitäten durchaus einen Effekt haben.

Von vielen wird der Umgang mit ethischen Fragen überhaupt problematisiert. Sie wird von vielen als zu kompliziert erachtet und eher als Aufgabe der Philosophie gesehen. Einmal liegen die Schwierigkeiten in der Natur der Ethik, denn man kann ethische Fragen ewig diskutieren, ohne zu einem Schluss zu kommen. Allgemeingültige Formulierungen sind schwierig, weil alle Produkte sowohl legal wie auch illegal genutzt werden können. Ethik ist kulturabhängig, und zudem ist es schwer zu entscheiden, wer die Verantwortung für Missbrauch haben soll: NutzerInnen, ErfinderInnen, diejenigen, die die Produkte verkaufen? Auch die Frage, ob ethisches Verhalten denn gelehrt werden kann oder ob man es nicht von Zuhause mitbringen muss, wird aufgeworfen. Und es findet sich die pessimistische Haltung, dass Ethik zwar wichtig ist, letztendlich aber doch ethische Grenzen irgendwann gebrochen oder umgangen werden, Ethik daher wirkungslos ist. Auch das Problem, dass InformatikerInnen in Firmen nicht immer an Entscheidungen beteiligt sind und daher Ethik nicht unbedingt in ihre Arbeit einbeziehen könnten, wird hier genannt.

Es zeigt sich damit klar, dass es allgemein an entsprechenden Lehr-/Lerninhalten mangelt, denn Ethik kann und soll keine eindeutige Antworten liefern, statt dessen ethisch-philosophisch fundiert eine tiefere Durchdringung informationstechnischer Problem- und Konfliktlagen ermöglichen und so – kontingent – Entscheidungshilfen bieten.

Mit Bezug auf das Wahrnehmen eigener Verantwortlichkeiten förderte die Weltbilderstudie so einen spürbaren Einfluss des Studiums, der sich in den Unterschieden zwischen den Erstsemester-Studierenden und denen der höheren Semester zeigen, zutage, ein weiteres Argument für die Dringlichkeit der Thematisierung ethischer Fragen im Informatik-Studium.

7. Geschlecht und Geschlechterwissen

Unabhängig von Universität und Semesterzahl sind die Sichtweisen der Studierenden auf Geschlecht von einem implizit differenzorientierten, bipolaren Geschlechterwissen geprägt. Entsprechend gehen sie bis auf wenige Ausnahmen von einem unhinterfragbaren Unterschied zwischen Mann und Frau aus, der den Mann dem technischen und die Frau dem sozialen, sprachlichen und/oder ästhetischen Bereich zuordnet. Daher sind Informatikerinnen, anders als andere, also als „normale“ Frauen, den Informatikern ähnlich, welche so androzentrisch als Norm konstruiert werden. Geschlechtsspezifische Unterschiede werden jedoch am häufigsten kulturell und/oder sozialisatorisch begründet und seltener biologisch/genetisch. Eine strukturelle Bedingtheit von geschlechtsspezifischen Bereichen wird allerdings nur von sehr wenigen Studierenden in Betracht gezogen, vielmehr wird die Verantwortung für geschlechtsspezifische Lebensverläufe individualisiert.

Dass ein höherer Frauenanteil kaum einen Einfluss auf die Informatik haben könnte, stellen sich die meisten Studierenden auch bei einer stärkeren Inklusion von Frauen in die Profession vor. Solche Frauen müssten sich an die Informatik anpassen und werden dann allerdings als unweibliche Ausnahmen betrachtet. Dennoch werden von manchen Studierenden Frauen „andere“ Herangehensweisen zugeschrieben, beispielsweise indem sie, ausnahmsweise positiv formuliert, strukturierter an Aufgaben herangehen oder neue Sichtweisen auf Probleme einbringen sollen. Manche halten einen höheren Frauenanteil jedoch gar nicht für möglich, da Frauen zu unbegabt für die Informatik seien. So wird die dominante Kultur implizit als die ‚richtige' bezeichnet und als unveränderbar angesehen. Die Ausschlüsse, die sie produziert, ergeben sich dann im Grunde von selbst.

Dabei zeigt die Typologisierung der Interviews der Weltbilderstudie (Götsch et al. 2011), dass es trotz einer dominanten impliziten Studierendennorm (Hauch et al. 2007), die durch Männlichkeit, Schulabschluss an Technischen Gymnasien, Computerkultur und abgeschlossenen Militärdienst gekennzeichnet ist, immer noch recht unterschiedliche Typen von Informatikstudierenden gibt (und zudem auch einen Typus, der der Norm nach Hauch et al. (2007) nicht entspricht), und dass diese Tatsache einfach nur zur Kenntnis genommen werden müsste.

Vor allem in Bezug auf Gender und Ethnizität zeigt sich, dass ein unreflektierter Umgang mit Diversität die Gefahr in sich birgt, essentialisierende und homogenisierende Zuschreibungen an eine Gruppe zu (re-)produzieren. Dies geschieht im Zusammenhang mit der Konstruktion der dominanten Gruppe als Norm.

Wenn aber bestimmte Personengruppen innerhalb der Informationstechnologie die Mehrheit stellen, dann werden in den Strukturen und den Realisierungen mittels dieser Technologie die entsprechenden Wahrnehmungsweisen widergespiegelt. Wichtig ist daher, durch einen personellen Diversitätsansatz solchen eventuellen Einseitigkeiten entgegenzusteuern und damit Diversität in die Technik einfließen zu lassen.

Resumé

Die Ergebnisse der Weltbilderstudie lassen es notwendig erscheinen, das Fach Informatik und Gesellschaft mit seinen Inhalten an Geschichte der Informatik, Philosophie und Verantwortung der Informatik, Gender Studies Informatik, Rechtsinformatik und Technikfolgenabschätzung an allen Informatik-Fakultäten zu

etablieren. Das würde u.a. helfen, das Klima zu verändern und die Diversität an Studierenden und Lehrenden zu erhöhen, um auch die Studierendennorm zu beseitigen, was beides insbesondere Frauen den Zugang zum Studium erleichtern würde. Das mag als ein nur schwierig und langsam aufzubrechender Zirkel angesehen werden, der allerdings an der Carnegie-Mellon-Universität in Pittsburgh in weniger als 10 Jahren gelang (Margolis/ Fisher 2002).

Literatur

Allhutter, Doris; Hanappi-Egger, Edeltraud (2006): The Hidden Social Dimensions of Technologically Centred Quality Standards: Triple-Loop Learning as Process Centred Quality Approach. In: Dawson, R./Georegiadou, E./Linecar, P./Ross, M./Staples, G. (eds.): Perspectives in Software Quality. The British Computer Society, 179-195

Bittner, Peter/Hornecker, Eva (2005): A Micro-Ethical View on Computing Practice. In: Critical Computing. Proceedings of the 4th decennial conference on Critical Computing: between sense and sensibility. New York: ACM Press. 69-78

BMBF (2007): Bericht zur technologischen Leistungsfähigkeit Deutschlands 2007. http://www.bmbf.de/pub/tlf_2007.pdf (17.12.2007)

Broy, Manfred/ Schmid, Detlef (2000): "… noch nicht zu spät". Das Walberberg-Memorandum zur Förderung der IT-Forschung. In: Informatik-Spektrum, No 23, April 2000, S. 109-117

Derboven, Wibke/Winker, Gabriele (2010a): Ingenieurwissenschaftliche Studiengänge attraktiver gestalten: Vorschläge für Hochschulen, Springer:Berlin.

Dijkstra, Edsger W. (1989): On the cruelty of really teaching computing science. In: Communications of the ACM 32, December, p. 1398-1404

Götsch, Monika/Heine, Yvonne/Kleinn, Karin (2011): "…dass auf einmal 'n blue screen 'n pink screen wäre"; Vortrag auf der GI-Jahrestagung, 7. Oktober 2011; erscheint im Tagungsband der GI-Jahrestagung 2011.

Hall, Edward T./Mildred Reed Hall (1990): Understanding cultural differences. Yarmouth: Intercultural Press Inc.

Hauch, Gabriella; Horvath, Ilona (2007): TEquality – Technik.Gender.Equality. Das Technikstudium aus der Sicht von Frauen und Männern

Hellige, Hans-Dieter (2004): Geschichten der Informatik: Visionen, Paradigmen, Leitmotive (History of Computer Science) Berlin: Springer.

Heublein, U., & al., (2005). Studienabbruchstudie 2005. Hannover: HIS-Hochschul-Informations-System GmbH.

Ihsen, Susanne (Hrsg.) (2010): Spurensuche TUM Gender-und-Diversity-Studies, Band 1, München, online: http://www.gender.edu.tum.de/spurensuche.html, (10.1.2012).

Ihsen, Susanne/Jeanrenaud, Yves/Wienefoet, Verena/Hackl-Herrwerth, Andrea/ Hantschel, Victoria/Hojer, Cornelia (2009): Potenziale nutzen, Ingenieurinnen zurückgewinnen. Drop-Out von Frauen im Ingenieurwesen: Analyse der Ursachen und Strategien zu deren Vermeidung sowie Handlungsempfehlungen für eine erfolgreiche Rückgewinnung. Wirtschaftsministerium Baden-Württemberg, Stuttgart.

Janshen, Doris/ Rudolph, Hedwig (1987): Ingenieurinnen. Frauen für die Zukunft. Berlin: de Gruyter

Lessig, Lawrence (1999): Code and other Laws of Cyberspace. New York: Basic Books

Margolis, J./Fisher, A (2002): Unlocking the clubhouse: somen in computing. Cambridge, Mass.: MIT Press

Schinzel, B./Kleinn, K./Wegerle, A./Zimmer, Ch. (1999): Das Studium der Informatik. Studiensituation von Studentinnen und Studenten. In: Informatik-Spektrum 22, 13-23

Schinzel, Britta (2006): Wissenschaft im Spannungsfeld zwischen (technologischer) Determination und (kultureller) Vision. In: Liebig, B.; Dupuis, M.; Kriesi, I.; Peitz, M. (Hrsg.): Mikrokosmos Wissenschaft. Transformationen und Perspektiven. Vdf Hochschulverlag ETH Zürich, 169-185

Schinzel, Britta (2007): Frauenförderung in Mathematik, Technik- und Naturwissenschaften an der Universität Freiburg: Curriculare und weitere Maßnahmen in höheren Qualifikationsstufen, In: Freiburger Universitätsblätter 177/3, 25-37.

Anmerkungen

1 *Gefördert 2008-2011 durch die DFG*

2 *Ausgenommen ist die Open Source-Gemeinde im weitesten Sinne, denn sie sieht sich als Vorkämpferin in einem Experimentierfeld neuer, auch wirtschaftlicher Modelle, heute sich als Piratenpartei auch schon politisch profilierend.*

3 *Informatikkultur ist nicht gleich Computerkultur: Die Computerkultur ist geprägt durch Kenntnisse des „Tagesgeschehens", Aktualität auf dem Markt und in der Open-Source-Welt, durch Programmierkenntnisse und Hackerwissen. Dagegen fördert die universitäre Informatikkultur eine formale Denkschulung und hat eine stärker mathematische Ausrichtung.*

4 *Dabei bleibt unklar, wer sich um das „pleasantness"-Problem kümmern sollte.*

5 *Diese Aufteilung/Zerstückelung von Aufgaben ist kulturanthropologisch gesehen typisch für „low-context"-Kulturen (Hall/Hall 1990). Während in „high-context"-Kulturen viel Information im Kontext steckt, d. h. periphere Informationen implizit mitberücksichtigt werden, besteht in den „low-context"-Kulturen eher die Gefahr, dass über die Konzentration auf die Aufgabe das Ganze aus dem Blick gerät. Als Information gilt dort nur das, was explizit ausgesprochen ist, der Kontext wird nicht automatisch mit berücksichtigt (daher „low-context"). In einem „low-context"-Arbeitsumfeld ist es somit auch schwierig, so genannte „unsichtbare Arbeit", zu der viele Anteile von Frauenarbeit gehören, zu sehen und zu berücksichtigen. Eine Informatik, die sich als Strukturwissenschaft (angelehnt an die Mathematik) versteht, die geschlossene Systeme einer vollständigen Lösung zuführen will, schafft ein Arbeitsumfeld mit starker „low-context"-Ausrichtung.*

6 *Dies zeigt sich deutlich in der zwar historischen, aber erhellenden Definition von Computer Science der Association for Computing Machinery (ACM) 1989 : „die Disziplin der Informatik ist das systematische Studium algorithmischer Prozesse, die Information beschreiben und transformieren, Theorie, Analyse, Entwurf, Effizienz, Implementierung und Anwendung dieser Prozesse. Nach dieser Definition ist die grundlegende Fragestellung der Informatik: was kann effizient automatisiert werden?"*

Daniela Wühr und Stefan Sauer

„Scrum“ als Innovations- und Emanzipationsgenerator?

Was traditionelle Branchen von der agilen Software-Entwicklung lernen können

Hier lesen Sie:

- wie die alternative Projektmanagement-Methode Scrum funktioniert
- warum Scrum den Bedürfnissen radikaler Innovationsarbeit besser entspricht
- welche Stolperfallen bei der Umsetzungspraxis von Scrum zu beachten sind

Das Thema Innovation scheint allgegenwärtig: Unternehmen, Interessenvertretungen, die Wissenschaft, sie alle sehen Innovation als die Strategie, um im weltweiten Wettbewerb zu bestehen. Innovation geht dabei oft mit einem Trend zu Standardisierung im Unternehmen einher. Häufig wird der Innovationsprozess dann von klassischem Projektmanagement begleitet, um beispielweise paralleles Arbeiten und gleichzeitiges Entwickeln zu ermöglichen. Allerdings birgt Innovation auch immer etwas Ungewisses in sich. Herkömmliches Projektmanagement ist in diesen Fällen in der Regel zu unflexibel und reagiert schwerfällig auf Unvorhergesehenes. Dieser Beitrag stellt die neue Projektmanagement-Methode Scrum *vor, die sich viel passgenauer auf die Anforderungen von Innovationsarbeit einstellen lässt als traditionelle Ansätze. Die Autoren erklären, wie Scrum funktioniert und weisen auf die Stolperfallen in der Umsetzungspraxis hin.*

Während sich Wissenschaftler darüber streiten, was genau man als Innovation bezeichnen könnte, wo die Abgrenzungen zur Invention sind oder welche Merkmale eine Innovation hat, geht es im Unternehmensalltag vor allem um die tagtägliche Umsetzung. Innovation beschränkt sich dabei nicht nur auf neue Produkte. Die Betriebe gehen mehr und mehr dazu über, die Organisation von Innovation selbst als entscheidenden Wettbewerbsfaktor zu betrachten und zu gestalten. Die Ergebnisse des Instituts für Sozialwissenschaftliche Forschung (ISF) München zeigen: die primäre Strategie der letzten Jahre liegt auf dem Weg der Standardisierung. Unabhängig von der Branche, scheint sich ein bestimmter Typ von standardisierten Innovationsprozessen durchzusetzen. Der Innovationsprozess wird dabei meist in unterschiedliche und zeitlich festgelegte Phasen eingeteilt. Begleitet wird die organisatorische Gestaltung von Innovationsprozessen von einer Vielzahl an IT- und Controlling-Tools, die eng mit traditionellen Projektmanagementansätzen verlinkt sind. Die Unternehmen beabsichtigen mit der Einführung dieser Prozesse und Tools, den Innovationsverlauf effektiver und schneller zu machen. Da Innovationen risikobehaftet sind, liegt ein weiteres Ziel darin, die Risikoabschätzung zu optimieren. Gleichzeitig soll die ökonomische Berechenbarkeit erhöht und die Kosten durch neue Funktionen wie „Target Costing“ minimiert werden. Kurz gesagt: mit Hilfe von projektförmigen, standardisierten Vorgehensweisen sollen „leane“, also möglichst schlanke, robuste und vor allem reproduzierbare Innovationsprozesse umgesetzt werden.

Flexibilität durch agile Methoden

Allerdings können die eingeführten Tools und Prozesse auch einen neuen Grad von Belastung bei den Innovationsakteuren hervorrufen. Diese haben wir ausführlich in unserem Artikel „Innovation trotz Standardisierung“ (siehe CuA 5/2010, 5 ff.) betrachtet. Unsere aktuellen Forschungsprojekte weisen auf Folgendes hin: Zusatzarbeiten und sogar weniger Freiraum für Innovation entstehen dann, wenn neue Prozesse und die zugehörige Software nicht richtig adaptiert oder nicht vollständig eingeführt sind. Außerdem haben wir weitere Hinweise gefunden: viele Prozesse und die dazugehörigen Tools passen nicht zu dem jeweiligen Branchen- bzw. Unternehmenshintergrund oder berücksichtigen nicht ausreichend, um welche Art von Innovation es sich handelt.

Das Kerngeschäft im Maschinen- und Anlagenbau etwa wird von Einzelfertigung *(engineering-to-order)* und Kleinstserien bestimmt. Das heißt, fast jedes entwickelte und gefertigte Produkt ist einzigartig. Diese Art von Produkten und Projekten liegen auf einem enormen Komplexitätsniveau und erfordern von den Innovationsakteuren eine hohe Antizipationskraft. Die Einbeziehung von Erfahrungswissen ist von gleicher Bedeutung, da bei diesen radikaleren Innovationen eine Menge Unwägbarkeiten bewältigt werden müssen. Die jeweils nächsten Schritte und Aktionen im Innovationsprozess müssen immer wieder neu und oft ad hoc angepasst werden. Diese besondere Logik bricht sich jedoch mit vielen umgesetzten Projektmanagement-Tools.

Traditionelle Projektplanungs-Systeme fußen auf einer rigiden ERP-Architektur und können diesem Flexibilitätsanspruch nicht genügen. Die Folge sind lange und permanente Anpassungsarbeiten, um die geplanten Soll- an die tatsächlichen Ist-Zahlen anzugleichen.

Scrum, ein anderer Typus von Projektmanagement, könnte den Bedürfnissen von radikaler Innovationsarbeit besser entsprechen. Scrum kommt ursprünglich aus dem Bereich der Software-Entwicklung und ist eine agile Organisationsform.[1]

Um Scrum näher vorzustellen, gehen wir zunächst auf die grundlegende Idee dieses neuen Projektmanagement-Tools ein. In einem zweiten Schritt stellen wir die definierten Benutzergruppen vor sowie die Prozesse und Abläufe.

Grundidee von Scrum

Scrum wird von ihren Erfindern als Gegenentwurf zu den „Taylorisierungs-Tendenzen" des IT-Sektors verstanden. Sie richtet sich also gegen eine Zergliederung des Arbeitsprozesses, die sonst für einzelne Entwickler eine isolierte Arbeit oftmals ohne (direkten) Bezug zum eigentlichen Arbeitsgegenstand zur Folge hat. Eine agile, teamförmige und vor allem selbstorganisierte Vorgehensweise ersetzt die übliche hierarchische Arbeitsorganisation. Im Gegensatz dazu besitzt in den traditionellen Modellen ausschließlich das Management Überblick und Oberhoheit über die Gesamtheit der Abläufe. Die zu vollbringenden Innovationsprozesse werden in der Praxis häufig „top-down" (von oben nach unten) aufgesetzt. Die Folge ist nicht selten ein erheblicher bürokratischer Aufwand über alle Hierarchie- und Abteilungsebenen hinweg.

Scrum dagegen sieht das Entwicklerteam nicht als bloßes Ausführungsorgan. Sondern gibt dem Innovationsteam vielmehr die Gestaltungsvollmacht über den Prozess, inklusive der Vereinbarungen mit den Kunden. Es werden also nicht nur Projektstrukturen geschaffen, die der geforderten Flexibilität und Innovationsfähigkeit nicht entgegenstehen, sondern diese explizit unterstützen. Zentrales Ziel ist eine klare „Emanzipationsperspektive" der Entwickler gegenüber dem Management. Die umsetzenden Innovationsakteure verhandeln Vorgehensweise und Details der Ausführung selbst, anstatt diese von oben vorgegeben zu bekommen. Doch wie sieht das in der konkreten Umsetzung aus? Welche Rollen gibt es in Scrum und wie werden sie verteilt? Diesen Fragen widmen wir uns im Folgenden.

Benutzergruppen

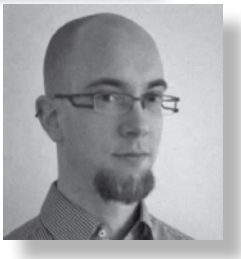
In einem Scrum-Entwicklerteam werden drei Rollen unterschieden: der *Scrum Master,* der *Product Owner* und die Entwickler.[2] Die Aufgabe des Scrum Masters ist es, auf die Einhaltung der Scrum-Prozesse zu achten. Die Arbeitsaufgaben des Teams werden im sogenannten *Sprint Backlog* gesammelt. Der Scrum Master pflegt die Arbeitsaufgaben in das Sprint Backlog und verwaltet sie. Die Entwickler werden durch diese Rollenstruktur von administrativen Aufgaben befreit und können sich ganz auf das Entwickeln konzentrieren. Der Scrum Master motiviert das Team, identifiziert mögliche Schwachstellen und Hindernisse beim laufenden Projekt und soll sie anschließend beseitigen. Er hat keine hierarchische Führungsrolle, sondern ist expliziter Unterstützer des Teams und des Product Owners.

Der Product Owner ist für die Kommunikation mit dem Kunden und die möglichst erfolgreiche Umsetzung des Projekts verantwortlich. Seine Aufgaben umfassen eine reibungslose Einbindung des Kunden, die Gestaltung des Fortgangs der Entwicklung unter Berücksichtigung der Projektfinanzen ebenso wie die Einhaltung relevanter Termine und regelmäßiges Erstellen von (Teil-)Produkten.

Die Entwickler können durch diese aufgeteilten Support- und Überblicksfunktionen möglichst ungestört und effektiv ihrer gemeinsamen Entwicklungsarbeit im Team nachgehen. Neben den dezidiert inhaltlichen Tätigkeiten gehört dazu auch die Verständigung über Stand und Fortlauf des Projekts. Also direkte Kommunikation der Entwickler untereinander. Um das zu gewährleisten und einen Rahmen für die flexible und innovationsfreundliche Arbeitsorganisation zu schaffen, ist die Einhaltung gewisser Prozesse relevant. Diese stellen wir im nächsten Abschnitt vor.

Agile Prozesse – agiles Tool

Während der Entwicklungsarbeit in einem laufenden Projekt können drei wesentliche Prozesse unterschieden werden: das *Sprint Planning,* der Daily Scrum sowie das Review.[3] Im Sprint Planning werden die anstehenden Aufgaben besprochen, wobei ein Sprint ein zeitlich fest definiertes Intervall von zwei bzw. vier Wochen umfasst. Die Arbeitsaufgaben, die in die Sprintplanung aufgenommen werden, ergeben sich aus der zur Verfügung stehenden Arbeitszeit des Teams und dem Aufwand, den das Team für die Bewältigung des jeweiligen Arbeitspakets schätzt. Wichtig dabei ist, dass nicht mehr Aufgaben in den Sprint aufgenommen werden können, als Zeit dafür zur Verfügung steht. Dauern die Aufgaben länger als die abgegebenen Schätzungen, muss priorisiert werden. Die niedriger gerankten Items werden dann in den nächsten Sprint verschoben. Alle Aufgaben werden im sogenannten Sprint Backlog in der Rubrik „To do" hinterlegt.



Daniela Wühr und Stefan Sauer

Dipl.-Soz. **Daniela Wühr** ist Soziologin am ISF München und Promotionsstipendiatin der Hans-Böckler-Stiftung. Sie forscht zu den Themen Fachkräftemangel, Innovation und Innovationsarbeit sowie zu betrieblichen Rationalisierungsstrategien.
daniela.wuehr@isf-muenchen.de

Dipl.-Soz. **Stefan Sauer** ist Soziologe am Institut für Sozialwissenschaftliche Forschung e.V. (ISF), München, mehr Informationen unter *www.isf-muenchen.de*.

Um die Aufgaben zu erfassen und die einzelnen Scrum-Schritte übersichtlich darzustellen, gibt es Unterstützung über verschiedenste Software-Anwendungen. Die IT-Umsetzungen von Scrum sind nicht nur vielfältig, sondern oft webbasiert und größtenteils Open-Source-Software.[4] Das bringt Unternehmen wie Beschäftigten einige Vorteile: zum einen entstehen keine horrenden Anschaffungskosten, lange Service-Verträge, Update-Pflichten oder sonstige Lizenzgebühren. Gleichzeitig ergibt sich dadurch eine grundlegende Offenheit, die Bedürfnisse der eigenen Entwickler aufzugreifen und im Scrum-Tool umsetzen zu können. Die Zufriedenheit der User entsteht vor allem dann, wenn sie partizipativ bei der Gestaltung miteinbezogen werden und die IT-Arbeitsmittel an die konkreten Arbeitserfordernisse angepasst werden.

Die Strukturen von Scrum wie auch die IT-Umsetzungen fördern den direkten Austausch der Entwickler und technischen Experten miteinander: in einem täglichen 15-minütigen Treffen berichten die Teammitglieder über den Fortgang ihrer Arbeiten und aufgetretene Probleme. Dieser Daily Scrum ist fest auf 15 Minuten begrenzt und artet somit nicht in einen typischen Meetingwust aus. Als positiver Nebeneffekt wird außerdem die persönliche Vernetzung des Teams gefördert, genau wie die Möglichkeit, bei Unsicherheiten unmittelbar von Teamkollegen Tipps und Hilfestellungen zu erhalten. Ganz im Sinne eines schlanken Wissensmanagements. Aufgaben, die gerade in Bearbeitung sind, werden im Sprint Backlog in die Rubrik „In Progress" gestellt, die bereits fertig gestellten in die Rubrik „Done".

Der Abschluss eines Sprints bildet die *Review-Phase*. Hier werden die aufgetretenen Probleme in einem Sprint besprochen, aber auch neue Ideen, die inzwischen entstanden sind. Am Ende eines Sprints soll ein Release-fähiges (Teil-)Produkt stehen. Ziel ist außerdem, dass dieses (Teil-)Produkt auch vom Kunden in Augenschein genommen wird. Das ist wichtig, um den Fortgang des Projekts zu überwachen und frühzeitig Fehlentwicklungen gegensteuern zu können. Die regelmäßige Einbindung des Kunden ermöglicht eine vertrauensvolle und flexible Zusammenarbeit und ist Basis für neue Innovationen.

Umsetzung in der Praxis

Unsere aktuellen Forschungsergebnisse aus der IT-Branche zeigen aber auch: Die Umsetzung von Scrum in der Praxis ist von der Theorie häufig sehr weit entfernt. Die von uns analysierten Fälle kann man in vier Idealtypen gliedern.[5] Zu unterscheiden sind der kommunikationsorientierte, der stabilitäts- und produktorientierte, der schutz- und prozessorientierte Typ sowie der nach Lehrbuch.

Beim kommunikationsorientierten Typ wird Scrum vorwiegend als Mittel zur Gestaltung der Kommunikation verwendet. Der Daily Scrum, der häufig ohne zeitliche Befristung stattfindet, ist hier der relevanteste Prozess. Die konkrete Projektplanung wird in diesem Fall nicht direkt von den Teammitgliedern gestaltet, sondern ist meist vom Management vorgegeben.

Beim stabilitäts- und produktorientierten Typ steht die Feinplanung mittels des Sprint Plannings im Vordergrund. Durch diese Planungsprozesse werden die vorgegebenen Entwicklungsschritte – ganz im Sinne des klassischen Projektmanagements – im Team lediglich verfeinert und auf die einzelnen Kollegen aufgeteilt.

Der schutz- und prozessorientierte Typus versteht den Sprint als Schutzraum für das Team. Mittels des Sprint Plannings erstellte Sprint Backlogs werden nicht mehr verändert, das Team erhält sich dadurch den nötigen Raum für Entwicklung und kreative Entfaltung.

Der vierte Typ „nach Lehrbuch" versucht die Scrum-Prozesse trotz teils widriger Umstände möglichst lehrbuchgetreu umzusetzen. Bei diesem Typ ist insbesondere der Scrum Master gefragt, der die Scrum-Prozesse gegen ein klassisches Projektmanagement verteidigen muss.

Die kurze Schilderung der vier Umsetzungstypen deutet auf einige Probleme hin. In den – empirisch am häufigsten angetroffenen – ersten beiden Typen wird Scrum bestenfalls als Ergänzung

Grafik: ISF München

zum klassischen Projektmanagement verwendet. Ein innovationsfreundliches Umfeld wird so meist nicht geschaffen, die Planungshoheit des Managements bleibt erhalten und wird lediglich um eine agile Feinplanung ergänzt.

Eine echte Emanzipationsperspektive der Entwickler ist ausschließlich in den letzten beiden Typen erkennbar. Ein besonders neuralgischer Punkt in den geschilderten Fällen ist die Kommunikation mit den Kunden. Diese erfolgte in beinahe allen Fällen über das Management und nach Maßgabe klassischer Projektmanagement-Logiken. An Stelle einer vertrauensvollen Zusammenarbeit, direkten Einblick des Kunden in die Entwicklung sowie Partizipation an den Prozessen und den Release-fähigen Teilprodukten, tritt ein „klassischer" (Rahmen-)Vertrag mit den Kunden. Anstatt innovationsfreundlicher Flexibilität, eine einseitige starre Stabilisierung, der sich die Entwicklerteams möglichst flexibel anpassen müssen.

Fazit

Ebenso wie zentrale Steuerungslogiken von einer Serienproduktion nicht ohne Folgen in Einzelfertigungsindustrien übernommen werden können, so ist auch eine nach Lehrbuch erfolgende Adaption von Scrum kritisch. Grundsätzlich gilt für das Scrum-Projektmanagement: Die Einführung von Tools und Prozessen aus anderen Kontexten in die eigene Organisation ist nicht unproblematisch. Um die Potenziale und Vorteile von Scrum optimal für das eigene Unternehmen, für die eigene Branche zu nutzen, braucht es eine „Übersetzung" in die eigenen Strukturen und jeweiligen Arbeitskontexte. Diese Übersetzung und Anpassungsleistung kann am besten durch die Beschäftigten selbst geschehen. Schließlich sind Prozesse und Tools dazu da, die Menschen bei ihrer Arbeit zu unterstützen. Die Anwendung im Arbeitsalltag gilt als Validierung, ob die eingeführten Strukturen passen oder nicht. Eine Adaption „bottom-up" (von unten nach oben) durch die Anwender führt nicht nur zu hohem *Commitment,* also dazu, dass die Anwendungen in der Praxis auch gelebt werden. Die Nutzer können selbst am besten einschätzen, welche Methodik, Tools oder Prozesse sie an welcher Stelle benötigen. Gute Innovationsarbeit ist untrennbar mit der Organisation von Arbeit – genauer gesagt: mit der Gestaltung von Projektmanagement – verbunden und daher eine wichtige Aufgabe von Interessenvertretung.

Als agiles Projektmanagement-Tool steht Scrum beispielhaft für innovationsfreundliche, agile Strukturen, emanzipierte Entwicklungsabteilungen sowie einer engen, vertrauensbasierten Zusammenarbeit mit dem Kunden. Unsere Forschungserkenntnisse zu den gängigen Scrum-Praktiken weisen auf zentrale Stolperfallen hin: die (eventuell notwendigen) Adaptionen von Scrum führen oft dazu, dass aus agilem Projektmanagement lediglich eine Unterfütterung der klassischen Projektorganisation wird. Gerade das liegt nicht im Interesse der Kollegen aus dem Engineering (Ingenieurwesen). Tritt dieser Fall jedoch ein, ist Scrum eine Form des demokratisierten Umgangs innerhalb des Entwicklerteams mit top-down gesetzten Anforderungen. Die Emanzipationsperspektive geht dabei größtenteils verloren und Flexibilität bleibt eine einseitige Forderung an die Entwickler, die durch stabile, unflexible Projektorganisation „von oben" noch verschärft wird.

Weiterführendes

Gloger, Boris: Scrum – Produkte zuverlässig und schnell entwickeln, 2009, Carl Hanser Verlag

Schwaber, Ken: Agiles Projektmanagement mit Scrum, 2007, Microsoft Press Deutschland

Schwaber, Ken: Scrum im Unternehmen, 2008, Microsoft Press Deutschland

Projektförderung

Das Projekt „Smarte Innovation" wurde im Rahmen des Forschungs- und Entwicklungsprogramms „Arbeiten – Lernen – Kompetenzen entwickeln. Innovationsfähigkeit in einer modernen Arbeitswelt" aus Mitteln des Bundesministeriums für Bildung und Forschung und aus dem Europäischem Sozialfonds der Europäischen Union gefördert. Betreut wurde das Projekt vom Projektträger im DLR Arbeitsgestaltung und Dienstleistungen. Förderschwerpunkt "Innovationsstrategien jenseits traditionellen Managements".

Das Projekt „TRUST – Teamwork in unternehmensübergreifenden Kooperationen" wird im Rahmen des Forschungs- und Entwicklungsprogramms „Flexibilität und Stabilität in einer sich wandelnden Arbeitswelt" aus Mitteln des des Bundesministeriums für Bildung und Forschung und aus dem Europäischem Sozialfonds der Europäischen Union gefördert. Betreut wird das Projekt vom Projektträger im DLR Arbeitsgestaltung und Dienstleistungen. Förderschwerpunkt "Balance von Flexibilität und Stabilität".

Anmerkungen

1 *Siehe hierzu auch Martin, Mit „Scrum" aus der Krise – Gefährdungsbeurteilung psychischer Belastungen, in: CuA 9/2010, 12 ff.*

2 *Neben den Entwicklerteams gibt es nach der Scrum-Logik das Enterprise Transition Team (ETC), das innerhalb eines Unternehmens die Gesamtverantwortung für die Implementierung von Scrum trägt, sowie das Scroll-Rollout-Team, das ebenfalls die Umsetzung der Prozesse zur Aufgabe hat. Im Text beschäftigen wir uns jedoch ausschließlich mit den Entwicklerteams, die am weitesten verbreitet sind und den deutlichsten Gegenpol zu standardisierten Entwicklungsprozessen bilden*

3 *Die spezifischen Implementierungsprozesse zu Beginn eines Projekts bleiben hier außen vor, vgl. dazu aber die Literaturhinweise unter „Weiterführendes" am Ende des Beitrags*

4 *Siehe zu Open Source auch Frijia, Open-Source-Software – „Freie" Programme für das Betriebs-/Personalratsbüro, in: CuA 10/2010, 33 ff.*

5 *Diese Idealtypen sind weder in der Realität exakt so vorgefunden worden, noch stellen sie „Idealfälle" im Sinne eines wie auch immer gearteten Ideals dar. Ein Idealtyp entsteht vielmehr dann, wenn ähnliche empirische Fälle anhand geteilter und typischer Eigenschaften zu einem solchen verdichtet und von anderen abgegrenzt werden*

Dieser Beitrag ist 2010 in der Zeitschrift Computer und Arbeit (CuA) erschienen. Wir danken den Autoren und CuA für die Genehmigung zum Nachdruck.

Ulrich Klotz

Das „geistige Eigentum“ ad-ACTA

Unlängst war zu lesen, dass den Abgeordneten des Deutschen Bundestags eine Reihe als „geheim“ deklarierter Anhänge des ACTA-Abkommens vorenthalten werden soll(t)en – falls das zutrifft, wäre dies allein schon Grund genug, die Sache abzulehnen und ad acta zu legen.

Dass Rechteinhaber demokratische Prozesse fürchten, ist nichts Neues. Als seinerzeit mit dem Buchdruck ein neues Medium in die Welt kam, versuchten die Verlierer dieses Wandels, die damaligen Rechteinhaber (Hohepriester, Schriftgelehrte u. ä.) auch lange Zeit, ihre Privilegien und Pfründe gegen die mit dieser Innovation einhergehende Umwälzung der (vordemokratischen) Machtverhältnisse zu verteidigen.

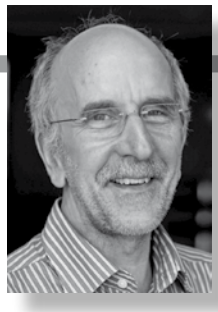
Die aktuellen Versuche, die Wirkungen der Digitalisierung einzufangen und damit nebenbei eine ganze Generation zu kriminalisieren, sind von ähnlicher Güte und Kurzsichtigkeit. Leider plappern viele Politiker den irreführenden Lobbyisten-Sprech vom „Diebstahl geistigen Eigentums“ nach, weil sie – unter anderem wegen dieser unangemessenen Begriffe – noch nicht begriffen haben, dass es bei immateriellen Gütern und deren gemeinsamer Verwendung auch um etwas anderes geht – zum Beispiel um Prozesse kultureller Evolution. Das Vokabular von Juristen ist nicht geeignet, um derartige Vorgänge überhaupt zu verstehen, geschweige denn sinnvoll zu beurteilen. Oder ist der Schüler, der das „geistige Eigentum“ seines Lehrers übernimmt, abkupfert, digitalisiert, „shared“ usw. ein Dieb? Nein, er ist Teil unserer Zukunft und genau darum geht es. Viele, vor allem junge, Menschen spüren genau, dass von der Frage, wie frei oder unfrei in der Wissensgesellschaft unser aller Wissen künftig fließen kann, ihre eigene Zukunft und die der Gesellschaft insgesamt abhängt.

Wenn sich Kommunikationsformen ändern, dann ändert sich das Fundament der Gesellschaft – und heute werden die Weichen gestellt, was auf diesem neuen Fundament erwachsen kann – oder auch nicht. Wohin es führt, wenn in einer Gesellschaft Minderheiten und Funktionäre darüber befinden, was an Kommunikation, was an Wissensaustausch erlaubt ist und was nicht, das sollte bekannt sein. Weil es um fundamentale Fragen gesellschaftlicher Entwicklung und nicht nur um die (organisierten) Interessen von Minderheiten geht, werden die Konflikte vermutlich noch erheblich an Schärfe zunehmen.

Wenn einerseits Jugendliche strafrechtlich verfolgt werden (sollen), bloß weil sie auf YouTube einen geschützten Pop-Song trällern, und es andererseits folgenlos bleibt, wenn Amtsträger mit anonymen Schecks hantieren – dann sind die Proteste gegen das eine wie das andere Indizien für ein gesundes demokratisches Rechtsempfinden, bei dem Twitter & Co. offenkundig eine durchaus förderliche Rolle spielen und von dem sich so mancher Rechtsanwalt (nicht nur im Bellevue) eine Scheibe abschneiden könnte. Die Generation Internet wird sich (hoffentlich) eine Politik nicht mehr bieten lassen, bei der Gesetzesvorlagen von Lobbyisten en detail formuliert und von Volksvertretern kaum noch gelesen, geschweige denn verstanden, sondern lediglich abgenickt werden – was schon Frank Zappa spotten ließ: „Politik ist die Unterhaltungsabteilung der Industrie.“

Statt sich vor den Karren einer kleinen Lobby spannen zu lassen, die wieder einmal – und natürlich vergeblich – versucht, die

Ulrich Klotz



Ulrich Klotz war nach dem Studium als Dipl.-Ing. der Elektrotechnik/Informatik in Computerindustrie und Werkzeugmaschinenbau sowie als Arbeitswissenschaftler an der TU Hamburg-Harburg tätig. Seit den 80er Jahren arbeitete er beim Vorstand der IG Metall und als Stiftungs-Professor an der Hochschule für Gestaltung in Offenbach im Themenfeld „Computer und Arbeit“ vor allem an der Entwicklung und Förderung neuer Arbeits- und Organisationsformen zur besseren Erschließung innovativer Potenziale. Er war langjährig beim BMBF als Beirat und Gutachter tätig und ist derzeit beim Bundeskanzleramt in der Expertengruppe „Zukunft der Arbeit“. Zahlreiche, teilweise preisgekrönte Veröffentlichungen zum Thema Arbeit, Technik und Innovation.

Was mich umtreibt:
Zur Bewältigung der vielfachen Herausforderungen, die sich uns und künftigen Generationen stellen, um unter würdigen Bedingungen auf unserem Planeten zu leben, sind Kreativität und innovative Ideen unabdingbar. Deshalb treibt mich die Frage um, wie wir endlich die Arbeitsformen und innovationsfeindlichen Kommando-Strukturen der Industriegesellschaft überwinden können – zugunsten einer Arbeitskultur, die von gegenseitiger Wertschätzung, Respekt und Toleranz geprägt ist. Beispielgebend hierfür ist die offene Innovationskultur der Open-Source-Communities im Internet – von diesen Kooperationsformen können unsere Institutionen und Unternehmen durchaus etwas über zeitgemäße Arbeitsgestaltung lernen.

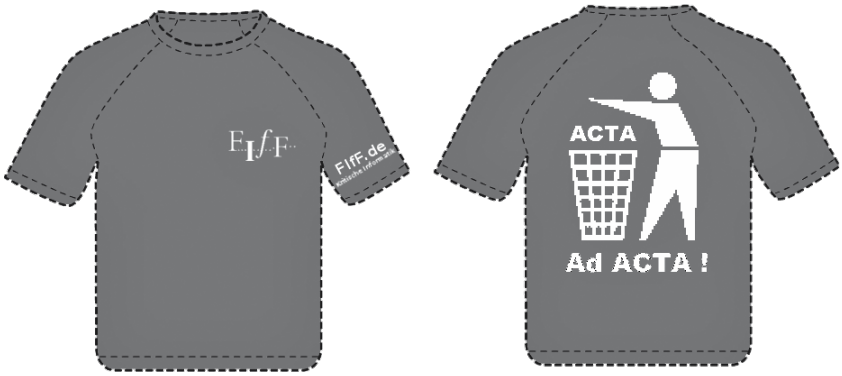
Vergangenheit festzuhalten, sollten die Parlamentarier eine ausufernde Abmahn- und Patentklagen-„Industrie“ in die Schranken weisen, deren oftmals absurde Methoden der Pfründeverteidigung der gesellschaftlichen (und auch der wirtschaftlichen) Entwicklung schaden, weil sie soziale, kulturelle und technische Innovationen massiv behindern und lediglich die Kassen der Anwaltskanzleien füllen.

Um abschließend noch einen Musiker, Neil Young, zu zitieren: „Musikpiraterie ist das neue Radio. So verbreitet sich heute Musik!“ Statt mit sturem Blick in den Rückspiegel den eigenen Karren gegen die Wand zu fahren, empfiehlt sich auch den Rechteinhabern der Blick nach vorne. Es werden sich zeitgemäße innovative Geschäftsmodelle für die Kreativen in der Internet-Ära entwickeln und die Frage ist lediglich, ob die heutigen Rechteverwerter, Verlage, Verbände usw. mit dabei sind oder ob sie Zaungäste eines neuen Spiels werden, dessen Regeln von neuen Playern bestimmt werden. Dass von solchen Innovationen letztlich alle profitieren können, belegen die schon heute erfolgreichen Beispiele.

FIfF e.V.

Legt ACTA ad ACTA!

Am Samstag, dem 11. Februar 2012, fand bundesweit der Aktionstag gegen das umstrittene ACTA Abkommen statt. Die Netzaktivisten trafen sich im Real Life bei klirrender Kälte. In München waren nach Polizeiangaben 16.000 Menschen auf der Strasse, bundesweit mehr als 30.000. Das FIfF ist auf der Unterstützerliste. Wir bieten ein T-Shirt an, mit dem Ihr Eure Meinung zu ACTA kundtun könnt.



Vorbestellungen bitte an die Geschäftsstelle: *fiff@fiff.de* (gewünschte Größe angeben)

Lesen –
Neues für den Bücherwurm

Robert Eppli

Post-Privacy, Prima Leben ohne Privatsphäre

Christian Heller, C.H. Beck, München 2011

Zurzeit erscheinen, auch für eine breite Öffentlichkeit, viele Bücher, die das Thema Datenschutz aufgreifen. Die fortschreitenden technischen Möglichkeiten, die regelrechte Industrialisierung und ständige Professionalisierung des Datensammelns und das damit einhergehende gesteigerte Missbrauchspotenzial machen den Datenschutz zu einem Thema für alle, die am Netz hängen. „Man muss aufpassen auf seine Daten und sich vor Missbrauch schützen“, so der berechtigte Tenor. Ein im letzten Jahr erschienenes Buch präsentiert eine andere Sichtweise: *Post-Privacy, Prima Leben ohne Privatsphäre* von Christian Heller. Der Autor ist Blogger und betreibt eine Webseite: *http://www.plomlompom.de/*.

Wie kommt ein Autor auf so eine Idee?

Das kann doch nicht ernst gemeint sein: *Prima* leben *ohne* Privatsphäre! Christian Heller ist überzeugt: Die *Post-Privacy*-Epoche wird kommen. Seiner Ansicht nach funktioniert das Netz nach dem Prinzip: *Geben und Nehmen*. Ich gebe persönliche Daten von mir preis – ich bekomme Informationen, Antworten

und Kontaktmöglichkeiten aller Art zurück. Wir haben nur die Wahl, am *Sozialkosmos Internet* teilzunehmen – mit der zwingenden Konsequenz der Aufgabe unserer Privatsphäre – oder eben nicht.

Das Netz ist grenzenlos und niemand außer uns selbst kann uns darin schützen. Auch die Justiz, sonst ein verlässlicher *Grenzzieher* in allen Lebenslagen von der Geschwindigkeitsbegrenzung bis zur Parkdauer, kapituliert vor dem Netz. Sollten wir deshalb auch kapitulieren? Christian Heller fragt in seinem Buch:

> *Worin besteht in der heutigen Zeit der Verdienst von Privatsphäre?*
> *Und könnte eine Welt ohne Privatsphäre eventuell auch neuartige Lösungen und Chancen mit sich bringen?*

Bevor der Autor sein persönliches Fazit zieht, durchleuchtet er den Begriff Privatsphäre, wie wir ihn kennen, in seiner geschichtlichen Dimension. Im Kapitel *Die Privatheit im Wandel der Zeit*, zeigt Heller anschaulich, wie sich „die Privatsphäre" erst im Laufe von Jahrhunderten entwickelte und mit dem Wandel des Menschenbilds an Bedeutung gewann. Er beginnt mit der Römerzeit, in der das öffentliche Tun oder Amt („res publica") das Wertvolle und „privare" das Unbedeutende waren. Privatheit kann ein Schutz sein, ihre *verbergende* Wirkung kann aber auch einen uneinsehbaren Raum erzeugen, in dem Ungerechtigkeit und Unterdrückung leichter möglich sind.

Heller geht in komprimierter Form auf die Digitalisierung von Daten und das Entstehen von Internet und Social Networks ein und nennt die neuen Chancen des Netzwerkens, wie beispielsweise Web-Seiten, über die sich Menschen mit der gleichen Erkrankung über die Wirksamkeit von Medikamenten und Therapien austauschen können. Konsequent beschreibt er die neuen positiven Möglichkeiten bis zu jener *The Quantified Self* genannten Spitze, an der eine Bewegung von Netz-Aktiven alles Quantifizierbare über sich ins Netz stellt.

Den neuen Möglichkeiten stellt Christian Heller einen kritischen Blick auf den Datenschutz gegenüber, dem er ein nicht zu leugnendes Vollzugsdefizit attestiert. Es bleibt die Frage: *Stechen die Versprechen der Datenfreiheit die Bedenken des Datenschutzes aus?* (S. 94)

Freiheit vs. Schutz; Wissen und Macht; Nichtwissen ist Ohnmacht

Der Autor verschweigt nicht die Gefahren der *totalen Überwachung*. Er führt dazu ein sehr anschauliches Beispiel an, das *Panopticon*, ein Gebäude, das zur perfekten Überwachung von Gefangenen erdacht wurde. Alle Zellen umschließen einen runden Hof, in dessen Mitte sich der Überwachungsturm befindet. Von dort aus sind alle Zellen einsehbar. Die Überwacher im Turm sieht man nicht.

Was hilft gegen Überwachung? Transparenz! Was hilft gegen Unterdrückung im Verborgenen? Öffentlichkeit! Das Private ist politisch! Es ist damit öffentlich, weil zur Debatte freigegeben. Das war ein Slogan der Frauenbewegung in den 60er-Jahren. Mit dem öffentlichen Bekenntnis „Ich habe abgetrieben" gaben Frauen ihre intimste Privatsphäre preis und haben damit die Gesetzgebung und die Gesellschaft hin zu größerer Freiheit verändert.

Die Beispiele zeigen, dass *Post-Privacy, Prima Leben ohne Privatsphäre* bei weitem nicht so tendenziös ist, wie es der Titel vorgibt. Christian Heller schlägt einen großen Bogen von Orwells *1984* über die Rechteverwertungs-Industrie, Wikileaks und die Piratenpartei. Kaum etwas bleibt auf den knapp 180 Seiten (inkl. Anmerkungsverzeichnis) unerwähnt.

Zwar stellt er seine These zu Beginn des Buches unmissverständlich dar: *Die Privatsphäre ist ein Auslaufmodell […] Wir müssen lernen damit klarzukommen.* (S. 7) Im weiteren Verlauf ist seine Argumentation überraschend (enttäuschend?) ausgewogen. Wer einseitige, beißende Polemik erwartet, könnte sogar enttäuscht sein. Christian Heller bringt unverbrauchte Perspektiven in die Diskussion ein. Er stellt in seinem Fazit den *Schutz der Privatsphäre* und damit einhergehende Regulierungen seiner Idee einer *transparenten Gesellschaft* gegenüber. Er setzt auf die Anarchie des Netzes, in der *informationelle Waffengleichheit* auch und gerade von unten nach oben gelten muss. „Alle Informationen für Jeden", weil die Möglichkeiten größer sind als die Risiken. Eine gewagte Utopie.

(Noch) kann (mit Einschränkungen) (fast) jede/r selbst frei entscheiden. Sind das schon zu viele Einschränkungen?

Über den Rezensenten

Robert Eppli arbeitet als System Engineer bei einem Softwarehersteller für Sicherheitslösungen. Er ist geprüfter Datenschutzbeauftragter und engagiert sich beim *Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V* im Arbeitskreis *Datenschutz geht zur Schule*.

Viren als Mittel des Cyberwar

Ein Rückblick auf die achtziger Jahre

Nicht erst heute wird in Militärkreisen über den Cyberwar diskutiert. Bereits in den achtziger Jahren – zu einer Zeit also, als die weltweite Vernetzung erst am Anfang stand – wurde über Möglichkeiten nachgedacht, in gegnerische Computersysteme einzudringen und sie zu schädigen. „Kampfviren" wurden damals als militärische Waffe gegen den Feind – noch waren wir im Kalten Krieg – propagiert. Gleichzeitig standen Militär und Geheimdienste vor der Frage, wie sie kompetente Spezialisten für diese Art der Kampfführung rekrutieren können.

Passend zum Schwerpunkt der FIfF-Kommunikation 4/2011, und dem Beitrag von Sylvia Johnigk und Kai Nothdurft in dieser Ausgabe, dokumentieren wir hier zwei Texte des FIfF aus dieser Zeit: In der Ausgabe 2/1989 nahm der damalige FIfF-Vorstand zu einem Artikel Stellung, in dem ein Oberstleutnant der Bundeswehr Viren als Mittel der Kriegführung empfiehlt. In der darauf folgenden Ausgabe schrieb Ingo Ruhmann über Computersabotage, militärisches „Hacken" und den Versuch, Personal dafür zu gewinnen.

Die heutige Vernetzung von Computersystemen war damals noch kaum vorstellbar – der Siegeszug des Internet und des World Wide Web setzte erst drei Jahre später ein. Heute wird im Zusammenhang mit Cyberwarfare bereits wieder über Entnetzung diskutiert. Letztendlich werden die immer gleichen Debatten geführt – Krieg oder Frieden ist aber keine Frage der verwendeten Technik. Abrüstung muss in den Köpfen beginnen – damals wie heute.

FIfF e.V.

Computerviren – ein Kampfmittel der Zukunft?

Stellungnahme des FIfF-Vorstands zu einem Artikel von Oberstleutnant Erhard Haak in: Soldat und Technik 1/89, S. 34f

Bei ihrer Suche nach neuen Zerstörungsmitteln haben Militärs jetzt das Computervirus entdeckt. Nach Haaks Aussagen ließen sie sich für militärische Programme und Computersysteme einfach entwickeln. Ihre „subversive Einnistung" in Computersysteme des Feindes sei „sowohl im Frieden als auch im Krieg" möglich. Eine moderne Armee „würde in ihrer Operationsführung unblutig und nahezu kostenfrei, dafür aber nachhaltig, beeinträchtigt werden, wenn es zum Einsatz von ‚Kampfviren' käme." Wäre, so fragt er, „der militärische Bereich nicht gut beraten, sich auf den Einsatz dieses Mittels zumindest präventiv einzustellen?"

Wenn sich Haak auch bei den Möglichkeiten, Computerviren im Feindesland einzubauen, überschätzen mag, so ist doch der Einbau von Virus-Minen in lebenswichtige Steuerungsprogramme des eigenen Lagers vergleichsweise ein Kinderspiel. Nach den Sprenglöchern für Atomminen in Brücken und wichtigen Verkehrswegen bieten sich Viren – beispielsweise in Telefonnetzen und in Kraftwerkssteuerungen – der Militärtechno-Logik geradezu an. Damit könnte ein Programm „Verbrannte Erde" billiger werden.

Feinsinnig – vielleicht präventiv? – bewertet Haak auch derartige Aktionen: „Die zivilen Virus-Programmierer können als Terroristen bezeichnet werden, ganz gleich, welche Motive hinter ihrer Arbeit stehen. Wird die Arbeit einmal zum Kampfauftrag im militärischen Sinne werden, dann können sie wohl nur als Saboteure agieren."

Als Computerfachleute müssen wir eindringlich vor dem Einnisten von Viren in lebenswichtige Computerprogramme – egal, ob militärischer oder ziviler Art – warnen. Programme, von denen wir wissen, daß sie nicht fehlerfrei sind, dürfen nicht absichtlich unberechenbar gemacht werden. Wir fordern alle Informatikerinnen und Informatiker auf, sich nicht an Entwicklung und Einbau von Viren in lebenswichtige Systeme zu beteiligen!

Fünfzig Jahre nach dem Überfall auf Polen und fünfundsiebzig Jahre nach dem Beginn des ersten Weltkriegs rufen wir darüberhinaus die verantwortlichen Politiker und Politikerinnen in der Bundesrepublik auf, den Primat der Politik endlich ernst zu nehmen und dem unheilvollen, verantwortungslosen Unfug computergläubiger Militärs Einhalt zu gebieten!

Originalquelle: F!FF-Kommunikation 2/1989, Seite 22.

Ingo Ruhmann

KGB-„khaker“ und CIA-Viren

Hacker, die fürs KGB arbeiten, Viren, mit denen CIA, NSA und andere Ost-Computer lahmlegen: aus den Spielchen gelangweiter Systemfreaks ist makaberer Ernst geworden. Was ist dran an militärischen Viren, wie bedrohlich sind sie, wie weit sind die Hacker in Uniform?

Informatik zwischen Ost und West war immer etwas von der anderen Art. Irgendeine Seite hatte immer etwas zu verbergen. Bis zum Anfang der achtziger Jahre gingen die Geschichten etwa so: Da wird ein Wartungstechniker zu einer darniederliegenden VAX irgendwo in der tiefsten Sowjetunion gerufen. Bepackt mit allen Schrankkoffern, die man so für eine größere Reparatur in entlegeneren Teilen der Welt braucht, macht sich unser guter Mann auf. Angekommen geleitet man ihn durch eine Tür hindurch, in einen aus Holzbrettern zusammengenagelten Gang. An seinem Ende weitet sich der Gang zu einem ebenfalls frischgezimmerten Raum, in dem die sieche Maschine steht. Abschußrampe, Fabrik? Der Techniker hat nie gesehen, wo der Computer stand.

Aufschneiderei oder Wahrheit – mit derartigen Stories war jedenfalls Schluß, als die Reagan-Regierung dem Ost-West-Technologietransfer den Hahn abdrehte. Nun hatte der Westen etwas zu verbergen: seine gesamte Computertechnologie. Seitdem gibt es in der Ost-West-Informatik nur noch „Techno-Bandits“, Spione und natürlich jede Menge Publicity-Stunts. Alles, was mit Computern zu tun hatte, wurde in den letzten Jahren genauso behandelt wie Kriegsgerät. Die Computertechnologie bekam vor allem für die USA strategische Wichtigkeit.

Passend zu diesem schweren strategischen Geschütz wurden in der Vergangenheit in aller Heimlichkeit die taktischen Waffen entwickelt. Computer-Viren sind eine dieser Waffen, beamtete „Hacker“, militaristische Computer-Saboteure, die Special Forces dieses Computerkrieges.

Der Fall der „KGB-Hacker“ im März dieses Jahres (1989, die Redaktion) hat den Vorhang über diesem neuen Kampfplatz gelupft. Dabei spielt es für die Militärstrategen keine Rolle, wie neu die ganze Story überhaupt war, wie viel die Freizeithacker zusammenkopiert haben und wie sinnvoll es für den KGB war, von Hannover an der Leine aus das Modem in Schwingungen zu bringen, statt von Halle an der Saale aus, was auch nur bedingt das Risiko mindert hätte, von den Überwachern der NSA erwischt zu werden. Wichtig ist für die Militärs, daß sie da ein neues Arbeitsfeld wittern. Zu den Vorstellungen eines Oberstleutnants der Bundeswehr gab es ja bereits in der F!FF-Kommunikation 2/89 eine Stellungnahme des FIFF.

Zwar gibt es bei den staatlichen „Stellen“ zur Zeit kaum findige Hacker, die wirklich dem Bild entsprechen, das sich die Geheimdienst- und Sabotagefritzen von den Möglichkeiten der Hacker machen, aber dem wird ja schon nachgeholfen. Steffen Wernery vom Chaos Computer Club erklärte, der Verfassungsschutz sei an ihn schon herangetreten mit dem Druckmittel, bei einer Zusammenarbeit gäbe es keinen Ärger mit den sogenannten „Hackerparagraphen“. Wernery lehnte ab – die Reaktion anderer ist jedoch nicht bekannt. Dieser Vorfall zeigt, wieviel Bedeutung das Thema Hacken für die Krieger unserer inneren und äußeren Sicherheit hat und wie verzweifelt sie nach Mitteln und Wegen suchen, um erstens einen Überblick zu bekommen, zweitens an fähige Leute zu kommen, drittens sich selbst so viel Ahnung zuzulegen, um diese Art des Umgangs mit Computern für die eigenen Zwecke zu nutzen und viertens ihre ungeliebten zivilen „Vorbilder“, die Hacker, auszuschalten: Hacker, die sich den freien Datenaustausch auf die Fahnen schreiben und denen Geheimhaltung eine Sauerei ist, sind ein dicker Dorn im Auge all jener Geheimniskrämer, die möglichst viel für sich behalten wollen.

Hacken für Vater Staat

Der Weg zur staatlichen Computer-Sabotage orientiert sich zur Zeit also an vier Punkten. In all diesen Punkten ist unser, sind andere Staaten aktiv:

1. Den Überblick bekommen

Vor allem aus Angst um Sicherheitslücken hat die Bundesregierung einen „Interministeriellen Ausschuß für die Sicherheit in der Informationstechnik (ISIT)“ gebildet und die Zentralstelle für das Chiffrierwesen (ZfCh)[1], die sich bisher mit Chiffrierfragen und der Abstrahlsicherheit von Computersystemen beschäftigt hat, mit der Entwicklung von Kriterien zur Computersicherheit allgemein betraut. Die ZfCh wird in Zukunft weiter ausgebaut werden zur „Zentralstelle für das Chiffrierwesen und die Sicherheit in der Informationstechnik“. Hier wird also fortgeführt, was bisher schon Hauptarbeitsfeld staatlicher Systemspezialisten war: die Erstellung „sicherer“ Systeme. Ein Nebenprodukt ist dabei eine Abschätzung über die Gefahrensituation und ihre Verursacher.

2. An Leute kommen

Was das BKA in der Entdeckung von Computerkriminalität sein will, wird offenbar vom Verfassungsschutz durch das Anwerben von Hackern fürs Hacken sinnig ergänzt. Steffen Wernery ist kaum ein Einzelfall. Hacken bedeutet für den Verfassungsschutz dabei nicht die bessere Eigensicherung, denn dafür arbeiten dort schon Experten, sondern gerade auch die Spionage in fremden Dateien und Mailboxen. „Legal“ hacken also nur noch für Vater Staat! BND und MAD für diesbezüglich gänzlich desinteressiert zu halten, wäre eine grobe Unterschätzung dieser Dienste.

3. Eigene Kompetenzen erwerben

Gerade was den BND angeht, so kannte man die immer etwas abseits stehenden Herren im Trenchcoat von der „Bundesvermögensverwaltung in Pullach“ bisher schon aus allen möglichen DV-Kursen, meist aber zu solch simplen Sachen wie Datenbanken, „mein Editor und ich“ und andere Einführungskurse. So werden langsam Geheimdienstler zu DV-Leuten geschult – andersherum ist es schwieriger, weil für den BND kaum sicher genug. Dort und anderswo hat man aber die jüngsten Entwicklungen sorgsam registriert und lernt jetzt dazu.

Hilfreich könnten bei diesem Lernprozeß zum Beispiel die Erfahrungen der Hochschule der Bundeswehr sein, die schon Ärger mit „Viren“ hatte: Zum Jahreswechsel 1984/85 zerstörte sich das Graphik-System GURUGS 2001, weil dessen Programmierer entlassen worden war. Und da die Bundeswehr nicht nur frustrierte Programmierer, sondern auch frustrierte Wehrpflichtige an ihre Computer läßt, dürfte dies kein Einzelfall sein. Auch mit ihren militarisierten PCs unter MS/DOS dürfte die Bundeswehr in Anbetracht der Viren für dieses Betriebssystem einem Feldversuch entgegengehen, den sie sich so nicht vorgestellt hatte. Hier besteht also ein weites Feld, praktische Kompetenz zu erwerben.

4. Die Hacker kaltstellen

Dazu hat man zwar jetzt geeignete Gesetze, aber es muß ja erst mal jemand einen Hacker bemerken und dessen dann auch noch habhaft werden. Mit ISDN versprechen sich einige besseren Schutz vor Attacken von außen, aber dies wird bestenfalls zu einer verbesserten Tarnung echter Hacker sowie zu geeigneten Manipulationen an ISDN-Komponenten führen.

Weil also Hacken von außen genausowenig aufhören wird, wie das Fummeln an Programmen durch Insider, und weil Wirtschaft und Staat eher ein paar Hacker jagen als ihre Systeme wenigstens ein wenig sicherer zu machen, wird sich die Hackerhatz verschärfen. Sobald irgend jemand in Wirtschaft und staatlicher Verwaltung künftig geärgert wird, werden die Antihackergesetze wesentlich verschärft werden.

007 im Rechenzentrum

Währendessen gehen im Ausland die Aktivitäten im Bereich Computer-Sabotage bereits viel weiter als die meisten glauben wollen. Nachdem ebenfalls Anfang März dieses Jahres ein sowjetischer Militärattaché aus den USA ausgewiesen wurde, weil er sich für Details von Computer-Sicherheits-Software interessierte, rückte das amerikanische Nachrichtenmagazin TIME mit der Nachricht heraus, daß amerikanische Dienste in der Vergangenheit „beachtlichen Erfolg dabei hatten, geheime militärische Computersysteme in der Sowjetunion und anderern Ländern zu penetrieren. Die Regel, erklärte ein Experte, sei, daß bei jedem Land, dessen sensitive Kommunikation wir (die USA) lesen können, wir auch in ihre Computer gelangen können.“ Dabei wird allerdings nicht nur per Telefon in entfernte Computersysteme, sondern auch durch Agenten vor Ort in Computerzentren eingebrochen. Dort kommt ihnen dann zupaß, daß eine Reihe von Computern Modelle US-amerikanischer Firmen sind.

Spezialist für alle Arbeiten dieser Art ist die NSA, deren weltumspannendes Abhörnetz ja erst kürzlich (im Spiegel 8/89) wieder für ein wenig Aufregung sorgte. NSA und CIA haben bereits mit Viren in Computersystemen „anderer Nationen“ experimentiert mit dem Ziel, diese Systeme lahmzulegen. Von welcher Art und welchem Umfang diese Viren-Infektionen sind, bleibt unklar; einigen Leuten bei NSA und CIA geht es jedoch zu weit – sie fürchten Vergeltungsaktionen.

Zwar glauben sich die US-Dienste und das Pentagon vor solcher Art der Vergeltung dadurch relativ sicher, daß sie in den letzten vier Jahren ihre Kommunikationsnetze vor allem durch Chiffrieren sicherer gemacht haben. Allerdings wird das nicht genug sein: 1985 stellte eine Studie des Department of Defense Computer Science Center fest, daß von den 17.000 DoD-Computern nur 30 die minimalen Sucherheitsstandards erfüllten, 99,83 % also als unsicher eingestuft werden mußten. Zwei Drittel der untersuchten DoD-Stellen gaben sich noch nicht einmal die Mühe, den Fragebogen der amtlichen Studie auszufüllen.

Computersabotage als Mittel geheimdienstlicher und militärischer Auseinandersetzung ist heute keine Science-Fiction mehr. Je mehr Ost und West auf dem Computersektor zusammenrücken – der erste amerikanisch-sowjetische Teleport existiert bereits und eröffnet NSA-Leuten vielleicht bald die Möglichkeiten der Teleheimarbeit –, desto größer werden die „Chancen“ für die dienstlichen Computersaboteure und die Risiken für Bürgerinnen und Bürger. Ziel derartiger Angriffe sind nicht nur militärische Computer, sondern alles, was Verwirrung bringt und leicht zu infizieren ist, also gerade auch die Systeme der zivilen Infrastruktur. Und es muß nicht immer der böse Gegner sein, der da am Code fummelt, denn viel öfter haben die besten Freunde Motiv und Gelegenheit, lästige Konkurrenten zu behindern, politische Strömungen zu beeinflussen oder ähnliches.

InformatikerInnen sollten sich hierfür nicht mißbrauchen lassen und ein echter Hacker wird kaum vergessen, daß Computersabotage mit Hacken nichts zu tun hat. Stattdessen sollten wir alle diesen Unsinn unterbinden, wo wir das können. Verantwortliches Handeln, das heißt in diesem Falle sowohl Öffentlichkeit herstellen als auch selbst für Abhilfe sorgen. Jedes für sich: die immer größere Abhängigkeit von Computersystemen und darin sabotierende Staatsterroristen, ist bereits Blödsinn genug. Beides zusammen können wir uns nicht leisten.

Anmerkungen

1 Das heutige Bundesamt für Sicherheit in der Informationstechnik (BSI).

Originalquelle: F!FF-Kommunikation 3/1989, Seiten 28-29.

Wir danken dem Autor für die Genehmigung zum Nachdruck.

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.

Das FIfF-Büro

Geschäftsstelle FIfF e.V.
Goetheplatz 4, D-28203 Bremen
Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56
E-Mail:fiff@fiff.de

Die aktuellen Bürozeiten entnehmen Sie bitte unseren Webseiten.

Bankverbindung:
Sparda Bank Hannover eG
Spendenkonto: 800 927 929
BLZ 250 905 00
IBAN: DE66 2509 0500 0800 9279 29
BIC: GENODEF1S09

FIfF im Netz

Das ganze FIfF:
www.fiff.de

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 Abmeldung unter
http://lists.fiff.de/mailman/listinfo/cctv-L
Beiträge an: *cctv-L@lists.fiff.de*

Beirat

Michael Ahlmann (Bremen); **Peter Bittner** (Bad Homburg); **Dagmar Boedicker** (München)**; 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); **Dr. Eva Hornecker** (Glasgow/UK); **Werner Hülsmann** (Konstanz); **Ulrich Klotz** (Frankfurt); **Prof. Dr. Klaus Köhler** (München); **Prof. Dr. Herbert Kubicek** (Bremen); **Prof. Dr. Klaus-Peter Löhr** (Berlin); **Dipl.-Ing. Werner Mühlmann** (Oppburg); **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); **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
Jens Rinne – Mannheim
Raffael Rittmeier – Bremen
Prof. Dr. Britta Schinzel – Freiburg im Breisgau
Ingrid Schlagheck – 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	**1.200 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
Schwerpunktredaktion	Dagmar Boedicker, Sylvia Johnigk und Kai Nothdurft
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@mtsf.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	Deckblatt vom Flyer zur FIfF-Jahrestagung 2011 in München Flyer-Layout & -Design: Idealistik
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.

Aktuelle Ankündigungen

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

SIGINT 2012
18. bis 20. Mai in Köln

FIfF-Jahrestagung 2012
9. bis 11. November in Fulda

FIfF-Vorstandssitzung

Mai in Frankfurt am Main (genauer Termin offen)
September in München (genauer Termin offen)
11. November in Fulda (im Rahmen der Jahrestagung)

FIfF-Kommunikation

2/2012 »Verfassungsbeschwerden«
Jens Rinne, Raffael Rittmeier u.a.
(Redaktionsschluss: 4.5.2012)

3/2012 »Visualisierung«
Britta Schinzel u.a.

4/2012 »Enquête-Kommission Internet und digitale Gesellschaft«
Stefan Hügel u.a.

W&F – Wissenschaft & Frieden:

4/11 – »Arabellion« Demokratie im Arabischen Raum
1/12 – Schafft Recht Frieden?

DANA – Datenschutz-Nachrichten:

1/12 – Europäische Datenschutzrichtlinie
2/12 – Soziale Netzwerke
3/12 – Umfragen

Das FIfF-Büro

Geschäftsstelle FIfF e.V.
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*

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

Wichtiger Hinweis: Postvertriebsstücke wie die FIfF-Kommunikation werden von der Post auch auf Antrag nicht nachgesandt; daher bitten wir alle Mitglieder und Abonnenten, dem FIfF-Büro jede Adressänderung rechtzeitig bekannt zu geben!

Schluss FIfF

Piero Masztalerz – www.masztalerz.wordpress.com

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