H 7625

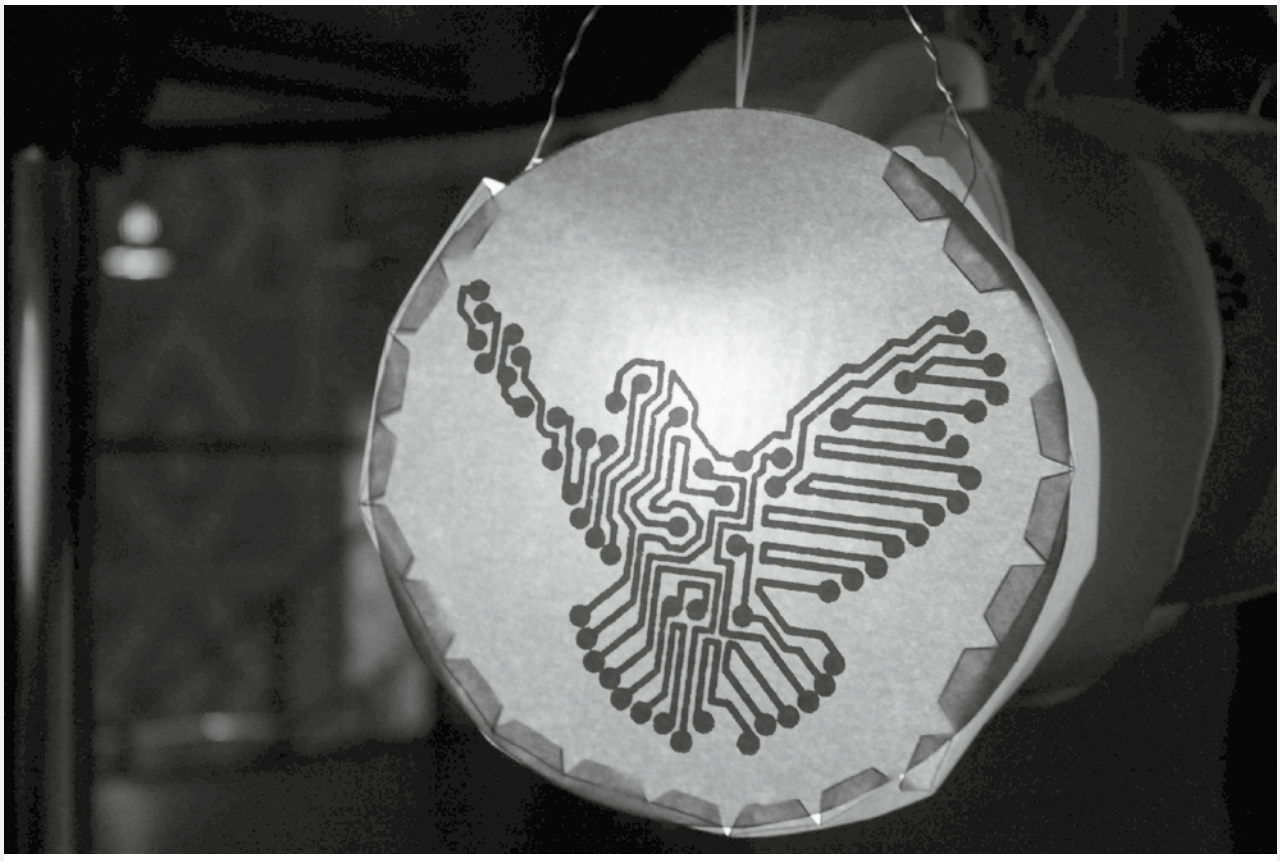
FIfF-Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

31. Jahrgang 2014 Einzelpreis: 7 EUR

4/2014 – Dezember 2014

30 Jahre FIfF –



Informatik für den Frieden

ISSN 0938-3476

• Laudatio Studienpreis • Elektroschrott in Ghana • 25 Jahre Internet •

FIfF-Kommunikation

Titelbild: Cyberpeace Laterne, Kai Nothdurft CC BY

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V.

Inhalt

Ausgabe 4/2014

inhaltt

FIfF e. V.

Aktuelles

Schwerpunkt „30 Jahre FIfF"

Lesen & Sehen

Rubriken

Editorial

Seit nunmehr 30 Jahren setzt sich das FIfF für die friedliche Nutzung der Informatik ein, und dafür, die militärische Kolonialisierung des Internets und der Kommunikationsinfrastrukturen zurückzudrängen. Sicherlich sind Erfolge hier schwer zu erreichen – zu übermächtig sind die Interessengruppen, die die militärischen Anwendungen der Informationstechnik vorantreiben, sei es aus politischen, sei es aus wirtschaftlichen Gründen.

Dennoch werden wir auf diesem Weg fortfahren. Im Schwerpunkt dieser Ausgabe der *FIfF-Kommunikation* blicken wir auf 30 Jahre FIfF zurück und auf die Anfänge im ersten Rundbrief des FIFF (sic!), der noch mit Schreibmaschine und Nadeldrucker hergestellt wurde. Gleichzeitig schauen wir in die Zukunft: zu den politischen Aufgaben, die das FIfF in den kommenden Jahren herausfordern werden.

Rückschau auf *30 Jahre FIfF* hält in seinem Beitrag *Ralf E. Streibl*: *warnen und mahnen. diskutieren und begleiten. vorausschauen und fordern. „Das FIfF ist weiter auf einem guten und wichtigen Weg. In einer von Schnelllebigkeit, Effekten und Unverbindlichkeit geprägten digitalen Welt geht das FIfF seine eigenen Wege – mal im Verbund mit anderen, mal alleine, mal digital, mal erfrischend analog, mal mit einzelnen Akteur.innen, mal in Kampagnen und im Team."*

Zwei Beiträge aus dem ersten Rundbrief vom August 1984 folgen. *Hans-Jörg Kreowski* schrieb über die Gründungsversammlung des FIfF am 2. Juni 1984 in Bonn: *Aufbruch zu einer neuen Informatik*. In ihrem Schlüsseltext für die Arbeit des FIfF stellte die Gründungsvorsitzende *Christiane Floyd* die Frage: *Wo sind Grenzen des verantwortbaren Computereinsatzes?*, und beantwortete sie mit einer Analyse, in der sie zwischen fachlicher, zwischenmenschlicher und moralisch/politischer Verantwortung unterschied. Durch die Diskussionen im FIfF wolle sie dazu beitragen, eine im Gegensatz zur militärischen Anwendung stärker an menschlichen Werten orientierte Informatik zu schaffen. Der Text hat nach 30 Jahren kaum an Aktualität eingebüßt.

In persönlichen Beiträgen zeichnen drei langjährige Mitglieder ihren Weg in die Informatik und in das FIfF nach. *Ein Leben in Frieden ist erstes Menschenrecht*, so die Motivation von *Klaus Fuchs-Kittowski*; er beschreibt als Bürger der ehemaligen DDR die Entwicklungen vor und nach der staatlichen Vereinigung ebenso wie seine Folgerungen aus heutiger Sicht. *Britta Schinzel* stellt ihren Weg in die Informatik und in das FIfF dar, bei dem ihr gesellschaftliches Engagement eine wesentliche Rolle spielte. *Dirk Siefkes* skizziert seine Arbeit an der Frage, welche Wechselwirkung zwischen unserer Vorstellung von geistigen Tätigkeiten mit der von Maschinenabläufen besteht und wie das die Entwicklung von IT und Informatik beeinflusst.

Mit Sicherheitspolitik befassen sich die folgenden beiden Beiträge: Mit *Unsicherheit und Institutionen* setzt sich *Dagmar Boedicker* unter dem Eindruck auseinander, dass manche unserer Institutionen dem 21. Jahrhundert nicht mehr gewachsen sind. Sie stellt in ihrem Beitrag *Schwächen der alten Institutionen, Perspektiven für neue und die Beziehung zum FIfF* dar. In ihrem Beitrag *Eine Frage der Begriffe* ordnet *Christine Hegenbart* diese ein und bietet Definitionen an. „*Der korrekte Umgang mit allem, was die Vorsilbe ‚Cyber-' besitzt, ist dringend notwendig*", stellt sie dazu einleitend fest.

Mit den neuen Kriegen setzen sich die folgenden vier Beiträge auseinander. Den Anfang machen unsere *Forderungen zur Cyberpeace-Kampagne*, die wir laufend weiterentwickeln und diskutieren. *Der Missbrauch der Informationstechnik für die ‚Revolution' des Kriegsgeschäfts* ist Thema des Beitrags von *Hans-Jörg Kreowski* und *Dietrich Meyer-Ebrecht*, der unserem in diesen Tagen erscheinenden Buch *Gesellschaftliche Verantwortung in der digital vernetzten Welt* entnommen ist und gleichzeitig darauf neugierig machen will. Unserer Kooperation mit der Zeitschrift *W&F – Wissenschaft und Frieden* verdanken wir den Beitrag von *Thomas Reinhold*: *Friedens- und sicherheitspolitische Fragen zur Militarisierung des Cyberspace*. „*Angesichts der einmaligen historischen Situation, dass der Cyberspace ein vollkommen vom Menschen geschaffener Raum ist und dessen Funktionsweise frei definierbaren Grundsätzen folgt, besteht Anlass zur Hoffnung auf eine friedliche Zukunft im Cyberspace*", so das optimistische Fazit des Beitrags. *Cyberwar – Schimäre oder reale Bedrohung?*, fragen *Sylvia Johnigk*, *Hans-Jörg Kreowski* und *Kai Nothdurft* in ihrem Beitrag, der auf die Tagung *Quo vadis NATO?* in Bremen zurückgeht. Er ist eine reale Bedrohung, so das Ergebnis ihrer Untersuchung: „*Cyberattacken sind alltäglich, Cyberkrieg erhöht die Kriegsgefahr, Cyberrüstung bedroht die Zivilgesellschaft.*"

Im aktuellen Teil gibt es in dieser Ausgabe neben den regelmäßigen Kolumnen – dieses Mal von *Aaron Lye*: *Betrifft: Cyberpeace* und *Sebastian Jekutsch*: *Betrifft: Faire Computer* – zunächst weitere Beiträge zum Ranking von IT-Produkten nach dem Gesichtspunkt fairer Herstellung und zum Umgang mit Elektroschrott in Ghana.

Marie-Theres Tinnefeld verweist danach auf die *Wahrung der Menschenrechte – Eine Voraussetzung der europäischen Friedensordnung*. „*Seit dem schwarzen Tag 9/11 werden häufig Gesetze ohne hinreichende Anbindung an Grund- und Menschenrechte in Parlamenten verabschiedet und von einer unbestimmten Furcht vieler Bürger mitgetragen*", stellt sie fest. Dietrich Meyer-Ebrecht erinnert an das 25jährige Bestehen des *World-Wide-Web* und zeichnet den Weg *von der Utopie einer grenzenlosen Freiheit zum total kontrollierten Raum*.

Weitere Beiträge runden die Ausgabe ab. Der FIfF-interne Teil enthält Berichte von der FIfF-Konferenz und vom Campact-Kongress im November in Berlin sowie mehrere aktuelle Stellungnahmen.

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

Stefan Hügel
für die Redaktion

Brief an das FIfF

Doppeldenk

Liebe Mitglieder des FIfF, liebe Leserinnen und Leser,

mit *Doppeldenk* – oder, in meiner älteren Ausgabe, *Zwiedenken* – bezeichnet George Orwell die Fähigkeit, im Denken zwei widersprüchliche Überzeugungen aufrechtzuerhalten und beide zu akzeptieren. Als wahre Meister dieser Disziplin erweisen sich gerade einige unserer Volksvertreter.innen in Berlin:

In umfangreichen Feierlichkeiten wird das 25jährige Jubiläum des Mauerfalls begangen, der das Ende von Stasi-Bespitzelung und DDR-Unrecht brachte – fast gleichzeitig wird der Bundesnachrichtendienst mit weiteren 300 Millionen Euro an Steuergeldern ausgestattet, um neue Bespitzelungstechnologien gegen die Bevölkerung zu entwickeln. Die Ausspähung durch NSA und Partnerdienste dauert nunmehr eineinhalb Jahre nach ihrer Aufdeckung weiter an, ohne dass die Bundesregierung erkennbare Versuche unternehmen würde, ihr ein Ende zu setzen. Eher wird versucht, dem NSA-Untersuchungsausschuss des Deutschen Bundestages die Arbeit zu erschweren.

Zu Recht trauern wir um die Opfer des DDR-Grenzregimes, um die Toten der Berliner Mauer und des Todesstreifens an der innerdeutschen Grenze. Gleichzeitig nehmen wir in Kauf, dass an den EU-Außengrenzen Zigtausende ihr Leben verlieren: Menschen, die vor Krieg und Elend aus ihren Heimatländern fliehen müssen.

Der gerade erfolgten Regierungsbildung in Thüringen ging die Diskussion voran, ob die DDR als Unrechtsstaat zu bewerten sei. Natürlich war die DDR ein autoritärer, repressiver Staat ohne rechtsstaatlichen Schutz seiner Bürger.innen, doch die Debatte wurde wohl eher zur politischen Diffamierung einer demokratisch gewählten Partei instrumentalisiert. Auch hier war Doppeldenk im Spiel; bei Twitter könnte man es vereinfacht vielleicht so formulieren:

> *Sicher war die #DDR ein Unrechtsstaat: Dort wurden die Menschen bespitzelt #nsa #bnd, und es gab eine nahezu unüberwindbare Grenze #frontex.*

Eine großartige FIfF-Konferenz konnten wir im November in Berlin erleben. *Der Fall des Geheimen – Ein Blick unter den eigenen Teppich*: Das hochkarätige Programm lockte rund 400 Besucherinnen und Besucher in die Technische Universität. Referentinnen und Referenten, darunter Matthias Bäcker, Wolfgang Nešković, Peter Schaar, Erich Schmidt-Eenboom, Patrick Sensburg, Hans-Christian Ströbele und viele mehr, die allein aus Platzgründen hier nicht genannt werden, haben die Rolle Deutschlands und der deutschen Geheimdienste im Kontext der älteren und jüngeren Erkenntnisse – von Echelon über PRISM bis Eikonal – beleuchtet und Handlungsoptionen erarbeitet. Unser Dank geht an das Berliner Organisationsteam und an unsere Unterstützer, die für eine fantastische Konferenz gesorgt haben.

Natürlich muss die Bearbeitung des Themas nun weitergehen – und da hilft uns eine weitere großartige Nachricht, die uns kurz vor der Tagung erreicht hat: Die Stiftung Bridge wird unsere Kampagne *Cyberpeace* mit einem fünfstelligen Betrag finanziell fördern und durch vielfältige Beratung die Kampagnenfähigkeit des FIfF verbessern helfen. Wir wollen mit unserer Kampagne dazu beitragen, das Internet zu entmilitarisieren, seine ausschließlich friedliche Nutzung zu erreichen und Cyberwaffen und Cyberkrieg entgegentreten, denn – man kann es nicht häufig genug wiederholen:

- Cyberwarfare beginnt mit der Überwachung der Zivilgesellschaft – diese Ausspähung verletzt die Privatsphäre des Menschen und damit die Menschenwürde als ein elementares Menschenrecht.

- Voraussetzung für die Überwachung ist die Manipulation von IT-Systemen und der Einbau von Schwachstellen. Die Folge sind unzuverlässige und unsichere Computer- und Kommunikationssysteme wie das Internet, von deren reibungslosem Funktionieren weite Teile unserer Gesellschaft abhängig sind. Für Cyberwarfare wird die Sicherheit der zivilen IT-Infrastruktur ausgehöhlt und untergraben.

- Staatliche Cyberkrieger sind heute die ressourcenstärksten Hackerorganisationen weltweit. Ihre Cyberangriffe sind nicht zu kontrollieren und gefährden neben ihren eigentlichen Zielen auch zivile Systeme – wie etwa Systeme zur Sicherstellung lebenswichtiger Ressourcen (Wasser, Energie), Krankenhäuser oder Einrichtungen wie Chemiewerke. Der gegen eine iranische Atomanlage gerichtete Stuxnet-Wurm breitete sich weltweit aus. Mittlerweile gibt fast ein Dutzend weiterer Trojaner offensichtlich staatlicher Herkunft.

- Der Einsatz von Cyberwaffen durch Staaten ist völkerrechtlich eine Kriegshandlung mit erheblichem Eskalationspotenzial, die die internationale Sicherheit erheblich gefährdet.

- Ausspähung und Computermanipulationen bereiten konventionelle militärische Operationen vor, beispielsweise rechtswidrige Drohnenangriffe durch die Ortung von Zielpersonen, und sind damit die Grundlage aggressiver (kriegerischer) Operationen.

- Drohnenangriffe fordern zahlreiche Opfer unter Unbeteiligten. Angriffe, die auf unsicheren Eigenschaften der Ziele basieren (*Signature Strikes*) richten sich gegen Opfer, gegen die nicht einmal ein hinreichender Verdacht besteht.

- Computergestützte militärische Operationen erzeugen die Illusion eines „sauberen" Krieges und senken damit die Schwelle des Einsatzes.

Wenn diese Ausgabe der FIfF-Kommunikation erscheint, ist es bereits Ende Januar. Dennoch wünsche ich noch – etwas verspätet – ein erfolgreiches und friedliches Jahr 2015.

Mit FIfFigen Grüßen

Stefan Hügel

Rainer Rehak

Rückblick FIfF-Konferenz 2014

Am 7. und 8. November 2014 fand an der TU Berlin die 30. Jahrestagung des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) statt – erstmalig unter dem neuen Namen FIfF-Konferenz*. Wir haben uns dabei mit der Rolle der deutschen Geheimdienste im globalen Ausspähungsskandal beschäftigt, weil wir es leid sind, dass bei der politischen Verantwortungsfrage nach wie vor mit dem Finger auf andere Länder und deren Dienste gezeigt wird. Der diesbezügliche, deutsche parlamentarische Untersuchungsausschuss wurde demnach konsequent* NSA-Ausschuss *genannt, obwohl die Bezeichnung und Ausrichtung* BND/Verfassungsschutz-Ausschuss *angebrachter gewesen wäre.*

Um uns diesem vieldimensionalen Thema auch in angemessener Breite zu nähern, luden wir Politiker, Hacker, Rechtswissenschaftler, Historiker, Geheimdienstexperten, Datenschützer und Politikwissenschaftler zur Mitwirkung ein, wobei wir vom FIfF unsere technische Expertise beisteuerten. Die Geladenen kamen gern – in einem Falle gerade deshalb, weil wir unsere Friedensausrichtung explizit im Namen führen –, und wir alle trugen unser Wissen zusammen, sodass interessante Erkenntnisse, lebhafte Diskussionen und neue Sichtweisen entstanden.

Zusammenfassend und zugespitzt könnte man sagen, dass deutsche Geheimdienste historisch konsistent mit einer Kombination aus fragwürdiger politischer Gesinnung, systematischer Unfähigkeit und fortgeschrittener Reformaversion jedoch keinesfalls außer Kontrolle geraten sind, sondern sich explizit und regierungsgestützt entlang sportlicher (lies: verfassungswidriger) Interpretationen von im Kern kaputten (G10)-Gesetzen aktiv gegen alle Grundrechtsträger richten; und das alles im Schulterschluss mit superb finanzierten befreundeten Diensten hüben und drüben. Aber auch über tagesaktuelle politische Entwicklungen und Lösungsperspektiven wurde gesprochen und debattiert.

Alle Vorträge wurden im Internet live übertragen und stehen auch zum Download bereit. Daran wirkten mit Ute **Bernhardt**, Matthias **Bäcker**, Wolfgang **Coy** (im FIfF-Beirat), Hans-Jörg **Kreowski**, Constanze **Kurz** (im FIfF-Beirat), Wolfgang **Nešković**, Frank **Rieger**, Anne **Roth**, Ingo **Ruhmann**, Peter **Schaar**, Erich **Schmidt-Eenboom**, Patrick **Sensburg**, Hans-Christian **Ströbele**, Gregor **Wiedemann**, Andy **Müller-Maguhn** und das **Nö-Theater** (mit ihrem Stück „V wie Verfassungsschutz“).

Parallel zum Vortragsprogramm gab es auch zwei interessante und sehr gut besuchte FIfF-Workshops. Erstens den Kickoff-Workshop zur FIfF-**Cyberpeace**-Kampagne, die eine ausschließlich friedliche Nutzung des digitalen Raumes anstrebt, unter anderem geleitet von Sylvia **Johnigk**; und zweitens den **Workshop Faire Computer,** in dem Sebastian **Jekutsch** die vergangene und aktuelle Arbeit der AG **Faire Computer** vorstellte und zur Mitarbeit aufrief.

Im Rahmen der Konferenz vergab das FIfF auch in diesem Jahr wieder den **FIfF-Studienpreis**, der besonders gute Abschlussarbeiten im Bereich der kritischen Informatik hervorheben soll. Diesjähriger Preisträger ist Benjamin **Kees**, der seine ausgezeichnete Diplomarbeit *Identifikation gesellschaftlicher Probleme automatisierter Videoüberwachung* auch selbst vorstellte.

Wer sich in den Pausen weitläufiger mit der digitalen Welt beschäftigen wollte, konnte auch die Stände der *Free Software Foundation Europe*, von *Tactical Tech*, der FIfF-AG *Faire Com-*

Hans-Jörg Kreowski bei der Begrüßung der Teilnehmer

puter und dem *Freifunk*-Projekt aufsuchen. Letzteres versorgte uns alle freundlicherweise auch gleich mit freiem WLAN.

Zu guter Letzt: Es waren ungefähr 400 Menschen vor Ort und zusätzlich ca. 150 per Livestream dazugeschaltet. Die mediale Wahrnehmung war auch zufriedenstellend: Arte, TAZ, die Zeit, ZDF, Heise.de, telepolis, Netzpolitik.org, Le Monde Diplomatique, allerlei Blogs und das Projekt *Wissenschaftsjahr 2014 – digitale Gesellschaft* berichteten wohlwollend und waren sogar teilweise länger anwesend. Wir haben jetzt, einen Monat später, immer noch ca. 100 Besucher pro Tag auf der Konferenzwebseite, was uns besonders für die Wahrnehmung des nach wie vor drängenden Themas sehr freut.

Abschließend sei uns noch ein herzlicher Dank für die großzügige Unterstützung durch unsere Freundinnen und Freunde vom Chaos Computer Club, von Netzpolitik.org, von der GI-Ethikgruppe, vom Lehrstuhl Informatik und Gesellschaft der TU Berlin, vom AStA der TU Berlin, von Uberspace.de und von den vielen helfenden Köpfen/Händen erlaubt. Es war eine wirklich schöne Veranstaltung, von den Keksen bis zu den Vorträgen, vom Kaffee bis zum Theaterstück. Damit hoffen wir, nicht nur den Inhalt und die Erkenntnisse der Konferenz weitergetragen zu haben, sondern auch die Freude an (friedens-)politischer Aktivität.

Weitere Informationen und die Videos zur FIfF-Konferenz:
https://fiffkon.de

Mitgliederversammlung des FIfF
Berlin, 8. November 2014, 10:00 – 12:15 Uhr

– Beschlussprotokoll –

Sitzungsleitung: Stefan Hügel als Vorsitzender des FIfF.

1. **Begrüßung und Feststellung der Beschlussfähigkeit und der Protokollführung**

   Zur Versammlung ist ordentlich eingeladen worden und diese ist dadurch beschlussfähig. Protokollführung: Werner Winzerling.

2. **Beschlussfassung über Tages- und Geschäfts- und Wahlordnung**

   Geschäfts- und Wahlordnung wird von der MV in bekannter Form genehmigt. Der Tagesordnung wurde in der vorliegenden Form zugestimmt.

3. **Bericht des Vorstandes (einschl. Kassenbericht)**

   Stefan Hügel berichtet über die kontinuierliche Arbeit des FIfF seit der letzten MV und über den Haushalt mit Stand 5.11.2014. Es wurden keine Beschlüsse gefasst.

4. **Bericht der Kassenprüfer**

   Für die am 2.5.2014 in Bremen durchgeführte Kassenprüfung berichtet Kurt Fussangel der MV. Aus dem Kassenprüfungsprotokoll: *„Dem Vorstand wird eine dem Vereinszweck entsprechende, ordnungsgemäße Kassenführung bescheinigt. Einer Entlastung des Vorstandes steht nach unserer Auffassung nichts entgegen. Wir beantragen die Entlastung des Vorstandes."* (Derzeitige Kassenprüfer: Michael Ahlmann, Kurt Fussangel, Klaus Lüttich und Gernot Lucks)

5. **Diskussion der Berichte**

   Es wurden keine Beschlüsse gefasst.

So viele waren leider nicht da ;-)
Abstimmung bei der Piratenpartei, Marcus Sümnick, CC-BY

6. **Entlastung des Vorstandes**

   Die Kassenprüfer schlagen die Entlastung des Vorstandes vor. Die MV entlastet den Vorstand einmütig bei 4 Enthaltungen.

7. **Neuwahl der Kassenprüfer**

   Die MV wählt im Block einmütig bei 4 Enthaltungen zu den neuen Kassenprüfern des FIfF:
   Kurt Fussangel (stimmt zu), Michael Ahlmann (stimmt zu), Klaus Lüttich (stimmt zu) und Gernot Lucks (vorbehaltlich der Zustimmung).

8. **Diskussion über Ziele und Arbeit des FIfF, aktuelle Themen, Verabschiedung von Stellungnahmen, Berichte aus den Regionalgruppen**

   Auf der Klausurtagung im März 2014 soll über die Einrichtung eines oder mehrerer Sprecher des FIfF beraten werden.

9. **Anträge an die Mitgliederversammlung**

   Ein Antrag über die Neuregelung des Mitgliedsbeitrages für Studierende wird diskutiert.

   Antrag Angelika Ohse*: „Studierende zahlen den ermäßigten Beitrag für den Zeitraum, für den sie {unaufgefordert Studiums-Nachweise | aktive Rückmeldungen} vorlegen. Für alle Mitglieder, die den Studierenden-Beitrag leisten, erhöht sich der Jahresbeitrag automatisch auf den vollen Betrag von dem Jahr an, das dem Datum folgt, bis zu dem der Studierenden-Status nachgewiesen ist. Diese Regelung wird auf dem Beitragsformular sichtbar gemacht."*

   Abgelehnt (8-ja/9-nein/10-Enthaltung)

   Antrag Dietrich Meyer-Ebrecht: „Die MV beauftragt den Vorstand einen geeigneten Vorschlag für eine Neuregelung des Mitgliedsbeitrages für Studierende zu erarbeiten, der die Diskussion der MV berücksichtigt. Der Vorstand beschließt dann über die Regelung."

   Einmütig angenommen bei 5 Enthaltungen.

10. **Verschiedenes**

    Es wurden keine Beschlüsse gefasst.

11. **Genehmigung des Protokolls**

    Das Protokoll wird einstimmig genehmigt.

FIfF e. V.

FIfF-Studienpreis 2014 verliehen

Herausragende Arbeit auf dem Gebiet Informatik und Gesellschaft ausgezeichnet

Im Rahmen der 30. FIfF-Konferenz 2014, die am 7. und 8. November 2014 unter dem Motto *Der Fall des Geheimen – Ein Blick unter den eigenen Teppich* an der Technischen Universität Berlin stattfand, wurde zum vierten Mal der Studienpreis des FIfF – *Forum Informatikerinnen und Informatiker für Frieden und gesellschaftliche Verantwortung* e. V. verliehen. Mit der jährlichen Auszeichnung herausragender Qualifikationsarbeiten aus dem Bereich *Informatik und Gesellschaft* will das FIfF einen Beitrag leisten, die immer wieder vom Sparzwang an den Hochschulen betroffene Forschung zu den gesellschaftlichen Auswirkungen der Informationstechnologie zu fördern und ins Licht der Öffentlichkeit zu rücken.

„Mit unserem Studienpreis verbinden wir vor allem zwei Ziele: Wir wollen hervorragende Abschlussarbeiten aus diesem Gebiet auszeichnen und die dahinter stehende Leistung würdigen. Und wir wollen Aufmerksamkeit für Themengebiete schaffen, die wir für die Entwickung einer digitalen Gesellschaft für essentiell wichtig halten", so Stefan Hügel, der Vorsitzende des FIfF, in seiner Einleitung. „Technik, die funktioniert, wird stets auch hergestellt und angewendet – unabhängig von ihrer Rechtmäßigkeit. Es ist Aufgabe der Informatikerinnen und Informatiker, technische Systeme auch von ihren ethischen und rechtsstaatlichen Anforderungen her zu denken, um eine Technik zu verhindern, die zum Selbstzweck wird und schädliche Nutzung als „Sachzwang" etabliert. Mit unserem Studienpreis wollen wir Arbeiten auszeichnen, die dieser Aufgabe gerecht werden."

In diesem Jahr ging der Studienpreis an *Benjamin Kees* für seine Diplomarbeit *Identifikation gesellschaftlicher Probleme automatisierter Videoüberwachung*. Die Arbeit, die im Fachbereich Informatik an der Humboldt-Universität zu Berlin verfasst wurde, entwirft ein automatisiertes Videoüberwachungssystem, das angesichts der technischen Möglichkeiten wahrscheinlich ist, und untersucht daraus resultierende gesellschaftliche Probleme, für die mögliche Lösungsansätze diskutiert werden. Zu den identifizierten Problemen zählen neben dem Eingriff in die informationelle Selbstbestimmung der Betroffenen auch die selbstdisziplinierende Wirkung der Überwachung, Diskriminierung und die Kriminalisierung bestimmter Verhaltenscharakteristiken.

Stefan Hügel bei der Preisübergabe an Benjamin Kees

„Mit ihrer Untersuchung der gesellschaftlichen Auswirkungen der Videoüberwachung behandelt die Arbeit ein immer noch hochaktuelles, gesellschaftlich und politisch relevantes Thema an der Schnittstelle von Informatik und Gesellschaft, das durch die jüngsten Enthüllungen noch einmal an Brisanz gewonnen hat. Sie ist interdiziplinär aufgebaut, umfassend, und kommt zu wichtigen Ergebnissen für die Debatte um unsere Rechte und unsere Sicherheit. Aus diesem Grund hat sich die Jury des FIfF-Studienpreises einhellig für die Auszeichnung der Arbeit entschieden", sagte Stefan Hügel in seiner Laudatio.

„Zu Ihrer Sicherheit wird dieser Bereich videoüberwacht, so steht es häufig auf den gesetzlich vorgeschriebenen Warnschildern", so Hügel weiter. „Richtig müsste es heißen, das bestätigt die Arbeit eindrucksvoll: *Vorsicht! In diesem Bereich werden Ihre Rechte der Videoüberwachung geopfert!*"

Stefan Hügel – Laudatio für den Studienpreis

Benjamin Kees: *Identifikation gesellschaftlicher Probleme automatisierter Videoüberwachung*

Liebe Mitglieder des FIfF, liebe Freundinnen und Freunde, liebe Gäste,

das FIfF verleiht heute seinen Studienpreis 2014.

Zu Beginn der 90er Jahre gab es noch so etwas wie eine Aufbruchstimmung: An mehreren Orten wurden Institute gegründet und Lehrstühle eingerichtet, die sich mit den gesellschaftlichen Auswirkungen der Technik im Allgemeinen und der Informatik im Besonderen auseinandersetzen sollten.

Auch wenn weiterhin wertvolle Arbeit auf diesem Gebiet geleistet wird, wird die Ausstattung des Fachs *Informatik und Gesellschaft* immer weiter zurückgenommen. Lehrstühle wurden umgewidmet, oder ihr Inhalt wurde im Rahmen einer Neubesetzung „angepasst". Die gesellschaftpolitischen Auswirkungen der Informatik drohen immer mehr aus dem akademischen Bereich zu verschwinden.

Das geschieht in einer Zeit, in der die Durchdringung der Gesellschaft mit Produkten der Informatik weiter zunimmt. Wie stark

die allumfassende Informationstechnik heute in unser Leben eingreift, können wir nicht zuletzt an der Diskussion über die Ausspähung unserer Kommunikation und unseres Lebens durch Geheimdienste sehen. Die Beiträge unserer Referentinnen und Referenten gestern und heute zeigen dies eindrucksvoll.

Laudator Stefan Hügel

Das FIfF will seine Möglichkeiten nutzen, dem Abbau des Fachgebiets entgegenzuwirken. Wir tun dies durch unsere inhaltliche Arbeit und durch Stellungnahmen – so haben wir uns in die Diskussion um die Neubesetzung des Lehrstuhls von Professor Coy an der Humboldt-Universität eingeschaltet. Und wir verleihen nun zum vierten Mal den FIfF-Studienpreis.

Mit unserem Studienpreis verbinden wir vor allem zwei Ziele:

1. Wir wollen hervorragende Abschlussarbeiten aus diesem Gebiet auszeichnen und die dahinter stehende Leistung würdigen.

2. Wir wollen Aufmerksamkeit für Themengebiete schaffen, die wir für die Entwickung einer digitalen Gesellschaft für essentiell wichtig halten.

Technik ist von der historischen Entwicklung her auf militärische, industrielle und wirtschaftliche Zwecke ausgerichtet. Technik, die funktioniert, wird stets auch hergestellt und angewendet – unabhängig von ihrer Rechtmäßigkeit. Prominente und aktuelle Beispiele sind die vom EuGH und vom Bundesverfassungsgericht verworfene Vorratsdatenspeicherung und die Videoüberwachung. Es ist Aufgabe der Informatikerinnen und Informatiker, technische Systeme auch von ihren ethischen und rechtsstaatlichen Anforderungen her zu denken, um eine Technik zu verhindern, die zum Selbstzweck wird und schädliche Nutzung als „Sachzwang“ etabliert. Mit unserem Studienpreis wollen wir Arbeiten auszeichnen, die dieser Aufgabe gerecht werden.

Auch dieses Jahr wurde eine Reihe von Arbeiten bei uns eingereicht, wofür wir uns herzlich bedanken. Eine Jury, besetzt mit

- Professorin Britta Schinzel aus Freiburg,
- Professorin Marie-Theres Tinnefeld aus München,
- Professor Jochen Koubek aus Bayreuth,
- Rainer Rehak aus Berlin,
- und mir selbst, Stefan Hügel aus Frankfurt am Main

hat aus den sehr guten Einreichungen eine Arbeit ausgewählt, die wir heute hier prämieren werden.

Wenn wir heute durch eine deutsche Großstadt spazieren, schauen hunderte von Kameras auf uns herab. Umfassende Videoüberwachung gilt allenthalben als die Lösung vieler Probleme nicht nur der Kriminalitätsbekämpfung. Und kann die heutige Überwachung eine Tat nicht verhindern, werden flugs Rufe laut, sie weiter zu verstärken und zu intensivieren.

Die Befürworter, die nicht müde werden, die Forderung nach Videoüberwachung immer wieder zu wiederholen, versprechen sich davon:

- einfache Lösungen für Sicherheitsprobleme,
- leichte Überwachung auch unübersichtlicher Räume,
- zentraler Betrieb mit wenig Personalaufwand,
- erschwingliche Technik, ohne dass ihr Betrieb besondere Kenntnisse erfordert.

Die praktische Anwendung verweist diese Hoffnungen häufig ins Reich der Mythen. Und: Videoüberwachung ist auch und vor allem ein großes Geschäft, für Entwickler, Hersteller und Betreiber – das wird aber gerne verschwiegen.

Ist der öffentliche Bereich dabei noch einigermaßen kontrolliert, erleben wir im privaten Bereich erheblichen Wildwuchs. Das Ergebnis sind häufig Videoüberwachungsanlagen, die völlig unkontrolliert alles überwachen, was in ihren Fokus kommt, und nicht selten einer rechtlichen Überprüfung nicht standhalten.

Dabei ist nicht nur der Nutzen der Überwachungsanlagen fraglich, sie bergen auch erhebliche Risiken für die Menschenrechte. Sie greifen in die Privatsphäre all jener ein, die ihren Sichtbereich durchqueren. Die ständige Möglichkeit der Überwachung beeinflusst unser Verhalten – wie bereits Jeremy Bentham im 18. Jahrhundert mit seinem Konzept des Panoptikon gezeigt hat. Und durch automatisierte Auswertung und Speicherung der Daten auf Vorrat werden umfassende Bewegungsprofile der Menschen möglich.

Nachdem wir heute wissen, dass Geheimdienste alle Daten speichern und auswerten, die sie bekommen können, ist zudem klar: Auch die Daten aus der Videoüberwachung fließen in den großen Pool ein, mit dem die Sicherheitsbehörden ihren Cyberwar gegen uns alle führen.

Diesen Fragen widmet sich die Arbeit **Identifikation gesellschaftlicher Probleme automatisierter Videoüberwachung** von **Benjamin Kees**, die an der Humboldt-Universität zu Berlin entstanden ist. Die Jury des FIfF-Studienpreises und der Vorstand des FIfF zeichnen die Arbeit heute mit dem **FIfF-Studienpreis** aus.

Im Rahmen der Arbeit wird ein automatisiertes System zur Videoüberwachung entworfen, das angesichts der heute bestehenden technologischen Möglichkeiten vorstellbar oder sogar wahrscheinlich ist. Anhand dieses Systems werden gesellschaftliche Implikationen und Probleme untersucht:

1. die Erhebung von personenbeziehbaren Daten, die gegen das Prinzip der Datensparsamkeit verstößt,

2. die Steigerung der Informationsasymmetrie zwischen Überwachenden und Überwachten,

3. der daraus resultierende Eingriff in das Prinzip der informationellen Selbstbestimmung und

4. die Steigerung der selbstdisziplinierenden Wirkung auf Betroffene.

Durch das beschriebene, repäsentative Informatiksystem kann die Videoüberwachung und der Kontext ihres Einsatzes anhand eines konkreten Systementwurfs umfassend untersucht werden. Diese Analyse anhand der Anforderungen und des technischen Aufbaus eines Informatiksystems, die über eine rein theoretische Betrachtung hinausgeht, zeichnet die Arbeit aus. Technikfolgen werden anhand der tatsächlich bestehenden Möglichkeiten der Technikanwendung analysiert.

Die Arbeit geht dabei über die unmittelbaren Auswirkungen hinaus, und behandelt auch mittelbare, langfristige Auswirkungen des Systemeinsatzes. Neben den direkten Effekten der Videoüberwachung werden so auch indirekte Effekte und die langfristigen Auswirkungen in die Untersuchung eingebunden. Beispielsweise wird die Gefahr der Diskriminierung einzelner Bevölkerungsgruppen durch den Einsatz von Videoüberwachung betrachtet. Die Arbeit kommt damit zu sehr umfassenden Ergebnissen, die uns der Preisträger sicherlich gleich noch darstellen wird.[1]

„Zu Ihrer Sicherheit wird dieser Bereich videoüberwacht", so steht es häufig auf den gesetzlich vorgeschriebenen Warnschildern. Richtig müsste es heißen, das bestätigt die Arbeit eindrucksvoll: *„Vorsicht! In diesem Bereich werden Ihre Rechte der Videoüberwachung geopfert!"*

Das FIfF hat sich, im Gleichklang mit anderen digitalen Menschenrechtsorganisationen, in der Vergangenheit immer wieder mit den Risiken der Videoüberwachung auseinandergesetzt. Gerade haben wir die Thematik in einem Schwerpunkt der *FIfF-*

Das FIfF verleiht 2015 wieder den

FIfF-Studienpreis

für herausragende Abschlussarbeiten aus dem Bereich Informatik und Gesellschaft.

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

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

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

Das Preisgeld beträgt:

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

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

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

Der Preis wird in einer Feierstunde im Rahmen der 31. FIfF-Konferenz 2015 verliehen, die voraussichtlich im Oktober oder November in Erlangen stattfindet.

Kommunikation von verschiedenen Seiten beleuchtet – auch der Preisträger hat dazu einen Beitrag geleistet. In Frankfurt am Main hat sich die Bürgerrechtsgruppe *die*Datenschützer Rhein-Main gebildet, die Datenschutzverstöße untersucht und anprangert und auch bei der Videoüberwachung ein weites Betätigungsfeld gefunden hat. Viele weitere Initiativen kommen hinzu. In diesem Umfeld ist die Arbeit von Benjamin Kees besonders wertvoll und von hohem Nutzen.

Mit ihrer Untersuchung der gesellschaftlichen Auswirkungen der Videoüberwachung behandelt die Arbeit ein immer noch hochaktuelles, gesellschaftlich und politisch relevantes Thema an der Schnittstelle von Informatik und Gesellschaft, das durch die jüngsten Enthüllungen noch einmal an Brisanz gewonnen hat. Sie ist interdiziplinär aufgebaut, umfassend und kommt zu wichtigen Ergebnissen für die Debatte um unsere Rechte und unsere Sicherheit. Aus diesem Grund hat sich die Jury des FIfF-Studienpreises einhellig für die Auszeichnung der Arbeit entschieden.

Herzlichen Glückwunsch, Benjamin Kees, zum FIfF-Studienpreis 2014.

Anmerkung

1 *Eine ausführliche Darstellung der Arbeit ist für die FIfF-Kommunikation 1/2015 geplant.*

Kai Nothdurft

Demokratie braucht Bewegung – und das FIfF bewegt mit!

Am 14. November 2014 feierte *campact* (*www.campact.de*) sein 10jähriges Bestehen mit einer großen Gala im Berliner Cosmos, einem ehemaligen Kino. Es waren etwa 750 Gäste anwesend und die Veranstaltung wurde live ins Internet gestreamt. *campact* feierte sich zu Recht selbst, denn die Organisation, die von ein paar Enthusiasten aus dem Attac-Umfeld im niedersächsischen Verden gegründet wurde, hat sich zu einer schlagkräftigen Bewegung entwickelt, die mit zahlreichen Aktionen aktiv und nachhaltig in die politische Willensbildung eingreift. Die Anzahl der Unterstützenden hat ein exponentielles Wachstum hingelegt; auf dem Mailverteiler stehen inzwischen 1,5 Mio Menschen. Besonders die geschickte Nutzung des Internets mit Online-Kampagnen und das Sammeln von Unterschriften hat sich zu einem wertvollen Multiplikator entwickelt. Die selbstorganisierte Europäische Bürgerinitiative gegen das Abkommen TTIP haben bereits über eine Million Menschen unterzeichnet. Auch das FIfF hat diese und mehrere weitere *campact*-Aktionen unterstützt.

Demokratie braucht Bewegung

Ein Highlight war die Grußbotschaft von Edward Snowden, der sich bei *campact* für die Solidaritätsaktionen bedankte, die ihm ein Asyl- und Aufenthaltsrecht in Deutschland verschaffen sollen. Er bedauerte, nicht persönlich zu der Feier kommen zu können.

Am nächsten Tag fand dann mit über 900 Teilnehmenden der Kongress *Demokratie braucht Bewegung* statt, bei dem zahlreiche Vorträge und Workshops zum Kampagnenmanagement angeboten wurden. Begleitend gab es Stände von Kooperationspartnern und Unterstützern. Da durfte das FIfF natürlich nicht fehlen. Unser Stand war zwischen dem BUND und digitalcourage plaziert und prominent mit drei unserer Vorstandsmitglieder besetzt, die zahlreichen Interessenten vor allem in den Vortragspausen Auskunft geben und häufig dem größtenteils sehr IT-fernen Publikum erstmal erläutern mussten, was das FIfF überhaupt ist. Ein Aktivist von *Ärzte ohne Grenzen* war hocherfreut, dass es auch noch andere Berufsgruppen gibt, die sich mit ethischen Fragen ihres Berufes beschäftigen. Natürlich nutzten wir die Gelegenheit fleißig zum Knüpfen von Kontakten, Netzwerken und der Werbung für die *cyberpeace*-Kampagne und sonstige Aktivitäten des FIfF. Auf großes Interesse stieß auch das Thema *Faire Computer*. Spontan wurde mit *campact* auch eine erste gemeinsame Aktion im *cyberpeace*-Kontext geplant, der Protest gegen die geforderte Budgetaufstockung des BND vor dem Bundestag am 27. November 2014 zum Ankauf von geheimgehaltenen Schwachstellen für den Cyberwarfare.

Katharina Nocun, Campaignerin bei Campact

Von der Veranstaltung ging eine Aufbruchstimmung aus. Es tut gut, zu sehen, dass es viele politisch motivierte Menschen auch außerhalb des offiziellen repräsentativen Politikbetriebs gibt, die sich aktiv in die Gestaltung unserer Gesellschaft einbringen und etwas verändern wollen. Im FIfF engagiert sich ein Teil davon.

FIfF e. V. – Pressemitteilung

Cyberpeace-Kampagne gestartet

Stiftung Bridge unterstützt neue Kampagne des FIfF e. V.

30. Oktober 2014 – Die Enthüllungen des letzten Jahres haben das Ausmaß von Cyberspionage und Cyberwarfare durch die NSA und andere Geheimdienste und den massiven und fortgesetzten Bruch der Verfassung gezeigt. Der virtuelle Raum mutiert mehr und mehr zum Ort der Ausspähung; Informationstechnologie wird zu einem Werkzeug für Kontrolle und Überwachung der Bevölkerung.

Dennoch kratzt der öffentliche Diskurs häufig nur an der Oberfläche. So wird die Verletzung der Privatsphäre thematisiert, nicht jedoch die militärische Dimension. Deren Methoden beginnen mit Ausspähung und Spionage und reichen von Informationsmanipulation über Sabotage und Destabilisierung lebenswichtiger Infrastrukturen bis zu vernetzten kriegerischen Operationen.

Ein Beispiel: Terrorverdächtige werden durch ausgespähten Mobilfunk zum Ziel völkerrechtswidriger Drohneneinsätze, meist auf Grund eines sehr vagen Verdachts. Die Cyber-Angriffe von NSA und befreundeten Diensten auf IT-Systeme in anderen Ländern werden selbst von NATO-Experten als legitimer Grund für militärische Reaktionen bewertet. Das gefährdet in höchstem Maße die internationale Sicherheitslage. Die Gefahren für den inneren und äußeren Frieden, für die Zivilgesellschaft und für jeden Einzelnen sind unabsehbar – Politik und Wirtschaft ignorieren oder verschweigen sie jedoch.

„Ziel der Cyberpeace-Kampagne ist es, diese Lücke im öffentlichen Bewusstsein zu schließen. Wir wollen im Rahmen einer breiten Mobilisierung massiven Druck auf Politik, Justiz und Wirtschaft ausüben", erläutert Sylvia Johnigk, Vorstandsmitglied des FIfF und Sprecherin der Kampagne. „Wir verlangen die Achtung der Menschenrechte im virtuellen Raum, des Völkerrechts und eine ausschließlich friedliche Nutzung der Informationstechnik! Ergänzend soll die Öffentlichkeit befähigt werden, organisatorische Maßnahmen durch aktiven informationellen Selbstschutz konstruktiv zu unterstützen." Stefan Hügel, Vorsitzender des FIfF und ebenfalls Sprecher der Kampagne ergänzt: „Fernziel ist es, jegliche Form von Cyberwarfare zu ächten, die Integrität des Internets zu garantieren, die menschenrechts- und verfassungswidrige Ausspähung der Zivilgesellschaft zu verhindern und eine Sicherheitsdoktrin zu beenden, die alle Menschen unter Generalverdacht stellt."

Im Rahmen der FIfF-Konferenz 2014 wird am 8. November 2014 in Berlin das Kick-Off-Meeting der Kampagne stattfinden.

Das FIfF freut sich über die Förderung der Kampagne durch die Stiftung Bridge.

FIfF e. V. – Pressemitteilung

Kreatives Singen für ein friedliches Internet

Friedenslieder und Laternen vor dem BND-Gebäude

8. November 2014 – Beim Licht von Laternen mit dem Kampagnen-Logo sangen Teilnehmerinnen und Teilnehmer der FIfF-Konferenz 2014 am Abend des 7. November 2014 vor dem BND-Gebäude eine neu getextete Version des Kinderliedes „Ich geh mit meiner Laterne". Die FIfF-Konferenz 2014 fand am 7./8. November 2014 mit rund 400 Teilnehmerinnen und Teilnehmern an der Technischen Universität Berlin statt.

Die Protestaktion ist Teil der Cyberpeace-Kampagne des *Forum Informatikerinnen und Informatiker für Frieden und gesellschaftliche Verantwortung* (FIfF e. V.).

„Das FIfF knüpft damit an eine Tradition der Friedensbewegung an, der zerstörerischen Logik des militärischen Denkens einen friedlichen Protest mit menschlicher Kreativität entgegenzusetzen", kommentiert Kai Nothdurft, Vorstandsmitglied der bundesweit aktiven Informatikerinnen und Informatiker.

> *„Ich geh mit meiner Laterne und meine Laterne mit mir.*
> *Staatstrojaner und Viren, das Internet, das zerstört Ihr."*

Das stimmungsvolle Licht und die kindlich naive Melodie kontrastieren mit der ernsten Botschaft, dass die Geheimdienste das Internet militärisch zur Massenüberwachung, Spionage und Sabotage von Webdiensten und Infrastrukturen missbrauchen und damit alle Nutzer gefährden.

„Internetdienste, Verschlüsselung und Lieferprozesse sind von Militär und Geheimdiensten unterwandert. Damit bedrohen sie essentiell alle Bereiche unseres persönlichen und gesellschaftlichen Lebens", sagt Sylvia Johnigk, eine Sprecherin der Kampagne. „Im Gegenzug soll die Cyberpeace-Kampagne Wege aufzeigen, wie wir das Internet und die Informations- und Kommunikationstechnologien zum Wohle der Menschheit nutzen können."

BND will Cyber-Angriffskrieg vorbereiten

Studie von NATO-Experten zeigt sicherheitspolitische Gefahren auf

11. November 2014 – Wie *Der Spiegel* in seiner aktuellen Ausgabe berichtet, beantragt der Bundesnachrichtendienst (BND) Haushaltsmittel, um das Wissen um Schwachstellen in Softwaresystemen aufzukaufen. Mit so genannten *Zero-Day-Exploits* – der Begriff umschreibt der Öffentlichkeit unbekannte Sicherheitslücken – will der BND weltweit in Computersysteme einbrechen, sie sabotieren und den Datenverkehr abfangen.

Der Einbruch in fremde Computersysteme bedeutet die Planung offensiver Cyberoperationen. Solche Cyberoperationen bergen erhebliche Gefahren. Das *NATO Cooperative Cyber Defence Center of Excellence* (NATO CCD COE) hat führende Experten im internationalen Recht mit einer detaillierten Bewertung von Cyberattacken beauftragt. Laut dem so genannten *Tallinn-Manual* sind Cyberangriffe bereits dann als kriegerische Handlung zu bewerten, wenn sie von zivilen Stellen ausgeübt werden, die von staatlicher Seite nicht daran gehindert werden. Hacker sind danach bereits legitime Angriffsziele, wenn sie ein System auf Schwachstellen untersuchen. Cyberangriffe durch staatliche Stellen werden eindeutig als internationaler Konflikt bewertet, die militärisch-geheimdienstliche Gegenreaktionen rechtfertigen. Sofern durch solche Computermanipulationen erhebliche materielle Schäden verursacht werden – z. B. an Infrastruktursystemen wie bei der Computersabotage am Energienetz – sind angegriffene Staaten sogar zu einer konventionellen militärischen Antwort berechtigt, so die NATO-Experten.

„Folgt man dieser Bewertung der NATO, will der BND in die Vorbereitung eines Cyber-Angriffskrieges einsteigen und beschwört mit seinen beabsichtigten Computermanipulationen geheimdienstliche und militärische Gegenreaktionen auf Computersysteme in Deutschland herauf", erklärt Stefan Hügel, Vorsitzender des FIfF und Sprecher der *cyberpeace*-Kampagne. „Bisher waren die zuständigen Behörden des Bundes offenbar nicht einmal in der Lage, ihre Systeme vor Ausspähung und Sabotage zu schützen. Wenn der BND das Wissen um IT-Sicherheitslücken kaufen will, um sie für Cyberangriffe zu nutzen, statt diese Lücken zu schließen, zeigt sich damit aufs Neue eine alarmierende Unkenntnis über die Gefahren von Cyberattacken und ein Mangel an Verantwortung gegenüber der Sicherheit unseres Landes."

Sylvia Johnigk, Vorstandsmitglied des FIfF und ebenfalls Sprecherin der Kampagne ergänzt: „Die Staatsgewalt ist dazu verpflichtet, das vom Bundesverfassungsgericht 2007 definierte *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* umzusetzen. Wenn Nachrichtendienste Sicherheitslücken in IT-Systemen vorsätzlich ausnutzen, statt sie zu schließen, ist dies ein Bruch von Grundrechten. Das FIfF fordert die Bundesregierung auf, die Sicherheit Deutschlands nicht zu gefährden und dem unverantwortlichen Spiel mit digitalen Angriffswaffen Einhalt zu gebieten!"

Freedom not Fear

Resolution

The *Freedom not Fear* movement, an assembly of human rights organisations, declares:

The respect for personal privacy and professional secrecy is an essential part of human dignity and any democratic society. A free and open society cannot exist without implicit private spaces and free communication.

Mass surveillance and blanket collection of information on our communications endanger our society. Such surveillance, as part of every day life, violates human rights, particularly:

- the right to privacy and to anonymity,
- religious freedom,
- freedom of expression and information,
- the right to a free press,
- the freedom of movement and association,
- the integrity and confidentiality of communications,
- the right to a fair trial and the presumption of innocence.

Everybody is exposed to measures of surveillance and control in an excessive manner, including:

- the personnel of psychological counselling services,
- medical practitioners,
- trade unionists,
- journalists,
- lawyers.

People who feel that they are constantly being watched and monitored are no longer free, are restrained from standing up for their rights and a just society in an unbiased and courageous manner. Accumulating information indiscriminately about all citizens does not enhance our protection against crime; it only costs us billions every year.

The Freedom not Fear movement *urges* the new European Commission to make the defence of human rights, in particular the right to privacy, the top priority.

We call on the Commission to begin by immediately instituting infringement proceedings against all Member States that

a) continue to have communications data retained indiscriminately on people who are not even remotely linked with serious crime despite the judgment of the Court of Justice of the EU of 8 April 2014,

b) have their intelligence services process communications data indiscriminately on people who are not even remotely a danger to national security, or that rely on foreign mass surveillance schemes to accomplish internationally what is not allowed nationally.

We also expect the Commission to follow the European Parliament's recommendations on IT security as set out in its resolution of March 12, 2014 on the US NSA surveillance programme.[1]

Brussels, September 28, 2014

Anmerkung

1 http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230

Nils Erik Flick

Informationstag *Die Macht der Computer*

Vier Vorträge zum Wissenschaftsjahr 2014 aus den Bereichen Kommunikation, Recht, Überwachung und Krieg

„Der meiste Schaden,
den der Computer potentiell zur Folge haben könnte,
hängt […] von den Eigenschaften [ab],
die das Publikum dem Computer zuschreibt."
Joseph Weizenbaum, DIE ZEIT, März 1973

Erfahrungsbericht von der gemeinsamen Informationsveranstaltung der FIfF-Regionalgruppe Hamburg mit dem AStA der Hochschule für Angewandte Wissenschaften zum Wissenschaftsjahr „Digitale Gesellschaft" 2014 des Bundesministeriums für Bildung und Foschung

Auf unserem Informationstag wurden vier Aspekte der zunehmenden Digitalisierung betrachtet. Jeder der vier Vorträge lieferte Material für heiße Diskussionen unter den dutzenden Zuhörern, die an Samstag, dem 27. September 2014 zu der dreistündigen Veranstaltung gekommen waren.

Erik und Jürgen vom FIfF sprachen in ihrem Vortrag über die Besonderheiten der computervermittelten Kommunikation, die geeignete Wahl des Mediums und die Gefahr der massenhaften Speicherung digitaler Inhalte und Metadaten. Sobald vertrauliche Kommunikation nicht mehr vertraulich ist, beginnen nämlich die unerwünschten Mitleser, sie auf ihre Art zu interpretieren. Die Konsequenzen für die Betroffenen sind unabsehbar und können durchaus schon heute unangenehm sein. Gegenstand des Vortrags waren deshalb auch Datenselbstschutz, die NSA, verantwortliches Nutzer/-Konsumverhalten (Stichwort Facebook und Smartphone) und die Frage der Hoheit über die eigene Elektronik, die uns mit *Cloud*, *Smart* und gegen den Nutzer abgesicherten *Closed-Source*-Komponenten immer weiter geraubt werden soll.

Ulrich Kühn von der Dienststelle des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit beleuchtete Stellen, an denen der Datenschutz inzwischen an Grenzen stößt. *Big Data* ist solch ein Phänomen, bei dem Zweckgebundenheit nicht mehr gegeben ist oder sinnvoll zugesichert werden kann. Als einen Kernpunkt gebe ich hier die Aussage wieder, dass es bei Big Data weniger ums Verstehen von Zusammenhängen geht als vielmehr darum, statistisch relevante Schlüsse zu ziehen – und das immer zu Lasten von Einzelnen geht. Das Beispiel einer in Hamburg ansässigen Firma, deren Software nach Eingabe möglichst vieler persönlicher Daten die Kreditwürdigkeit einstuft, bei der aber selbst der Geschäftsführer nicht sagen konnte, was denn die wichtigsten Kriterien sind – es interessierte ihn auch nicht – macht diesen Punkt sehr deutlich. Hier wurde die Entscheidungsgewalt an die Software abgegeben und nicht einmal mehr ein Versuch unternommen, die automatische Deutung kritisch zu hinterfragen.

Thomas Reinhold, wissenschaftlicher Mitarbeiter des Instituts für Friedensforschung und Sicherheitspolitik an der Universität Hamburg brachte uns in seinem Vortrag über Cyberkrieg auf den aktuellen Stand in Punkto Cyberwaffen und die laufenden Bestrebungen, internationale Konventionen zu ihrer Kontrolle zu schaffen. Die Schwierigkeiten beginnen bereits bei der Definition (kann man etwa Viren und Trojaner zählen wie Atomsprengköpfe und eine quantitative Beschränkung der Arsenale fordern?) Interessanterweise orientiert man sich beim Versuch, Cyberwaffen als eine eigene Waffengattung zu fassen, etwa im *Tallinn-Manual*, offenbar an kinetischen Waffen (also Bomben) und versucht damit eine Legitimation für eine militärische Antwort auf Cyberattacken abzuleiten – dabei ist solch ein Angriff oft nicht unmittelbar zweifelsfrei zu attribuieren, sondern die Attribution erfordert eine aufwendige forensische Untersuchung. Weitere Hindernisse auf dem Weg zu einer Kontrolle sind die Dual-Use-Problematik und das hinter den Kulissen längst entbrannte Wettrüsten um Offensivfähigkeiten.

Daniela Kirf-Busenbender, Rechtsanwältin und Senior Consultant für Datenschutz und IT-Compliance bei *Intersoft Consul-*

ting Services AG, referierte über digitales Recht. Im bundesdeutschen Recht gibt es keine einheitliche Definition für digitales Recht, die relevanten Paragraphen sind in vielen älteren Gesetzen zu finden. Die Quellen sind hier BGB, StGB, über TMKG, Urheber-, Marken- und Wettbewerbsrecht bis hin zu EU-Recht und natürlich das Grundgesetz. Besondere Punkte waren die Rechtssprechung bei Beleidigungen und übler Nachrede, *File-sharing*-Fällen und der Nutzung von Bildern aus dem Internet. Bei Filesharing-Fällen werden die Streitwerte inzwischen meist niedriger angesetzt – offenbar dürfen sich Abmahnkanzleien den Gerichtsstandort nicht mehr aussuchen. Bei der Nutzung von Bildern ist größte Vorsicht geboten, weil die Rechtekette oft schwer nachzuvollziehen ist und das Risiko im Zweifel am Nutzer hängenbleibt. An einigen Punkten ist die Rechtssprechung also deutlich anders als landläufig – auch in Informatikerkreisen – vermutet.

Natürlich war es innerhalb von drei Stunden nicht möglich, mehr als einen Überblick über jedes der Themen zu geben, trotzdem war unser Gesamteindruck positiv, das Publikum sehr interessiert und wir hoffen, dass die Erfahrungen als Grundlage für weitere Veranstaltungen dienen können.

Humanistische Union

20 Jahre Auslandseinsätze der Bundeswehr

Völlige Entgrenzung des Verteidigungsbegriffs und drohender Kontrollverlust der Kriegsführung durch bewaffnete Drohnen

3. Juli 2014 – Vor zwanzig Jahren, am 12. Juli 1994, hat das Bundesverfassungsgericht den Weg für weltweite bewaffnete Einsätze der Streitkräfte verfassungsrechtlich geöffnet. „Die Entscheidung des Bundesverfassungsgerichtes hat seitdem in der Sicherheitspolitik zu einer völligen Entgrenzung des Verteidigungsbegriffes des Grundgesetzes geführt. Mit dem Einsatz von Kampfdrohnen für die Bundeswehr als Teil des zukünftigen Cyberwars droht zudem ein gefährlicher Kontrollverlust der Kriegsführung“, erklärte der Vorsitzende der Humanistischen Union, Werner Koep-Kerstin, zu den Plänen von Verteidigungsministerin von der Leyen zur Anschaffung von Kampfdrohnen für die Bundeswehr. Es sei zudem eine Illusion, wenn Verteidigungsministerin von der Leyen meine, das Parlament könne jederzeit den zukünftigen Einsatz von Kampfdrohnen einhegen, erklärte Koep-Kerstin.

Mit großer Sorge betrachtet die Humanistische Union die zunehmende Aufweichung des sogenannten Parlamentsvorbehaltes, den das Bundesverfassungsgericht seinerzeit für Auslandseinsätze geltend gemacht hatte. Demnach ist die Bundesregierung verpflichtet, „für einen Einsatz bewaffneter Streitkräfte die grundsätzlich vorherige Zustimmung des Deutschen Bundestages einzuholen.“ Inzwischen mehren sich Stimmen, die den Parlamentsvorbehalt grundsätzlich problematisieren hinsichtlich der Effizienz von Entscheidungen und damit verbunden der Bündnisfähigkeit Deutschlands. Mit Bedauern wird konstatiert, dass Deutschland und die Niederlande zu den Ländern gehören, deren Regierungen auf Billigung des Parlaments bei der Entscheidung über bewaffnete Auslandseinsätze ihrer Streitkräfte angewiesen sind.

Die Art und Weise, wie der Deutsche Bundestag die inzwischen mehr als fünfzig Anträge der jeweiligen Bundesregierungen für bewaffnete Auslandseinsätze der Bundeswehr noch stets gebilligt hat – beispielsweise bei den Afghanistan-Mandaten – kann realistisch nur als „Genehmigungs-Automatik“ beschrieben werden. Der Parlamentsvorbehalt bietet „keine Sicherheit dafür, dass die deutschen Streitkräfte strikt nach Maßgabe der Vorgaben des Grundgesetzes und der UNO-Charta verwendet werden“, erklärte der Verfassungsrechtler Prof. Martin Kutscha, zugleich Vorstandsmitglied der Humanistischen Union.

Politischer Gegenspieler der Regierung ist eben nicht das Parlament, sondern nur dessen oppositionelle Minderheit. Nur diese hat ein politisches Interesse, wirksame Kontrolle auszuüben. Das hat das BVerfG am 02.08.1978 sehr deutlich zum Ausdruck gebracht, als es feststellte, im heutigen parlamentarischen Regierungssystem überwache „in erster Linie nicht die Mehrheit die Regierung, sondern diese Aufgabe wird vorwiegend von der Opposition – und damit in der Regel von einer Minderheit – wahrgenommen“. Wie schwach diese Minderheit sein kann, belegten die Stimmenverhältnisse im gegenwärtigen Deutschen Bundestag, ergänzte Kutscha.

Die Humanistische Union lehnt die Anschaffung und den Einsatz von Kampfdrohnen ab, denn:

- Die Hemmschwelle zum Einsatz von Gewalt sinkt, wenn Waffen eingesetzt werden können, ohne das Leben eigener Soldaten zu riskieren.

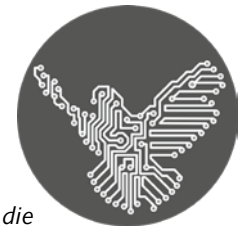
- Die Automatisierung und Verselbstständigung von Kampfdrohnen ist absehbar, da Computer Informationen wesentlich schneller verarbeiten können als Menschen. Am Ende werden Entscheidungen über Leben und Tod an Computer abgegeben. Es droht der Kontrollverlust über die Kriegsführung.

- Die Zahl der zivilen Opfer von Drohneneinsätzen, sogenannten Kollateralschäden, ist erschreckend hoch; Kampfdrohnen sind nicht die Präzisionswaffen, als die sie ausgegeben werden.

Mit Blick auf die jüngsten Äußerungen von Bundespräsident Gauck zu möglichen Militäreinsätzen erklärte der Vorsitzende der Humanistischen Union: „Der Bundespräsident sollte sich eher die Forderung der fünf Friedensforschungsinstitute im jährlichen Friedensgutachten zu eigen machen und für die weltweite völkerrechtliche Ächtung von Kampfdrohnen plädieren. Und er sollte eine Lanze für die dringend notwendige Rüstungskontrolle bei diesen Waffensystemen brechen.“

Quelle: Pressemitteilung der Humanistischen Union e. V.

Aaron Lye



Betrifft: Cyberpeace

Selbstverständlich unverändert

Es ist die Aufgabe der Geheimdienste, alles zu wissen, zu speichern und zu analysieren. Trotzdem ist uns erst durch die Enthüllungen von Edward Snowden *in den letzten eineinhalb Jahren das Ausmaß der Fähigkeiten und Praktiken von Geheimdiensten bekannt. Ihre Methoden von Cyberwarefare und Cyberspionage sind umfassender, als viele gedacht haben, und gehen weit über die Möglichkeiten von Cyberkriminellen hinaus. Mit dem Ziel der allumfassenden Datenspionage und Sabotage von Millionen von Systemen wird selbst vor kritischer, lebenswichtiger und ziviler Infrastruktur nicht haltgemacht. Zur Verfügung steht ihnen ein Milliardenbudget für militärische und geheimdienstliche Aufklärung, Rechenzentren, Supercomputer und zehntausende Mitarbeiter_innen.*

Der virtuelle Raum ist ein Ort der Ausspähung, und die Informationstechnik ist Werkzeug für Kontrolle und Überwachung. Zwar gibt es noch Möglichkeiten der Anonymität im virtuellen Raum, doch unternehmen weltweit Geheimdienste erhebliche Anstrengungen, Infrastrukturen wie beispielsweise das *Tor*-Netzwerk anzugreifen. Insbesondere erfolgen dabei die Angriffe auf Exit-Nodes, mit denen man sich mit dem Tor-Netzwerk verbindet, und auf Directory-Authorities, in denen alle Tor-Server und die Zugriffe darauf aufgelistet sind. Das Ziel ist es, Teilnehmer_innen des Tor-Netzwerks zu de-anonymisieren, mit dem Anspruch, keine anonymen Räume im Internet zulassen zu wollen[1,2]. Es entsteht ein digitales Panoptikum, ein Überwachungssystem, das unterdrückt, bei dem alle Tätigkeiten im virtuellen Raum unter permanenter Beobachtung stehen. Zwar handelt es sich bei den Datenmengen um Größenordnungen, die kaum effektiv verarbeitbar erscheinen, die Algorithmen werden allerdings immer effizienter und die Daten auf Vorrat gespeichert, um später darauf zugreifen zu können. Klar ist, je größer die analysierten Datenmengen, desto größer ist auch die Wahrscheinlichkeit, Muster in den Daten zu erkennen.

In diesem Zusammenhang wird die Untätigkeit staatlicher Stellen bezüglich der digitaler Welt kritisiert. Allerdings sollte klar sein, dass von staatlichen Stellen kein Schutz zu erwarten ist, da sie selbst daran beteiligt sind, flächendeckende Totalüberwachung zu realisieren. „Was im öffentlichen Interesse ist, sollte in grenzüberschreitenden Verfahren von der Öffentlichkeit selbst beurteilt werden, nicht von einer Regierungsinstanz oder einem Geheimgericht“[3], so Edward Snowden. Dabei sollte man sich allerdings nicht nur auf die als geheim eingestuften Maßnahmen der Programme zur Massenüberwachung konzentrieren. Die militärische Dimension der Ausspähung und Spionage, Informationsmanipulation, Sabotage und Destabilisierung – also im weiteren Sinne vernetzte kriegerische Handlungen und Operationen – ist vielfältig. Dabei stehen die *Five Eyes*, die Geheimdienste der USA, UK, Neuseeland, Kanada und Australien, mit ihren Programmen nicht allein da. Weltweit arbeiten Geheimdienste an vergleichbaren Systemen, und die Apparate in Russland und China unterscheiden sich Edward Snowden zufolge von der NSA nur durch ein knapperes Budget[4]. Auch die Rolle der Geheimdienste der BRD ist nicht unerheblich. Die offizielle Linie des Verteidigungsministeriums ist, dass die BRD international – gerade auch militärisch – mehr Präsenz zeigen müsse.[5] Bezüglich der strategischen Aufklärung und flächendeckenden Überwachung sind die folgenden drei Punkte besonders interessant:

1. Das als *Ringtausch* bekannte Verfahren, wodurch Überwachungsrestriktionen im eigenen Land einfach über Partnerdienste umgangen werden, bezeichnete der NSA-Whistleblower *Thomas Drake* als *Routinepraxis* von Geheimdienstkooperationen. Nach Drake ist die Zusammenarbeit zwischen BND und NSA fast so eng wie bei den Five Eyes untereinander und auch „unkonventionelle spezielle“ Zugriffsmöglichkeiten auf Glasfaserleitungen seien Bestandteil der Übereinkunft mit der NSA[6].

2. Die Entwicklung von Schadsoftware, um nicht nur flächendeckend Internet-Daten abzugreifen, sondern auch konkrete Ziele zu überwachen, nimmt zu. So wird die Entwicklung von Bundestrojanern immer weiter vorangetrieben. Teilweise wurde in letzter Zeit die Rolle der an der Entwicklung beteiligten Firmen verdunkelt. Bekannt ist, dass *CSC, 4Soft, Gamma* (inzwischen umbenannt in *FinFisher*) und *Elaman* an der Entwicklung und Erprobung der Staatstrojaner beteiligt sind. Bekannt ist auch, dass Elaman den vom BKA genutzten Trojaner zunächst einer Prüfung unterzieht. Viele Details bleiben allerdings offen, da sie gegenüber der Öffentlichkeit als geheim eingestuft sind. Beispielsweise, in welchem Umfang der Bundesnachrichtendienst oder Zollkriminalämter Trojaner einsetzen. Auch die Funktionsweise der staatlichen Schadsoftware ist nebulös, da es natürlich auch keine unabhängige technische Prüfung gab[7]. Inzwischen plant der BND den Kauf von *Zero Day Exploits*, also Schadcode für Sicherheitslücken in Programmen bei denen die Entwickler_innen der angegriffenen Software nicht wissen, dass diese Sicherheitslücken existieren. Insgesamt sind 4,5 Millionen Euro hierfür eingeplant.[8]

3. Währenddessen nimmt die Vermischung von Polizei, Geheimdiensten und Militär immer weiter zu. Ihre gemeinsame Bestrebung ist es, noch mehr *Data-Mining* zu betreiben. So

Aaron Lye

Aaron Lye ist FIfF-Mitglied aus Bremen. Dort studiert er Informatik an der Universität Bremen und ist hochschulpolitisch aktiv

plant der BND derzeit ein größeres Programm zur technischen Modernisierung. Konkret handelt es sich beispielsweise um die Anschaffung mehrerer Analysetools, um soziale Netzwerke auszuforschen, obwohl jetzt schon durch legale Anfragen solche Dienste zur Herausgabe von Informationen zu einzelnen Nutzer_innen verpflichtet werden können. Mit den neuen Analysetools sollen Plattformen wie Blogs, Foren, aber auch Portale und soziale Netzwerke wie *Flickr, Facebook* und *Twitter* zukünftig systematisch beobachtet und analysiert werden, um so Rückschlüsse auf soziale Kontakte ihrer Nutzer_innen zu ziehen. Zudem verspricht sich der Geheimdienst „Stimmungen in den Gesellschaften von Krisenländern schneller zu erfassen und in seine Lagebilder einflechten"[9] zu können. Aber auch das Zentrum *Operative Kommunikation* der Bundeswehr will „allgemeine Meinungs- und Stimmungslagen" in den „Einsatz- und Interessengebieten der Bundeswehr" analysieren. Geplant ist, mit dem Forschungsprogramm *WeroQ* zunächst Möglichkeiten ausloten. Die frei verkäuflichen Software-Pakete *TEXTRAPIC* und *BRANDWATCH* sollen eingesetzt werden.[10] Ziel ist die Beherrschbarkeit sozialer Phänomene und politischer Situationen, also diese Daten für Polizei und Militär permanent zu speichern und nutzbar zu machen, um so Unzufriedenheit wahrzunehmen, Prognosen darüber zu berechnen, Unruhen im Vorfeld aufzuspüren und natürlich auch gezielt zu manipulieren. Die aktuellen EU-Förderprogramme *CAPER* und *PROACTIVE* als Nachfolger von *INDECT* fördern entsprechende Vorhaben. Die Ziele sind klar: Mit dem selben rassistischen Motiven und Vermutungen, die auch hinter No-Fly-Listen oder in den Datenbanken von Europol stecken, haben sie zum Einen das Motiv Flüchtlinge abzuwehren. Des Weiteren sollen mithilfe dieser Information innenpolitische und außenpolitische Interventionen vorbereitet und Kriege geführt werden.

Darauf bereitet sich die NATO aktuell durch eine Vielzahl von Übungen vor, in denen Cyberwaffen immer mehr Raum einnehmen.[11,12] 2011 fand die transatlantische NATO-Übung mit dem Namen *Cyber Atlantic* zur Simulation eines Cyber-Angriffsfalls statt.[13] Seitdem werden zivil-militärische Krisenübungen der EU zu Störungen des Internets fortgesetzt. So beispielsweise die seit 2012 jährlich stattfindenden *Cyber-Defence-Exercises* mit dem Namen *Locked Shields* vom *NATO Cooperative Cyber Defence Center of Excellence*[14]; oder die zweite *Multi-Layer*-Krisenübung (ML14) der EU im Oktober 2014[15]. Neben konventionellen Waffen waren auch Cyber-Angriffe Bestandteil der Übung. Kurz danach begann der zweite Teil von *Cyber Europe 2014*[16], der bislang größten Übung für Cyberwar, geplant von der Europäischen Agentur für Netz- und Informationssicherheit und unterstützt von diversen anderen Behörden, wie beispielsweise dem Bundesamt für Sicherheit in der Informationstechnik. Eine dritte Phase von *Cyber Europe 2014* ist für Anfang 2015 geplant.[17] Begründet werden diese Aktivitäten von der NATO folgendermaßen:

> *„We agree that cyber attacks can reach a level that threatens the prosperity, security and stability of our countries, and the Euro-Atlantic area. They could harm our modern societies as much as a conventional attack. So today, we declare that cyber defence is part of NATO's core task of collective defence."*[18]

Hinzu kommt, dass die EU-Mitgliedsstaaten durch die Solidaritätsklausel zur gemeinsamen Intervention gezwungen werden sollen.[19] Sie sieht gemeinsames Handeln der Mitgliedsstaaten bei Natur- oder von Menschen verursachten Katastrophen vor, wobei Letzteres auch Cyberangriffe einschließt. Sie legt damit die Grundlagen für EU-weite polizeiliche, militärische und nicht-militärische Bündnisse, um Cyberangriffe mit militärischen, polizeilichen und geheimdienstlichen Mitteln zu beantworten. In diesem Zusammenhang soll Ende November 2014 eine weitere Übung stattfinden und auch für 2015 sind das NATO-Manöver *Cyber Coalition* und die Operation *Cyber Storm* geplant, die ebenfalls sowohl defensive als auch aggressive Komponenten beinhalten[20].

Obwohl diese Ereignisse durch die Medien bekannt wurden, hören wir parallel die ständigen Beteuerungen, dass die parlamentarische Kontrolle der Geheimdienste funktioniere. Um den Anschein zu erwecken, der massenhaften Überwachung zukünftig Einhalt gebieten zu wollen, preisen Bundesregierung und Parlament medienwirksam immer neue Maßnahmen an. Die aktuellen Ereignisse lassen allerdings auf gegenteilige Entwicklungen schließen. Die flächendeckende Totalüberwachung durch die enge Zusammenarbeit von Geheimdiensten, Unternehmen und Behörden bleibt weitgehend unverändert und wird immer noch von Teilen der Politik unter Missachtung von Verfassung und Menschenrechten als legitimes Mittel betrachtet[21].

Mehr und mehr wird ein Überwachungsstaat ausgebaut, der Widerstand im Keim zu ersticken versucht und seine Macht festigt und ausbreitet. Ein Überwachungssystem, das unterdrückt, und das Bewusstseins- und Verhaltensänderung von Menschen verursacht bis hin zum Konformismus. Deshalb ist es notwendig, Räume für Widerständigkeit zu behalten und zu schaffen, in denen freies und kritisches Denken noch möglich ist, ohne der permanenten Kontrolle, Überwachung und Repression ausgesetzt zu sein.

Es bleibt wichtig, weiterhin Menschen für diese Themen zu sensibilisieren und für Datensparsamkeit zu plädieren. Genauso wichtig ist es, aktiv Hilfe zur Selbsthilfe zu geben und durch Selbstorganisation und Eigeninitiative Menschen Open-Source und Kryptographie näher zu bringen. Trotzdem bleiben unsere Systeme angreifbar. Es liegt zwar an Informatiker_innen, sichere Systeme zu entwickeln, sichere Software zu schreiben und bestehende Systeme zu auditieren, um Sicherheitslücken in zentralen Komponenten auszuschließen. Diese technischen Lösungen können uns allerdings nur unterstützen, uns selbst und andere zu schützen. Das eigentliche Problem von Macht und Herrschaft können sie nicht lösen.

Anmerkungen

1 *http://www.heise.de/newsticker/meldung/XKeyscore-Quellcode-Tor-Nutzer-werden-von-der-NSA-als-Extremisten-markiert-und-ueberwacht-2248328.html*
2 *http://www.heise.de/newsticker/meldung/Russland-3-9-Millionen-Rubel-fuer-De-Anonymisierung-von-Tor-2268010.html*
3 *http://www.heise.de/newsticker/meldung/Snowden-fordert-internationale-Schiedsstelle-fuer-Whistleblower-2237661.html*
4 *ebd.*
5 *ebd.*

6 *http://www.heise.de/newsticker/meldung/NSA-Zeuge-BND-befluegelt-US-Drohnenkrieg-2249399.html*
7 *http://andrej-hunko.de/component/content/article/7-beitrag/2157-bundestrojaner-angeblich-einsatzbereit-erstmals-mehr-hinweise-zu-beteiligten-firmen*
8 *http://www.heise.de/newsticker/meldung/BND-will-SSL-geschuetzte-Verbindungen-abhoeren-2444901.html*
9 *http://www.heise.de/newsticker/meldung/Lehren-aus-der-NSA-Spaehaffaere-Bundesjustizminister-will-Geheimdienste-kritisch-pruefen-2282500.html*
10 *http://andrej-hunko.de/component/content/article/7-beitrag/2152-wie-der-bundesnachrichtendienst-und-die-bundeswehr-das-internet-ausspaehen-wollen*
11 *https://netzpolitik.org/2014/ueben-ueben-ueben-wie-die-eu-sich-auf-den-cyber-ernstfall-vorbereitet/*
12 *http://www.enisa.europa.eu/activities/Resilience-and-CIIP/*
13 *https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-atlantic*
14 *https://www.ccdcoe.org/locked-shields-2014.html*
15 *http://eeas.europa.eu/statements/docs/2014/140926_01_en.pdf*
16 *https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/cyber-europe-2014-information/briefing-pack/cyber-europe-2014-2013-questions-and-answers*
17 *(siehe 11)*
18 *http://www.nato.int/cps/en/natohq/opinions_112871.htm*
19 *(siehe 11)*
20 *http://www.dhs.gov/cyber-storm-securing-cyber-space*
21 *http://www.spiegel.de/netzwelt/web/snowden-enthuellungen-staats-versagen-beim-schutz-der-buerger-a-973272.html*

Sebastian Jekutsch

Betrifft: Faire Computer

Fair wie in *Faire Kleidung*.

Am Ende der letzten Kolumne berichtete ich von Krebs-Fällen bei der Herstellung von Computerchips heute (z. B. Samsung) und früher (z. B. IBM). Daran kann ich nun nahtlos anknüpfen: Auch in der Endmontage der Geräte bei *Foxconn* sind in einem Werk nun mehrere Leukämie-Fälle aufgetaucht, und noch weiß niemand so genau, was sie verursacht hat. Foxconns wichtigster Kunde *Apple* hatte einen Monat vorher schon reagiert, indem er einige krebserzeugende Chemikalien aus dem Produktionsprozess verbannte. Das freilich kam viel zu spät für die Produktion des neuen iPhone 6 und gilt im übrigen auch gar nicht für die Produktion der Bauteile, beispielsweise der Chips. Es ist auch nicht so, dass Apple neue Erkenntnisse umgesetzt hätte: Eine Bewegung für das Verbot von Benzol in China gibt es schon seit vielen Jahren. In den USA startete Anfang des Jahres eine Petition zu dem Thema.

Ebenfalls an die Kolumne 3/2014 anschließen können wir bei den Elektronikfirmen-Rankings: *Greenpeace* hat mit der *Guide to Greener Electronics*-Tradition gebrochen und spricht nun lieber von *Green Gadgets*. Auch dort stehen Chemikalien im Fokus sowie der Energieverbrauch und die Materialien. Greenpeace lobt Apple als vorbildlich. Von Fairness ist bei Greenpeace allerdings gar nicht mehr die Rede. Dafür aber bei den Schweizer Organisationen *Brot für alle* und *Fastenopfer.* In ihrem *High-tech-Ranking* wurden von den Herstellern ausgefüllte Fragebögen ausgewertet. „Auf gutem Weg" seien lediglich *HP* und *Nokia*. Das zur Darstellung genutzte Ampelsystem ist sicherlich praktisch und intuitiv, aber haben sie wirklich ein Grün verdient? *Germanwatch* kritisiert diese Rankings als eher verwirrend, denn „wirklich faire und nachhaltige Geräte gibt es noch nicht", zudem seien die „bei den Produktrankings angelegten ökologischen und sozialen Kriterien ... sehr unterschiedlich" und sie „beruhen hauptsächlich auf Aussagen der Hersteller und nicht auf unabhängigen Informationen Dritter". (Siehe zu dem Thema auch den Artikel von Rank-a-brand in dieser Ausgabe.)

Mit den *Informationen Dritter* sind Audits und investigative Recherchen gemeint. *TCO Development* (die mit dem Siegel) haben dieser Tage veröffentlicht, wie weit sich ihre Kunden aus der IT-Branche überhaupt an ihre eigenen Ethikversprechungen halten. Ergebnis: 11 von den 17 taten es in sogar schweren Fällen nicht. Namen nennt TCO leider nicht. Es gab in den letzten Monaten zudem einige investigative Recherchen in chinesischen Fabriken mit Erkenntnissen, an die wir uns leider beinahe schon gewöhnt haben:

- Bezahlung unter Mindestlohn, hoher Arbeitsdruck und Verweigern von Pausen bei *Jabil Circuit* in Wuxi, fertigt Teile bislang nur für Apple.

- 15-Stunden-Tage und Gesundheitsrisiken durch Chemikalien bei *Pegatron Corp*. in Suzhou, fertigt für Apple, Acer, Asus, Cisco, Dell, Microsoft, Sony u. a.

Sebastian Jekutsch

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

- Fehlende Einarbeitung, Pflichtüberstunden und verweigerte Einzahlung in Sozialversicherungen bei *Catcher Technology* in Suqian, fertigt Gehäuse u. a. Teile für Apple, Dell, HP, Lenovo, Sony, HTC, Motorola u. a.

- 12-Stunden-Schichten im Stehen und Kinderarbeit bei *HEG Technology* in Huizhou, endfertigt für Samsung, Lenovo u. a.

- Illegale Arbeitsvermittlungsgebühren, Überstunden bei Praktikanten und fehlende Erholungstage bei *Quanta Computer* in Shanghai und Shangshu, endfertigt für Apple, Sony, Dell, HP u. a.

- Kinderarbeit, enorme Überstunden und Diskriminierung von Leiharbeitern bei *Shinyang Electronics* in Dongguan, fertigt Gehäuse u.ä. vermutlich ausschließlich für Samsung.

Apropos *Samsung*: Sie haben auch beim Berufungsgericht den Prozess verloren gegen zwei klagende Familien von an Krebs gestorbenen Ex-Mitarbeiterinnen und müssen nun Kompensationsgelder zahlen. Die Gespräche mit der Zivilorganisation *SHARPS/Banolim* gestalten sich weiterhin schwierig. Samsung strebt außergerichtliche Einigung mit lediglich sechs weiteren Familien an. SHAPRS besteht auf Vertretung aller Opfer.

Kurz zu den innovativen Fair-IT-Projekten:

- *Fairphone*: Eine neue Version mit *eigenem Design* soll ab Mitte 2015 bestellbar sein, während die vorhandenen Geräte fast ausverkauft sind. Die ArbeiterInnen der *Fairphone-Fabrik* haben zudem entschieden, sich die Gelder aus dem *Worker Welfare Fund* auszahlen zu lassen. Damit dürfte die Belegschaft im Nachhinein einen Monat lang die vielleicht bestbezahlten Handy-Zusammenbauer Chinas gewesen sein.

- *NagerIT*: Es soll eine detaillierte Kostenaufstellung entwickelt werden, aber offen, ehrlich und wahrhaftig zu sein, ist gar nicht so einfach wie es scheint: Ein Diskussionsaufruf auf der Website *www.nagerit.de*. Zudem kommt bald das hölzerne Scroll-Rad, welches das aus unfairem Plastik ablösen soll.

- *Fairlötet*: Das Projekt zur Herstellung fairen Lötdrahts startete unter *www.fairloetet.de* und begann mit einer Umfrage an potenzielle Kunden. Das Ziel soll mit Recycling-Zinn erreicht werden.

- *ShiftPhone*: Noch stehen detaillierte Informationen aus, wie die weitreichenden Fairnessversprechen des Herstellers aus Hessen umgesetzt werden, aber immerhin gibt es ein freundliches Foto des chinesischen Entwicklungsteams.

Eine gute Nachricht am Ende: Die Proteste gegen die Entlassung von 24 *NXP*-Betriebsräten auf den Philippinen hatte Erfolg. Nicht nur wurde die eine Hälfte wieder eingestellt und die andere Hälfte ordentlich abgefunden, sondern auch der laufende Tarifkonflikt wurde mit einem guten Ergebnis für die ArbeitnehmerInnen abgeschlossen. Der *Philips*-Spinoff NXP ist ein bedeutender Produzent von Halbleiterbauteilen, auch in Deutschland. In Hamburg, bei mir um die Ecke, werden vermutlich die neuen NFC-Chips vom iPhone 6 hergestellt.

Steckt da also tatsächlich ein faires Bauteil im iPhone?

Mario Dziamski

Wie nachhaltig ist dein Smartphone? Und dein Computer? Und dein TV?

Rank-a-Brand als Orientierungshilfe beim Kauf nachhaltiger Elektronik

In Zusammenarbeit mit Friends of the Earth Niederlande *hat* Rank-a-Brand *in diesem Jahr wieder 20 Markenhersteller für Verbraucherelektronik untersucht. Im Vergleich zum Vorjahr haben wir unsere Auswahl auf Hersteller für Unterhaltungs- beziehungsweise Kommunikationselektronik spezifiziert. Aufgrund vielfacher Wünsche unserer Nutzer haben wir dabei auch den niederländischen Smartphone-Hersteller* Fairphone *erstmals in unser Ranking aufgenommen. Unsere Bewertungskriterien wurden zudem weiterentwickelt – mit einem stärkeren Fokus auf Konfliktmineralien, Müllvermeidung und Produktlebenszyklus. Im Juni hatten wir unsere Untersuchungsergebnisse im* Elektronik-Report 2014 *veröffentlicht. Seitdem haben wir unsere Rankings fortwährend aktualisiert, sofern weitere oder neue Informationen zur Nachhaltigkeitsleistung der Hersteller öffentlich wurden.*

Angeführt wird das diesjährige Ranking von *Fairphone*. Das niederländische Start-Up erhält als einziger Hersteller die Beurteilung *empfehlenswert*. Unter den etablierten Herstellern kann Apple die beste Bewertung für sich verbuchen, gefolgt von Nokia und HP. Im Schlussfeld des Rankings sind mit ZTE, HTC, Nintendo und Huawei vor allem asiatische Hersteller angesiedelt. Jedoch auch Microsoft ist in der Gruppe der Schlusslichter zu finden (siehe Abbildung 1).

Methodik

Die wichtigste Informationsgrundlage für unsere Bewertungen ist die veröffentlichte Nachhaltigkeitsberichterstattung der Unternehmen. Darüber hinaus werden auch öffentliche Angaben von Akteuren wie *Friends of the Earth*, *CDP, IDH, GeSI* oder *EICC* in die Bewertung einbezogen. Nach Abschluss unserer Untersuchungen Anfang dieses Jahres wurden den Unternehmen die Ergebnisse zugesandt. Die mehrwöchige Frist zur Bereitstellung weiterer Informationen nutzten jedoch die wenigsten.

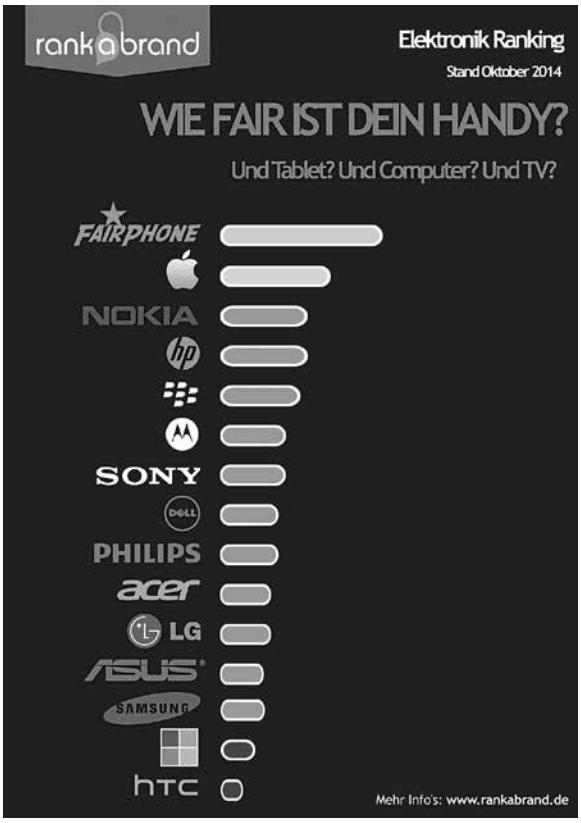


Abbildung 1: Ranking Scorecard, Stand Oktober 2014

Für unsere diesjährigen Untersuchungen haben wir den Kriterienkatalog für Elektronikhersteller von 20 auf 37 Bewertungsfragen erweitert. Während sich die Bewertungskriterien zum Klimaschutz im Vergleich zum Vorjahr kaum verändert haben, wurden die Themenbereiche Umweltschutz und Arbeitsbedingungen um wesentlich mehr Bewertungsfragen erweitert. Mit Bezug auf Maßnahmen zum Klimaschutz interessiert uns weiterhin vor allem, welche Emissionssenkungen die Unternehmen aufweisen können, welche Reduktionsziele für die Zukunft formuliert wurden, wie es um die Energieeffizienz der produzierten Geräte bestellt ist und in welchem Maße erneuerbare Energie bezogen wird.

Beim Umweltschutz haben wir neben Kriterien zur Entfernung von kritischen Chemikalien, wie PVC oder bromierte Flammschutzmittel, der Rücknahme von Altgeräten sowie dem Recycling von Plastik insbesondere Bewertungsfragen hinzugefügt, die die Verlängerung der Lebensdauer der Geräte sowie die Bilanzierung des Land- und Wasserverbrauchs betreffen. Darüber hinaus wurden die Bewertungskriterien punktuell anspruchsvoller. Dies betrifft ebenso den Themenbereich Arbeitsbedingungen. Eine Neuerung zum Vorjahr stellen beispielsweise spezifische Bewertungsfragen zur Zahlung existenzsichernder Löhne dar. Darüber hinaus richtet sich der Fokus nun noch stärker auf Maßnahmen, um den Bezug von Konfliktmineralien zu vermeiden. Ebenso wurde die Forderung nach Transparenz in Bezug auf Lieferantenbeziehungen weiter verstärkt.

Transparenz/Berichterstattung

Grundsätzlich kann festgestellt werden, dass alle untersuchten Elektronikhersteller über Nachhaltigkeit berichten. Die Berichterstattung zu den getroffenen Maßnahmen, erreichten Resultaten sowie gesetzten Zielen führt aktuell jedoch dazu, dass lediglich 1/3 unserer Bewertungsfragen eindeutig beantwortbar sind. Im Vergleich zu Unternehmen aus anderen Industrien wie Textilien oder Lebensmittel berichten die untersuchten Hersteller von Verbraucherelektronik somit noch vergleichsweise schwach über Maßnahmen zum Klima- und Umweltschutz sowie fairen Arbeitsbedingungen in der Produktion. 13 der 20 untersuchten Marken sind demgegenüber auf unserem *Greenwashing Alert* gelistet. Bei diesen Unternehmen liegt der Verdacht nahe, dass ökologische und soziale Nachhaltigkeit entweder insgesamt oder in einem spezifischen Themenbereich nicht substanziell, sondern vorrangig kommunikativ angegangen wird.

Die stichhaltigste Berichterstattung weist jenes Unternehmen auf, welches sich Unternehmensverantwortung mit der Gründung auf die Fahnen geschrieben hat und im Vergleich zu allen anderen Unternehmen deutlich am kleinsten ist: Fairphone. Zu 23 von 37 Bewertungsfragen liefert das Unternehmen Antworten, welche entsprechend unserer Bewertungskriterien mit einem „Ja“ oder „Nein“ beantwortbar sind. Bei den etablierten Unternehmen weist wiederum Apple mit 19 von 37 klar beantwortbaren Bewertungsfragen die kompletteste Berichterstattung auf. Insbesondere bei den asiatischen Herstellern Huawei, ZTE, HTC und Nintendo wurde hingegen deutlich, dass Offenheit zur Nachhaltigkeitsleistung bisher keinen großen Stellenwert einnimmt.

Abbildung 2: Greenwashing Alert, Stand Oktober 2014

Ergebnisse Klimaschutz

Zum aktuellen Zeitpunkt – Stand Oktober 2014 – kann sich kein Unternehmen als klarer Leader in puncto Klimaschutz hervortun. Was die eigenen betrieblichen Operationen betrifft, berichten zwar alle Unternehmen über Maßnahmen zum Klimaschutz. Lediglich Nokia, HP und Lenovo wissen jedoch auch mit entsprechenden Klimaschutzmaßnahmen in der Produktionskette zu überzeugen. Ein ähnliches Bild ergibt sich bei der Formulierung weiterer Klimaschutzziele. Nur *Sony, Philips, Microsoft* und *Dell* sind in diesem Punkt überzeugend. Mit Blick auf den Gebrauch von erneuerbarer Energie lichtet sich das Feld schließ-

lich so sehr, dass nur noch ein Hersteller überzeugt: Apple bezog im Jahr 2013 zu 75 % erneuerbare Energie und lässt damit alle anderen Markenhersteller deutlich hinter sich.

80 % der Hersteller veröffentlichen hingegen eine aussagekräftige Klimabilanz. Die knappe Mehrheit der Hersteller (55 %) kann weiterhin mit einer Verringerung der Treibhausgas-Emissionen in den eigenen Betriebsbereichen überzeugen. Die relativ deutlichste Reduktion der absoluten Klimabilanz kann dabei *Samsung* aufweisen. Zwischen 2011 und 2012 wurden die Treibhausgas-Emissionen von 11.304.000 Tonnen auf 7.486.000 Tonnen reduziert.

Ergebnisse Umweltschutz

Die Themen zum Umweltschutz fristen im Vergleich zum Klimaschutz und Arbeitsbedingungen das größte Schattendasein. Bisher kann beispielsweise kein Hersteller aufzeigen, dass alle der folgenden schädlichen Chemikalien nicht mehr verarbeitet werden: PVC, bromierte Flammschutzmittel, Beryllium, Antimon und Phthalate. In Bezug darauf erfüllen Nokia und Motorola noch am ehesten die Erwartungen. Diese Hersteller haben zumindest jeweils PVC und bromierte Flammschutzmittel aus ihren Produkten entfernt, Nokia zudem auch Beryllium sowie Motorola Phthalate. Die Bilanzierung zum Verbrauch von Wasser, Land und Materialien ist bisher ebenfalls sehr dürftig. In puncto Berichterstattung zu verarbeiteten Materialien setzen aktuell Apple und Toshiba Maßstäbe. Immerhin 25 % der untersuchten Hersteller veröffentlichen zudem Bilanzen zum Wasserverbrauch. Kein Unternehmen präsentiert jedoch bisher eine Bilanz zum Landverbrauch im Zuge der Produktion.

Bei den Bewertungsfragen zum Produktlebenszyklus und Müllvermeidung konnte lediglich Fairphone mit überzeugenden Maßnahmen und Resultaten klar punkten. So weist der niederländische Hersteller beispielsweise eine sehr hohe Rücknahmequote von alten Mobiltelefonen in Relation zum Absatz von Neugeräten auf. Gemeinsam mit Samsung ist Fairphone zudem der einzige Hersteller, der zu über 10 % recyceltes Plastik in den Geräten verarbeitet. Das Fairphone ist außerdem mit einer austauschbaren Batterie ausgestattet und verkauft nur auf expliziten Wunsch ein Ladegerät, weil es ohnehin in den meisten Haushalten schon vorhanden ist. Ebenfalls werden in Kooperation mit iFixit Do-It-Yourself Reparaturanleitungen online bereitgestellt. Ersatzteile können direkt geordert werden. Für die Produktverpackung werden gezielt umweltfreundliche Materialien verwendet. In der Summe bleiben alle anderen untersuchten Hersteller bezüglich solcher Maßnahmen zum Produktlebenszyklus und Müllvermeidung deutlich zurück. Kein Hersteller bietet jedoch eine Produktgarantie, die über drei Jahre hinausgeht. Einhergehend mit der schlechten Reparierfähigkeit einzelner Komponenten einiger Geräte sowie geplanter Obsoleszenz sorgt dies für kein gutes Gefühl, je näher das Ende der Garantiezeit rückt.

Ergebnisse Arbeitsbedingungen

Die bisherigen Untersuchungsergebnisse lassen eindeutig vermuten, dass das Thema menschenwürdige Arbeitsbedingungen in der Produktion im Vergleich zum Klima- und Umweltschutz den höchsten Stellenwert bei den Herstellern besitzt. Jedoch nur Fairphone, HP und Apple überzeugen bisher mit entsprechenden Maßnahmen und Resultaten zumindest in Ansätzen. 19 der 20 untersuchten Elektronikhersteller informieren über die Anwendung eines Verhaltenskodexes für Zulieferer. Abgesehen von Fairphone und HP nutzt aber keiner der Hersteller einen Kodex, bei dem alle *ILO Kernarbeitsnormen* für Zulieferbetriebe verpflichtend sind. Bezüglich Transparenz zu den Lieferantenbeziehungen in der Endfertigung sowie den Schmelzhütten veröffentlichen zudem nur Dell, Apple, HP und Fairphone entsprechende Listen, die einen Überblick verschaffen, wer die Zulieferer dieser Hersteller sind.

Über die Resultate der umgesetzten Maßnahmen zur Verbesserung der Arbeitsbedingungen in den Fabriken berichten ebenfalls nur HP und Fairphone schlüssig. Jedoch auch diese beiden Hersteller können nicht den Nachweis liefern, dass zumindest die Hälfte der Gesamtproduktion entsprechend der Arbeitsnormen im Verhaltenskodex fair hergestellt wurde – einschließlich eines zum Leben ausreichenden Gehalts. Beim Thema Konfliktmineralien ergibt sich ein ähnliches Bild. 85 % der untersuchten Hersteller wirken zwar in mindestens einer Initiative mit, um den Notwendigkeiten zur Verbesserung des Arbeitnehmer- und Umweltbedingungen beim Abbau von Metallen und Mineralien nachzugehen. Nur Fairphone und Apple können jedoch aufweisen, dass mindestens eines der verarbeiteten Mineralien konfliktfrei bezogen wird. Insgesamt bleibt somit festzuhalten, dass zum aktuellen Zeitpunkt kein Hersteller wirklich fair sowie konfliktfrei produzierte Elektronik gewährleisten kann.

Fazit

Der Weg der Elektronikhersteller zu fairen und umweltfreundlichen Produktionsbedingungen ist noch sehr weit. Erste Schritte in die richtige Richtung sind zwar gemacht. Mehr als ein Anfang ist das allerdings nicht. Dass vor allem Fairphone auf so viel positiven Widerhall bei den Konsumenten trifft, zeigt jedoch deutlich, dass die Nutzer der Geräte zunehmend für nachhaltigere Elektronik bereit sind.

Mario Dziamski

Mario Dziamski lebt in Berlin und ist seit 2011 für *Rank-a-Brand* aktiv. Er leitet die Untersuchungen der gesamten Organisation sowie den Aufbau von *Rank-a-Brand* in Deutschland.

Sebastian Beschke (Interview, Übersetzung) und **Sebastian Jekutsch** (Interview, Foto)

„Es ist ein Verbrechen“

Interview mit Mike Anane über Elektroschrott

Es gibt viele Berichte über den illegalen Export von Elektroschrott von Europa nach Ghana. Obwohl alle europäischen Länder Unterzeichner der Baseler Konvention *sind, welche den Export von Giftmüll (worunter auch Elektroschrott zählt) in nicht-OECD-Länder verbietet, können neue, funktionierende oder reparierbare Geräte legalerweise verschifft werden – zum Beispiel nach Indien, China, Nigeria oder Ghana. Das führt dazu, dass auch Elektroschrott oft als Gebrauchtware deklariert wird. Dadurch landet Elektroschrott aus Deutschland und anderen westlichen Ländern in* Agbogbloshie*, einer illegalen Müllkippe in der ghanaischen Hauptstadt Accra. Die zwei deutschen Dokumentarfilme „Giftige Geschäfte – Der Elektromüll-Skandal“ und „Die GPS-Jagd – Wo landet mein Schrottfernseher“ haben in letzter Zeit für Aufsehen gesorgt. Wir haben uns bei einer Fotoausstellung von* Kevin McElvaney *in Hamburg mit* Mike Anane *getroffen, einem Umweltaktivisten und Journalisten aus Accra. Wir sprachen mit ihm über soziale Aspekte der Elektroschrott-Entsorgung, über die Verantwortung der Hersteller, und warum er in jeder Dokumentation zum Thema vorkommt.*

FIfF: **Wie lange beobachtest du schon die Situation in Agbogbloshie?**

Mike Anane: *Seit 11 Jahren. Damals habe ich erstmals die Lastwagen mit Elektroschrott vom Hafen nach Agbogbloshie fahren sehen. Ich kenne Agbogbloshie gut. Ich war oft dort, als es noch ein üppig grünes Feuchtgebiet war, voller Vögel und wilder Tiere. Der Fluss und die Lagune dort hatten damals viele Fische. Viele Menschen in den angrenzenden Orten bezogen daraus ihren Lebensunterhalt. Agbogbloshie war damals unglaublich schön, wie ein Garten Eden. Ein Feuchtgebiet erfüllt sehr wichtige ökologische Funktionen. Wenn das Wasser aus der Stadt zum Meer fließt, wird es im Feuchtgebiet gefiltert. Fische aus dem Meer kommen, um sich zu vermehren. Feuchtgebiete sind in jedem Land der Welt wichtig, für die Natur und die Menschen.*

Jetzt aber sind der Fluss und die Lagune tot: keine Fische, überhaupt kein Leben mehr. Wenn die Fischer nahe der Mündung am Meer ihre Netze auswerfen, fangen sie keine Fische, sondern Computer, Fernseher oder Kühlschränke. Deren Giftstoffe fließen jeden Tag ins Meer. Wo die Lagune und der Fluss ins Meer münden, ist das Wasser so schwarz und giftig, dass es nach Benzin riecht. Auch am Strand liegen Computer und Kühlschränke herum. Deshalb ist dieser Garten Eden für mich nun das verlorene Paradies.

FIfF: **Was für einen Entwicklung siehst du? Verschlimmert sich die Situation immer noch?**

Mike Anane: *Die Verschmutzung nimmt zu. Trotz all den Filmen, die gemacht wurden, der Aufmerksamkeit in den Medien, hat sich überhaupt nichts geändert. Falls sich irgend etwas geändert hat, ist es die Wahrnehmung. Bis vor kurzem wussten nur wenige Menschen von dem Elektroschrottproblem. Mittlerweile wird es etwas mehr wahrgenommen – wenn ich irgendwohin gehe, stellen die Leute Fragen und haben anscheinend schon ein paar Filme gesehen und so. Aber aus dieser gesteigerten Wahrnehmung hat sich noch keinerlei Handlung ergeben, keine Reduktion der Mengen an Elektroschrott, die illegal nach Ghana verschifft werden.*

Zu Weihnachten kaufen die Leute neue Flachbildfernseher und Handys als Geschenke. Die Frage ist nur, was mit diesen alten Telefonen und Fernsehern passiert, die sie dann wegwerfen. Sie tragen zu dem Berg an Elektroschrott bei, der nach Ghana verschifft wird. Immer um die Weihnachtszeit erhöht sich die Menge an Elektroschrott, die in Ghana abgeladen wird. Normalerweise kommen pro Monat 500 bis 600 Containerladungen Elektroschrott aus industrialisierten Ländern an. Zu Weihnachten sind es etwa 800 bis 1000.

Mike Anane während des Interviews bei der Fotoausstellung

FIfF: **In einem Dokumentarfilm, der kürzlich im Fernsehen lief, hattest du mit Behörden im Vereinigten Königreich gesprochen. Was hältst du von ihrer Einstellung zum Elektroschrottproblem? Nehmen die Behörden in Großbritannien, Deutschland und anderswo in Europa das Problem ernst genug?**

Mike Anane: *Wenn man sich mit Behörden in den Ländern, die ich besucht habe, unterhält, hört es sich so an, als ob sie das Problem sehr ernst nehmen würden. Wenn das aber so wäre, dann müssten sich doch die Mengen an Elektroschrott verringern, die in Ghana landen. Das ist aber nicht passiert. Es gibt viel Gerede und Versprechen, und es wurden natürlich auch ein paar Gesetze erlassen. Aber all dies führt nicht zu einer Reduktion des Elektroschrotts.*

FIfF: **Was sollten wir Europäer tun – individuell, und auch in der Politik?**

Mike Anane: *Wenn man sich anguckt, wo der Elektroschrott herkommt, würde man erwarten, dass die Ursprungsländer ihre Verantwortung besser erfüllen. Alle diese Länder haben die Baseler Konvention unterzeichnet, die es im Wesentlichen ver-*

bietet, gefährliche Abfälle über Grenzen hinweg zu bewegen. Elektroschrott gehört dazu. Diese Länder müssen stringente Maßnahmen implementieren, um die illegale Verschiffung von Elektroschrott aus ihren Häfen zu unterbinden. Wenn Elektroschrott die Häfen von Deutschland, den Niederlanden und anderen Ländern verlässt, ist das alleine schon ein Verbrechen. Warum können die Regierungen dieser Länder diese Container nicht kontrollieren?

Auch die Hersteller von Elektronikprodukten, wie Hewlett-Packard oder Philips, spielen eine wichtige Rolle. Sie sollten von der Wiege bis ins Grab für ihre Produkte verantwortlich sein. Sie stellen diese Produkte mit hochgiftigen Bestandteilen wie Blei, Cadmium, bromierten Flammschutzmitteln und Quecksilber her. Wenn der Hersteller sich nicht um solchen Abfall kümmert, wie sollen es die Verbraucher tun?

Die Hersteller sollten damit aufhören, Schwermetalle und anderen Chemikalien bei der Herstellung von Fernsehern und anderen Produkten zu verwenden. Warum verwenden sie diese gefährlichen Stoffe – gibt es keine Alternativen dazu? Wir müssen die Hersteller unter Druck setzen, um sie zu Veränderungen zu bewegen.

FIfF: **In Deutschland sind die Hersteller tatsächlich für die Entsorgung verantwortlich. Es gibt ein System, in dem die Verbraucher den Schrott zu Sammelstellen bringen. Das Problem ist, dass sie ihn auch für ein paar Euro verkaufen können, und dieser Schrott geht dann nach Ghana. Wir haben also ein System der Herstellerverantwortung, aber es funktioniert nicht.**

Mike Anane: *Das stimmt. Deswegen sagte ich, dass es auf dem Papier viele Versprechungen gibt, die Realität aber anders aussieht. Ich sehe in Ghana immer noch viel Elektroschrott aus Deutschland. Das heißt, dass die Hersteller die Geräte nicht einsammeln. Und ich rede hier von vielen Containerladungen: in den letzten fünf Monaten kam der größte Teil des Elektroschrotts in Ghana aus Deutschland. Davor kam er immer aus verschiedenen Ländern wie Dänemark, den Niederlanden, dem Vereinigten Königreich und Deutschland. Dann kam eine Zeitlang viel aus dem Vereinigten Königreich. Von dort kommen besonders viele völlig kaputte Geräte, rostig und als ob sie irgendwo eingegraben gewesen wären. Jetzt liegt Deutschland vorne.*

FIfF: **Lass uns über die Situation in Ghana reden. In einem Dokumentarfilm wurde gezeigt, wie Container im Hafen ankommen und oft nicht richtig überprüft werden. Meinst du, dass die Behörden dort das Problem auch ernster nehmen müssen?**

Mike Anane: *Jede Regierung, jedes Land trägt seinen Bürgern gegenüber Verantwortung. Auch die ghanaische Regierung trägt eine Mitschuld. Sie müsste dafür sorgen, dass die Dinge, die ins Land kommen, nicht die Menschen vergiften. An unseren Grenzen müssten wir dafür sorgen, dass Container mit Giftmüll zurückgeschickt werden. Aber ich glaube, dass der Zoll und die anderen Behörden an den Häfen in Ghana nicht in der Lage sind, mit den Mengen an Elektroschrott umzugehen, die dort ankommen. Und vergessen wir nicht, dass diese Container nicht als Elektroschrott deklariert sind. Stattdessen heißt es, es seien Rohstoffe, Haushaltswaren, Schuhe, Reifen, Autos. Für ein Entwicklungsland mit seinen begrenzten Ressourcen ist es sehr schwer, dies umfassend zu prüfen.*

FIfF: **Ich finde es interessant, dass Ghana auch eine ganze Menge gebrauchter, aber funktionstüchtiger Elektronikprodukte importiert. Grenzbehörden stehen daher vor dem Problem, kaputte von noch funktionstüchtigen Geräten zu unterscheiden. Welche wirtschaftliche Rolle spielen diese Güter in Ghana?**

Mike Anane: *Früher gab es Leute, die funktionierende Gebrauchtwaren gekauft und verkauft haben. In letzter Zeit ist das aber schwierig geworden. Wenn man als armer Mensch in einen Laden geht und einen gebrauchten Fernseher oder Computer kaufen will, wird einem dort erzählt, dass die Geräte ungetestet seien, daher sei der Preis auch so niedrig. Es ist also ein Glücksspiel. Wenn man einen Flachbildschirm kauft, ihn zu Hause anschalten will und er nicht funktioniert, muss man ihn irgendwie wegwerfen.*

Die Händler verkaufen ungetestete Waren, weil aus Europa immer mehr Geräte kommen, die nicht funktionieren. Früher hatten sie jemanden, der versuchen konnte, sie zu reparieren. Sie stellen jetzt aber fest, dass sie nicht alles reparieren können, und dass das Reparieren oft zu teuer ist. Daher geben sie diese Kosten an die Verbraucher weiter, die diese Waren nun irgendwie entsorgen oder loswerden müssen.

FIfF: **Würdest du sagen, dass mehr Gutes oder mehr Schaden durch den Import dieser Waren angerichtet wird?**

Mike Anane: *Ich würde das gar nicht als Import bezeichnen. Für mich geht es immer noch um Entsorgung, denn von all diesen Containern enthalten nur etwa 20 % funktionsfähige Geräte, und 80 % sind Müll. Jemand in Europa, Amerika oder sonstwo möchte diese Dinge loswerden, und sie müssen irgendwo hin. Ich glaube, dass das, was die Leute ohne diese Geräte verlieren würden, fast vernachlässigbar ist, weil sie sowieso Abfall sind. Sie müssten in den Ländern, wo sie herkommen, entsorgt oder recycelt werden. Ich finde es falsch, wenn ein Land Giftmüll, oder überhaupt Müll, in ein anderes Land schickt. So läuft es einfach nicht. Unterm Strich ist es ein Verbrechen und sollte nicht passieren.*

FIfF: **Was passiert mit dem Elektroschrott aus Ghana selbst, all den als ungetestet verkauften Geräten, die nicht funktionieren? Landen sie auch auf illegalen Müllkippen?**

Mike Anane: *Definitiv. Selbst wenn man eines der 20 % funktionierenden Geräte erwischt, haben sie in der Regel nur noch eine kurze Lebensdauer, vielleicht zwei bis sechs Monate. Wenn sie schließlich kaputtgehen, laden die Menschen sie einfach an der Straße ab. Sie wissen nicht, wohin damit.*

Das Problem ist sogar noch größer. Wenn jemand ungetestete Fernseher einkauft, um sie weiterzuverkaufen, und vielleicht zehn davon nicht funktionieren, wird er sie ebenfalls einfach draußen abstellen. Elektronikprodukte haben nur eine bestimmte Lebensdauer. Wenn sie in Ghana benutzt werden und kaputtgehen, landen sie auch auf illegalen Müllkippen.

FIfF: **Wie ist in Ghana die öffentliche Einstellung zu Elektroschrott? Ist die Bevölkerung über das Problem informiert?**

Mike Anane: *In den meisten Entwicklungsländern haben die Menschen kein besonders tiefgehendes Wissen über Naturwissenschaften, Ökologie, Physik oder Biologie. Die Menschen kämpfen damit, Geld zu verdienen, um sich für den heutigen Tag zu ernähren. Natürlich sehen viele Ghanaer immer mal wieder den Schrott. Immer mehr Menschen werden auf die Giftigkeit und die physikalischen und chemischen Zusammenhänge aufmerksam. Sie sehen den Schrott an jeder Straßenecke.*

Ich sammle Elektroschrottteile, auf welchen noch Inventaretiketten kleben. Wenn man sich die anschaut, ist es interessant zu sehen, dass die meisten Teile von renommierten Institutionen in Europa kommen, die sich eigentlich der Gefährlichkeit des Mülls bewusst sein müssten und ihn daher nicht schicken dürften. Ich habe Elektroschrott von der US-amerikanischen Umweltschutzbehörde EPA*, aus dem niederländischen Umweltministerium, und aus deutschen und britischen Krankenhäusern und Banken. Die Giftigkeit dieses Mülls sollte ihnen wohlbekannt sein.*

Im Allgemeinen denken sich die Menschen in Ghana nicht so viel dabei, wenn sie Elektroschrott sehen. Sie wissen, dass er aus Europa kommt. Sie haben auch einen Spottnamen dafür: sie nennen ihn den „Müll des weißen Mannes". Aber sie wissen nichts von den giftigen Bestandteilen. Wir arbeiten daran, dieses Wissen nach und nach zu verbreiten.

FIfF: **Wie arbeitest du in Ghana? Alleine oder gibt es eine Organisation, die dich unterstützt?**

Mike Anane: *Ich habe ein Team, das ich ausgebildet habe und das mir hilft. Wenn ich verhindert bin, können sie zum Hafen oder an andere Orte gehen. Manchmal möchte ich auch nicht alleine unterwegs sein. Es sind aber nur ein paar Leute.*

FIfF: **Gibt es noch andere Gruppen, die sich mit den gleichen Themen beschäftigen?**

Mike Anane: *Nein, ich glaube nicht. Das ist ein ziemlich spezialisiertes Gebiet. Außerdem weht einem auf der Müllkippe ständig giftiger Rauch ins Gesicht. Die meisten Leute gehen da nicht gerne hin, machen diese Arbeit nicht gerne. In Ghana kann ich nicht wie jetzt ein schickes Hemd anziehen. Man sieht immer dreckig aus, darauf haben die meisten Leute keine Lust.*

FIfF: **Es gibt viele Dokumentarfilme über Elektroschrott in Ghana, und in jedem tauchst du auf.**

Mike Anane: *Das stimmt, weil ich nun mal der Erste war, der das publik gemacht hat. Als mir klar wurde, wie ernst das Problem war, habe ich lokale Journalisten zur Müllkippe gebracht. Dann habe ich auch angefangen, mit ausländischen Journalisten zusammenzuarbeiten. Natürlich bin ich dabei ein Experte geworden. Nicht viele Leute wollen diese Arbeit tun. Manchmal muss man verdeckt arbeiten, um an Informationen zu kommen, und gerät dabei in gefährliche Situationen. Manchmal läuft man im Dunkeln herum. Normale Menschen wollen das nicht machen (lacht).*

FIfF: **Wie viele Menschen, würdest du schätzen, arbeiten in Agbogbloshie? Was treibt sie dorthin?**

Mike Anane: *Neben Agbogbloshie gibt es eine Ortschaft, die als „Sodom und Gomorrha" bekannt ist. Dort wohnen etwa 40.000 Menschen. Tausende Kinder zwischen fünf und 17 Jahren arbeiten jeden Tag auf der Müllkippe. Sie nehmen den Schrott mit ihren kleinen Fingern auseinander oder zerbrechen ihn, indem sie ihn auf den Boden werfen. Die meisten von ihnen sind sehr arm und kommen aus dem verarmten Norden des Landes. Sie suchen in der Stadt nach Arbeit, aber die gibt es dort nicht. Also versuchen sie, mit dem Schrott ihren Lebensunterhalt zu verdienen, denn der ist verfügbar, er wird dort einfach abgeladen. Die Kinder finden das interessant, weil sie neben Handys, Computern und Fernsehern auch Spielekonsolen finden. Sie versuchen, mit ihnen zu spielen – und dann zerschlagen sie sie mit einem Hammer. Sie suchen nach Metallen, vor allem Kupfer, um mit dem Erlös Lebensmittel zu kaufen. Einige der Kinder geben auch ihren Müttern Geld. Und einige sparen, um in die Schule gehen zu können.*

FIfF: **Wenn dort kein Elektroschrott mehr ankommen würde, müssten diese Menschen sich eine andere Einnahmequelle suchen. Wie könnte man ihre Situation dann verbessern?**

Mike Anane: *Früher, als im Land noch kein Elektroschrott ankam, haben die armen, jungen Leute auf der Straße Wasser oder Orangen verkauft. Diese Tätigkeiten waren für sie nicht gefährlich. Sie waren nicht Blei und anderen giftigen Substanzen ausgesetzt. Falls kein Elektroschrott mehr ankommen würde, würden viele Kinder wieder zur Schule gehen, denn der Elektroschrott produziert Schulschwänzer. Viele Kinder hängen lieber mit ihren Freunden auf der Müllkippe herum. Sie würden dann wieder zur Schule gehen. Diejenigen, die das nicht können, würden Wasser, Orangen oder Mangos auf ihren Köpfen transportieren und so ihren Lebensunterhalt verdienen, denn so haben das die Menschen vorher auch gemacht. Einige ältere Arbeiter könnten das allerdings nicht.*

Die Arbeiter dort müssten umgeschult werden. Sie brauchen alternative Einnahmequellen. Landwirtschaft, Näherei, Schweißen – irgendetwas, das weniger gefährlich ist, als sich ständig Blei, Merkur und Cadmium auszusetzen. Falls der Schrott nicht mehr ankommt, gibt es so viele Dinge, die diese Leute tun können. Dabei braucht es Kooperationen zwischen Ländern des Südens und des Nordens, zwischen Ghana und Deutschland.

FIfF: **Viele Organisationen appellieren aus Umweltsicht an die Verbraucher, ihre Telefone nicht alle zwei Jahre wegzuwerfen, sondern weiterzubenutzen, zu reparieren und upzugraden. Glaubst du, dass es eine gute Strategie ist, dass Verbraucherverhalten durch solche Appelle zu verändern?**

Mike Anane: *Es ist wichtig, bei den Verbrauchern ein Bewusstsein zu schaffen. Der Konsumismus hat schon so viel zu den Bergen von Elektroschrott beigetragen, der in Entwicklungsländern landet. Die Verbraucher sollten sich bewusst sein, dass sie sich ein Gadget nicht kaufen müssen, wenn sie es nicht wirklich brauchen. Aber der Knackpunkt ist, dass man dies nicht durchsetzen kann. Wenn sie das Geld haben und etwas kaufen wollen, kannst du sie nicht davon abhalten.*

Wenn sich die Einstellung der Konsumenten ändern würde, könnte das schon etwas dazu beitragen, die Mengen von Elektromüll zu

reduzieren. Aber ich denke, dass das Problem hauptsächlich von den Herstellern gelöst werden muss. Sie sorgen ganz unverblümt für die rapide Obsoleszenz der Geräte. Aufgrund des Herstellers ist ein iPhone, das man heute kauft, nach zwei Jahren schon kaputt und man braucht ein neues. Das ist volle Absicht. Die Mobiltelefone, die man früher kaufen konnte, haben hundert Jahre gehalten, selbst wenn man sie fallen gelassen hat. Die heutigen Android-Telefone lässt man einmal fallen und der Bildschirm bricht.

FIfF: **Also sollten eher die Verbraucher an die Hersteller appellieren?**

Mike Anane: *Auf jeden Fall. Alle Bürger sollten sich der Bewegung anschließen. Sie sind herzlich willkommen. Sie sollten an die Hersteller nicht nur appellieren, sondern sie unter Druck setzen. Sie sollten Druck ausüben, die Geräte nach Ablauf ihrer Lebenszeit wieder einzusammeln und keine toxischen Bestandteile zu verwenden, denn am Ende sind es die Verbraucher, die darunter leiden. Viele Verbraucher werden durch Elektronikmüll krank, weil sie nichts von seiner Giftigkeit wissen. Ich kenne Leute, die Telefone sammeln und sie am Ende ihrer Lebenszeit in die Schublade im Schlafzimmer legen, und sich so den Schwermetallen aussetzen.*

FIfF: **Möchtest du uns sonst noch etwas mitteilen?**

Mike Anane: *Ich würde gerne sagen, dass wir alle im selben Boot sitzen. Die Luftqualität wird zerstört, und wir atmen alle die gleiche Luft. Der Rauch geht überall hin. Die Gewässer, die abgetötet und mit Schrott gefüllt wurden, fließen alle ins Meer, das eine globale Allmende ist. Wir alle benutzen es, überall auf der Welt. Deshalb sollten wir uns bewusst sein, dass wir ernten werden, was wir säen. Wir sollten zusammenarbeiten, um der Bedrohung durch Elektroschrott zu begegnen. Unsere Nachkommen werden uns nicht verzeihen, wenn wir uns jetzt nicht um eine Lösung dieser Krise bemühen. Unsere Kinder und Kindeskinder werden uns verantwortlich machen, wenn wir jetzt den Mund halten und die Arme verschränken.*

Zuerst erschienen auf Englisch im Blog „Faire Computer" unter http://blog.faire-computer.de/mike-anane-on-the-e-waste-menace/

Marie-Theres Tinnefeld

Wahrung der Menschenrechte

Eine Voraussetzung der europäischen Friedensordnung

Das Ziel dieses Beitrages ist es, unveräußerliche Menschenrechte mit Bildern des Friedens und der Gerechtigkeit zu verbinden. Es geht dabei um eine Begriffspaarung, die sich schon im Alten Testament findet und nach dem Zweiten Weltkrieg in das Zentrum einer europäischen Friedensordnung gerückt ist. Seit dem 11. September 2001 wächst aber nicht nur im europäischen Recht ein sicherheitsbetontes Denken. Es entsteht auch eine Sicherheitspolitik, in der die Verantwortung für eine umfassende Überwachung der Bürger von der staatlichen Gewalt in die statistisch untermauerte Welt der Logik, Mathematik und Informatik verlagert wird. Diese Entwicklung ist eine Herausforderung für eine verfassungsgemäße Allianz von Technik und Recht, die hier angesprochen werden soll.

I. Einführung

Der große Rechtsphilosoph Arthur Kaufmann hat im Jahre 1986 ein Buch mit dem thesenhaften Titel: *Gerechtigkeit – Der vergessene Weg zum Frieden*[1] zu einer Zeit veröffentlicht, in der das Wettrüsten zwischen Ost und West einem Höhepunkt zutrieb. Die neuerlichen Kältegräben in Europa und weltweit legen es nahe, sich auch auf Kaufmanns Betrachtung zu besinnen.

Das Begriffspaar *Gerechtigkeit und Frieden* ist eine uralte Formel, die sich auch im deutschen Verfassungsgrundrecht findet. In Artikel 1 Absatz 2 Grundgesetz klingt an, dass der Weg zum Frieden an unveräußerliche Grundrechte gebunden ist. Arthur Kaufmann bezieht sich in seinem Werk insbesondere auch auf die biblische Ausformung der alten Formel: „Das Werk der Gerechtigkeit wird der Friede sein" (Jes. 32, 17).[2]

Kaufmann interpretiert den Treuebund von *Iustitia und Pax* im Sinne der Prinzipien der Gerechtigkeit: dem *Suum cuique,* die *Goldene Regel,* Kants *Kategorischen Imperativ* im Sinne des Gebots der Gleichgewichtswahrung, des Grundsatzes (der Tugend) der Toleranz[3] und des Prinzips Verantwortung. Gemeint sind Prinzipien, die zur Grundarchitektur des europäischen Menschen- und Grundrechtsschutzes gehören.

Seit dem schwarzen Tag des 11. Septembers 2001 haben sich grundrechtliche Wege deutlich verengt. Die Chancen für ein freiheitliches Strafrecht nehmen ab. Das Sicherheitsrecht wird weltweit umfassend verschärft, die maßvolle Balance zwischen Freiheit und Sicherheit wird zu Lasten der Freiheitsrechte verschoben und dies auch mit Hilfe von Speicher- und Netzkapazitäten.

Aufgrund der Logik softwaregestützter statistischer Datenanalysen werden Menschen automatisch nach bestimmten Suchmerkmalen in Kategorien eingeteilt, beurteilt und häufig diskriminiert. Zygmunt Baumann spricht in diesem Zusammenhang von Tendenzen im Überwachungsbereich, die keinem moralischen Urteil unterworfen sind, für die niemand moralisch verantwortlich ist.[4] Es zeichnet sich eine Entwicklung ab, die sowohl den Schutz der informationellen Selbstbestimmung als auch Diskriminierungsverbote verletzen, obwohl sie menschen- und grundrechtlich verortet sind.

Wie nie zuvor findet sich eine vollwertige Grundrechtsarchitektur in Europa: in der Europäischen Menschenrechtskonvention, in der Europäischen Grundrechtecharta und in den Verfassungen der Mitgliedstaaten. Und trotzdem bleiben viele Bürger zögerlich vor den Toren der höchsten europäischen Gerichte, dem Straßburger Gericht, dem Luxemburger Gericht oder dem Karlsruher Gericht stehen, obwohl sie allenthalben auf Gesetze sto-

ßen, die ihre verfassungsrechtlich garantierten Freiheitsrechte zugunsten einer vermeintlichen Sicherheit massiv einschränken.

Der Jurist und Literat Franz Kafka befasst sich eindringlich mit der menschlichen Vorstellung vom Gesetz. In seiner Erzählung *Vor dem Gesetz* zeigt er, dass das Tor zum Gesetz zwar offen steht und der Türhüter den Mann Josef K. keineswegs mit Gewalt daran hindert, in das Gebäude des Gesetzes einzutreten.[5] Diese irritierende Erzählung sagt sinngemäß etwas zum Thema aus. Mit Kafka lässt sich fragen: Warum können Bürger nicht in das Gebäude des Gesetzes eintreten, obwohl sie es könnten?

II. Von der Grundrechtssicherung zum Bann-Opticum

In seiner Parabel *Der Bau* beschreibt Kafka eine kreatürliche Existenz, die auf ein zwanghaft-ängstliches Streben nach Selbsterhaltung reduziert ist. Es handelt sich um ein Leben, das nicht auf ein menschliches Miteinander bezogen ist. Es handelt sich auch um die maßlose technische Absicherung des eigenen Baus.[6] Dort gibt es kein Hin und Her mehr zwischen öffentlichen und privaten Räumen, das für ein individuelles und politisches Leben erforderlich ist. Es fehlt insbesondere die abgeschirmte Sphäre des privaten Lebens, die von Hannah Arendt „die Dunkelheit des Verborgenen und Geborgenen" genannt wird.[7] Dieser Bereich wird als räumliche und mentale Privatheit von den Menschen- und Grundrechten erfasst. Sein Schutz soll die freie und selbstverantwortliche Lebensgestaltung im menschlichen Miteinander sichern.[8]

Die zentrale Funktion der europäischen Grundrechtssicherung wird seit *9/11* durch eine stetig wachsende Überwachung aller Lebensbereiche mit Zustimmung vieler Bürger unterhöhlt. Dass eine solche Entwicklung selbst in rechtsstaatlichen Demokratien möglich ist, hat George Orwell bereits im Jahre 1948 vorausgesehen und in seinem fiktiven Roman *1984* vor den totalitären Potenzialen westlicher Demokratien gewarnt.

Noch älter als Orwells *Großer Bruder* ist die Idee des englischen Utilitaristen und Strafvollzugsreformers Jeremy Bentham. Bentham erfand einen architektonisch geschlossenen Ort, ein *Panopticum,* in dem Verhalten und Motivation der Eingeschlossenen durch unsichtbare Wächter beobachtet und diszipliniert werden.[9]

Die staatlichen Sicherheitssysteme konstituieren sich zunehmend über eine vernetzte Allround-Überwachung realer und virtueller Räume. Die neue Transparenz soll die Überwachten im Zweifel darüber lassen, wer etwas über sie weiß, woher das Wissen der Überwacher stammt, und welche Folgen es für sie hat.[10] Ins Spiel kommt auch eine neue Rolle der Wahrsager, die menschliches Verhalten berechnen sollen.[11]

Ein Klassiker der Thematik, dass menschliches Handeln vorausgesehen werden kann, ist die Kurzgeschichte *The Minority Report*[12] des amerikanischen Autors Philip K. Dick aus dem Jahre 1956. Um zu zeigen, wie Verbrechen in der Zukunft berechnet werden, stattete er in seiner Determinismus-Parabel drei Menschen mit hellseherischen Fähigkeiten aus: die *Precognitives*. Was damals ins Reich der Science Fiction gehörte, zeichnet sich heute als Realität ab. Nährlösung sind die Potenziale unbemannter Drohnen, die ein Aufklärungssystem ermöglichen, das die amerikanische Air Force *Operation Gorgon Stare* nennt. Dabei handelt es sich um einen Komplex von Überwachungs- und Aufklärungsinstrumenten wie vernetzte Digitalkameras, die Tag und Nacht die Lebewesen beobachten, die zu seinen Zielobjekten werden sollen. Das Vorgehen beschränkt sich nicht auf die erfassten Daten. Sie gelangen in Datenspeicher, in die auch Informationen einfließen, die Menschen selbst von sich preisgeben, indem sie googeln, shoppen, mailen oder Apps für sich denken lassen.[13]

In der Abfolge unaufhörlicher informationeller Operationen der Geheimdienste wird zunehmend das lebendige Individuum aus der Verantwortung herausgenommen. Mithilfe softwaregestützter statistischer Datenanalysen werden Menschen aufgrund ihrer ethnischen Herkunft oder ihrer Religion als *gefährlich* eingestuft. Dadurch entstehen automatisch „soziale Klassifizierungen".[14] An die Stelle des Bentham'schen Panopticum tritt ein *Bann-Opticum,* das sich aus der Funktionalität nichtmenschlicher Apparate und Netzwerke bildet.

Ein Beispiel für die Logik der neuen *Transparenz* ist, dass *Araber* und *Muslime* häufiger als andere auf westlichen Flughäfen einer Überprüfung unterzogen werden. Anders ausgedrückt: Nach den Suchkriterien ist da ein Araber, der die Eigenschaft hat, ein Muslim zu sein, und dem nun weitere Eigenschaften zugeschrieben (angeklebt) werden wie die, *gefährlich zu sein*. Doch das ist nach dem Urteil des Rechtsphilosophen Lothar Philipps der Ausdruck einer falschen Sichtweise, die man als existenzbedrohend bezeichnen kann. Der Sache nach werden Menschen auf Grund von bestimmten Merkmalen stigmatisiert und diskriminiert. Damit wird der Gleichheitsgedanke in Frage gestellt, der ein wesentlicher Teil der europäischen Werteordnung ist.

Das langjährige Vorstandsmitglied im FIfF, der Computerpionier und Gesellschaftskritiker Joseph Weizenbaum, hat sich mit den neuen Konfliktlagen befasst, die durch automatische Entscheidungen entstehen, für die *niemand* verantwortlich zeichnet.[15] Er fordert von jedem Bürger: „[...] man muss sich so verantwortlich verhalten, als ob das Schicksal der Welt von einem abhinge." Und „[…] die Welt fängt mit mir selbst an [...]."[16] Der Mensch kann nicht „*in terms of the machine*" definiert werden[17] Eine Maschine allein kann keine wesentlichen Entschei-

Marie-Theres Tinnefeld

Prof. Dr. **Marie-Theres Tinnefeld** ist Juristin und Publizistin, mit zahlreichen Konferenzen und Veröffentlichungen im In- und Ausland zum Thema *Informationsrecht und europäische Rechtskultur*. Sie ist Mitglied im Beirat des FIfF e. V.

dungen anstelle derer treffen, die für ihren Einsatz verantwortlich sind, selbst dann nicht, wenn sie aufgrund angeblich sicherer Analysen *Entscheidungen* trifft, die weniger risikobehaftet zu sein scheinen.

Schließlich lassen sich auch im Dienste des Menschenrechts auf Privatheit und informationelle Selbstbestimmung Schutzmechanismen aufzeigen, die ausschließlich mechanische Entscheidungen in persönlichen Lebensbereichen verbieten und den Einzelnen ihren eigenen Anteil an der kommunikativen Bestimmung ihrer Identität sichern. Dies ergibt sich aus europäischen Diskriminierungsverboten, wonach es unzulässig ist, aus automatisch und stereotyp erzeugten Persönlichkeitsbildern digitale Doppelbilder oder Fremdbilder zu erschaffen, die den Betroffenen die Chance nehmen, auf sie einzuwirken. Gesetze, die diese Grundarchitektur des Menschenrechtsschutzes missachten, werden zu einer sinnentleerten neutralen Erscheinung.

III. Herausforderungen und Perspektive

Rechtsstaatliche Demokratien haben nach dem Zweiten Weltkrieg den Weg zum Frieden auf dem Weg der Menschenrechte neu beschritten. Der 11. September 2001 hat diesen Prozess unterbrochen. Geheimdienste und global tätige Unternehmen agieren wie professionelle Solisten. Den Menschenrechten zu folgen, halten sie häufig nicht nur für überflüssig. Sie bringen auch eine technisch bestimmte soziale Realität hervor, die geeignet ist, Verstandes- und Wahrnehmungskompetenzen zu verringern, und darum auch Grundsätze der Gleichheit, Toleranz und Verantwortung gefährdet.

Seit dem schwarzen Tag *9/11* werden häufig Gesetze ohne hinreichende Anbindung an Grund- und Menschenrechte in Parlamenten verabschiedet und von einer unbestimmten Furcht vieler Bürger mitgetragen. Die Folgen hat Kafka in seiner Parabel *Der Bau* sichtbar gemacht und den davon Betroffenen als „kleinen Ruinenbürger" bezeichnet.

Der Treuebund von Iustitia und Pax kann gelingen, wenn Kafkas Text sinngemäß verstanden und *das Gesetz* von der Grundarchitektur des Menschen- und Grundrechtsschutzes im Sinne einer Friedensordnung getragen wird.

Anmerkungen

1 *Arthur Kaufmann, Gerechtigkeit – der vergessene Weg zum Frieden: Gedanken eines Rechtsphilosophen zu einem politischen Thema, (Piper) 1986.*
2 *Siehe auch Hasso Hofmann, Bilder des Friedens oder Die vergessene Gerechtigkeit, Privatdruckreihe der Carl Friedrich von Siemens Stiftung, 1997, S. 7 ff.*
3 *Zu Verknüpfung der Frage von Gerechtigkeit und Toleranz vgl. Rainer Forst, Toleranz im Konflikt, (Suhrkamp) 2003, S. 615 f.*
4 *Zygmunt Baumann und David Lyon, Daten, Drohnen, Disziplin. Ein Gespräch über flüchtige Überwachung. Aus dem Englischen von Frank Jakubzik, (Suhrkamp) 2013, S. 19 und S. 26 mwN.*
5 *Erzählung, Teil des Romans ‚Der Prozeß' (1915), zitiert nach Malcolm Pasley (Hg.), Franz Kafka, Der Prozeß, Roman in der Fassung der Handschrift, 8. Auflage, 2000, S. 226 – 235.*
6 *Franz Kafka, Der Bau, in: Jost Schillermeit (Hg.), Nachgelassene Schriften und Fragmente, Bd. II, 1992, S. 599; Zur Parabel vgl. Wolfgang Schmale und Marie-Theres Tinnefeld, Privatheit im digitalen Zeitalter, 2014, S. 104.*
7 *Hannah Arendt, Vita activa oder vom tätigen Leben, 1967, S. 50.*
8 *Gabriele Britz, Freie Entfaltung durch Selbstdarstellung, 2007, S. 27 f.*
9 *Michel Foucault, Überwachen und Strafen. Die Geburt des Gefängnisses. Aus dem Französischem übertragen von W. Scitter, 1977, S. 260.*
10 *Wolfgang Schmale und Marie-Theres Tinnefeld, 2014, S. 104.*
11 *Philip K. Dick, The Minority Report, in: Fantastic Universe, Jan. 1956.*
12 *Marie-Theres Tinnefeld und Friedrich Lachmayer, Transparenz der Kontexte und die Rolle der Wahrsager, in: Erich Schweighofer et al. (Hrsg.), Transparenz, IRIS 2014, S. 377 f.*
13 *Dazu Cornelia Fiedler, Bei Algorithmus Mord, SZ vom 18. 09.2014, S. 11.*
14 *Baumann und Lyon (Fn. 3).*
15 *Joseph Weizenbaum mit Gunna Wendt, Wo sind sie, die Inseln der Vernunft im Cyberspace, (Herder) 2006, S. 16 f.*
16 *Weizenbaum (Fn. 15), S. 78 f.*
17 *Weizenbaum (Fn. 15). S. 86.*

Dietrich Meyer-Ebrecht

Das Web ist 25 geworden

Von der Utopie einer grenzenlosen Freiheit zum total kontrollierten Raum

Vor 25 Jahren, genau am 19. August 1989, veröffentlichte Tim Berners-Lee*, zu jener Zeit als beratender Ingenieur und Software-Entwickler am CERN tätig,* seinen *Code. Der Code, der über die ganze Welt verteilte digitale Dokumenten zu einem Beziehungsnetz zusammenknüpft. Der Code, der sie auffindbar und im Kontext nutzbar macht: Aus Texten wird* Hypertext*, Inhalte werden miteinander verwoben, unabhängig von Ort und Zeit. Die eine Zutat war eine Konvention zur Darstellung der Verknüpfungen, die* Hypertext Mark-up Language*, kurz HTML – die andere eine Vereinbarung zur Regelung des Datenverkehrs, das* Hypertext Transport Protocol*, kurz HTTP. Mit den Grundideen war Berners-Lee nicht der Erste, aber er hat die verschiedenen Elemente genial zusammengefügt. Und was ihn als Ingenieur auszeichnet: Er hat sie technisch umgesetzt, mit Weitblick und Umsicht. Denn, was in der Rückschau erstaunt, die Informatikergemeinde hat sich sehr schnell auf Berners-Lees Konzept geeinigt und mit seinen Vorgaben als de-facto-Standard das globale Wissensnetz geknüpft, das* World-Wide Web*, das* WWW*.*

Mit dem World-Wide Web hat Berners-Lee gleichsam eine Metaebene auf einem Datentransportmedium geschaffen, dem 1989 bereits existierenden Internet. Dieses Netz aus weltweit verteilten Computersystemen hatte seinen Ursprung in einem US-militärischen Projekt. Bereits 1969 hatte die *ARPA* (heute *DARPA*, Defense Advanced Research Projects Agency des US-Verteidigungsministeriums) die erste Datenfernverbindung zwischen Rechnerknoten in den USA realisiert. Hinter dem Projekt

stand das strategische Ziel, die militärischen Rechenzentren angesichts ihrer zunehmenden Bedeutung geografisch zu verteilen und Redundanzen zu schaffen, um die Verletzlichkeit der USA durch Angriffe auf die Anlagen zu mindern – es war die Zeit des Kalten Kriegs mit ihrer Angst vor Atomschlägen. Mit der Entwicklung des ersten Email-Programms begann 1971 die Nutzung des Netzes für die Person-zu-Person-Kommunikation. Eine wichtige Entwicklung für die Verbreitung der Rechner-Rechner-Kommunikation war die Spezifizierung des *Transmission Control Protocol*, *TCP,* im Jahre 1974, das die Standardisierung der Schnittstellen ermöglichte. Erweitert wurde es 1978 zum *Internet Protocol*, *TCP/IP*, das bis heute den Mechanismus der Datenflüsse im Internet festlegt. Und schließlich wurde 1984 das *Domain Name System*, *DNS,* eingeführt, über das die Daten ihren Weg zu ihrem Zielrechner finden, ohne dass der Pfad im Netz vorgegeben werden muss. Ein weltweites Datennetz entstand, in dem sich die Rechenzentren von Universitäten und Forschungseinrichtungen untereinander verbanden. Tim Berners-Lee setzte den Schlussstein ein: Mit seinem Konzept wurde das verteilte Wissen zu einem Netz verwoben.

Noch eine Entwicklung war nötig, um dieses Gewebe der Dokumente komfortabel nutzen zu können: der *Browser*, die Benutzerschnittstelle zum Web. Die Grundidee stammte wieder von Berners-Lee. Am 1. April 1993 erschien die Version 1.0 des Browsers *Mosaic,* die erste Realisierung eines Browsers für den *Hausgebrauch*. Dies war die Zeit, in der PCs an den Arbeitsplätzen schon zur Grundausstattung gehörten und nun auch in die Privathaushalte einzogen. Und dies war auch die Zeit, in der wir uns mit Telefonmodems den Weg ins Internet über unseren privaten Telefonanschluss bahnten. Die Metapher des *virtuellen Raums* wurde geboren, in dem man sich orts- und zeitungebunden bewegte, um zu kommunizieren und um sich zu informieren.

Der Faszination des virtuellen Raumes erlegen, ließen wir das Internet schnell in unser Privatleben einziehen, trieben mit unserem IT-Konsum eine rasante Entwicklung der Technologie an und stimulierten Wirtschaft und Handel zu immer neuen Dienstleistungsangeboten. Wir genossen den Komfort, freuten uns über kostenlose Dienste, gewöhnten uns an die Informationsmonopolisten, ließen die Unternehmen fleißig unsere Daten sammeln, protestierten nicht einmal gegen die Gängelung durch obligatorische *Appstores* – und glitten dabei unmerklich in eine neue Art von Abhängigkeit. Wie das Haus seine Autarkie mit der Einführung des Gaslichts und dem Hausanschluss an städtische Gasleitungsnetze verlor (nach Wolfgang Schivelbusch in seinem kleinen Band zur Geschichte der künstlichen Helligkeit),[1] so gaben wir mit dem Smartphone als unserem unverzichtbaren Begleiter – *always online* – die Autarkie unseres Intellekts auf.

Nun zwingt uns niemand, das zu kaufen, was Amazon schon als unseren nächsten Wunsch errechnet hat. Wir müssen nicht Lexika und Telefonbücher in die Papiertonne werfen. Wir sind nicht auf die von Google, Bing oder Facebook für uns *personalisierten* Nachrichtenzusammenstellungen angewiesen. Es gibt doch dieses großartige Web, das unsere intellektuellen Möglichkeiten enorm erweitern könnte – allerdings müsste man dafür auch unsere alten Kulturtechniken noch beherrschen, um das neue Medium kritisch und kreativ, bewusst und verantwortungsvoll nutzen zu können. Aber haben wir nicht längst begonnen, diese als Ballast über Bord zu werfen und uns wohlig in der Bevormundung eingerichtet? Man müsste dies nicht weiter bedauern – das Leben ist halt immer ein Abwägen zwischen einer Bequemlichkeit zum Preis einer Abhängigkeit und einer unbequemeren Selbstbestimmtheit –, wenn der Preis nicht hoch wäre und die wahren Kosten offen lägen. Wir zahlen mit Daten, der Währung des Internets. Wir zahlen mit der Preisgabe von Informationen über unser Privatleben bis in intime Sphären. Wie es ein Naturgesetz ist, dass ein System nicht beobachtet werden kann, ohne dass es beeinflusst wird, so kann man im Internet seine Fühler nicht ausstrecken, ohne Spuren zu hinterlassen. Und diese Spuren werden gnadenlos gesammelt und mit immer leistungsfähigeren *Big-Data-Tools* zu Profilen zusammengesetzt. Denn diese sind echtes Geld wert. Weil der Kommerz sie zur Manipulation unseres Konsumverhaltens nutzen kann. Das einstmals offene, unkontrollierte *Internet-for-everybody* wird längst von großen Unternehmen beherrscht – ganz sicher nicht in erster Linie, um uns das Leben angenehmer zu machen. Die Grenze zwischen fairem Handel und krimineller Ausbeutung ist schon lange nicht mehr eindeutig zu ziehen.

Aber wir leben damit. Das World-Wide Web hat unsere Gesellschaft verändert. Unter seiner Schubkraft ist das Internet zu einem *backbone* der Zivilgesellschaft geworden. In Vergessenheit ist geraten, dass seine Entwicklung von den Militärs initiiert worden war: Die Wiege des Internets war das ARPA-Net. Nicht vergessen haben dies die Militärs. Ihren Herrschaftsanspruch über das Internet hat uns Edward Snowden vor knapp zwei Jahren jäh in Erinnerung gebracht. Seine Enthüllungen haben offengelegt, in welch verletzliche Position wir uns begeben haben, indem wir das Internet in unser Leben integriert haben. Sind die Konsequenzen einer leichtfertigen Preisgabe persönlicher Informationen an Kommerz oder Kriminelle meist nur finanzieller Natur, birgt das Datensammeln der militärischen Geheimdienste existenzielle Gefahren, wenn wir als *Kollateralschäden* ins Visier der nach geheimen Kriterien betriebenen automatisierten Auswertung geraten.

World-Wide Web, ein etwas aus der Mode gekommener Begriff, das Akronym WWW längst nicht mehr präsent in allen Web-Adressen. Wir sagen heute wieder *Das Internet*, wenn wir das Medium meinen. Und doch war es das World-Wide Web, Berners-Lees Konzept der logischen Vernetzung weltweit verteilten Wissens, das das Internet zu dem gemacht hat, was es heute für uns ist: der *Cyberspace* mit seinen vielfältigen Optionen – und seinen ebenso vielfältigen Gefahren. Tim Berners-Lee, der weiter aktiv an der Weiterentwicklung des Internets gearbeitet hat, hat seine Augen vor den problematischen Entwicklungen nicht verschlossen. Er hat die Bewegung „the Web We Want" ins Leben gerufen.[2] Und er fordert dringend eine „Magna Carta des Internets", die das Internet, das *Web* zu einem Raum mit demokratischen Spielregeln macht.

Anmerkungen

1 *Wolfgang Schivelbusch: Zur Geschichte der künstlichen Helligkeit im 19. Jahrhundert. Hanser, München, 1983*

2 *http://webwewant.org*

Autoreninfo siehe Seite 66

Christiane Schulzki-Haddouti

Kritische Informatik

Hätten kritische Informatiker viele Schwachstellen verhindern können, die von der NSA ausgenutzt wurden? Und müssten sie nicht Sicherheitslücken unmittelbar der Öffentlichkeit mitteilen? In der Praxis verhindern das oft vertragliche Zwänge. Und Whistleblowing gehört noch nicht zum Berufsethos.

Die NSA nimmt seit Jahrzehnten über Standardisierungsgremien Einfluss, um abhörfreundliche technische Fakten zu setzen. Die renommierte amerikanische Standardisierungsorganisation *NIST* hat erst dieser Tage einen ihrer Standards zur Erzeugung von Zufallszahlen zurückgezogen und will künftig die Beratungsprozesse transparenter gestalten. Sind Verschlüsselungsstandards schwach, ist der Lauschangriff später kein Problem mehr. Auch schaffte die NSA es, dafür zu sorgen, dass sogar renommierte Kryptofirmen wie die *RSA* sich auf geschwächte Sicherungstechnik einlassen.

Edward Snowden ist nicht nur der wohl inzwischen berühmteste Whistleblower, er ist auch ein Informatiker, der seinem Gewissen folgte und Zivilcourage zeigte. Weitere Snowdens sind gefragt, denn: „Das Problem ist nicht die NSA, das Problem ist Big Data, genauer: die Haltung und Denkweise, die hinter Big Data steht", meint der Informatiker Stefan Ullrich. Er ist Sprecher der Fachgruppe *Informatik und Ethik* der Gesellschaft für Informatik (GI), der größten Informatikfach-Vertretung im deutschsprachigen Raum. Ullrich erinnert an den „viel zu früh verstorbenen" Informatikprofessor Andreas Pfitzmann, der sagte: „Wo ein Trog ist, kommen nun einmal die Schweine."

Dass Whistleblowing auch im alltäglichen Sicherheitsgeschäft wichtig sein könnte, zeigt die jüngste Diskussion um den *Heartbleed-Bug*, der Millionen von Internet-Servern betrifft: Nämlich als der Verdacht aufkam, die NSA hätte aufgrund eines privaten Sicherheitsberichts von der gravierenden Sicherheitslücke zwei Jahre lang gewusst, aber nicht davor gewarnt, um sie für eigene Ausspähzwecke nutzen zu können. Jeder Informatiker, der *Zero-Day*-Lücken, also noch nicht publizierte Schwachstellen, auffindet, steht aber vor dieser Entscheidung: Soll er die Öffentlichkeit informieren oder nur das jeweils betroffene Unternehmen?

In Deutschland werden Angriffe in der Regel mit der ausdrücklichen Zustimmung des angegriffenen Unternehmens durchgeführt. Diese verlangen dann aber in einem *Non Disclosure Agreement (NDA)*, dass man Stillschweigen über die Ergebnisse wahrt. „Da in der Regel eine solche NDA auch von Mitarbeitern eines Unternehmens, einer Behörde etc. unterschrieben werden muss, ist das so eine Sache, wenn man im Rahmen seiner Tätigkeit von einer Schwachstelle erfährt, die nicht geschlossen wird, oder aber dass das Unternehmen die Produkte an Diktaturen verscherbelt", sagt Sylvia Johnigk, Vorstandmitglied des Informatikervereins FIfF.

Bricht man die Schweigevereinbarung, können die Folgen erheblich sein: Strafzahlungen in Millionenhöhe, Kündigung oder Auftragsverlust. Johnigk: „Auch wenn es moralisch sicher der saubere Weg ist, scheuen viele den Aufwand und Stress, zumal nicht alle Schwachstellen derart spektakulär sind wie die von Snowden". So rutsche „man mitunter auch stückchenweise immer weiter selbst in den Sumpf, und das Gewissen meldet sich viel zu spät".

Hat sich das Denken über das „Alarm schlagen" bei den deutschen Informatikern seit Snowden verändert? Stefan Ullrich sagt: „Im persönlichen Umfeld dreht sich das Thema stets wieder um Snowden". Aber in den aktuellen *Ethischen Leitlinien* der GI findet sich noch kein Passus, der das Whistleblowing unterstützen würde. Die GI spricht lieber von *Zivilcourage* im Arbeitsumfeld. Eine moralische Verpflichtung, Fehlentwicklungen auch der Öffentlichkeit zu melden, gibt es nicht. Anders ist das im *Code of Ethics* der amerikanischen *Association for Computing Machinery*. Sie verlangt den Schritt an die Öffentlichkeit, wenn die Verantwortlichen nicht angemessen reagieren, um „Gefahren im System" zu beseitigen. In den USA gibt es allerdings auch einen gesetzlichen Schutz für Whistleblower.

Eine entsprechende Aktualisierung der Ethischen Leitlinien der GI ist derzeit nicht geplant. Auch setzt sich die GI nicht aktiv für eine Whistleblower-Gesetzgebung in Deutschland ein. Ingo Ruhmann, der sich seit Jahrzehnten mit *kritischer Informatik* auseinandersetzt, sagt: „Whistleblower als Notwendigkeit anzuerkennen bedeutet, die Unehrlichkeit und das illegale Handeln in Unternehmen und auch Behörden als Realität zu akzeptieren und Wege zu öffnen, dem gesetzeskonformen Mitarbeiter, der gegen illegale oder unethische Praktiken opponiert, zu helfen."

Die Gesellschaft für Informatik bietet sich jedenfalls bei Konflikten nur als Vermittlerin an. „Das bleibt hinter dem zurück, was Gewerkschaften hier an Hilfe leisten", kritisiert Ruhmann. Er glaubt auch: „Beamte und Angestellte in einer Firma riskieren ganz persönlich bei gesetzwidrigen Überwachungsmaßnahmen ihre Entlassung oder gar eine Strafverfolgung." In vielen Fällen werde die Schuld auf dem kleinen Mitarbeiter abgeladen. Ruhmann: „Für viele entsteht der Konflikt genau dann, wenn sie erkennen, dass von ihnen Illegales verlangt wird, aber kein Vorgesetzter dafür die Verantwortung übernehmen will."

Der Beitrag ist in gekürzter Form in den VDI-Nachrichten erschienen. Wir danken herzlich für die Genehmigung zum Abdruck.

Christiane Schulzki-Haddouti

Christiane Schulzki-Haddouti, geb. 1967, arbeitet seit 1996 als freie IT- und Medienjournalistin. Seither hat sie in über 50 Tageszeitungen, Online-Medien, Fachzeitungen und -zeitschriften veröffentlicht. Ihre Berichterstattung befasst sich mit dem Leben in der Informationsgesellschaft und all seinen Chancen und Schwierigkeiten.

Ulrich Klotz

Arbeit ohne festen Arbeitsplatz

Im Wettbewerb von morgen zählen gute Ideen und kreative Köpfe. Beide können sich in hierarchisch organisierten Firmen wenig entfalten, sagt der Informatiker und Arbeitswissenschaftler Ulrich Klotz.
Ein Interview von Hans Königes *für die* Computerwoche.

CW: **Wie wird das Internet unsere Arbeitswelt weiter verändern?**

Ulrich Klotz: *Ohne die Bindung an Ort und Zeit werden viele Arbeiten zu einer Ware, die weltweit gehandelt werden kann. Was wir heute als Outsourcing, Offshoring oder allgemeiner als „Globalisierung" kennen, sind erst die Anfänge neuer Formen grenzenloser Arbeitsteilung, denn das Netz ermöglicht auch vollkommen neuartige Unternehmensmodelle.*

CW: **Was meinen Sie mit grenzenloser Arbeitsteilung?**

Ulrich Klotz: *Ein Beispiel: Ein globaler IT-Konzern plant eine „Verflüssigung" seiner Arbeitsstrukturen durch weitgehenden Verzicht auf festangestellte Mitarbeiter. Künftig sollen Projekte in kleine Arbeitspakete zerlegt und diese via Internet weltweit ausgeschrieben werden. Um diese Minijobs kann sich jeder bewerben, auch die ehemaligen Angestellten. Die weltweit verstreuten Auftragnehmer kooperieren dann über das Internet in „Talent Clouds". Bei dieser Art von Crowdsourcing verschwindet nicht die Arbeit, aber der feste Arbeitsplatz. Sozialpartnerschaftliche Modelle und nationalstaatliche Einwirkungsmöglichkeiten, etwa beim Arbeitsrecht, werden durch die Spielregeln privater Konzerne ersetzt. Ob das so funktionieren wird, sei dahingestellt. Auf jeden Fall sollten wir solche Entwicklungen aufmerksam beobachten. Es ist klüger, sich beizeiten mit der Konstruktion von Brunnen zu befassen, als hinterher über die hineingefallenen Kinder zu jammern.*

CW: **Arbeit ohne Arbeitsplatz – ist das die Zukunft?**

Ulrich Klotz: *Wir befinden uns in einer Übergangsphase, in der verschiedene Arbeitsformen und unterschiedliche Kulturen von Arbeit nebeneinander existieren. Die Situation ist ähnlich wie zu Beginn der Industrialisierung: Damals ließen neue Techniken wie Dampfmaschine, Eisenbahn oder später das Fließband allmählich das entstehen, was wir heute als Arbeit kennen – mit allem, was dazugehört: Arbeitsplatz, Arbeitszeit, Arbeitsort, Ausbildungs- und Entlohnungsformen.*

CW: **Nun ist alles wieder auf Anfang?**

Ulrich Klotz: *Seit dem Aufkommen der Computer in den 70erahren des vorigen Jahrhunderts wird Arbeit wieder neu definiert: Immer mehr Menschen können überall und jederzeit arbeiten, dabei verschwimmen die Grenzen zwischen Arbeits- und Freizeit, zwischen Arbeits- und Wohnort, zwischen Arbeit und Lernen, zwischen Abhängigkeit und Selbständigkeit, zwischen Produzenten und Konsumenten. Arbeit bezeichnet wieder das, was man tut, und nicht das, wohin man geht. Die Arbeitswelt wird vielfältiger, die Ausnahmen werden zur Regel, das Normalarbeitsverhältnis und die Normalbiografie sind auf dem Rückzug.*

CW: **Wie bewerten Sie das Verschwinden klassischer Arbeitsverhältnisse?**

Ulrich Klotz: *Das alles ist zwiespältig. Die aus bürokratischen Unternehmenszwängen gegen ihren Willen Entlassenen werden oft zu Wander-Wissensarbeitern, denen Fesseln neuer Freiheiten umgelegt werden: ein Höchstmaß an Eigenverantwortung und Selbstorganisation kombiniert mit minimalen Absicherungen und Planbarkeiten.*

CW: **Inwieweit werden Computer menschliche Arbeit übernehmen?**

Ulrich Klotz: *Früher war vor allem in Gewerkschaftskreisen die Meinung verbreitet, dass diese Maschine – man sprach ja vom „Elektronengehirn" – uns das Denken abnimmt. Das Gegenteil ist der Fall. Der Computer übernimmt Routinetätigkeiten, das Vorhersehbare: alles, was planbar, regelhaft und programmierbar ist. Menschen werden noch für die Bewältigung von Ausnahmesituationen gebraucht. Hierzu zählen viele Arbeiten, die gar nicht so einfach sind, wie es auf den ersten Blick scheint – zum Beispiel im Haushalt, im Gesundheitssektor oder in der Pflege. Hingegen werden wir sehen, dass aufgrund der rapiden Fortschritte beim automatischen Verstehen menschlicher Sprache zahllose routinehafte Tätigkeiten, etwa in Call-Centern, Banken, Versicherungen oder Anwaltskanzleien, unter die Räder kommen.*

CW: **Welche Arbeit bleibt den Menschen?**

Ulrich Klotz: *Was immer hier oder dort an menschlicher Arbeit übrig bleibt, wird intellektuell anspruchsvoller, erfordert eine immer bessere Ausbildung und permanente Weiterbildung. Dies auch, weil infolge der Informatisierung die Informationsmenge exponentiell anwächst. Diese gigantische Lawine an Informationen und neuem Wissen kann man nur durch stärkere Spezialisierung bewältigen.*

Für diese Spezialisten hat der Management-Papst Peter Drucker vor gut 50 Jahren den Begriff Wissensarbeiter geprägt. Ein Wissensarbeiter ist jemand, der mehr über seine Arbeit weiß als jeder andere im Unternehmen. Bei uns sind inzwischen die Mehrzahl der Menschen Wissensarbeiter, wir finden sie heute überall, egal ob im Blau- oder Weißkittel.

CW: **Vor welchen Problemen stehen diese neuen Wissensarbeiter?**

Ulrich Klotz: *Wissensarbeiter brauchen Strukturen, in denen sie ihr Know-how optimal mit dem anderer Spezialisten verbinden können. Tatsächlich arbeiten Wissensarbeiter aber in Organisationen, die noch vom hierarchischen Modell der Industrieära geprägt sind: Oben wird entschieden, unten wird ausge-*

führt. Wissen ist aber nicht hierarchisch strukturiert, sondern situationsabhängig relevant oder irrelevant. Hier entsteht ein Dilemma: Die da oben entscheiden über Dinge, von denen sie meist weniger verstehen als die da unten. Die Folgen: Demotivation, Reibungsverluste, Fehlentscheidungen und Frustration. Entscheidungsträger glauben, sie wüssten etwas besser, weil sie eine bestimmte Position innehaben – das traf zu Frederick Taylors Zeiten vielleicht zu, ist aber heute absurd. Die erschreckenden Ergebnisse von Umfragen über Arbeitszufriedenheit und Motivation sind direkte Folge der Tatsache, dass zu viele Manager an den 100 Jahre alten Konzepten eines Taylor festhalten, die im Zeitalter der Wissensarbeit kontraproduktiv sind.

CW: **Wie muss die Welt der optimalen Wissensarbeit aussehen?**

Ulrich Klotz: *Ein gutes Beispiel liefern die Open-Source-Gemeinschaften. Das sind weltweite Netzwerke freiwilliger Programmierer, die komplexe Projekte wie etwa Linux, Firefox, Wikipedia oder auch wesentliche Teile des Internets realisieren. Die Menschen arbeiten in solchen Projekten mit hoher Motivation, oft Begeisterung – und das alles ohne Bezahlung. Warum tun sie das? Weil hier Menschen anders miteinander umgehen als in der hierarchisch-bürokratischen Arbeitswelt: Hier basiert Wertschöpfung auf gegenseitiger Wertschätzung. Die Beteiligten arbeiten auf Augenhöhe miteinander, deshalb wird Wissen nicht als Herrschaftswissen missbraucht, sondern bereitwillig mit anderen geteilt, daher auch der Name: Open Source = Offene Quelle. Anerkennung, Vertrauen, Respekt, Toleranz und Fairness sind nicht bloße Sonntagsreden, sondern gelebte Realität. Führungsfunktionen basieren auf Sachkompetenz und nicht auf formaler Autorität. Im Netz zählt nicht das größere Büro, sondern die Leistung. Neue Ideen haben hier viel bessere Chancen als in bürokratischen Strukturen. Darum sind viele Open-Source-Produkte der kommerziellen Konkurrenz oft schon nach kurzer Zeit voraus.*

CW: **Warum setzen sich diese Ideen so langsam durch?**

Ulrich Klotz: *Wo Organisationen noch auf dem alten Prinzip „Wissen ist Macht" basieren, wird neues Wissen als Bedrohung empfunden und zunächst bekämpft. Zwar wird überall von Innovation geredet, aber wirkliche Veränderungen sind oft gar nicht gewollt – das habe ich im Verlauf meiner Berufstätigkeit sehr häufig erlebt. Innovationen sind Bottom-up-Prozesse, die sich mit Top-down-Strukturen nun einmal schlecht vertragen. In den klassisch hierarchischen Organisationspyramiden – oben die Würdenträger, unten die Innovationsträger und dazwischen jede Menge Bedenkenträger – ist Loyalität wichtiger als Leistung. Den Entscheidungsträgern geht es zuerst um Machterhalt und danach um Inhalte, da können Ideen noch so gut sein. Wo bevorzugt pflegeleichte Ja-Sager Karriere machen und Opportunismus als Qualifikationsersatz dient, gibt es kaum noch Weiterentwicklung, weil andere Meinungen – neue Ideen sind anfänglich stets Minderheitenmeinung – keine Fürsprecher finden. Aus diesem Grund wurden schon zahllose Firmen, ja ganze Branchen, Opfer ihrer internen Strukturen und Innovationsbremsen – wie zum Beispiel die gesamte deutsche Computerindustrie, die Unterhaltungselektronik, die Fotoindustrie und einiges mehr.*

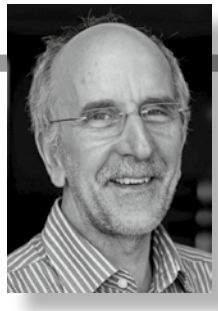
CW: **Wie sieht Ihr Lösungsvorschlag aus?**

Ulrich Klotz: *Mich treibt die Frage um, wie wir endlich die innovationsfeindlichen Kommandostrukturen der Industriegesellschaft überwinden können – hin zu einer Arbeitskultur, die von gegenseitiger Wertschätzung, Respekt und Toleranz geprägt ist. Von den Open-Source-Communities können wir eine Menge über zeitgemäße Arbeitsgestaltung lernen. Die junge Generation, die mit Wikis, Blogs und Social Networks groß geworden ist, lebt ohnehin eine neue Kultur des Wissensaustauschs. Viele dieser „Digital Natives" werden sich nicht mehr in eine graue Sachbearbeiter-Welt einsperren lassen, wo sie zwischen Karriereleitern, Gehaltsgittern, Planstellen und Dienstwegen viel Zeit und Energien mit internen Machtspielen vergeuden.*

Unsere Unternehmen werden von diesen Internet-Communities lernen müssen, weil sie andernfalls diese Generation nicht als kreative Mitarbeiter gewinnen oder halten können werden. Natürlich wird unsere Welt keine Open-Source-Welt werden. Aber ich bin davon überzeugt, dass sich intelligentere Formen der Zusammenarbeit und offene Innovationskulturen langfristig durchsetzen und künftig zu einem neuen Verständnis von Arbeit führen werden. Unternehmen, die hingegen zu lange an den überkommenen Arbeitsstrukturen der Industrieära festhalten, werden aufgrund ihrer internen Innovationsbarrieren untergehen.

CW: **Wie weitreichend werden diese Veränderungen sein?**

Ulrich Klotz: *Wenn sich Kommunikationsformen ändern, dann wandelt sich das Fundament einer Gesellschaft. Wenn sich*



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.

die Art und Weise verändert, wie Menschen ihre Fähigkeiten verbinden und weiterentwickeln, dann wirkt sich das auf jeden Aspekt unseres Denkens aus: Wahrnehmung, Gedächtnis, Sprache, Vorstellungsvermögen, Kreativität, Urteilskraft, Entscheidungsprozesse und vieles mehr.

In der neuen Gesellschaft wird nicht nur Arbeit neu definiert. Auch das Bild des Menschen wandelt sich. Wenn Menschen nicht mehr wie Maschinenteile arbeiten müssen, dann zählt das, was uns von Maschinen unterscheidet: Kreativität, Emotionen und Intuition. Menschen können Informationen in Bedeutung und Erfahrungen in Wissen verwandeln, das kann man Computern (noch?) nicht beibringen – wie auch unsere Fähigkeit, intelligent mit Unvorhersehbarem umzugehen. Weil wir künftig mehr kreative Individuen brauchen als brave, angepasste Ausführer, müssen wir vor allem unser industriegeprägtes Bildungssystem radikal umkrempeln. Fleiß, Ausdauer und das Erlernen von Fertigkeiten allein reichen nicht mehr, denn irgendwo wird irgendwer immer noch fleißiger sein. Im Wettbewerb von morgen zählen vor allem gute Ideen.

Hier ist Eile geboten, denn die soziale Kluft zwischen den Gewinnern und Verlierern dieses Strukturwandels wird immer größer. Die zunehmende Spreizung bei den Einkommen ist eine direkte Folge der Informatisierung in der Arbeitswelt. Kolonnenhafte Vervielfältigungsarbeiten werden mehr und mehr technisiert und/oder in andere Länder verlagert. Auf der anderen Seite werden kreative Unikat-Arbeiten immer bedeutsamer und besser bezahlt, hier ist das Einkommen aber oft nicht mehr an Arbeitszeit etc. gekoppelt. Denken wir an einen Romanautor: Um erfolgreich zu sein, kommt es nicht darauf an, wie schnell er wie viele Zeilen schreibt, sondern wie gut seine Ideen sind. Ideen von heute sind das Geld von morgen. Bei allen Gütern, die man digitalisieren kann, zählt nur die Idee, das Design oder die Entwicklung – also ein Unikat. Die Vervielfältigung und weltweite Verteilung des Endprodukts, also das, was heute noch Industriearbeit ist, übernimmt die Technik.

CW: **Ist das Ende der Industriegesellschaft gekommen?**

Ulrich Klotz: *Die Produktion materieller Güter wird nicht verschwinden, genauso wenig wie die Landwirtschaft beim Übergang zur Industriegesellschaft verschwunden ist. Doch in allen hochentwickelten Ländern wird Innovation und Wertschöpfung mit immateriellen, digitalisierbaren Geistesprodukten immer wichtiger. Das gilt auch bei Industrieprodukten – bei Mobiltelefonen, aber etwa auch bei Autos kommt es mehr und mehr auf die Qualität der Software und des Designs an. Wer auf diesen Feldern nicht ganz vorne mitspielen kann, wird auch bei der Produktion von materiellen Gütern existenzielle Probleme bekommen.*

Wir Europäer müssen verdammt aufpassen, um nicht im Zangengriff zwischen innovativen US-Hightech-Konzernen und nachrückenden asiatischen Massenproduzenten zerquetscht zu werden. Dafür müssen wir den Ideenreichtum der gesamten Gesellschaft zur Entfaltung bringen. In unserer starren Arbeitswelt liegen viele Fähigkeiten brach, weil Menschen hier oft nicht das tun dürfen, was sie können und wollen. Wir vergeuden heute viel mehr menschliche Potenziale, als wir nutzen. Diese Verschwendung können wir uns in Zukunft nicht mehr erlauben.

Der Beitrag ist in der ComputerWoche erschienen: http://www.computerwoche.de/a/arbeit-ohnefesten-arbeitsplatz,2552098. Wir danken herzlich für die Genehmigung zum Abdruck.

Sara Stadler

Log 4/2014

Ereignisse, Störungen und Probleme der digitalen Gesellschaft

Immer wieder gibt es Ereignisse, Verlautbarungen und Entscheidungen, die im Zusammenhang mit dem fortschreitenden Abbau der Bürgerrechte 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.

Juli 2014

24. Juli 2014: Neue Enthüllungen zeigen, wie leicht es geht, in den USA als „Terror-verdächtig" abgestempelt und gespeichert zu werden. Dafür, eine Person als „mutmaßlichen Terroristen" einzustufen und sie entweder in der zentralen Terroristendatenbank auf der *No-Fly-List* (was der Person den Zugang zu Flugzeugen versperrt) oder der *Selectee List* (was zu verschärften Grenzkontrollen führt) zu erfassen, sind dem Dokument zufolge weder „konkrete Fakten" noch „unbestreitbare Beweise" nötig. Ausreichend ist offenbar der Verdacht auf ein Handeln, das unter die aufgelisteten „terroristischen Aktivitäten" fällt. Eine Reihe von Schlupflöchern würde sogar ein Listing ohne eigentlichen Verdacht ermöglichen, etwa indem Personen allein auf der Basis einer nicht näher definierten Gruppenzugehörigkeit erfasst werden können. Inwieweit es möglich ist, die Löschung eines einmal stattgefundenen Eintrages in eine der Dateien zu bewirken, bleibt unklar (Quellen: The Intercept, Heise).

25. Juli 2014: Wie aus der Antwort der Bundesregierung auf eine kleine Anfrage der Linksfraktion hervorgeht, werten die Bundeswehr und der Bundesnachrichtendienst (BND) massenhaft Daten aus *offenen Quellen*, also etwa sozialen Netzwerken, aus, um das „Informationsumfeld" bei Auslandseinsätzen

auszukundschaften und Trends und Tendenzen in den „Einsatz- und Interessengebieten“ auszumachen. Das Zentrum *Operative Kommunikation* der Bundeswehr setzt dazu aktuell das Analysetool *Textrapic* und die Social-Media-Monitoring-Software *Brandwatch* ein, weitere Werkzeuge sollen in dem Forschungsprojekt *Wissenserschließung in offenen Quellen* entwickelt werden. Welche Software der BND für die Echtzeitanalyse von Streaming-Daten einsetzt, wird nicht bekannt gegeben (Quelle: Heise).

26. Juli 2014: Ein niederländisches Gericht erklärt die Praxis der Nachrichtendienste *AIVD* und *MIVD* für rechtmäßig, Daten, deren Erhebung in den Niederlanden illegal ist, von *befreundeten* Geheimdiensten zu beziehen. (Quelle: Heise).

August 2014

6. August 2014: Auf Twitter werden Werbebroschüren zu den Trojanern *FinFisher* und *FinSpy* der *Gamma Group* veröffentlicht. Die Software, die dem Ausspionieren von Computern und Smartphones dient, soll aktuell auch vom deutschen Bundeskriminalamt (BKA) getestet werden. Aus weiteren Veröffentlichungen geht hervor, dass die Software unter anderem auch nach Bahrain geliefert wurde, wo sie zur Überwachung von MenschenrechtsaktivistInnen eingesetzt wird (Quelle: Heise).

8. August 2014: Wie *Technology Review* berichtet, fördert das US-Militär mit dem Projekt *Subnets* die Entwicklung von Gehirnimplantaten zur Gefühlssteuerung. Die Zielgruppe seien in erster Linie Veteranen. Bei dieser Gruppe träten häufig Depressionen oder posttraumatische Belastungsstörungen auf, welche auf diese Art behandelt werden sollten (Quelle: Technology Review, Heise).

9. August 2014: Wie aus der Antwort der Bundesregierung auf eine Kleine Anfrage der Fraktion *Die Linke* zu neu angeschafften Beweissicherungs- und Dokumentationsfahrzeugen hervorgeht, erforscht die deutsche Polizei im Rahmen des Projektes *EILT* (*Emitter-Lokalisierung unter Mehrwegausbreitungsbedingungen*) den Einsatz von Mehrwegpeilern zur Präzisions-Lokalisierung von Mobiltelefonen. In den 76 neu angeschafften Fahrzeugen könnte diese Technik neben HDTV-Kameras und Mikrofonen bereits eingesetzt werden (Quelle: Heise).

14. August 2014: In einem Interview mit dem US-Magazin *Wired* berichtet der Whistleblower Edward Snowden, dass der Geheimdienst NSA an einer Cyberkriegs-Software mit dem Namen *MonsterMind* arbeite, die Cyberangriffe automatisch erkennen und darauf reagieren solle. Das Programm bedeute zudem einen zusätzlichen Eingriff in die Privatsphäre Unbeteiligter, da in seinem Rahmen sämtlicher Datenverkehr überwacht werden solle, der in die USA gelange (Quelle: Wired, Heise).

15. August 2014: Wie aus einer Antwort der Bundesregierung auf eine schriftliche Anfrage des Abgeordneten Andrej Hunko (Fraktion *Die Linke*) hervorgeht, ist die eigenständig vom BKA entwickelte Software zur Onlinedurchsuchung nunmehr zugelassen und einsatzbereit. Eine weitere Eigenentwicklung, die zur Telekommunikationsüberwachung eingesetzt werden solle, befinde sich dagegen noch in der Implementierungsphase (Quelle: Heise).

25. August 2014: Die Enthüllungsplattform *The Intercept* berichtet von einer von der NSA betrieben Suchmaschine namens *ICREACH*. Auf das System, das Datenbanken mit Hunderten Milliarden Metadaten aus aller Welt durchsuche, hätten neuen Snowden-Dokumenten zufolge MitarbeiterInnen der Drogenfahndungsbehörde *DEA*, des *FBI*, der *CIA* und des militärischen Nachrichtendienstes *DIA* Zugriff (Quelle: The Intercept, Heise).

28. August 2014: Die Videobloggerin Anita Sarkeesian, die sich aufgrund ihrer feministischen Kritik an Sexismus in Videospielen seit Jahren Anfeindungen und verbalen Angriffen ausgesetzt sieht, muss in Folge heftiger Drohungen auf Twitter ihre Wohnung verlassen. Der entsprechende Bericht auf *heise online* zieht eine Fülle sexistischer und den Feminismus diffamierender Forenbeiträge nach sich (Quelle: Heise).

September 2014

5. September 2014: Ein neuer Bericht von *China Labor Watch* und *Green Amerika* dokumentiert die unverändert katastrophalen Arbeitsbedingungen bei dem *Apple* Zulieferer *Catcher*. Obwohl Apple von den Arbeitsrechteorganisationen bereits 2013 über die Missstände informiert worden sei, seien erzwungene Überstunden, schlechte Entlohnung sowie Feuer- und Sicherheitsrisiken – unter anderem blockierte Notausgänge und unzureichender Schutz gegen giftige Chemikalien – in dem Werk weiter an der Tagesordnung (Quelle: Heise).

8. September 2014: *Der Spiegel* berichtet von der umfangreichen Datensammlung durch den Bundesnachrichtendienst (BND). So würde an der Spionagestation in Bad Aibling sämtliche Daten aus allen in Afghanistan, Somalia und dem Nahen Osten angezapften Verbindungen sieben Tage lang gespeichert und für die elektronische Auswertung aufbereitet. Zudem würden Daten an die NSA weitergeleitet, von der der BND im Gegenzug verschiedene Überwachungssysteme erhalten habe. Insgesamt habe die Kooperation zwischen den Geheimdiensten standardmäßig die Weiterleitung von rund 500 Millionen Daten monatlich an die NSA umfasst (Quelle: Der Spiegel, Heise).

10. September 2014: Das Türkische Parlament verabschiedet ein Gesetzespaket, welches das seit Februar bestehende Gesetz zur Internetkontrolle weiter verschärfen soll. Vorgesehen ist unter anderem, dass die türkische Kommunikationsbehörde *TiB* ohne richterliche Genehmigung aufzeichnen darf, welche Websites NutzerInnen besucht haben. Zudem soll sie Websites sperren lassen können, und dafür erst nachträglich die Genehmigung eines Gerichtes einholen müssen. Anfang Oktober wird diese Verschärfung des Internetgesetzes jedoch durch das türkische Verfassungsgericht gekippt (Quelle: Heise).

15. September 2014: Unter Berufung auf Snowden-Dokumente berichtet die Enthüllungsplattform *The Intercept*, dass der neuseeländische Geheimdienst *GCSB* gemeinsam mit der NSA sämtliche Verbindungsdaten zu der Kommunikation innerhalb Neuseelands abfange und auswerte (Quelle: The Intercept, Heise).

15. September 2014: In den USA wird das Sammeln von Metadaten jeglicher Telefonate für weitere 90 Tage durch das Ge-

heimgericht *FISC* (*Foreign Intelligence Surveilleance Court*) genehmigt (Quelle: Heise).

16. September 2014: Das FBI stellt die umstrittene Biometriedatenbank *NGI* (*Next Generation Identification*) fertig. Das von BürgerrechtlerInnen scharf kritisierte System wurde um ein Gesichtserkennungssystem (*Interstate Photo System*) und um eine Komponente erweitert, die es autorisierten Stellen erlaubt, sich automatisiert über Konflikte ihrer Angestellten mit dem Gesetz informieren zu lassen (*Rap Back*) (Quelle: Heise).

25. September 2014: Die Bundesnetzagentur verfestigt in einem aktuellen Referentenentwurf zur geplanten Transparenz-Verordnung den Router-Zwang. Sollte die Verordnung in dieser Form vom Bundestag abgenickt werden, könnten Provider ihren KundInnen weiterhin die zu verwendenden Router vorschreiben (Quelle: Heise).

25. September 2014: Wie die *Washington Post* unter Berufung auf ihr vorliegende Marketingdokumente der Firma *Veint* berichtet, vertreiben verschiedene Konzerne Überwachungstools, die es den abnehmenden Staaten erlauben, Handy-NutzerInnen weltweit zu orten. In der Regel würde die Software gemeinsam mit IMSI-Catchern vermarktet, die im Anschluss an die Standortbestimmung des Endgeräts die vollständige Überwachung der Kommunikation ermöglichen (Quelle: Washington Post, Heise).

26. September 2014: Nachdem eine Änderung des „Gesetzes über die Datenverarbeitung der Polizei" (PolDVG) durch den Hamburger Senat dies möglich macht, werden auch Hamburger PolizistInnen mit Bodycams ausgestattet. Hessen, wo die rechtlich fragwürdigen Überwachungskameras bereits seit Frühjahr 2013 im Einsatz sind, schafft bald darauf weitere Geräte an und auch Bayern und Baden-Wüttenberg testen den Einsatz in entsprechenden Pilot-Projekten (Quelle: Heise).

29. September 2014: In China werden die Internetsperren immer weiter ausgeweitet. Zunächst ist *Instagram* betroffen, in der Folge weitere Websites, unter anderem jene mit dem Katalog der Firefox-Erweiterungen und die Seite des Online-Projektes *Drupal* (Quelle: Heise).

Oktober 2014

1. Oktober 2014: Der russische Präsident Vladimir Putin kündigt eine Ausweitung der staatlichen Überwachung des Internets „zum Schutz der nationalen Sicherheit" sowie das Sperren von Websites mit als extremistisch kategorisierten Inhalten an (Quelle: Heise).

1. Oktober 2014: Das australische Repräsentantenhaus stimmt einer unter anderen von DatenschützerInnen heftig kritisierten Ausweitung der Überwachungsbefugnisse des Geheimdienstes *ASIO* zu. Damit wird nicht nur die Überwachung von „Computernetzwerken" (also auch des gesamten Internets innerhalb Australiens) mit lediglich richterlicher Genehmigung legal, sondern auch die Kriminalisierung von Whistleblowern ausgeweitet (Quelle: Heise).

5. Oktober 2014: Aus geheimen Dokumenten, die die Bundesregierung dem Untersuchungsausschuss des Bundestags zur NSA-Affäre vorgelegt hat, geht Medienberichten zufolge hervor, dass der BND jahrelang auch Daten von Personen mit deutscher Staatsbürgerschaft an die NSA übermittelt habe (Quelle: Süddeutsche Zeitung, Heise).

7. Oktober 2014: Wie aus verschiedenen Medienberichten hervorgeht, haben Undercover-Ermittler der US-amerikanischen Drogenfahndungsbehörde *DEA* zu Fahndungszwecken ohne das Wissen der Betroffen ein falsches Facebook-Profil einer verhafteten Verdächtigen eingerichtet und dazu von ihrem Smartphone entwendete private Fotos genutzt (Quelle: Washington Post, Heise).

7. Oktober 2014: Das E-Book-Programm *Adobe Digital Editions*, auf das viele E-Book LeserInnen angewiesen sind, sendet im Klartext Informationen über die in der Bibliothek vorhandenen und gelesenen E-Books an Adobe. Möglicherweise werden von der Software auch andere E-Book-Programme sowie die gesamte Festplatte nach Büchern durchsucht (Quelle: Heise).

9. Oktober 2014: Wie die Datenschutzbeauftragte des Bundesnachrichtendienstes (BND) bei ihrer Zeugenvernehmung im NSA-Untersuchungsausschuss des Bundestages einräumt, würden von dem Geheimdienst zwei Datenbanken mit Inhalts- und Metadaten ohne grundrechtliche Prüfung betrieben. In der Datenbank *Veras* werden Metadaten wie Telefonnummern, E-Mail-Adressen, Verbindungs- und Standortdaten von Bekannten verdächtiger Personen bis in die fünfte Ebene erfasst (Quelle: Heise).

10. Oktober 2014: Innenpolitiker der CDU/CSU-Bundesfraktion legen Vorschläge zu einem neuen Anti-Terror-Paket vor, das neben einer Neuauflage der Vorratsdatenspeicherung den Ausbau der internationalen Geheimdienstzusammenarbeit, eine umfassende Überwachung des Internets und das Knacken verschlüsselter Kommunikation umfasst. Zudem soll mit der Begründung einer Bedrohung durch Personen, die dem *Islamischen Staat* (IS) angehören, unter anderem der Strafbestand der „Sympathiewerbung" wieder im Strafgesetzbuch eingeführt und ein „Vermerk" im Pass oder Personalausweis möglich werden (Quelle: Heise).

11. Oktober 2014: Durch die Enthüllungsplattform *The Intercept* veröffentlichte Dokumente aus dem Fundus Edward Snowdens legen nahe, dass AgentInnen der NSA im Rahmen eines Programms namens *TAREX* Postsendungen zur Manipulation der darin enthaltenen Netzwerktechnik nicht nur in den USA, sondern auch in Deutschland, Südkorea, China und Peking abgegriffen haben. Zudem kooperiere der Geheimdienst im Rahmen weiterer Programme unter dem Decknamen *Sentry Eagle* mit Unternehmen in verschiedenen Staaten, um deren Produkte (zum Beispiel auch Kryptografie-Systeme) für NSA-Überwachungsprogramme zu nutzen. Schließlich würden im Rahmen dieses Programms auch Undercover-AgentInnen bei Unternehmen in verschiedenen Ländern eingesetzt (Quellen: The Intercept, Heise).

13. Oktober 2014: Der Rat der Europäischen Union verabschiedet ein Kapitel zu technischen und organisatorischen Schutzmaß-

nahmen, in dem er umfassende Änderungen an den Entwürfen der EU-Kommission und des Parlaments zur Datenschutzreform fordert. Insbesondere vertritt er einen „risikobasierten Ansatz", dem zufolge datenverarbeitende Stellen nur dann besondere Schutzanforderungen (wie Datenschutzfolgeanalysen oder das Melden von Sicherheitspannen) erfüllen müssen, wenn ihre Tätigkeit oder die verarbeiteten Daten besonders kritisch sind (Quelle: Heise).

22. Oktober 2014: Wie aus der Antwort der Bundesregierung auf eine kleine Anfrage der Fraktion *Die Linke* hervorgeht, unterstützt diese das Drängen des EU-Rats auf ein europäisches System zum Sammeln und Auswerten von Fluggastdaten. Aktuell werden bereits sogenannte *Advanced Passenger Informations* (*API*) bezüglich ankommender Flüge über die EU-Außengrenzen zwischen Fluggesellschaften und Grenzbehörden ausgetauscht. Diese Systeme sollen im Rahmen der Fluggastdatendatensammlung zu PNR-Daten (*Passenger Name Records*) erweitert werden. Statt „nur" Angaben zu Personaldokumenten sowie Abreise- und Ankunftszeit würden dann künftig auch Kontakt- und Kreditkartenangaben, Essenswünsche oder Informationen über den gesundheitlichen Zustand der Reisenden erfasst (Quelle: Antwort der Bundesregierung auf die Kleine Anfrage des Abgeordneten Andrej Hunko u. a. und der Fraktion *Die Linke*, Heise).

27. Oktober 2014: In einer von der EU-Kommission in Auftrag gegebenen Machbarkeitsstudie zur elektronischen Grenzkontrolle sprechen sich ExpertInnen gegen das Vorhaben aus, alle zehn Fingerabdrücke der einreisenden Personen zu erfassen. Stattdessen sollen „nur" acht Fingerabdrücke und zusätzlich Gesichtsbilder zur automatischen Gesichtserkennung erfasst werden (Quelle: Heise).

30. Oktober 2014: Über einen Bericht des Berliner Tagesspiegels wird bekannt, dass der Einsatz von Körperscannern („Nacktscannern") an deutschen Flughäfen sukzessive weiter ausgebaut werden soll. Die aktuell 14 Scanner an sechs deutschen Flughäfen (Berlin, Düsseldorf, Frankfurt am Main, Hamburg, München und Stuttgart) sollen noch in diesem Jahr um 14 und im kommenden Jahr um 75 weitere Scanner bundesweit ergänzt werden (Quelle: Der Tagesspiegel, Heise).

November 2014

6. November 2014: Das Bundesinnenministerium legt den Ländern und Kommunen einen neuen Referentenentwurf für ein IT-Sicherheitsgesetz vor, der, wie DatenschützerInnen kritisieren, sogar noch über eine „Vorratsdatenspeicherung durch die Hintertür" hinausgeht. Nicht nur Verbindungs- und Standortdaten, sondern auch Inhalte dürften damnach für sechs Monate gespeichert und ausgewertet werden. Zudem stelle der Entwurf die Möglichkeit bereit, NutzerInnen zwecks „Beseitigung von Missbrauch" vom Netzzugang auszuschließen (Quelle: Heise).

8. November 2014: Die Bayerische Polizei testet aktuell die Prognosesoftware *Precobs* (*Pre Crime Observation System*), die mit Daten über mehreren tausend Einbrüchen in den vergangenen Jahren gefüttert wurde, um zukünftige Einbrüche vorherzusagen. Es ist anzunehmen, dass sie sich damit dem aktuellen Trend des *predictive* oder *proactive policing* anschließt, der auf dem Massendaten-gestützten Vorausberechnen menschlichen Handelns und der Konstruktion von „Gefährdern" basiert (Quelle Heise).

9. November 2014: Wie der Spiegel berichtet, will der Bundesnachrichtendienst (BND) sogenannte *Zero Day Exploits*, also bislang unbekannte Sicherheitslücken in Software, aufkaufen, um beispielsweise die Verschlüsselung von im Internet übertragenen Daten brechen zu können (Quelle: Der Spiegel, vgl. dazu auch die Pressemitteilung des FIfF: *http://fiff.de/presse/pm-cyber-angriffskrieg* und in dieser Ausgabe).

10. November 2014: Mit einer offiziellen Vorstellung im Universitätklinkum Essen nimmt die von DatenschützerInnen kritisierte *Nationale Kohorte* (NAKO) ihren Auftakt. Mit der Kampagne sollen 200.000 Personen rekrutiert werden, um langfristig Körpersubstanzen für eine zentrale Biodatenbank zur Verfügung zu stellen (Quelle: Die Tageszeitung, Bioskop).

12. November 2014: In einer Anhörung des Bundestagsausschusses *Digitale Agenda* spricht sich die Medizininformatikerin Britta Böckmann dafür aus, die *Elektronische Gesundheitskarte* mit den *Körpertrackern* von *Apple* zu vernetzen (Quelle Heise).

12. November 2014: Aus einer geleakten Liste, die *heise online* vorliegt, geht hervor, dass das Bundeskriminalamt, die Bundespolizei und der deutsche Zoll vielfältige Software zum Knacken der Verschlüsselung von Computern, Smartphones und externen Speichermedien einsetzen (Quelle: Heise).

14. November 2014: Einer anonymen Quelle zufolge überwacht der Geheimdienst NSA Mobiltelefone mittels an eigenen Flugzeugen angebrachter IMSI-Catcher (Quelle: Heise).

17. November 2014: Nach Verhandlungen mit der britischen Regierung weiten die Internetprovider *BT*, *Sky*, *Talk Talk* und *Virgin Media* ihre Netzfilter aus. Die sogenannten Jugendschutzsysteme, die bereits Pornographie und Websites zu Themen wie Essstörungen, Alkohol, Rauchen oder Suizid filtern, sollen dem Guardian zufolge nun auch als terroristisch oder extremistisch kategorisierte Inhalte aussortieren. Zukünftig sollen die Provider die Verbreitung solcher Inhalte zudem melden. Die Kriterien, nach denen eine solche Kategorisierung erfolgt, sind nicht bekannt (Quelle: Guardian, Heise).

Sara Stadler

Sara Stadler studiert Informatik an der Hochschule Bremen und arbeitet in der FIfF-Geschäftsstelle.

30 Jahre FIfF

Ralf E. Streibl

warnen und mahnen
diskutieren und begleiten
vorausschauen und fordern

– 30 Jahre FIfF –[1]

„Aufbruch zu einer anderen Informatik“

Die frühen 80er Jahre waren in der Bundesrepublik Deutschland gekennzeichnet von den Massenprotesten der Friedensbewegung. Im „heißen Herbst“ der Friedensbewegung 1983 zeigten Millionen von Bundesbürgern mit Unterschriftenlisten, Großdemonstrationen, Blockadeaktionen, Menschenketten und vielen anderen Aktionen ihren Widerstand gegen die Pläne zur Stationierung atomar bestückter Mittelstreckenraketen und Cruise Missiles in Deutschland. Viele Berufsgruppen hinterfragten, welche Zusammenhänge von ihren jeweiligen Tätigkeiten zu Rüstung bzw. Krieg bestehen. Dies führte zur Gründung vieler berufsständischer Friedensinitiativen und Vereinigungen, wie z. B. der Ärzte für die Verhütung des Atomkrieges (*IPPNW Deutschland*), der *Friedensinitiative Psychologie – Psychosoziale Berufe* (heute: *Forum Friedenspsychologie*) oder der *Pädagogen gegen den Rüstungswahnsinn* (heute: *Pädagoginnen und Pädagogen für den Frieden*). Auch bezogen auf die Informatik wuchs bei manchen die Sorge über die zunehmende Verflechtung des Fachgebiets mit Rüstung und die damit einhergehende Militarisierung. An verschiedenen Informatikstandorten existierten dezentrale Friedensinitiativen. Aufbauend auf eine Initiative *Informatiker warnen vor dem programmierten Atomkrieg* (1983) wurde dann am 2. Juni 1984 in Bonn das FIfF gegründet, damals noch unter dem Namen *Forum Informatiker für Frieden und gesellschaftliche Verantwortung* – die Umbenennung zu *„Forum InformatikerInnen …“* erfolgte 1988. Als Vorbild für die Gründung des FIfF diente die amerikanische Vereinigung *Computer Professionals for Social Responsibility (CPSR)*.

Das in mehrfacher Hinsicht gesellschaftlich brisante Klima im Vorfeld der Gründung des FIfF wird bei einer Analyse der Titel des Magazins Der Spiegel *aus dem Jahr 1983 offenkundig: Vier Titelbilder bezogen sich auf die Volkszählung sowie Überwachungthemen, fünf auf die Raketenstationierung in Westdeutschland und den Widerstand der Friedensbewegung.*

Ein weiterer Aspekt, der mit jener Zeit verbunden ist, ist der Widerstand gegen die für das Jahr 1983 geplante Volkszählung, die aufgrund der Beschwerden beim Bundesverfassungsgericht zunächst ausgesetzt und dann mit dem sogenannten „Volkszählungsurteil“ (Az: 1 BvR 209/83) vom 15. Dezember 1983 ganz untersagt wurde. In seinem Urteil formulierte das Verfassungsgericht ein Grundrecht auf informationelle Selbstbestimmung,

basierend auf Artikel 1 des Grundgesetzes (Schutz der Menschenwürde), welches seither zu einer wesentlichen Grundlage aller Datenschutz- und Überwachungsdiskussionen wurde (vgl. Büllesbach & Garstka 2005; Steinmüller 2007). Es mag als eine Ironie der Literaturgeschichte angesehen werden, dass George Orwell für seine bekannte Dystopie just das Jahr 1984 Jahr als Titel wählte, indem er die Ziffern des Entstehungsjahres 1948 vertauschte.

Der erste Rundbrief des FIfF – der Vorläufer der *FIfF Kommunikation* – erschien im August 1984. Zu den Zielen des neu gegründeten Forums schrieb Hans-Jörg Kreowski unter der Überschrift „Aufbruch zu einer anderen Informatik“:

> *„Zweck des Forums ist dabei, die Verwendung von Computer- und Informationstechnik in der Rüstung und bei der Kriegsvorbereitung und -führung in Gegenwert und Zukunft zu untersuchen, zu kritisieren, öffentlich zu machen und Alternativen aufzuzeigen. Außerdem sollen regionale Gruppen, Initiativen und Einzelpersonen mit ähnlichen Zielen unterstützt werden. Perspektivisch jedoch wird die gesellschaftliche Verantwortung der Informatiker umfassender in das Wirken des Forums einbezogen werden. Vor allem soll dem Computer als Instrument der Arbeitsplatzvernichtung und der staatlichen Kontrolle gebührend Aufmerksamkeit gewidmet werden.“* (Kreowski 1984, S.16)

Selbstverständnis des FIfF war von Anfang an, dass seine Mitglieder kritische Analysen nicht auf militärische Anwendungen der Informatik beschränken wollen (vgl. Löhr 1984), vielmehr werden „Frieden“ und „Verantwortung“ als zwei eng verbundene Aspekte professionellen Handelns betrachtet:

> *„Frieden und gesellschaftliche Verantwortung im Namen des FIfF stehen nicht nebeneinander, sondern sind in einem Zusammenhang zu sehen. Zusammen sind sie Handlungsperspektive für tägliche Praxis im Forschungs- und Entwicklungsbereich. (...) Eine friedliche Informatik kann sich erst dann entwickeln, wenn von InformatikerInnen ganz bewusst fachliche und gesellschaftliche Verantwortung übernommen wird.“* (Bernhardt, Genrich, Ruhmann 1992, S.252)

Das FIfF setzt sich für eine Technikgestaltung ein, welche die Menschenwürde achtet und dazu beiträgt, die Demokratie und die Grundrechte weiterzuentwickeln. Es arbeitet für eine Informationstechnik, die Menschen in den Mittelpunkt stellt. Von Beginn an bis heute versteht sich das FIfF als Forum für eine kritische und lebendige Auseinandersetzung – offen für alle, die daran mitwirken wollen. Zur Professionalisierung der FIfF-Arbeit wurde Anfang 1987 in Bonn das FIfF-Büro gegründet, wo es bis Ende 1998 ansässig war. Nach ca. zwei Jahren in Medemstade-Ihlienworth erfolgte dann Anfang 2001 der Umzug zum heutigen Standort Bremen: Dort befindet sich die FIfF-Geschäftsstelle seither in zentraler Lage am Goetheplatz 4. In der „Villa Ichon“, einem Friedens- und Kulturhaus, teilt sich das FIfF ein Büro mit der *Bremischen Stiftung für Rüstungskonversion und Friedensforschung* (Streibl 2001).

„Die Würde des Menschen ist unverNETZbar“

Das FIfF hat oft sehr frühzeitig auf neue Themen aufmerksam gemacht. Ziel war und ist es dabei, das Augenmerk von Fachkolleg*innen und Öffentlichkeit auf die damit einher gehenden Fragen, Probleme aber auch Möglichkeiten zu richten und Raum für Austausch zu schaffen. Ein Mittel hierfür sind die Tagungen, die in der Regel jährlich an wechselnden Orten stattfinden.

1989, fünf Jahre nach Gründung des FIfF, fand die Jahrestagung in Frankfurt am Main statt. Sie trug den heute mehr denn je aktuellen und treffenden Titel *Die Würde des Menschen ist unverNETZbar*. Weit jenseits technischer Sichten auf Netzknoten, u. a. hinsichtlich Verkehr, Wirtschaft, Militär und Medien, rückten andere Qualitäten in den Vordergrund. In den vorbereitenden Gedanken der die Tagung ausrichtenden Regionalgruppe Frankfurt hieß es bereits:

> *„(...) In der Beschäftigung mit den ‚NETZEN‘ tat sich für uns eine ‚neue‘ Welt auf, die die Begriffe der ‚alten‘ Welt benutzte, aber nach dem, was wir bis dahin wussten und ahnten, etwas ganz anderes meinte: Es war nicht das ‚NETZ‘, es war die Sicht der Welt, in der das ‚NETZ‘ wirken soll. (...)“* (Schaaf 1990, S.12).

5 Jahre FIfF: „Die Würde des Menschen ist unverNETZbar“ Tagungsplakat der FIfF-Jahrestagung 1989 in Frankfurt am Main

„FIfFig in die Zukunft“

10 Jahre FIfF: „Gemeinsam können wir ein Zeichen gegen die Ratlosigkeit setzen.“ (Floyd 1994, S.12)

Die FIfF Jahrestagung in Bremen *1984 plus 10 – Realität und Utopien der Informatik* bot zum zehnjährigen Bestehen des FIfF 1994 eine Gelegenheit, Rückschau zu halten. Den Umbrüchen im Osten und der Hoffnung auf Entspannung des Ost-West-Konflikts steht der Golfkrieg mit seinen High-Tech-Waffensystemen und der Mediatisierung gegenüber. Helga Genrich nimmt in ihrem Beitrag für den Tagungsband Bezug auf von ihr wahrgenomme Veränderungen von Zielen und Sichtweisen im FIfF und stellt diejenigen, *„die Informatik zu einer ökologisch ausgerichteten Gestaltungswissenschaft entwickeln wollen“*, denjenigen gegenüber, welche *„die radikale Kritik der Informatik auch weiterhin für unverzichtbar halten“* (Genrich 1995, S.74). Ob dies wirklich unvereinbare Positionen sind oder ob aus der Kontroverse heraus ein weitergehendes Verständnis und verantwortliches Handeln resultieren kann, muss die Zukunft zeigen. Mit neuen Konzepten und Entwicklungen im Bereich der Informationstechnik müssen aufs neue kritische Fragen gestellt und Tabus aufgebrochen werden. *„FIfF soll politisch weiterhin die Wächterrolle spielen, die es immer gespielt hat“*, ermunterte Wolfgang Coy als Sprecher des Fachbereichs *Informatik und Gesellschaft* der *Gesellschaft für Informatik (GI)* die Zuhörer in seinem Grußwort. Oder, wie es Helga Genrich ausdrückte: *„FIFF lebt und wird, das zeigen die täglichen Anfragen, gebraucht“* (Genrich 1995, S.77).

In der Informatik war inzwischen die Beschäftigung mit den gesellschaftlichen Auswirkungen auch Teil der Disziplin geworden. Auch die Arbeit des FIfF – so das Resümee der Tagung – habe mit dazu beigetragen, die Fachöffentlichkeit für solche Fragen zu sensibilisieren. 1994 – im gleichen Jahr, in dem das FIfF sein 10jähriges Bestehen feiern konnte – verabschiedete die *Gesellschaft für Informatik* erstmals *Ethische Leitlinien*. Auch gab es inzwischen mittlerweile einige Universitäten, an denen das Fachgebiet „Informatik und Gesellschaft“ direkt personell verankert und in das Studium integriert war. Dies bot einige Jahre später die Gelegenheit, eine Reihe von Hochschullehrer*innen zu bitten, in einem Themenheft der *FIfF-Kommunikation* ihre jeweiligen Sichten auf *Informatik und Gesellschaft als akademische Disziplin* vorzustellen. Wenn es im Editorial heißt, dass sich *„das Dilemma zwischen mitmachen und kritisieren, zwischen Bedenken und Begeisterung“* (Engbring & Streibl 2001, S.4) wie ein roter Faden durch die Beiträge des Heftes zieht, so verdeutlicht dies das andauernde Ringen um ein Selbstverständnis des Fachgebiets und seiner Herangehensweisen. Die Ähnlichkeit zu manchen Diskussionen auf der Suche nach der Rolle des FIfF zwischen politischer Positionierung, kritischer Analyse, Politikberatung, Widerstand und Gestaltung liegt dabei auf der Hand.

„ReVisionen“

Zehn Jahre später – zum zwanzigjährigen Bestehen des FIfF – lautete das Motto der Jahrestagung *ReVisionen kritischer Informatik*. Ziel war es, auf der Tagung eine Brücke zu schlagen von einer Rückschau auf die Anfänge kritischer Informatik bis zu konkreten Visionen für die Zukunft. Über die Jahre sind immer wieder neue Themen und Schwerpunkte in der FIfF-Arbeit aufgetaucht, manche sind nach einiger Zeit auch wieder verschwunden. Gleichzeitig zeigt sich jedoch nicht nur bei den Kernthemen, wie hilfreich und notwendig die langjährige Erfahrung im FIfF und damit auch die Konstanz der Auseinandersetzung ist – etwas, das kurzfristige Initiativ- und Aktionsplattformen nicht leisten können. Eine Problematik vieler Gestaltungs-, aber auch Analyseansätze liegt in der oft ahistorischen, augen-

„Rüstung und Informatik ist in den letzten Jahren von einem tabuisierten Randthema zu einem wichtigen Politikfeld mutiert. (...) Die Fachdisziplin Informatik hat sich allerdings dem Thema noch kaum gestellt (...)“ – (Bernhardt & Ruhmann 2004, S.27)

blickzentrierten und kontextvernachlässigenden Perspektive, die das Verstehen von Entwicklungen und ein Betrachten verborgener Konflikte und Prozesse verhindert (vgl. hierzu Rolf 2008, S. 23f).

Kontinuität und Wandel: Der Rundbrief und verschiedene Generationen der FIfF-Kommunikation

Lange schon steht das FIfF nicht alleine in den Auseinandersetzungen mit seinen verschiedenen Themenfeldern da. Informatik bzw. Informations- und Kommunikationstechnik und Digitale Medien sind heute in nahezu allen Gesellschaftsbereichen wirksam und auch nicht auf einen nationalen Raum beschränkt. Das FIfF kooperiert bei seiner Arbeit mit vielen Organisationen, Initiativen und Vereinigungen sowie mit Journalist*innen, Wissenschaftler*innen, und vielen anderen Akteur*innen, die sich in Deutschland, Europa und darüber hinaus mit derartigen Fragen auseinandersetzen. Eine überblicksartige und dennoch nur ausschnitthafte Momentaufnahme verschiedener Kooperationen zeigte 2009 das Schwerpunktheft *Kritische Informatik* der FIfF Kommunikation (Büttemeier, Hügel, Streibl 2009).

Die Genese, Entwicklung und Konjunktur verschiedener Themen im FIfF lässt sich zumindest ansatzweise beim Betrachten des inhaltlichen Spektrums der Artikel in der Quartalszeitschrift *FIfF-Kommunikation* erkennen. Zwischen 1984 und 1987 verschickte das FIfF zunächst einen *Rundbrief* im DIN-A5-Format, zusammengestellt von einem Team aus Kaiserslautern. Dieser wurde ab 1988 von der *FIfF-Kommunikation* abgelöst, damals betreut von einer Redaktion in München. Ab 1995 übernahm dann für einige Zeit ein schwerpunktmäßig in Paderborn angesiedeltes Team diese Arbeit. Inzwischen hat sich seit mehreren Jahren eine verteilte Redaktionsarbeit etabliert: Neben der Hauptredaktion, die den allgemeinen Teil organisiert und die Gesamtplanung und -abläufe koordiniert, werden wechselnde Schwerpunktredaktionen gebildet, welche die Zusammenstellung von Beiträgen zum zentralen Heftthema übernehmen. Beide Redaktionen sind heute nicht mehr an einen Ort gebunden.

„Verantwortung 2.0“

Neben vielen anderen Aktivitäten kommt vor allem auch den Tagungen des FIfF eine große Bedeutung zu – auch wenn aus Platzgründen in diesem Beitrag exemplarisch nur die „Jubiläumstagungen“ genannt werden. Die Jahrestagungen bieten Raum für Interessierte und Mitglieder, sich in in Vorträgen und Arbeitsgruppen zu aktuellen Themen zu informieren, miteinander zu diskutieren und Aktivitäten zu planen. Zum bislang letzten großen Jubiläum – 25 Jahre FIfF – lag es daher nahe, als Schwerpunkt *Verantwortung 2.0* zu wählen. Das Motto sollte den Blick auf die wachsenden Herausforderungen lenken, die durch die fortschreitende Durchdringung aller gesellschaftlichen Bereiche mit Hervorbringungen bzw. Errungenschaften der Informatik entsteht (Kreowski & Streibl 2010, S.3).

Von „Informatiker warnen vor dem programmierten Atomkrieg“ zu „CyberPeace“

Über 30 Jahre hinweg hat das FIfF mit bewundernswerter Konstanz das Themenfeld *Informatik und Gesellschaft* in seiner Breite kritisch begleitet. Mal trägt das FIfF aktiv zum „Agenda Setting“ bei, mal reagiert es auf aktuelle Entwicklungen – und häufig beides zugleich. Zuletzt widmete sich die Jahrestagung 2014 in Berlin in Reaktion auf die aktuellen Ereignisse und Enthüllungen schwerpunktmäßig den deutschen Geheimdiensten, der NSA, Fragen der IT-Sicherheit und der Datenschutzkontrollen bei Sicherheitsbehörden (siehe http://fiffkon.de/medien.html).

Neben vielen anderen Themen kehrte in den letzten Jahren auch das Gründungsthema wieder stärker in den Fokus zurück. Sowohl gesellschaftspolitische als auch technische Entwicklungen

Pro „Informatik und Gesellschaft“: Nicht zuletzt auch als Antwort auf die Nicht-Wiederbesetzung vakanter „Informatik und Gesellschaft“-Professuren beschließt die Mitgliederversammlung des FIfF 2009 die Einrichtung eines Studienpreises (www.fiff.de/studienpreis)

tragen dazu bei, dass die Themen Krieg, Frieden, Rüstung und Militär weiterhin im FIfF präsent sind. Nach der viel beachteten Jahrestagung 2008 in Aachen zum Thema *Krieg und Frieden – digital* und weiteren Aktivitäten, die sich beispielsweise mit robotischen Waffensystemen auseinandersetzten, ist hier besonders die aktuelle Kampagne *CyberPeace* zu nennen. Damit will das FIfF „*die gefährliche Durchdringung des virtuellen Raumes mit militärischen Aktivitäten*" angehen und politisch mobilisieren. Anknüpfend an die o.g. Kernthemen und früheren Aktivitäten des FIfF geht es um den Schutz der Privatsphäre und der informationellen Selbstbestimmung. Hierfür sind sichere IT-Infrastrukturen eine technische Voraussetzung – aber vor allem braucht es ein Bewusstsein und Respekt im Hinblick auf die Achtung der Menschenrechte im virtuellen Raum. Es ist ein gutes Zeichen, dass die *stiftung bridge – Bürgerrechte in der digitalen Gesellschaft* entschieden hat, die Kampagne *Cyberpeace* des FIfF mit einem Zuschuss zu fördern.

Das FIfF ist weiter auf einem guten und wichtigen Weg. In einer von Schnelllebigkeit, Effekten und Unverbindlichkeit geprägten digitalen Welt geht das FIfF seine eigenen Wege – mal im Verbund mit anderen, mal alleine, mal digital, mal erfrischend analog, mal mit einzelnen Akteur*innen, mal in Kampagnen und im Team.

Quellen

Bernhardt, U. (1994): Die ersten 10 Jahre FIFF – Eine Chronik der Aktivitäten von 1984 bis 1994. In: FIFF Kommunikation, 11 (3), S.13-19.

Bernhardt, U.; Genrich, H.; Ruhmann, I. (1992): Der Prozess Verantwortung. In: Hans-Jörg Kreowski (Hrsg.): Informatik zwischen Wissenschaft und Gesellschaft. Zur Erinnerung an Reinhold Franck. Informatik-Fachberichte Nr. 309. Berlin: Springer, S.242-254.

Bernhardt, U.; Ruhmann, I. (2004): Ein Rückblick auf 20 Jahre Rüstung und Informatik. In: FIFF Kommunikation, 21 (2), S.24-28.

Büllesbach, A.; Garstka, H.-J. (2005): Computerrecht – Meilensteine auf dem Weg zu einer datenschutzgerechten Gesellschaft. In: Computer und Recht, 21 (10), S.720-724.

Büttemeier, C.; Hügel, S.; Streibl, R.E. (2009): Kritische Informatik – Editorial. In: FIFF Kommunikation, 26 (2), S.3.

Engbring, D.; Streibl, R.E. (2001): Informatik und Gesellschaft als akademische Disziplin – Editorial. In: FIFF Kommunikation, 18 (4), S.3-4.

Floyd, Ch. (1994): FIFFig in die Zukunft – 10 Jahre FIFF. In: FIFF Kommunikation, 11 (3), S.11-12.

Genrich, H. (1995): 10 Jahre FIFF – Orientierungen und Aktivitäten. In: Kreowski, H.-J.; Risse, T.; Spillner, A.; Streibl, R.E.; Vosseberg, K. (Hrsg.): Realität und Utopien der Informatik. Münster: Lit, S. 71-78.

Kreowski, H.-J. S.10f. (1984): Aufbruch zu einer anderen Informatik. In: Rundbrief 1/1984 des FIfF, S.14-16 und in dieser Ausgabe, S.40-41.

Kreowski, H.-J. (2007): Demokratie sichern und entfalten. In: Wider den Zeitgeist. Sonderbeilage zur FIfF Kommunikation 3/2007,

Kreowski, H.-J. (Hrsg.) (2008): Informatik und Gesellschaft. Verflechtungen und Perspektiven. Reihe: Kritische Informatik, Bd. 4. Münster: Lit.

Kreowski, H.-J. (2009): ... vorher – 25 Jahre Informatik mit FIfF – nachher ... In: FIFF Kommunikation, 27 (1), S.42-46.

Kreowski, H.-J.; Streibl, R.E. (2010): Verantwortung 2.0 – Editorial. In: FIFF Kommunikation, 27 (1), S.3.

Löhr, K.-P. (1984): Zur Entstehung des FIfF. In: Rundbrief 1/1984 des FIfF, S.17-19.

Rolf, A. (2008): Mikropolis 2010. Marburg: Metropolis 2008.

Steinmüller, W. (2007): Das informationelle Selbstbestimmungsrecht. Wie es entstand und was man daraus lernen kann. In: FIfF Kommunikation, 24 (3), S.15-19.

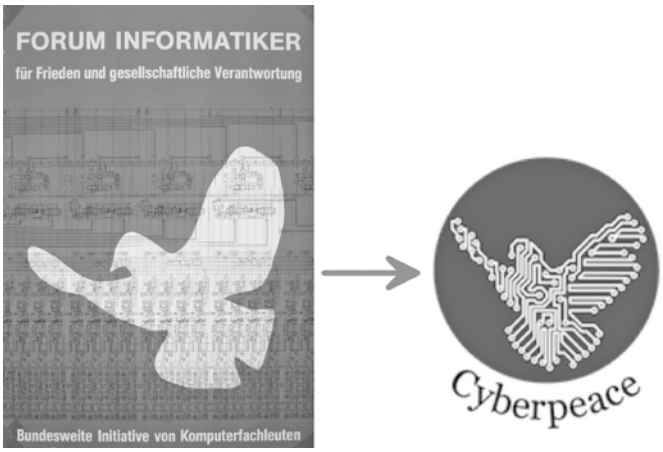
Streibl, R.E. (2001): Ein paar Kleinigkeiten zum neuen FIfF-Büro ... In: FIfF Kommunikation, 18 (2), S.12-16.

Streibl, R.E. (2009a): FIfF – Impressionen aus 25 Jahren. Vierseitige Farb-Beilage zur FIfF Kommunikation 2/2009.

Streibl, R.E. (2009b): Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V. – Impressionen aus 25 Jahren. In: Drewes, F.; Habel, A.; Hoffmann, B.; Plump, D. (eds.): Manipulation of Graphs, Algebras and Pictures. Essays Dedicated to Hans-Jörg Kreowski on the Occasion of his 60th Birthday. Festschrift. Bremen, p.341-352. http://www.fiff.de/publikationen/festschriften-kreowski/essay.pdf

Anmerkung

1 *In diesem Betrag wurden vereinzelt Passagen früherer Publikationen des Autors zum Teil leicht modifiziert nochmals verwendet (Streibl 2009a, 2009b).*



Ralf E. Streibl

Ralf E. Streibl, Diplom-Psychologe, tätig an der Universität Bremen im Fachbereich Mathematik/Informatik (Schwerpunkt in der Lehre unter anderem „Informatik und Gesellschaft") sowie im Personalrat.

Mitglied des FIfF-Beirats. Vorher mehrere Jahre Mitglied des FIfF-Vorstands sowie aktiv in der Redaktion der FIfF-Kommunikation.

Hans-Jörg Kreowski

Aufbruch zu einer anderen Informatik

2. Juni 1984: Dieser Sonnabend könnte ein denkwürdiger Tag für die Informatik in der Bundesrepublik werden. Rund 200 Informatiker und Fachleute aus dem Datenverarbeitungsbereich kamen in Bonn zusammen, um ein Forum zu gründen, das für den Frieden wirkt und gesellschaftlich verantwortlichem Handeln verpflichtet ist:

Forum Informatiker für Frieden und gesellschaftliche Verantwortung[1]

Die Veranstaltung wurde mit drei kurzen Referaten eingeleitet:

Joseph Weizenbaum (Cambridge, Massachusetts) mahnte die Versammelten, unnachgiebig vor der neuen qualitativen Stufe des globalen Wettrüstens zu warnen, deren besonderes Merkmal der massive Einsatz von Informationstechnik ist. Als Beispiel beschrieb er ein geplantes, neuartiges Waffensystem, das sich selbständig tief in feindlichem Territorium bewegen und dort geeignete Angriffsziele aufspüren können soll. Diese „autonomen Vehikel" sind eine von drei beabsichtigten Entwicklungen im Rahmen des „Strategic Computing"-Projekts, das mit 600 Millionen US-Dollar während der nächsten fünf Jahre von der DARPA („Defence Advanced Research Projects Agency"; einer Einrichtung des US-amerikanischen Verteidigungsministeriums) gefördert werden soll. Expertensysteme und „Computervision" sollen diesem Schlachtgefährt Selbständigkeit verleihen.

Joseph Weizenbaum mit Wilfried Müller und Hans-Jörg Kreowski bei der Verleihung der Ehrendoktorwürde durch die Universität Bremen 1998, Foto: Universität Bremen

Im Anschluß daran sprach Alan Borning (Seattle, Washington), ein Mitglied der nordamerikanischen Organisation „Computer Professionals for Social Responsibility" (CPSR), über die Möglichkeit eines „nuklearen Krieges aus Versehen", der durch Computerfehler in Frühwarnsystemen ausgelöst werden könnte. Nach seiner Einschätzung ist die Gefahr groß und wächst erschreckend; denn es werden Systeme vorbereitet, die auf eine Angriffswarnung hin automatisch mit dem Auslösen eines atomaren Gegenschlags antworten („launch on warning"), obwohl die Zuverlässigkeit solcher Systeme in Software und Hardware gering ist und bleibt und weder durch Test noch Korrektheitsbeweis sichergestellt werden kann. Die Verwendung von Methoden der „Künstlichen Intelligenz" wird die Risiken weiter erhöhen.

Abschließend erläuterte Alan Borning die bisherige Arbeit des CPSR, das aus mehreren regionalen Gruppen besteht und vierteljährlich ein Informationsorgan („The CPSR Newsletter") herausgibt. Die Mitglieder der regionalen Gruppen veranstalten Seminare, halten Vorträge und verbreiten ihre Kritik an der engen Verflechtung von Informatik und Rüstung in Zeitungsartikeln und anderen Veröffentlichungen.

Das dritte Referat hielt Reinhard Keil (Berlin), der engagiert den Computer als Waffe geißelte. Schon in den Anfängen der Computertechnik dienten Rechner vor allem militärischen Zwecken. Die Wasserstoffbombe etwa hätte nicht geschaffen werden können ohne die Durchführung umfangreicher Computerberechnungen. Inzwischen kommt kaum ein Waffensystem mehr ohne Rechnerunterstützung und -steuerung aus. Umgekehrt sind nahezu alle wichtigen Entwicklungsschritte in Computertechnik und Informatik von den Wünschen und dem Geld der Militärs stark beeinflußt, so daß eine Tätigkeit im Bereich der Informatik vielfach Kriegsdienst darstellt. Reinhard Keil forderte deshalb die Informatiker auf, sich gegen die militärische Nutzung ihrer Arbeit zu stellen und auch so ihr Grundrecht auf Kriegsdienstverweigerung wahrzunehmen. Überhaupt hat die Informatik ein besonderes Verhältnis zum Grundgesetz. So mußte es geändert werden, damit die Bundesregierung die Informatik in den 60er Jahren gründen konnte. Denn vorher waren die Hochschulen Angelegenheit der Länder, und dem Bund fehlte jegliche Kompetenz. Ein anderes Beispiel ist die Verfassungsbeschwerde der Hochschullehrer Wolfgang Däubler, Wolfgang Gebhardt, Klaus Haefner, Jörg Siekmann und Wilhelm Steinmüller gegen den Betrieb von Frühwarn- und Entscheidungssystemen in Europa, durch deren Unzuverlässigkeit die Beschwerdeführer ihr Leben und ihre körperliche Unversehrtheit bedroht sehen.

Der Beitrag endete mit dem Appell, das Forum zu nutzen, damit eines Tages nicht mehr gesagt werden muß: Jeder in der Informatik arbeitet an der Waffenentwicklung mit.

Nachmittags wurde die von einer Vorbereitungsgruppe vorgelegte Satzung diskutiert. Viele Redebeiträge kritisierten die Diskrepanz zwischen dem vorgeschlagenen Namen **Forum Informatiker für soziale Verantwortung** und der ursprünglichen Zweckbestimmung des Forums, die auf die Arbeit für den Frieden konzentriert sein sollte. Andererseits wiesen gewerkschaftlich orientierte Kollegen darauf hin, daß das Forum angesichts der fortschreitenden Rationalisierung durch Computereinsatz und der steigenden, den „inneren Frieden" bedrohenden Arbeitslosenzahlen nicht auf die Rüstungsproblematik eingeengt werden dürfte. Sowohl der endgültige Name als auch eine Satzungsänderung wurden den Einwänden gerecht. Das Thema Frieden – nun auch namentlich – soll vorläufig im Mittelpunkt stehen. Zweck des Forums ist dabei, die Verwendung von Computer- und Informationstechnik in der Rüstung und bei der Kriegsvorbereitung und -führung in Gegenwart und Zukunft

zu untersuchen, zu kritisieren, öffentlich zu machen und Alternativen aufzuzeigen. Außerdem sollen regionale Gruppen, Initiativen und Einzelpersonen mit ähnlichen Zielen unterstützt werden. Perspektivisch jedoch wird die gesellschaftliche Verantwortung der Informatiker umfassender in das Wirken des Forums einbezogen werden. Vor allem sollen dem Computer als Instrument der Arbeitsplatzvernichtung und der staatlichen Kontrolle gebührend Aufmerksamkeit gewidmet werden.

Das Forum steht allen offen, die mithelfen wollen, die unselige Verbindung zwischen Informatik und Militär zu (zer-)stören. Es wird die aktive Mitarbeit vieler brauchen, aber auch aus finanzieller Sicht wird es auf eine große Mitgliederzahl und reichlich Spenden ankommen. Denn allein einen regelmäßigen Informationsdienst aufrecht zu erhalten, ist teuer; erst recht aber werden die notwendige Öffentlichkeitsarbeit und die wünschenswerte Einrichtung einer arbeitsfähigen Geschäftsstelle Geld kosten.

Der Beitrag erschien im Original im FIFF-Rundbrief 1/1984, S. 14-16

Anmerkung

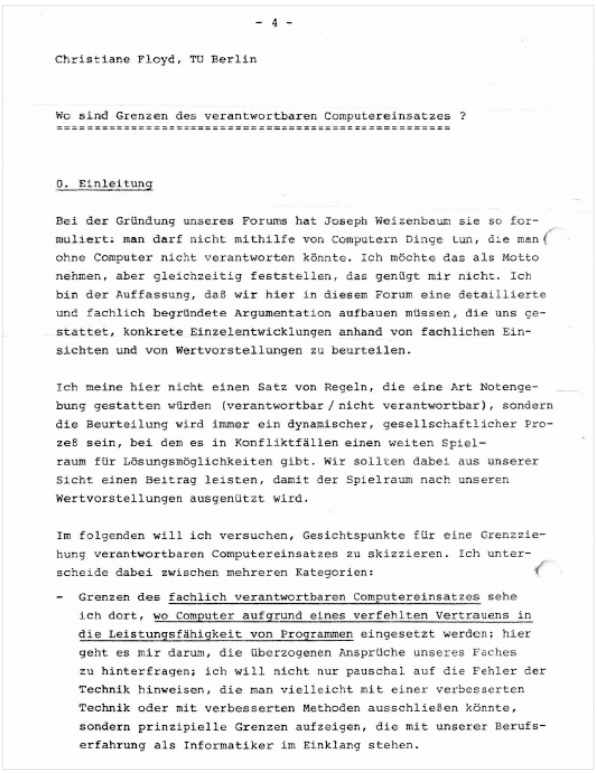
1 *Ausschließlich aus dem Grund historischer Authenzität wird in diesem Fall auf die geschlechtsneutrale Form verzichtet. Informatikerinnen mögen es uns nachsehen – die Redaktion.*

Christiane Floyd

Wo sind Grenzen des verantwortbaren Computereinsatzes?

0. Einleitung

Bei der Gründung unseres Forums[1] hat Joseph Weizenbaum sie so formuliert: man darf nicht mithilfe von Computern Dinge tun, die man ohne Computer nicht verantworten könnte. Ich möchte das als Motto nehmen, aber gleichzeitig feststellen, das genügt mir nicht. Ich bin der Auffassung, daß wir hier in diesem Forum eine detailliertere und fachlich begründete Argumentation aufbauen müssen, die uns gestattet, konkrete Einzelentwicklungen anhand von fachlichen Einsichten und von Wertvorstellungen zu beurteilen.



- 4 -

Christiane Floyd, TU Berlin

Wo sind Grenzen des verantwortbaren Computereinsatzes ?

0. Einleitung

Bei der Gründung unseres Forums hat Joseph Weizenbaum sie so formuliert: man darf nicht mithilfe von Computern Dinge tun, die man ohne Computer nicht verantworten könnte. Ich möchte das als Motto nehmen, aber gleichzeitig feststellen, das genügt mir nicht. Ich bin der Auffassung, daß wir hier in diesem Forum eine detailliertere und fachlich begründete Argumentation aufbauen müssen, die uns gestattet, konkrete Einzelentwicklungen anhand von fachlichen Einsichten und von Wertvorstellungen zu beurteilen.

Ich meine hier nicht einen Satz von Regeln, die eine Art Notengebung gestatten würden (verantwortbar / nicht verantwortbar), sondern die Beurteilung wird immer ein dynamischer, gesellschaftlicher Prozeß sein, bei dem es in Konfliktfällen einen weiten Spielraum für Lösungsmöglichkeiten gibt. Wir sollten dabei aus unserer Sicht einen Beitrag leisten, damit der Spielraum nach unseren Wertvorstellungen ausgenützt wird.

Im folgenden will ich versuchen, Gesichtspunkte für eine Grenzziehung verantwortbaren Computereinsatzes zu skizzieren. Ich unterscheide dabei zwischen mehreren Kategorien:

- Grenzen des fachlich verantwortbaren Computereinsatzes sehe ich dort, wo Computer aufgrund eines verfehlten Vertrauens in die Leistungsfähigkeit von Programmen eingesetzt werden; hier geht es mir darum, die überzogenen Ansprüche unseres Faches zu hinterfragen; ich will nicht nur pauschal auf die Fehler der Technik hinweisen, die man vielleicht mit einer verbesserten Technik oder mit verbesserten Methoden ausschließen könnte, sondern prinzipielle Grenzen aufzeigen, die mit unserer Berufserfahrung als Informatiker im Einklang stehen.

Ich meine hier nicht einen Satz von Regeln, die eine Art Notengebung gestatten würden (verantwortbar/nicht verantwortbar), sondern die Beurteilung wird immer ein dynamischer, gesellschaftlicher Prozeß sein, bei dem es in Konfliktfällen einen

- Grenzen des *zwischenmenschlich verantwortbaren Computereinsatzes* sehe ich dort, *wo Computer aufgrund einer verfehlten Gleichsetzung von Menschen mit Maschinen* eingesetzt werden; hier geht es um Bereiche, in denen wegen der Ersetzung von Menschen durch Programme zwischenmenschlicher Austausch behindert wird, menschliches Erleben verkümmert, menschliche Zuwendung wegfällt und soziale Netze zerstört werden; als Informatiker müssen wir uns dagegen wehren, daß der Computer zum „Partner" für Menschen erhoben wird.

- *Moralisch / politische Grenzen des Computereinsatzes* schließlich sind dort zu ziehen, *wo* (im Sinne Weizenbaums) *mit Computern versucht wird, was ohne Computer nicht gemacht werden darf*; wir können uns nicht von der Verantwortung für das, was unsere Programme auslösen, distanzieren; der Einsatz von Computern ermöglicht ein noch stärker zerstückeltes Verantwortungsbewußtsein als komplexe Technikanwendungen bisher: zwischen dem Vorausplanen (Programmieren) von Ereignissen und Handlungsabläufen und ihrem Eintreten ist jetzt der Computer als nicht-menschli-

che Instanz geschaltet; trotzdem verbleibt die Verantwortung für das, was Computer „tun", bei den Menschen, die sie herstellen, programmieren, ihren Einsatz planen und leiten; das heißt, wir tragen diese Verantwortung mit.

Im folgenden will ich diese Grenzen anhand allgemeiner Prinzipien ausformulieren. In der Arbeit des Forums können wir sie vorwiegend anwenden, um problematische Entwicklungen im militärischen Bereich zu kritisieren, damit hört unsere Verantwortung aber nicht auf, sondern wir müssen Grenzen des verantwortbaren Computereinsatzes in allen gesellschaftlichen Bereichen erarbeiten helfen. Mein Anliegen ist vor allem auch, dass wir durch diese Diskussion in unserem Forum *ein Umdenken unter Informatikern fördern*, jeder in unserem Arbeitsbereich und gemäß unserer Kompetenz, so daß wir insgesamt die fachlichen Voraussetzungen für eine *stärker an menschlichen Werten orientierte Informatik* schaffen.

1. Grenzen des fachlich verantwortbaren Computereinsatzes

Obwohl ich es für notwendig halte, die Argumentation hier sehr detailliert zu führen, kann ich in diesem Beitrag nur einen Ansatz dazu leisten. Ich vertrete hier die Auffassung, daß die folgenden Grenzen prinzipielle sind, das heißt, daß sie durch eine Verbesserung in Technik und Methoden zwar verschoben, aber nie aufgehoben werden können:

- *Alle in einem Programm verankerten Modelle der Realität sind prinzipiell reduktionistisch*. Das heißt, daß wir beim Spezifizieren bzw. Implementieren von Programmen immer gezwungen sind, die Fülle der Wirklichkeit mithilfe von endlich vielen ausgewählten Objekten (bzw. Objektklassen), deren ausgewählten, aber dann festen Merkmalen sowie der auf diesen Objekten zulässigen Operationen zu modellieren. Damit schaffen wir immer eine künstliche, abgeschlossene Mikrowelt, die alleine für die Arbeitsweise des Programmes maßgeblich ist. In der Realität muß man dagegen immer auf unvorhergesehene Ereignisse oder Objekte mit neuen relevanten Merkmalen gefaßt sein, diese Grenze der Modellierung mithilfe von Programmen ist prinzipiell nicht überwindbar.

- *In einem Computer verankerte Intelligenz unterscheidet sich in folgenden Punkten von der menschlichen*: Sie beruht immer auf einem Modell, das auf feste Regeln (gegebenenfalls mit weiteren Regeln zur dynamischen Weiterentwicklung solcher Regeln) gegründet ist; demgegenüber gehen in menschliche Intelligenz die jeweilige Situation mit ihrer erlebten Vorgeschichte, die erlebten Bedürfnisse und Werte als wesentliche Aspekte ein. Künstliche Intelligenz ist nicht im Sinnlich-Körperlichen verankert, es fehlt ihr daher der für uns selbstverständliche und immer gegebene Bezug zum Fühlen und Handeln, der erst zu einer menschlichen Sinngebung führt. Entscheidungen aufgrund von Programmergebnissen dürfen daher nicht von weiteren Programmen getroffen werden, wenn nicht gesichert ist, daß Menschen mit ausreichender Entscheidungsgrundlage verantwortlich in den Entscheidungsprozeß eingreifen können. Nur Menschen bewerten Ergebnisse und ordnen sie sinnvoll in den immer neuen Interpretationskontext, der selbst aufgrund von Kommunikation zwischen Menschen entsteht, ein.

- *Wir werden Programmfehler nie ausschließen können*, weil Irren menschlich ist. Irren ist nicht nur eine menschliche Schwäche, sondern eine menschliche Stärke, ist es doch mit der Fähigkeit zu lernen so eng verbunden. Jedes Programm kann nur das Ergebnis einer begrenzten Einsicht von Menschen zu einem gegebenen Zeitpunkt sein. Wir wissen alle, daß Fehler in Programmen sehr veschiedene Ursachen haben können: mangelndes Problemverständnis, unzulängliche Kommunikation, mißverständliche Verabredungen, Unkenntnis des tatsächlichen Einsatzkontextes von Programmen, mangelnde Kenntnis über die verfügbaren Betriebsmittel, logische Denkfehler, Flüchtigkeit, Nicht- oder Anders-Motiviert-Sein. Keinen dieser Aspekte werden wir durch eine Verbesserung von Technik oder Methoden je ausschalten können, Programmfehler legen daher prinzipielle Grenzen des Computereinsatzes fest: *Computer können nur dort verantwortbar eingesetzt werden, wo die Möglichkeit zum Auffinden und Beseitigen von Programmfehlern besteht*.

- Ohne ein genaues Maß angeben zu können, sehe ich eine prinzipielle Grenze für verantwortbaren Computereinsatz in der *Undurchschaubarkeit großer Programmsysteme* und der damit verbundenen Unmöglichkeit, die Ursachen erkannter Fehler schnell zu finden und verläßlich zu beseitigen; diese Grenze halte ich nicht für überwindbar durch verbesserte Spezifikations-, Programmier- oder Dokumentationsmethoden, sondern sie erfordert eine *bewußte Beschränkung auf lose gekoppelte kleine Programmsysteme, zwischen denen interpretierende und bewertende Menschen stehen*, die die Funktionsweise der genügend kleinen Programme durchschauen und im Fehlerfalle ändern bzw. durch manuelles Um-das-Programm-Herumarbeiten ausgleichen können.

- Es ist zwingend erforderlich, *Programme durch einen Probebetrieb unter realen Bedingungen und durch darauffolgende Adaption an die tatsächlichen Erfordernisse des Einsatzkontextes anzupassen*: hiermit meine ich nicht nur das Beseitigen von Programmfehlern anhand einer vorgegebenen Spezifikation, sondern das Zusammenspiel des Programms mit seinem umgebenden technischen bzw. sozialen System; insbesondere bei den immer häufiger verwendeten eingebetteten Systemen liegt ja die erwünschte Funktionalität von Programmen nicht immer eindeutig und kontextfrei fest, sondern die Funktionsweise des Programmes kann nur im Kontext des umgebenden Systems verstanden werden; *wo eine Erprobung in diesem Kontext unter realen Bedingungen nicht möglich ist, kann auch keine Aussage über die Angemessenheit der Programme gemacht werden; es ist daher nicht verantwortbar, Menschen in wichtigen Belangen von der Funktionsweise solcher Programme abhängig zu machen*.

- Eine prinzipielle Grenze für verantwortbaren Computereinsatz sehe ich letztlich auch in der *Fehler- und Störanfälligkeit des Rechnerbetriebs*; wir werden durch keine organisatorischen Maßnahmen ausschalten können, daß irgendwann einmal nicht doch Geräte fehlerhaft arbeiten, Programme irrtüm-

lich mit falschen Daten versehen werden oder durch andere nicht voraussehbare Ereignisse selbst korrekt arbeitende, für ihren Einsatzkontext angemessene Programme dennoch zu falschen Ergebnissen kommen; *letztlich sind nur Menschen durch Einschätzung der Gesamtsituation aufgrund viele einzelner und unterschiedlicher Wahrnehmungen imstande, zwischen echten und nur mithilfe von Daten simulierten Ereignissen ohne realen Hintergrund zu unterscheiden*.

2. Grenzen des zwischenmenschlich verantwortbaren Computereinsatzes

Was ich hier zu schreiben habe, erscheint mir selbstverständlich, dennoch meine ich, ist es angesichts der gegenwärtigen Entwicklung des Computereinsatzes in unserer Gesellschaft notwendig, das ganz Einfache geltend zu machen.

Beim Einsatz von Computern werden das Rechnen, das Verarbeiten von Daten und die Symbolmanipulation von allen anderen dem Menschen möglichen Umgangsformen mit der Realität losgelöst und kommen allein zum Tragen. Dies scheint nur dann gerechtfertigt zu sein, wenn

- Computer dort eingesetzt werden, wo das Rechnen und die Symbolmanipulation als Umgangsform mit der Realität angemessen sind,

- genügend Freiraum außerhalb des Computereinsatzes bleibt, daß andere menschliche Fähigkeiten und Erlebnisweisen nicht verkümmern.

In der gegenwärtigen Situation werden diese beiden Punkte nach meiner Auffassung nicht oder viel zu wenig beachtet. Dabei stützt sich die Informatik auf kongeniale mechanistische Theorien in den Humanwissenschaften, die in Anlehnung an die Vorgehensweise der klassischen Naturwissenschaften unsere *Innenwelt in sauber abgegrenzte Teilbereiche zu gliedern versuchen*, indem sie z. B. nur Aussagen über die kognitiven Fähigkeiten des Menschen machen, um so zu konkreten Ergebnissen zu gelangen. Ich will hier nicht in Frage stellen, ob eine derartige getrennte Betrachtung wissenschaftlich sinnvoll ist; wesentlich erscheint mir aber zu betonen, daß *aus der Trennung in der wissenschaftlichen Betrachtung nicht folgt, daß diese Bereiche auch in der Realität je trennbar sind*.

Wir Menschen wechseln zwischen Geisteszuständen, in denen wir rechnen, fühlen, Information verarbeiten, uns erinnern oder träumen zu jeder Zeit mit so großer Leichtigkeit hin und her, daß wir uns dessen meist kaum bewußt sind. *In der Informatik ist dagegen nach meiner Auffassung ein Menschenbild verankert, bei dem die Vielfalt menschlichen Erlebens und Handelns auf Informationsverarbeitung im technischen Sinne und auf Objektmanipulation reduziert wird*. Dabei erscheinen mir folgende Aspekte besonders problematisch:

- die postulierte *Strukturgleichheit von Mensch und Computer* als informationsverarbeitende Systeme,

- die damit verbundene Auffassung, *menschliches Verhalten beim Problemlösen erfolge nach Regeln* und sei daher klassifizierbar und voraussagbar,

- die bereits erwähnte Annahme, man könne *die beim Menschen stets vorhandene Einbettung* von Rechnen und Symbolmanipulation *in andere Erlebnisweisen* wie Fühlen und Handeln, die sowohl durch den *Zusammenhang von Geistigem und Körperlichem* als auch durch die Gegebenheiten der *jeweils einmaligen Situation* und *ihrer Interpretation durch den erlebenden Menschen* geprägt sind, *vernachlässigen*.

Ich möchte hier nicht im Einzelnen auf konkurrierende Theorien der Humanwissenschaften eingehen, in denen andere Menschenbilder dem mechanistischen gegenübergestellt werden, und auch nicht die empirische Evidenz für oder gegen das mechanistische Menschenbild überprüfen. Ich will mich aber *von diesem Menschenbild als alleiniger Grundlage für den Entwurf und den Einsatz von computergestützten Systemen mit Nachdruck distanzieren*, weil es meiner Selbsterfahrung und meiner Erfahrung im Umgang mit anderen Menschen in entscheidenden Punkten zuwiderläuft und zudem Qualitäten im zwischenmenschlichen Zusammenleben, die für mich wesentlich sind, gefährdet.

Ich meine auch, wir müssen Grenzen für den verantwortbaren Einsatz von Computern dadurch erarbeiten, daß wir uns *bewußt ein reichhaltigeres Menschenbild zu eigen machen* und als Grundlage für unsere Arbeit verwenden. Dabei geht es sowohl um die Auseinandersetzung mit Theorien über den Menschen, die dem mechanistischen Menschenbild widersprechen, als auch und vor allem darum, daß wir den Unterschied zwischen Mensch und Maschine in unserem eigenen Erleben und in unseren Beziehungen zu anderen Menschen wahrhaben und ihn somit verkörpern.

Die hier aufgezeigten Gesichtspunkte scheinen mir für eine Reihe konkreter Einzelentwicklungen in der Informatik und im Computereinsatz von Bedeutung zu sein, für die ich hier einige Beispiele geben will:

- *der Bereich Mensch-Maschine-Interaktion*, in dem wir klarstellen müssen, daß zwischen Menschen und Maschinen keine Kommunikation stattfindet, kein Dialog geführt wird, der Computer niemals ein Partner für Menschen sein wird, und somit sichergestellt werden muß, daß auch an Bildschirmarbeitsplätzen die Kommunikation, der Dialog und die partnerschaftliche Zusammenarbeit zwischen Menschen erhalten bleibt,

- *die Veränderung von Arbeitsprozessen durch Computereinsatz*; wir müssen dafür Sorge tragen, daß in DV-gestützten Systemen menschliches Arbeitshandeln nicht zu sinnentleerter Routinetätigkeit und Computerbedienung verkümmert, sondern daß die Bearbeitung sinnvoller Aufgaben durch den Computer angemessen unterstützt wird,

- *der Einsatz von Computern in Bereichen, in denen zwischenmenschliche Beziehungen von ausschlaggebender Bedeutung sind*; so müssen wir aufrechterhalten, daß das menschliche Verhältnis von Lehrer und Schüler nicht durch computergestützten Unterricht ersetzt werden kann, daß menschliche Zuwendung in der Altenpflege nicht mit dem von einigen Informatikern vorgeschlagenen Einsatz von Robotern gleichgesetzt werden kann, daß Rechtsprechung

mehr ist als Informationsverarbeitung über den vorliegenden Fall und die maßgeblichen Gesetze, daß die Beurteilung der Leistungen von Mitarbeitern nicht auf die numerische Auswertung ausgewählter Leistungsmerkmale zurückgeführt werden kann,

- *das Eindringen der Computer in die Freizeit und in das Familienleben*, bei dem sich zu Recht die Frage stellt, inwieweit angesichts der fortgesetzten und einseitigen Beschäftigung mit Computern andere menschliche Fähigkeiten , die dabei nicht zum Tragen kommen, noch die Chance haben, sich in ausgewogener Weise zu entwickeln.

Die *Grenzziehung zwischen Menschen und Maschinen* kommt letztlich nicht von außen, sondern *liegt im handelnden Menschen selbst*; es besteht die Gefahr, daß wir durch ständige Konfrontation mit dem Computer zu maschinenartigem Denken und Handeln ermutigt werden, während andere Fähigkeiten brachliegen. Wenn wir uns gegen die Auswirkungen des Computers in unserer Umwelt wehren wollen, müssen wir uns nicht zuletzt mit der Maschine in uns selbst auseinandersetzen.

3. Moralisch/politische Grenzen des verantwortbaren Computereinsatzes

In jedem Bereich, in dem Computer überhaupt eingesetzt werden, besteht die Gefahr, daß sie zur Durchsetzung von Interessen Einzelner oder bestimmter Gruppen eingesetzt werden, um mit Computern zu tun, was man ohne Computer nicht darf. Ich will daher nicht einen Überblick über besonders gefährdete Bereiche versuchen, sondern skizzieren, wie Computer zum Umgehen von anerkannten moralischen oder politischen Grenzen verwendet werden können.

- Mithilfe von Computern kann man versuchen, *Maßnahmen zu verstecken*, die aufgrund geltender und in Gesetzen verankerter Wertvorstellungen offen nicht durchgesetzt werden können. Beispiele dazu sind Überwachung und Kontrolle von Einzelnen durch Staat, Organisationen und Betriebe.

- Mithilfe von Computern kann man anstreben, *menschlich-moralisches Handeln zu umgehen*, um das Eintreffen von vorgeplanten Ereignissen entgegen dem Verantwortungsbewußtsein von Menschen durchzusetzen. Hierher gehören z. B. Überlegungen, wonach die Zerstörung einer Stadt in einem nuklearen Krieg im Ernstfall durch Computer ausgelöst werden müßte, da Menschen vermutlich auch in Streßsituationen und auch auf Befehl dazu nicht bereit wären.

- Mithilfe von Computern kann man sich der Verantwortung für das Eintreffen von programmierten Ereignissen entziehen wollen, indem man *die Verantwortung auf die Maschine abwälzt*. Obwohl der Computer als nichtmenschliche Instanz zwischen Programmierung und Ausführung steht, verbleibt dennoch die Verantwortung für das, was der Einsatz unserer Programme bewirkt, bei den Menschen.

- Mithilfe von Computern kann man letztlich *die Grenzen des überhaupt von Menschen Verantwortbaren überschreiten wollen*. Insbesondere sind wir heute dabei, den Einsatz von Programmen zu planen, die aufgrund eines lokal eingetretenen Problems in der Lage wären, ohne menschliches Zutun das Leben auf der ganzen Erde zu vernichten.

Günter Anders zieht die Grenze für die erlaubte Höchstgrenze menschlicher Produkte so:

> *„Und da dem Menschen das Herstellen von Dingen nun einmal freisteht, verfügt er wohl überhaupt über kein derartiges Kriterium: es sei denn, er mache sich* selbst *zum Kriterium, das heißt: er definiere den Grenzpunkt als in demjenigen Augenblick erreicht, in dem er,* ‚kleiner als er selbst', *mit sich selbst ‚nicht mehr mitkommt', das heißt: seinen Produkten nicht mehr gewachsen ist. Also heute."*[2]

Der Beitrag erschien im Original im FIFF-Rundbrief 1/1984, S. 4-13

Anmerkung

1 *Das Forum InformatikerInnen für Frieden und gesellschaftlliche Verantwortung wurde im Juni 1984 in Bonn gegründet.*

2 *Aus: Die Antiquiertheit des Menschen, Band I, Über die Seele im Zeitalter der zweiten industriellen Revolution, Verlag C.H. Beck, München 1980, Seite 45*

Christiane Floyd

Christiane Floyd promovierte 1966 nach einem Mathematik-Studium an der Universität Wien. Nach verschiedenen Informatik-bezogenen Tätigkeiten in der Industrie und im Computer Science Department der Stanford University wurde sie 1978 auf eine Professur für Informatik an die TU Berlin berufen. 1991 folgte sie einem Ruf an an die Universität Hamburg, wo sie bis zu ihrer Emeritierung die Fachgruppe Software-Technik leitete. Christiane Floyd war Gründungsmitglied des FIfF und dessen erste Vorsitzende (von 1984 bis 1987). Bis heute ist sie Mitglied des FIfF-Beirats.
Zum Wirken und zur Wirkung von Christiane Floyd sei verwiesen auf den Beitrag von Susanne Maaß in der FIfF-Kommunikation 2/2009: 30 Jahre kritisch in der Informatik – Nachgedanken zur Emeritierung von Christiane Floyd. Siehe auch: Christiane Floyd – Emanzipation durch Computer, Die Zeit 29.3.2011, *http://www.zeit.de/digital/internet/2011-03/floyd-informatik-frauen*.

Klaus Fuchs-Kittowski

Mein Weg zum FIfF

Ein Leben in Frieden ist erstes Menschenrecht

Mein Weg zum FIfF war sicher nicht geradlinig, aber doch aufgrund meines Lebensweges konsequent. Kurz nach meinem Eintritt ins „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung" (FIfF) begegnete ich Joe Weizenbaum und fragte ihn, war dies richtig? Er antwortete: „Natürlich ist es richtig, Du konntest doch gar nicht anders handeln!"

Dass mein Weg zum FIfF nicht geradlinig war, liegt zunächst an dem äußeren Umstand, dass es diese Organisation in der DDR nicht gab. Aber auch daran, dass es verschiedene Einflüsse gab, die dazu führten, dass ich auf der ersten Tagung des FIfF nach der Wende Mitglied wurde und auch in den Vorstand gewählt wurde.

Der erste Einfluss, der mich unmittelbar mit der Gründung und Existenz des FIfF und seiner Friedensarbeit bekannt machte, war das Zusammentreffen mit Christiane Floyd, Michaela Reisin und Reinhard Keil. Zur Vorbereitung unseres Kolloquiums zur *Organisation der Informationsverarbeitung* an der Humboldt-Universität waren sie mehrfach, zur Durchführung gemeinsamer Seminare, von der Technischen Universität Berlin (West) zur Humboldt-Universität zu Berlin (Ost) gekommen. Natürlich sprachen sie mit uns auch über ihre Bemühungen, eine Organisation zu gründen, die sich stärker den Problemen der Friedenssicherung und der Verantwortung der InformatikerInnen dafür zuwendet, als die Gesellschaft für Informatik (GI) derzeit dazu bereit sei.[1]

Es war ja die Zeit des Nato-Doppelbeschlusses. Es galt, den Kalten Krieg zu überwinden und die schreckliche Gefahr, die von der Stationierung von Raketen auf beiden Seiten der deutsch-deutschen Grenze für Deutschland und den Weltfrieden heraufbeschworen wurde, zu bannen.

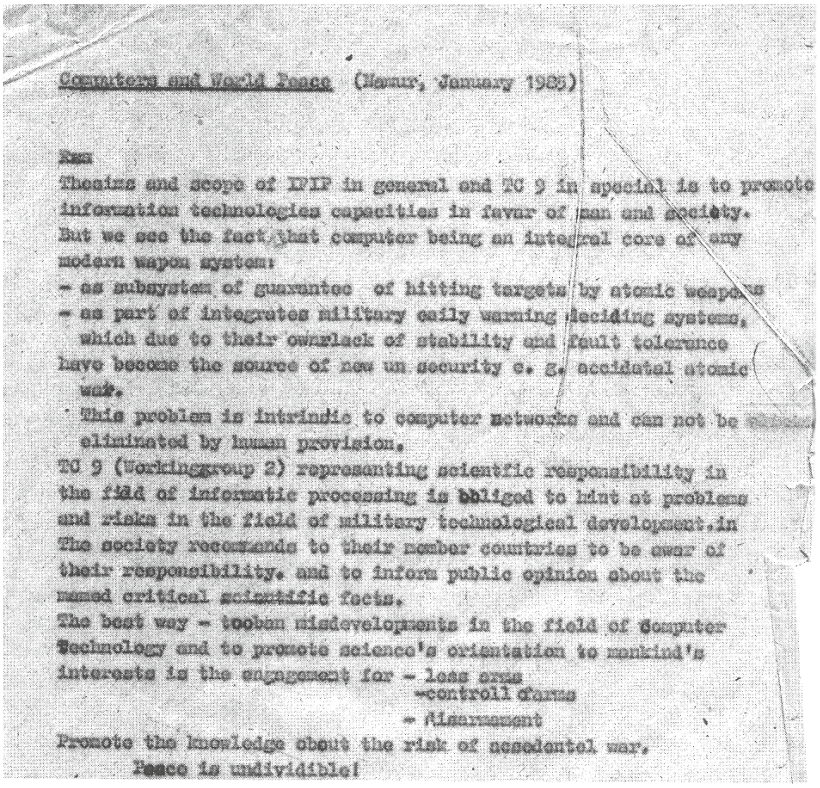
Zugleich gab es noch einen zweiten starken Einfluss für den Weg zum FIfF. Es wuchs der Druck auf die Internationale Föderation für Informationsverarbeitung (IFIP) sich offiziell gegen das Wettrüsten und für allgemeine Abrüstung, speziell auf dem Gebiet der Atomwaffen, auszusprechen. Es war insbesondere der Vertreter Neuseelands, der in der Generalversammlung der IFIP immer wieder die Forderung nach einem offiziellen Wort gegen das Wettrüsten und für die Verantwortung der InformatikerInnen in diesem Ringen erhob. Dies führte dazu, dass das Technische Komitee 9 (TC9) *Computer und Gesellschaft* vom Präsidenten der IFIP, Heinz Zemanek, wiederholt darum gebeten wurde, eine entsprechende Ausarbeitung vorzulegen. Von Hal Sakmann (USA), dem damaligen Vorsitzenden des TC9, wurde zu diesem Zweck eine Task Force *Freedom and Disarmament* gebildet, der Ulrich Briefs (BRD), Paul Kolm (Österreich) und ich (DDR) angehörten. Wir machten mehrere Resolutionsentwürfe, die immer wieder als zu politisch zurückgewiesen wurden, denn schließlich waren ja die Sowjetunion und die USA in der IFIP vertreten. Es bedürfe einer rein fachlichen Begründung.

In der Tat brauchten wird eine Aussage wie die der Bewegung *Ärzte gegen den Atomkrieg*. „Nach einem Atomschlag gibt es keine Heilung mehr!"

Hier war es Christiane Floyd, die mir bei den schon erwähnten Treffen in der Humboldt-Universität von der tapferen Haltung von David Parnas gegenüber den Star-Wars-Plänen der USA berichtete. Er sagt nur: „Die Software ist ungenügend getestet. Ein Krieg aus Zufall wird daher immer wahrscheinlicher." Damit lieferte uns D. Parnas die treffende rein fachliche, wenn sicher auch nicht unpolitische Begründung.

So vorbereitet entstand der Text einer Resolution, die in Namur auf der IFIP-Konferenz *Can Information Technology Result in Benevolent Bureaucracies?* im Januar 1985, insbesondere mit Vincent Brannigan (USA), Richard Sizer (Großbritannien), Jacques Berleur (Belgien), Wilhelm Steinmüller (BRD) und mir (DDR) erarbeitet wurde.

In dieser Resolution aus Namur – die zugleich für die IFIP-Generalversammlung bestimmt war, damit alle Mitgliedsländer und alle TCs angesprochen werden – wird wiederholt auf die Gefahr eines Krieges durch Zufall verwiesen; damit hatten wir analog zu der Bewegung *Ärzte gegen den Atomkrieg* das rein fachliche Ar-



Computers and World Peace (Namur, January 1985)

Aim
Theaims and scope of IFIP in general and TC 9 in special is to promote information technologies capacities in favor of man and society.
But we see the fact, that computer being an integral core of any modern wapon system:
- as subsystem of guarantee of hitting targets by atomic weapons
- as part of integrates military early warning deciding systems,
which due to their ownslack of stability and fault tolerance have become the source of new un security e. g. accidatel atomic war.
This problem is intrindic to computer networks and can not be eliminated by human provision.
TC 9 (Workinggroup 2) representing scientific responsibility in the field of informatic processing is obliged to hint at problems and risks in the field of military technological development.in
The society recommends to their member countries to be aware of their responsibility. and to inform public opinion about the named critical scientific facts.
The best way - to ban misdevelopments in the field of Computer Technology and to promote science's orientation to mankind's interests is the engagement for - less arms
-controll of arms
- disarmament
Promote the knowledge about the risk of accedentel war.
Peace is undividible!

Resolution der IFIP zur Abrüstung

gument, dem alle Mitgliedsländer der IFIP zustimmen bzw. sich nicht verweigern konnten.

Diese Resolution wurde auch im Rahmen der Friedensforschung an der Humboldt-Universität, an der Akademie der Wissenschaften der DDR und im Zusammenhang mit der Gründung der Gesellschaft für Informatik (GI-DDR) in der DDR diskutiert.

Es muss hier auch unbedingt erwähnt werden, dass insbesondere in der BRD die Aktivitäten engagierter InformatikerInnen weiter gingen.

Auf dem Höhepunkt des Kalten Krieges, mit der Einführung von Kurzstreckenraketen, wurde zugleich dem Computer, ausgerüstet mit undurchschaubaren Softwaresystemen, immer größere Entscheidungskompetenz übertragen. In einer solchen Situation, in der die Raketen – SS 20, Pershing II und Cruise Missile – auf beiden Seiten der deutsch-deutschen Grenze stationiert wurden, blieben nur noch wenige Minuten, um über einen Gegenschlag zu entscheiden. Man konnte, wie es Albert Schweizer vorhergesagt hatte, nur noch automatisiert entscheiden. Die Lebensfrage der Menschheit – Krieg oder Frieden – wird damit dem Computer überlassen. Dies darf nicht sein! Ein Krieg aus Zufall wird immer wahrscheinlicher! Informatiker, unter ihnen an führender Stelle Willhelm Steinmüller, Klaus Brunnstein, Klaus Haefner verlangten beim Bundesverfassungsgericht Aufklärung darüber, wie unter solchen Bedingungen die Sicherheit des Volkes noch zu gewährleisten ist.

Klaus Brunnstein, Vertreter der BRD im TC9 der IFIP und ich (Vertreter der DDR im TC9) hatten in diesem Zusammenhang eine interessante Diskussion. K. Brunnstein mahnte wiederholt, dass der Informatiker dazu verpflichtet ist, die Einhaltung der Menschenrechte zu unterstützen, und sprach dabei von individuellen, sozialen und internationalen Menschenrechten. Mir war die Erwähnung internationaler Menschenrechte neu, wenn ich von einem Artikel von Klaus Fuchs[2] absehe, in dem er die Forderung: „Ein Leben in Frieden ist erstes Menschenrecht" erhoben hatte.

Es war mehr oder weniger klar, dass mit den individuellen Menschenrechten u. a. der Schutz der Privatsphäre, mit den sozialen Menschenrechten der Schutz vor Verlust des Arbeitsplatzes gemeint war. Was war aber damals ein internationales Menschenrecht, das InformatikerInnen mit zu gewährleisten hätten – wenn nicht die Sicherung des Friedens auf der Welt? Klaus Brunnstein war in seinem Denken offensichtlich seiner Zeit voraus, denn damals stritt man in der sog. Systemauseinandersetzung, z. B. bei den KSZE-Verhandlungen, noch darum, ob es außer den bürgerlichen Freiheitsrechten überhaupt noch andere Menschenrechte zu verteidigen gelte, und umgekehrt wollte man nur über die Einhaltung sozialer Menschenrechte diskutieren. Ein Leben in Frieden wurde m.W. nicht als ein zu schützendes Menschenrecht diskutiert.

Damit komme ich zu den noch tiefer liegenden Gründen meines Weges zum FIfF.

Seit den 50er-Jahren war mein Großvater, Emil Fuchs, Mitglied des Friedesrates der Karl-Marx-Universität Leipzig. Ich erlebte, wie auch unter seiner aktiven Mitwirkung sich schrittweise vielerorts christliche Arbeitskreise zur Friedensarbeit bildeten. Vor allem kam es unter seiner Mitwirkung, unter der Führung des bekannten tschechischen Theologen Josef L. Hroma´cka, zur Bildung der *Prager christlichen Friedenskonferenz*.

Ich beteiligte mich selbst aktiv an der großen Bewegung des internationalen Friedensrates, die mit dem *Stockholmer Appell zur Ächtung der Atomwaffen* verbunden war.

Über die Arbeit der *Prager christlichen Friedenskonferenz* wird u. a. in dem Buch von Werner Wittenberger „Die Entstehung der Christlichen Friedenskonferenz im Kontext von Weltpolitik: Ein unzeitgemäßer Beitrag zur Aufarbeitung der Vergangenheit"[3], Reinhard Scheerer (Herausgeber), berichtet. Hier wird z. B. ausführlich dargestellt, wie man sich aus theologischer Sicht mit der Problematik des Kalten Krieges auseinandergesetzt hat. Es wird berichtet: „Ein Ausschuss unter dem Vorsitz von Hroma´cka wurde gegründet, der ein Papier erarbeitete, das durch die Plenarsitzung angenommen wurde und als Studienmaterial gelten sollte. Dieses Papier dokumentiert den Zug zum politisch Konkreten, ohne sich von Vogels grundsätzlichen Auffassungen in dieser Frage abzusetzen. Das Papier besteht aus 28 Thesen, die a) über das Wesen des Kalten Krieges und b) über die Methoden des Kalten Krieges handeln.[4] Das Wesen des Kalten Krieges ist Krieg. „Er schafft die Gefahr, dass alle Möglichkeiten friedlicher Verständigung verbaut werden." So steht der Kalte Krieg in gewisser Hinsicht unter einem schwereren Gericht als ein schon angefangener Krieg und die Gewalttaten während eines Krieges." Verwiesen wird auf Mt5, 21-26. Auch der Kalte Krieg will mit seinen Mitteln den Feind in eine solche Situation zwingen, in der er sich unterwirft. Auch der Kalte Krieg will siegen und unterwerfen. Die Aufgabe des Gedankens der Koexistenz und der Verhandlungen ist schon Kalter Krieg, ein Anfang des Krieges."[5]

Warum hatte ich aber Joe Weizenbaum die Eingangs erwähnte Frage gestellt, ob ich mit dem Eintritt ins FIfF richtig handeln würde? Dem waren wohl 10 Minuten Schnellkurs in die damalige politische Situation in der Bundesrepublik, zu der die DDR gerade beigetreten war, vorangegangen. Zwei damals führende Mitglieder des FIfF sagten zu mir:

1. Alle Professorenstellen an den Universitäten der DDR werden aufgelöst und ihr werdet Euch alle neu bewerben müssen, da wird Dir eine Mitgliedschaft im FIfF nicht gut angerechnet.

2. Denn die Tätigkeit des FIfF wird vom Verfassungsschutz überwacht.[6]

3. Deine Verbindungen zu den norddeutschen Fachbereichen der Informatik werden Dir hierbei auch nichts nutzen, denn die sind, einschließlich Berlin, viel zu links. Du musst Dir auch Unterstützung bei süddeutschen Fachbereichen der Informatik suchen.

4. Außerdem haben wir aus einer Liste entnommen, dass Du auch Mitglied des Friedensrates bist.

5. Wir können Dir also von einer Mitgliedschaft im FIfF nur abraten.

Ich kann nicht verhehlen, dass mir dies alles wirklich Angst machte, auch wenn man sich das ganze Ausmaß der Abwicklung an den Universitäten und an der Akademie der Wissenschaften der DDR noch gar nicht vorstellen konnte. Doch nahm ich den 3. Punkt ernst und besuchte Wilfried Brauer in München, von dem ich wusste, dass er und seine Frau mir wohl gesonnen waren, denn ich hatte ihm geholfen, die Weichen in der IFIP-Generalversammlung so zu stellen, dass Hamburg und nicht Helsinki den Zuschlag zur Ausrichtung des nächsten IFIP-Computer-Weltkongresses erhielt. Wir hatten dann auch ein sehr schönes, ernsthaftes Gespräch, aber er konnte am weiteren Lauf der Dinge auch nichts ändern.

Joe Weizenbaum konnte natürlich nicht wissen, dass ich aus diesem Schreck und der damit gegebenen Verunsicherung heraus, nach Vollzug meines Eintritts ins FIfF, diese Frage an ihn stellte. Ich erinnere mich aber sehr gut daran, wie mich seine Worte: „Du konntest doch, Deiner ganzen Haltung entsprechend, gar nichts anderes tun", sehr über die, durch das vorangegangene Gespräch geschürten, Ängste hinweg halfen. Merkte ich doch aus diesen Worten, wie gut wir uns verstanden. Dass aus den früheren Treffen, unter anderem auf unseren Tagungen an der Humboldt-Universität, aber auch auf zwei Tagungen (auch ein wichtiger Impuls auf dem Weg zum FIfF) der Bruder-/Schwester-Organisation des FIfF, des von Joe Weizenbaum in den USA initiierten Verbandes *Computer Professionals for Social Responsibility* (CPSR) eine enge freundschaftliche Bindung entstanden war. Schon aufgrund dieses Einvernehmens und der Freundschaft mit Christiane Floyd und sich herausbildender und festigender weiterer Freundschaften werde ich den Weg zum FIfF sicher nicht bereuen. Aber auch deshalb natürlich nicht, weil auch heute um die Sicherung des Friedens gerungen werden muss.

Es gilt vor allem das zu schaffen, was Albert Schweitzer in seiner Rede zur Verleihung des Friedens-Nobel-Preises den erforderlichen friedlichen Geist nannte, ohne den auch die geschaffenen Institutionen wie die UNO nicht wirksam werden können. Aber man gewinnt gerade gegenwärtig den Eindruck, dass sich ein großer Teil der Massenmedien daran beteiligen, die in der Bevölkerung vorherrschende friedliche Gesinnung abzubauen. So weist die Philosophin Susan Neiman in ihren Vortrag: „Moralische Klarheit für erwachsene Idealisten"[7] m.E. sehr zu Recht darauf hin, dass die Tat von Bundeskanzler Gerhard Schröder, Deutschland aus dem Irak-Krieg herauszuhalten, die doch Deutschland in der Welt eher Ansehen verschafft hätte, ganz offensichtlich von der Presse in Deutschland kleingeredet und nur als taktisches Wahlmanöver dargestellt wurde. Man könnte ergänzen, dass auch die militärische Zurückhaltung von Guido Westerwelle in seinem Wirken als Außenminister von einem großen Teil der Presse eher negativ beurteilt wurde, ihm zumindest kaum Lob einbrachte. Dagegen kann man durchaus verzeichnen, dass die Äußerung des Bundespräsidenten, mit der er ein größeres, auch militärisches Engagement Deutschlands bei internationalen Konflikten forderte, in großen Teilen der Presse ein positives Echo fand. Es ist aber, nachdem oben über die christliche Friedensarbeit in der DDR berichtetet wurde, nicht zufällig, dass ihm eine Gruppe von Pfarrern aus den neuen Bundesländern heftig widersprach und ihm vorwarf, dass er die Prinzipien der Friedensbewegung missachte.[8]

Von einem kreativen Ingenieur, Automatisierungstheoretiker und -praktiker wurde mir erst in jüngster Zeit eine E-Mail zugesandt, die sehr deutlich macht, wie die Bevölkerung wirklich über diese ständigen Versuche denkt, die Lehren aus der Vergangenheit zu überspielen oder direkt zu missachten. Er schrieb:

> *„Die Bundeswehr steht vor dem Einsatz von Kampftruppen in der Ostukraine. Deutsche Fallschirmjäger bereiteten sich in Seedorf bei Bremen darauf vor, die OSZE bei der Überwachung der Waffenruhe im Krisengebiet abzusichern.[9] … Diese Meldung hat mich sehr betroffen gemacht, schließlich ist mein Vater bei Stalingrad gefallen, und mein Großvater ist im ersten Weltkrieg in Russland umgekommen, und jetzt soll schon wieder die Enkelgeneration dorthin geschickt werden. Sicher muss die ausgehandelte Waffenruhe vor Ort auch überwacht werden, aber wegen unserer jüngeren Historie bitte nicht von deutschen Kampftruppen, die wahrscheinlich dort auch wenig Akzeptanz finden dürften. Für eine solche Mission gibt es in Europa genügend andere geeignete Länder (GB, F, S …) bzw. darüber hinaus die Blauhelme der UNO. Ich halte dieses Vorhaben der Kanzlerin und ihrer Verteidigungsministerin für einen staatspolitischen Kardinalfehler in der ohnehin verfahrenen Ostpolitik.*
>
> *Lieber Klaus, bitte bilde Dir hierzu Deine eigene Meinung, und vielleicht kannst Du das Problem in Deinem Freundes- und Bekanntenkreis thematisieren. Hierbei*

Klaus Fuchs-Kittowski

Prof. Dr. habil. **Klaus Fuchs-Kittowski** (Jahrgang 1934) ist Professor für Informationsverarbeitung. Er war Leiter des Bereichs Systemgestaltung und automatisierte Informationsverarbeitung der Sektion Wissenschaftstheorie und Wissenschaftsorganisation der Humboldt-Universität zu Berlin. Er war Mitglied des TC 9 (Wechselbeziehungen zwischen Computer und Gesellschaft) der Internationalen Föderation für Informationsverarbeitung (IFIP) und langjähriger Chairman der WG 9.1 (Computer und Arbeit) des TC 9 der IFIP und ist Mitglied der Leibniz-Sozietät der Wissenschaften.

habe ich insbesondere auch an Deine Mitgliedschaft im „Deutschen Friedensrat" sowie im „Forum der InformatikerInnen für Frieden und gesellschaftliche Verantwortung" (FIfF) gedacht.

In der Hoffnung auf Deine politische Aktivität verbleibe ich mit vielen Grüßen aus Leipzig.

Werner"

Werner Kriesel spricht m.E. richtig von einer verfahrene Ostpolitik. Dazu sei daran erinnert, dass die in diesen Tagen zu Recht gefeierten mutigen Demonstranten, die vor 25 Jahren friedlich den Fall der Mauer erzwangen, in ihrer überwiegenden Anzahl bestimmte Ziele verfolgten. Sie forderten Reisefreiheit und wollten eine verbesserte, d. h. demokratische DDR. Sie wollten aber vor allem auch die Beendigung des Kalten Krieges, denn sie hofften damit eine allgemeine Abrüstung zu erreichen. Auch als eine Voraussetzung für die Wiedervereinigung. Nun zeigt die Geschichte, dass bei solchen historischen Umbrüchen selten das vollständig erreicht wird, was die eigentlichen Akteure der Bewegung erhofften. Die Chance für eine allgemeine Abrüstung, die mit dem Zusammenbruch des Ostblocks gegeben war, wurde leider nicht wahrgenommen. Was diesen Wunsch anbelangt, sind die Akteure der friedlichen Revolution von Beginn an betrogen worden. Vor einiger Zeit wurde das Buch von Alexander von Plato „Die Vereinigung Deutschlands – ein weltpolitisches Machtspiel – Bush, Kohl, Gorbatschow und die geheimen Moskauer Protokolle"[10] vorgestellt. Die Vorstellung wurde von keinem geringeren als dem ersten und letzten frei gewählten Ministerpräsidenten der DDR, Lothar de Maizière, vorgenommen. Er sagte dabei sehr viele aufschlussreiche Dinge, aber insbesondere, dass er und die ganze DDR-Delegation bis zum Schluss der 2 + 4 Verhandlungen darum gekämpft hätten, dass die Nato nicht auf das Gebiet der DDR ausgedehnt würde. Bis sie gemerkt hätten, dass Gorbatschow[11] diese Forderung schon längst aufgegeben hatte. L. de Maizière fügte dann hinzu: „Offensichtlich war schon genug Geld geflossen!" Heute hören wir, dass der Außenminister Hans-Dietrich Genscher dann versprochen habe, weiter keiner Ausweitung der Nato zuzustimmen. Sie erfolgte aber doch schrittweise, bis zu dem Versuch, auch noch die Ukraine einzubeziehen. Man hat also von vornherein auf die Ausdehnung des eigenen militärischen Machbereiches gesetzt und steht nun vor dem voraussehbaren, unglücklichen Ergebnis, dass beide Konfliktparteien in der Ukraine zu kriegerischen Mittel greifen.

Als nach dem II. Weltkrieg die UNO gegründet wurde, beschäftigte sie sich schon auf ihrer ersten Sitzung mit den Möglichkeiten der Kontrolle der Atomwaffen und ihrer möglichen Ächtung. Auch wir sollten heute, statt den Einsatz von Drohnen (sei es auch nur zur Beobachtung) mit Unterstützung deutscher Soldaten zu propagieren, zu allererst die Kontrolle dieser neuen Waffen fordern, um ein neues gefährliches Wettrüsten auf diesem Gebiet zu verhindern. Es gilt, wie dies von InformatikerInnen auch schon gefordert wurde, die Ächtung von Kriegsrobotern und mit Atomwaffen bestückten Drohnen zu erreichen.

Denn ein Leben in Frieden ist das höchste Menschenrecht!

Anmerkungen

1 Wenn hier insbesondere von der Friedensarbeit als Motiv für den Eintritt ins FIfF gesprochen wird, so war natürlich die Hinwendung zu den sozialen und gesellschaftlichen Wirkungen der modernen Informations- und Kommunikationstechnologien, die Beschäftigung insbesondere mit den Arbeiten von Ulrich Briefs, Wilhelm Steinmüller und Bernd Lutherbeck und die Diskussion mit ihnen ein ebenso starkes Motiv. Denn ich hatte eine Vorlesung zum Thema: „Informatik und Gesellschaft" begonnen und auch Dissertationsthemen zu Fragen des Datenschutzes in der Medizin, zu Problemen einer Persönlichkeitsentwicklung fördernden Arbeitsgestaltung im Zusammenhang mit dem Computereinsatz ausgegeben.

2 Klaus Fuchs, Günter Flach, Das erste Menschenrecht: ein sinnvolles Leben in Frieden, in: Hiroshima und Nagasaki. Verpflichtung zum Frieden. Informationen des DDR-Komitees für wissenschaftliche Fragen der Sicherung des Friedens und der Abrüstung, 3/1985, S. 2-18.

3 Werner Wittenberger, Die Entstehung der Christlichen Friedenskonferenz im Kontext von Weltpolitik: Ein unzeitgemäßer Beitrag zur Aufarbeitung der Vergangenheit, Die Deutsche Nationalbibliothek, im Internet unter dnb.d-nb.de abrufbar, Verlag Books on Demand, Norderstedt

4 Werner Wittenberger: Erwägungen über den „Kalten Krieg" als theologisches Problem. Ständige Kommission der Prager Christlichen Friedenskonferenz. Debrecen, Ungarn, 31. Okt. 2. Nov. 1958, CFK-Archiv, Prag, Ordsner AA 1958, Dok.6

5 Werner Wittenberger: Die Entstehung der Christlichen Friedenskonferenz im Kontext von Weltpolitik: Ein unzeitgemäßer Beitrag zur Aufarbeitung der Vergangenheit, Die Deutsche Nationalbibliothek, im Internet unter dnb.d-nb.de abrufbar, Verlag Books on Demand, Norderstedt, S. 205

6 Eine Überprüfung dieser Aussage im Gespräch, welches damalige Leitungsmitglieder mit Klaus Fuchs-Kittowski führten, ergibt glücklicherweise, dass das FIfF niemals vom Verfassungsschutz überwacht worden ist – lediglich eines dieser Leitungssmitglieder selbst sei zeitweilig Mitglied in einer als verfassungsfeindlich eingestuften Organisation gewesen und ist evt. deswegen überwacht worden.

7 Susan Neiman, Moralische Klarheit für erwachsene Idealisten, Herausgegeben von Julian Nida-Rümelin u. a. Philosophie und Politik XI, Philosophy MEETS Politics XI, Klartext, Kultur in der Diskussion Band 16, 2011, S.17

8 Markus Decker, Nach Gaucks Kriegsäußerungen – Ost-Pfarrer kritisieren Bundespräsidenten, Berliner Zeitung, Politik, 23.06.2014

9 Bundeswehr-Fallschirmjäger sollen nach einem Medienbericht die Mission der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) in der Ostukraine absichern. Nach internen Plänen seien 200 Soldaten für die Mission eingeplant, die Soldaten bereiteten sich in Seedorf auf den Einsatz vor, berichtete die „Bild"-Zeitung. 150 der Soldaten sollen demnach das Krisengebiet mit Drohnen überwachen, 50 weitere seien für den Schutz der OSZE-Vertreter vorgesehen. Das Verteidigungsministerium gehe davon aus, dass ein Bundeswehr-Einsatz in der Ostukraine mit bewaffneten Truppen vom Bundestag gebilligt werden müsste. (Quelle: n-tv.de , ppo/AFP/dpa)

10 Alexander von Plato: Die Vereinigung Deutschlands – ein weltpolitisches Machtspiel – Bush, Kohl, Gorbatschow und die geheimen Moskauer Protokolle, Ch. Links Verlag, Berlin. 2002

11 "Zusammenbruch des Vertrauens" Gorbatschow: Westen hat Zusagen von 1989 gebrochen, 08.11. 2014 14:33 dpa

Britta Schinzel

Mein Weg in die Informatik und in das FIfF

Nach der Matura interessierte ich mich für alle möglichen Berufe und Fächer und begann dann mit Philosophie, Physik, Mathematik. „Sehnsucht nach Objektivität", so formulierte es eine der in der DFG-Studie *Weltbilder Informatik* befragten Studentinnen, das war auch für mich der Grund, Philosophie rasch hintan zu stellen und mich mehr auf die anderen Fächer zu konzentrieren. In Innsbruck und Wien habe ich dann Mathematik und das Nebenfach Physik studiert und in Innsbruck bei Prof. Wolfgang Gröbner promoviert. In Innsbruck gab es auch den ersten Computer an einer österreichischen Universität, eine ZUSE Z 23, an der ich auch gerechnet habe. Nach dem Studium wollte ich weiter in diskreter Mathematik und nicht in Gebieten wie Statistik oder Numerik arbeiten und kam so in die junge deutsche Computerindustrie zu AEG-Telefunken, wo wir Compiler-Compiler entwickelten, das sind Übersetzer von höheren Programmiersprachen in eine Zwischensprache, BCPL, die Vorgängerin von C, von der dann das Übersetzungsprodukt ein für alle Mal auf Assemblerebene heruntergezogen wurde. Die Arbeitsrechner dort waren ein Hybridrechner TR 86 und eine Mainframe TR 440, die durch Operateure im Batch-Betrieb bedient wurden. Die Eingabe geschah mit 5-Kanal-Lochstreifen, die wir uns wie mehrreihige Ketten um den Hals hingen. (Das Markenzeichen der stolzen IBM-er waren die in die Brusttaschen gesteckten Lochkarten, als Notizzettel weiterverwendet.) Man gab einen aus handschriftlichen Aufzeichnungen von Stanzerinnen gestanzten Lochstreifen ab und erhielt nach 2-3 Tagen einen Ausdruck auf Endlospapier zurück, der vor allem aus syntaktischen Fehlermeldungen (Komma statt Semikolon, etc.) bestand. Wenn möglich, versuchte man den alten Lochstreifen durch eigenhändige Überstanzungen zu korrigieren und gab diesen dann wieder ab, bis der Prozess konvergierte. Damit war immer noch nicht gesichert, daß das Programm Sinnvolles leistete, also endlich auf Eingaben Ausgabedaten lieferte, aber auch dieser Prozess kam irgendwann zu einem Ende und stolz konnte man die Leistungen seines Programms bewundern.

Von den Lochstreifen führt ein direkter Weg zum Thema Frauen und Technik:

Hedy Lamarr, eine Wiener Schauspielerin (im Film *Ekstase* spielte sie 1933 die erste Nacktszene der Filmgeschichte) arbeitete mit Lochstreifen für Pianolas. Sie war vor ihrem österreichischen Ehemann Fritz Mandl 1937 nach Paris geflohen. Er war Waffenfabrikant, was später noch relevant wurde, und er war sehr eifersüchtig (er hatte deshalb auch alle Exemplare des Films *Ekstase* aufgekauft), und er hatte sie eingesperrt, denn sie galt als die schönste Frau der Welt. Von Paris fuhr sie über London nach Amerika und kam sofort mit größtem Erfolg bei Metro Goldwyn Meyer unter Vertrag, was äußerst ungewöhnlich war. Über ihre Film-Erfahrungen gibt es folgendes Zitat: „Any girl can be glamorous. All you have to do is stand still and look stupid."

Bei ihrer Beschäftigung mit Filmmusik hatte sie zusammen mit dem Komponisten Georges Antheil das Frequenzsprungverfahren zur Synchronisation von durch 16 Lochstreifen gesteuerten mechanischen Klavieren erfunden.

© Österreichische Post

Während des 2. Weltkriegs wollte sie die deutsche Marine bekämpfen, indem sie aufgrund ihrer von ihrem Ehemann erfahrenen Kenntnisse über Funktechnik dieses Frequenzsprungverfahren umnutzte und es der unverfolgbaren Steuerung von Torpedos anpasste. Diese Methode wird heute für jede Kommunikation zwischen mobilen Telefonen, Funknetzwerken und mobilem Internet eingesetzt, um sie störungs- und abhörsicher zu machen. Praktisch jedes Smartphone, jeder Laptop und jedes Navigationssystem operiert auf Basis dieser Erfindung.

Zurück zu AEG-Telefunken. Das Vorgehen beim Compiler-Compilerbau in Ulm war, wie man damals sagte, handgestrickt, d.h. methodenlos. Gleichzeitig entwickelte allerdings Prof. Günter Hotz auch von AEG-Telefunken Konstanz aus Elemente für eine mathematische Theoriebasis der Informatik, zunächst für die Schaltkreistheorie. Obgleich mir die Computerei gefiel, wollte ich doch mein Studium nicht ganz unter den Tisch fallen lassen und ging deshalb, wieder mein Gebiet wechselnd, nach vier Jahren Industrietätigkeit als Assistentin an die TH Darmstadt in die Theorie-Abteilung zu Prof. Walter, einem Hotz-Schüler. Hier wurde gerade der neue Studiengang Informatik aufgebaut, das Curriculum entwickelt und die sofort zahlreichen Studierenden in einer Mischung aus Mathematik und E-Technik unterrichtet. Mathematisch waren die Chomsky'sche Theorie der Formalen Sprachen und logische Semantik formaler Sprachen, die u. a. von John v. Neumann und McCulloch und Pitts begonnene Automatentheorie, sowie die logischen Grundlagen der Algorithmik, die Theorie rekursiver Funktionen. Ich hatte mir die Letztere als Habilitationsgebiet ausgesucht, was dort eine Nische war, denn mein Gebiet „Nummerierungen" wurde vor allem in den Ostblockländern, u. a. der DDR, im Rahmen der mathematischen Logik bearbeitet. Deshalb fand ich auch vor allem zunächst in der DDR und Polen Anklang und machte meine Erfahrungen mit den Beschränkungen, mit denen meine KollegInnen dort leben

mussten, und in Folge auch mit den Kommunikationsschwierigkeiten der weitestgehend verbotenen wissenschaftlichen Kontakte, die, wenn nicht auf Tagungen, in geheimen Treffen in Parks etc. stattfinden mussten. Briefe mussten an Privatadressen geschickt werden. Eine Ausnahme stellte die Universität Jena dar, wohin ich mehrfach eingeladen wurde. Aber die Humboldt-Universität Berlin durfte ich nicht betreten, obgleich ich mit dortigen Kollegen befreundet war, wofür sie sich sehr entschuldigten.

Die wissenschaftlichen Texte und Briefe wurden damals im Sekretariat, am Ende auf einer teuren IBM Kugelkopfmaschine, je nach verfügbarer Zeit von der Sekretärin des Chefs, oder abends und am Wochenende von uns selbst geschrieben.

Ich habilitierte mich an der TH Darmstadt in Theoretischer Informatik und mein Professor war stolz, dass unter seinen Fittichen eine Frau sich habilitierte. Es war eine Aufbruchzeit, die MathematikerInnen und E-TechnikerInnen, die sich für die Informatik entschieden hatten, viele Möglichkeiten bot. Auch ich bekam Rufe auf C3-Stellen und ich entschied mich 1981 für die RWTH Aachen.

Anfang der 80-er Jahre wurden die Mainframes und persönlichen Monitore an Timesharing-Maschinen zunächst ergänzt durch Homecomputer, wie der Name schon sagt, für Kochrezepte und Kalender gedacht. Später lösten Personal Computer die Mainframes weitgehend ab, eine Entwicklung, die niemand erwartet hatte. Mit der privaten Verbreitung erweiterten sich die Anwendungsfelder und so wurde auch die zuvor Frauen überlassene Software[1] sehr viel wichtiger als die bisher vorrangige und Männern vorbehaltene Hardware, was sich Mitte der 80er-Jahre auch in einem drastischen Einbruch der Frauenbeteiligung am Informatik-Studium niederschlug. In Aachen ging ihre Zahl von 24 % auf 10 % zurück. Im Folgenden gab es zwar arbeitsmarktabhängige Schwankungen, aber der ursprüngliche Frauenanteil wurde nie mehr erreicht[2]. Im Ostblock war das übrigens ganz anders, in der DDR gab es Anfang der 1980er-Jahre noch eine Frauenbeteiligung von 60-80 %, die mit der Wiedervereinigung auf 8 % herunterfiel[3]. Und in arabischen Ländern dominieren Frauen in der universitären Informatik[4], in ostasiatischen Ländern mit Ausnahme Japans sind sie weitgehend paritätisch vertreten. Heute sind die Informatik-Frauenanteile in Deutschland ein wenig gestiegen, aber sie sind vermutlich auf den höheren AusländerInnenanteil zurückzuführen. Immer schon haben die Ausländerinnen den Frauenanteil in der Informatik in Deutschland hinaufgedrückt.[5]

Inzwischen hatten wir je einen Monitor zum Timesharing-Mainframe oder einen Homecomputer am Arbeitsplatz. Für zu Hause wurden die kleinen Amiga, Commodore oder Atari angeschafft, mit denen man experimentieren und spielen, später auch Texte schreiben, Tabellen und Datenbanken anlegen konnte. Ab Mitte der 1980er-Jahre hatten wir bereits vernetzte PCs und Monitore auf den Schreibtischen, konnten unsere Texte in Wordstar allmählich selbst schreiben und die Sekretärinnen konnten sich zunehmend organisatorischen Aufgaben widmen. Und auf einmal konnten auch Männer tippen, während es vorher geheißen hatte, die beweglicheren Finger von Frauen seien dafür geeigneter. Heute können sogar dicke Würstelfinger kleine Handytastaturen bedienen. Es wurde möglich, über das USENET E-Mails zu schreiben und zu empfangen. Neben den proprietären Betriebssystemen von IBM, Mac und später Microsoft Windows gab es schon das (von den UNIX-Frauen mit entwickelte) Betriebssystem UNIX, das auch für das spätere Internet und die gesamte OpenSource Bewegung grundlegend war. Der Batch-Betrieb wurde abgelöst durch direkte Ein-/Ausgabe, sodass das Programmieren auf eigenen PCs – für Studierende in Rechnerpools – aufwandsärmer möglich wurde.

In Aachen begann ich interdisziplinäre Kooperationen mit den Ingenieurswissenschaften, Wirtschaft, Medizin, Biologie, Materialforschung und Linguistik etc. Diesen Weg in die Praxis nahm ich über die Künstliche Intelligenzforschung (KI), in Fortsetzung der Darmstädter Arbeit am rekursionstheoretischen Lernmodell, der Induktiven Inferenz. So hatten wir viele Expertensystemprojekte (eins zur Haltbarkeit von Kunststoffen in unterschiedlichen Einbettungsmaterialien, eins zur geschmacklich konstanten Schokoladeproduktion bei Lambertz, eins zu ökonomischen Simulationen), Robotikprojekte der Bewegungsgeometrie im Maschinenbau, Wissensbasierte Systeme in der Neuroanatomie, neuronale Netze zur Simulation von Sehleistungen, lernende Systeme und neuronale Netze, Bildgebung für die Medizin, etc. Dabei lernte ich auch den Lehrstuhlinhaber für Bildverarbeitung Dietrich Meyer-Ebrecht kennen, der Bildverarbeitungsmaschinen für die Medizin entwickelte. Er machte mich auf die zweite FIfF-Jahrestagung aufmerksam, wohin wir dann fuhren. Dort traf ich meine alten Kollegen aus Darmstadt und war fortan angefixt, denn es traf zusammen mit meiner Beschäftigung mit philosophischen Aspekten und gesellschaftlichen Wirkungen der KI. So bestellte ich zunächst die FIfF-Kommunikation, deren Beiträge mich sehr beeindruckt hatten und mir auch für meine Lehre halfen. Wenige Jahre später trat ich dem Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) bei.

Britta Schinzel

Britta Schinzel stieg nach ihrem Studium der Mathematik und Physik in die Compiler-Entwicklung in der deutschen Computerindustrie ein. Von dort wechselte sie in die Theoretische Informatik an der TH Darmstadt und habilitierte 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.

Mit der Kompetenz, die ich nicht zuletzt auch beim FIfF erworben hatte, bekam ich einen Ruf an die Universität Freiburg ans Institut für Informatik und Gesellschaft, wo ich bis zu meiner Pensionierung blieb. Damit endete zwar nicht meine Tätigkeit als Informatikerin, aber jetzt mein Text.

Tja, und ich wurde sogar im FIfF aktiv und wurde mehrfach in den Vorstand gewählt. Für dieses Vertrauen danke ich Euch sehr!

Anmerkungen

1 *Nicht nur wurde das erste Programm von einer englischen Gräfin geschrieben, auch der erste industriell gefertigte Computer Mark I wurde von Frauen programmiert. Die erste Programmiersprache COBOLwurde wesentlich von Marine-Leutnant Grace Hopper entwickelt. Das erste Standardwerk über Programmiersprachen wurde von Jean Sammet geschrieben, die ebenfalls im Standardisierungskommitte für COBOL saß und die Programmiersprache FORTRAN und die mathematische Formelsprache FORMAC mit entwickelte. Sie war Vorsitzende der SIGPLAN innerhalb der ACM und wurde später Präsidentin der ACM.*

2 *Schinzel, Britta: Kulturunterschiede beim Frauenanteil im Studium der Informatik (2005) Teil II: Frauen im Informatikstudium in Deutschland vor und nach der Wiedervereinigung; http://mod.iig.uni-freiburg.de/cms/fileadmin/publikationen/online-publikationen/Informatik.Frauen.Deutschland.pdf*

3 *Schinzel, Britta: Kulturunterschiede beim Frauenanteil im Studium der Informatik (2005) Teil III: Partikularisierung der Informatik Frauenbeteiligung; http://mod.iig.uni-freiburg.de/cms/fileadmin/publikationen/online-publikationen/Frauenbeteiligung.Informatikstudien.pdf; Teil IV: Abschließende Interpretation und Literaturangaben; http://mod.iig.uni-freiburg.de/cms/fileadmin/publikationen/online-publikationen/Informatik.Kultur.Literatur1.pdf*

4 *Schinzel, Britta: Kulturunterschiede beim Frauenanteil im Studium der Informatik (2005) Teil I: Frauenanteil Computer Science International; http://mod.iig.uni-freiburg.de/cms/fileadmin/publikationen/online-publikationen/Frauenanteil.Informatik.International.pdf*

5 *Schinzel, Britta: Kulturunterschiede ... (2005) Teil II; s.o.*

Dirk Siefkes

Mein Weg mit dem FIfF

Von ökologischer zu kultureller Theorie der Informatik

Meinen Weg ins FIfF – von Mathematik zu Ökologie – habe ich in der kurzen Notiz in diesem Heft (Sie14c) skizziert (Sie82-95). In den 80er Jahren redete ich bei Treffen der GI oft mit Wolfgang Coy. Beide Theoretische Informatiker, waren wir uns einig: Diskrete Mathematik liefert gute Grundlagen für die Kerninformatik (so wie stetige für die Technische), aber nicht für Anwendungen. Da geht es um soziale Voraussetzungen und Folgen, da müssen Humanwissenschaften her. Also initiierte er ein interdisziplinäres Projekt Theorie der Informatik*, in dem wir – Informatiker und andere – 1988-92 an einer solchen Theorie arbeiteten (TdI92). Angeregt dadurch führten wir in meiner Gruppe 1993-97 ein Projekt* Sozialgeschichte der Informatik *durch (SGI97f). Gemeinsam mit Soziologen, Psychologen, Semiotikern und anderen lasen wir frühe Texte zu Computer und Informatik und sahen, dass alle – Wissenschaftler wie Entwickler – beim Umgang mit Computern Mensch und Maschine „in eins sehen", hybridisieren. Dieses durchgängige „Orientierungsmuster" (Ale77) leckt von der Praxis in die Wissenschaft; das macht Informatik so faszinierend (Siefkes in SGI98, Sie14b).*

2001 nahmen Frieder Nake, Arno Rolf und ich die Arbeit an der Theorie der Informatik wieder auf (TdI01ff, Sie12a). In drei Arbeitstagungen einigten wir uns auf TdI als „eine Position von außen, die von innen getragen wird" (Sie07), d.h. von Informatikern, die ihr Gebiet von innen *und* außen erforschen, gemeinsam mit Humanwissenschaftlern. Dann trennten sich unsere Wege; ich arbeitete an einer „kulturellen TdI" (Sie02ff): Wie wechselwirken unsere Vorstellungen und Gewohnheiten von geistigen Tätigkeiten mit solchen von Maschinenabläufen? Wie beeinflusst das die Entwicklung von IT und von Informatik? Wie die unserer Kultur? Wie wechselwirken so Informatik und Kultur? Diese Arbeit skizziere ich jetzt.

Kulturelle Theorie der Informatik

Nach *Gregory Bateson* lässt sich jede Entwicklung beschreiben – und nur so verstehen – als eine „Zick-Zack-Leiter der Dialektik von Form und Prozess" (Bat79, p. 215ff). Für die *biologische Evolution* sieht das so aus: *Leben* ist Prozess; Lebewesen entstehen, verändern, entwickeln sich, vergehen. *Gene* sind Form; sie geben Lebewesen ihre Eigenart, prägen ihr Leben, werden an Nachkommen weitergegeben. Abgesehen von der primitivsten Ebene schlägt sich Leben in Sequenzen von Genen nieder, die in neuer Umgebung neues Leben auslösen können. Beim einzelnen Lebewesen ist die Entwicklung bis auf Abnormitäten durch die Gene vorgegeben, auf den höheren Ebenen (Familien, Gruppen, Ökosysteme usw.) verändert sich der „Genpool" durch zufällige Kombinationen. *Bateson´s These:* Geistige Entwicklung des Menschen „folgt denselben Prinzipien": *Denken* ist Prozess; Gedanken kommen und gehen, verändern sich, wir entwickeln sie. *Begriffe* sind Form; sie prägen unser Denken, geben ihm seine Eigenart, lassen sich mitteilen, erinnern, verwenden. Deswegen nennt Bateson die Form in der Entwicklung ihren *Code*: Die Eigenart von Lebewesen ist in ihren Genen „codiert", die Eigenart unseres Denkens in den Begriffen, die wir benutzen. Wir nehmen nicht die Welt selber wahr, sondern die Veränderungen, die bei solchen Wechselschritten von Codierung/Decodierung entstehen. „Information is the difference which makes a difference" (Bat79, p. 76). Für Bateson ist das eine Analogie; biologische Evolution ist nicht Vorbild, erst recht nicht Träger menschlicher Entwicklung.

Die These ist umfassender als es so klingt. Geist (*mind*) ist bei Bateson nicht rational; es umfasst alles, was Lebewesen brauchen, um mit der Umwelt umzugehen: neben Denken im engeren Sinn sinnliche Wahrnehmung (perception) und Gefühle (emotions), mit denen wir auf Wahrnehmung reagieren. Mind besteht nicht für sich, es ist Teil eines lebendigen Körpers, entwickelt sich mit ihm (Joh87). Lebendiges hat nicht Geist, es ist Geist. Geist und Natur, eine notwendige Einheit – so der Titel von (Bat79).

Weil es bei Bateson fehlt, buchstabiere ich die Analogie auch für emotionale und soziale Entwicklung aus (Sie92ff, s. auch Cio97): *Fühlen* ist Prozess; Gefühle kommen und gehen, verändern sich, wir können sie steuern oder auch nicht, sie bewegen uns. *Werte* (gut und schlecht, gut und böse, schön und hässlich,...) sind Form; sie kennzeichnen unsere Gefühle, prägen unseren Umgang mit ihnen, verändern sich dabei. *Tun* ist Prozess; wir kommunizieren, arbeiten, schlafen. Das prägt die Form unserer *Fähigkeiten* und *Gewohnheiten,* und umgekehrt. Und die drei Entwicklungen sind verflochten wie tierisches und pflanzliches Leben, beeinflussen sich gegenseitig auf vielfältige Weise, ob wir es wollen, glauben, wahrnehmen oder nicht.

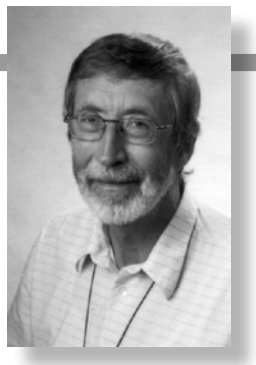
Entwicklung verstehen wir daher, wenn wir die *Muster* suchen, die die Stufen in diesen Schritten verbinden. „The pattern which connects" („das Muster, das verbindet" oder „zusammenhält") bietet Bateson als alternativen Titel für sein Buch an (Bat79, p.8). Dadurch bin ich auf *Christopher Alexander* gestoßen, der Entwicklung als Musterbildung sieht (Ale77; Sie07ff). Ein *Muster* ist eine Folge ähnlicher Phänomene, erzeugt von einem *Generator*, der jeweiligen Situation angepasst. Die Folge entsteht durch zeitliche oder räumliche Schritte, durch den historischen oder vergleichenden Blick; „context is pattern through time" (Bat79, p.15) or space. Nehmen wir umgekehrt ein Muster wahr, können wir es durch seinen *Kern* beschreiben, der in all den Phänomenen steckt. Kern und Generator sind dasselbe, aus unterschiedlicher Sicht (vom Generator auf das Muster, vom Muster auf den Kern). Entwicklungspsychologen nennen den Generator eines Verhaltensmusters *Schema* (Ste95, Sie99ff).

Muster hängen von der Umgebung ab: sie liefert die Situationen, in denen die Phänomene erscheinen, die wir als ähnliche wahrnehmen. Umgekehrt beeinflussen Muster ihre Umgebung; wir können eine Umgebung durch die Muster charakterisieren, die sie zulässt. Die Umgebungen biologischer Evolution sind die Lebensräume, die wir betrachten – die Region, in der eine Herde lebt, der Bereich einer Art oder Rasse, die ganze Erde. Die Umgebungen der Entwicklung eines Menschen sind die sozialen Gruppen, an denen er teilhat: Familien- und Freundeskreise, Arbeitsplätze, Reise- und Urlaubszirkel, Hobby-Gruppen etc. Menschen und ihre „kleinen Systeme" (Sie82ff) konstituieren sich gegenseitig; der Mensch ist ein „relationales Wesen" (Ger09). Ebenso, wenn auch auf andere Weise, wechselwirken die kleinen Systeme mit ihren größeren Umgebungen – Firmen, Vereine, Verbände, Städte, Institutionen, Länder. Jede dieser Umgebungen hat ihre „Kultur", ihre emotionalen, geistigen und sozialen Muster (Sie82ff).

In dem Sinn sehe ich biologische Evolution und *kulturelle Entwicklung* als analog. Und in dem Sinn habe ich gesagt: Informatik ist nicht nur eine Wissenschaft; sie ist eine kulturelle Entwicklung. Informationstechnik (IT), um die es in der Informatik geht, bestimmt zunehmend unsere Kultur; diese Kultur steuert den Kurs der Informatik; diese wiederum entwickelt sich in, wenn auch undurchsichtiger und widersprüchlicher, Wechselwirkung mit IT. So bin ich auf unserer Suche nach einer allgemeinen Theorie der Informatik (s.o.) auf den kulturellen Pfad geraten (Sie97ff).

So verstehe ich auch die Bedenken derer, die die Rolle der IT in der Entwicklung unserer Kultur mit Sorge sehen. Ich nenne Muster *starr*, wenn ihre Phänomene nicht nur ähnlich, sondern gleich sind, oder doch leicht aus den vorhergehenden bestimmbar; Muster des anderen Extrems, deren Phänomene sich nicht ähneln, sondern willkürlich variieren, nenne ich *chaotisch*; Muster dazwischen – die Phänomene variierend mit der Situation, aber ähnlich – nenne ich *lebendig*. Von Computern erstellte Muster sind starr, zufällig erzeugte chaotisch (Sie07ff). Die Frage ist: Werden unsere Verhaltensmuster starrer, wenn wir IT benutzen? Lässt sich so der Unterschied zwischen unserer Generation und der nächsten, zwischen „digital natives" und „digital immigrants" (Hyp12, Sie13a,b) verstehen? Wie gehen wir mit solchen Veränderungen um? Ist die derzeitige Entwicklung eine „digitale Revolution", vergleichbar mit der industriellen vor 200 Jahren?

Dirk Siefkes



Dirk Siefkes ist seit 1973 Professor für Theoretische Informatik an der TU Berlin. Die Beschäftigung mit mathematischen Theorien von Computern und Programmierung brachte ihn dazu, an einer allgemeinen Theorie zu arbeiten, die die Informatik mit den Kulturwissenschaften verknüpft. 1988 gründete er mit anderen Informatikern eine Initiative, die sich der Suche nach einer solchen Theorie widmet. In den 90er Jahren leitete er ein Interdisziplinäres Forschungsprojekt „Sozialgeschichte der Informatik" und ein Studienreformprojekt „Geschichte als Zugang zur Informatik". Seit 2003 ist er emeritiert.

Kunst

Besonders drängend stellen sich die Fragen in der Kunst, die sich ja mit aktuellen Phänomenen, also heute mit IT, auseinandersetzen will. „Computerkunst" begann in den 60ern mit „algorithmischer Kunst" (Lie09, Man11, Nak09ff): Künstler denken sich eine Zeichnung, beschreiben sie formal, erstellen daraus ein Programm, mit dem der Computer die Zeichnung auf einem „Plotter" ausdruckt. Die Künstler sind also nur denkend tätig, die Ausführung (der handwerkliche Teil) wird dem Computer überlassen. Die daher fehlende künstlerische Intuition wird durch den Zufall ersetzt: an vorgegebenen Stellen „würfelt" das Programm (mathematisch) und verfährt entsprechend. Es gibt also kein Kunstwerk im klassischen Sinn, sondern eine ganze Klasse von Werken: bei jedem Durchgang druckt der Computer etwas anderes. Daher haben für mich die einzelnen Ausdrucke etwas Starres, die Klasse wirkt chaotisch. Weiter verbreitet sind inzwischen Verfahren, in denen Mensch und Computer sich die Arbeit teilen: „computergestützte Kunst" (Künstler malen z. B., scannen das Bild ein und bearbeiten es auf dem Computer weiter), „Installationen" (das Werk, z. B. ein Bild oder ein technisches Arrangement, verändert sich, während wir es betrachten), „interaktive Installationen" (Veränderungen werden durch unsere Bewegungen ausgelöst). Mehr z. B. in (Lie09).

Persönlich finde ich in der algorithmischen, wie in jeder Kunst Schönes und Hässliches, Langweiliges und Anregendes bunt gemischt. „Aber ist es Kunst?" (Fre01, Sie14a; auch schon Ben63) Die Künstler wenden sich ja nicht direkt an den Betrachter, sondern an den Computer; sie haben keine „Botschaft" (Nak13a,b). „Unsere Botschaft ist: Wir können das jetzt alles mit dem Computer," hat Frieder Nake mir einmal gesagt. Aber können solche Werke, in denen der Code (im Sinne Bateson's) weitgehend von Computer und Zufall bestimmt ist, andere als starre bzw. chaotische Muster auslösen? Beeinflusst algorithmische Kunst die Entwicklung der Beteiligten (Künstler wie Betrachter)? Spielt sie eine Rolle in der kulturellen Entwicklung heute? Die Akteure sprechen heute nicht mehr von algorithmischer Kunst, sondern von z. B. „information aesthetics" (M&N14). Ob das Kunst ist oder etwas ganz Neues, soll die Gesellschaft entscheiden. Aber warum rufen dann einige das Ende herkömmlicher Kunst aus, auch der modernen? „Als die Algorithmen schreiben lernten" (Bun12), besser: als man lernte, auf dem Computer mithilfe von Parametern und Zufall gewisse Gutachten und Romane zu erstellen, hat niemand vom Ende der Poesie und Literatur gesprochen. Kunst entwickelt sich mit der Kultur, und Entwicklung lebt von der Vielfalt (Bro79).

Auf dem genannten Workshop ging es insbesondere um die digitale Codierung von Bildern. Kann man Bilder so codieren, dass sie dem Computer zugänglich sind, d.h. dass er sie reproduzieren (Ben63!), vergleichen, ähnliche finden kann, aber auch dem Menschen, der sie wiedererkennen, einordnen, bewerten will? Die übliche pixelweise Codierung leistet das nicht. Eine solche Codierung müsste beim Menschen gleichermaßen das konzeptionelle Denken wie die sinnliche Wahrnehmung ansprechen und so eine geistige Entwicklung, eine „Evolution" auslösen. Aber ist das möglich? In dem Projekt „Sozialgeschichte der Informatik" (s.o.) haben wir Programme und andere Zeichen, mit denen wir im Computer Aktionen auslösen, „Hybridobjekte" und „selbstbewegend" genannt: Wir lesen sie gleichzeitig als Signale an den Computer, die dort automatisch Schritte auslösen, wie als Texte, die die Schritte beschreiben, als wenn Menschen sie ausführten. Frieder Nake nennt solche Zeichen „algorithmisch"; sie haben eine Ober- und eine Unterseite, die sie dem Menschen bzw. dem Computer zuwenden (Nak01). Christiane Floyd nennt sie „autooperationale Form" (Flo97). Alle drei etwa gleichzeitig, unabhängig voneinander! Um Bilder von Künstlern digital zu codieren, müsste man also eine algorithmische Sprache entwickeln, die das, was Künstler schaffen wollen, hybrid beschreibt. Man müsste das, was man mit IT für die Arbeit, dann für Organisation, für Unterhaltung, fürs Spiel und für immer weitere Bereiche geleistet hat, für die darstellende Kunst erreichen. Insbesondere müsste man den „Dreischritt" von De-, In-, Konstruktion, in dem man Arbeitsprozesse auf den Computer bringen sollte (C&H09, Ses09, Sie07,14a), auf die Kunst übertragen: die künstlerische Tradition analysieren, das Werk programmieren, das Ergebnis „kunstverträglich" machen.

Bilder lösen bei verschiedenen Menschen oft ganz verschiedene Reaktionen aus; also müssten die Codierungen das auch leisten. Aber alle Computer würden auf ein codiertes Bild gleich reagieren. Die Evolution des Menschen, biologische wie kulturelle, käme zum Stillstand, wenn alle Männer auf eine Frau, alle Frauen auf ein Kind, alle Kinder auf eine Katze, alle Katzen auf einen Mann gleich reagierten. (Diese Feststellung verdanke ich meiner Frau, auch unser Kater hat sich eingemischt; beiden danke.) Anders ausgedrückt: Computermuster sind starr, Zufallsmuster chaotisch, menschliche Muster hoffentlich weder noch; Computer und Würfel können Entwicklung beeinflussen, aber nicht tragen. Also kommt es in der Kunst, wie überall, auf die Rolle an, die wir Computern zubilligen, Maschine, Werkzeug oder Partner (C&H01f; Sie07ff). Dann können wir auch mit Computerkunst eine „neue Realität" (Flo92) schaffen.

Dirk Siefkes

Mein Weg ins FIfF

Mein Weg ins FIfF begann – wie viel Gutes in meinem Leben – mit meiner Frau und einem Zufall: Ich hatte in Mathematischer Logik promoviert und übernahm 1973 eine Professur für Theoretische Informatik (THI) an der TU Berlin. Meine Wissenschaft war formal, mit Technik, Praxis, gar Politik hatte ich nichts im Sinn. In den USA gerieten wir zufällig in einen Kurs „Literature of Ecology". Ich befasste mich mit ökologischen Systemen, übertrug deren Entwicklungsprinzipien auf menschliche und kreierte „kleine Systeme": soziale Gruppen, die sich flexibel entwickeln, nicht erstarrt wie eine tote Partnerschaft oder eine verregelte Massenveranstaltung, aber mit gemeinsamer Basis; feste Beziehungen, aber offen für Neues. Daheim führte ich Seminare zu ökologischem Denken und formalem Arbeiten ein. Später machte ich auch große Lehrveranstaltungen „klein": Tutorien waren nicht Übungen, sondern Arbeitsplatz, Vorlesung wurde „Nachlese". Und ich wurde „politisch". Als Kollegen das FIfF gründeten, weil die Gesellschaft für Informatik (GI) ihren Protest gegen automatische US-Abwehrsysteme unterdrückte, wurde ich Mitglied. Seit Gründung bin ich Mitglied im FIfF-Beirat. Arbeit und Leben hat das stark beeinflusst. Danke.

Referenzen

(Ale77) Christopher Alexander: A Pattern Language: Towns, Buildings, Construction. New York: Oxford UP.

(Bat79) –"- : Mind and Nature – a Necessary Unity. Bantam Books. Deutsch: Geist und Natur – eine notwendige Einheit. Suhrkamp 1982.

(Bau01) K. Bauknecht et al. (Hg.): Informatik 2001, Jahrestagung GI & OCG. Workshop „Erkenntnistheorie – Semiotik – Ontologie". Österreich. Computergesellschaft, Wien.

(Ben63) Walter Benjamin: Das Kunstwerk im Zeitalter der technischen Reproduzierbarkeit. Ed. Suhrkamp 28.

(Bro79) Urie Bronfenbrenner: The ecology of human development. Harvard University Press.

(Bun12) Mercedes Bunz: Die stille Revolution. Suhrkamp, edition unseld 43.

(Cio97) Luc Ciompi: Die emotionalen Grundlagen des Denkens. Entwurf einer fraktalen Affektlogik. Vandenhoeck.

(Coy12) Andrea Knaut et al.: Per Anhalter durch die Turing-Galaxis. Münster: MV-Wissenschaft. <http://turing-galaxis.de/torrentz/42/Per-Anhalter-durch-die-Turing-Galaxis.epub>

(C&H01) Cecile Crutzen, Hans-Werner Hein: Die bedenkliche Dienlichkeit und Sicherheit von Softwaresystemen und die erlebte Verlässlichkeit. In (Bau01), S. 782-787.

(C&H09) –"- : Dekonstruktion und Konstruktion. In (TdI09).

(Flo92) Christiane Floyd et al (eds.): Software Development and Reality Construction. Springer.

(Flo97) Christiane Floyd: Autooperationale Form und situiertes Handeln. In C. Hubig (Hrsg.): Cognitio humana – Dynamik des Wissens und der Werte. XVII. Deutscher Kongress für Philosophie, Vorträge und Kolloquien, S. 237-252.

(Fre01) Cynthia Freeland: But is it art? Oxford University Press.

(Ger09) Kenneth J.Gergen: Relational Being. Beyond Self and Community. Oxford University Press.

(Hyp12) Martin Warnke et al.: Digital Nativity – die Normalität des Digitalen. HyperKult XXI, Conf. Uni Lüneburg, 12.-14.7.2012.

(Joh87) Mark Johnson: The Body in the Mind. University of Chicago Press.

(Lie09) Wolf Lieser: Digital Art. h.f.ullmann, Tandem Verlag.

(Man11) Lev Manovich: Cultural Software. Manuskript. www.manovich.net

(M&N14) -"- , Frieder Nake: Cultural Analytics, Information Aesthetics, and Distant Readings. Workshop MECS Uni. Lüneburg, org. Martin Warnke et al., July 2014.

(Nak01) Frieder Nake: Das algorithmische Zeichen. In Bau01, S.736-742.

(Nak09) -"- : Was ist digitale Kunst? Wurzeln und Zufall – Eine Sicht der Anfänge digitaler Kunst. In (Lie09), S. 10-25, 46-51.

(Nak13a) -"- , Susan Grabowski: No message whatsoever. Exhibition Dam Gallery Berlin, 15.11.13-25.1.14.

(Nak13b) -"- & Friends: Licht ins Dunkel, 25x50 Jahre Computerkunst. Exhibition Gallery HfK Bremen, 25.-28.12.13.

(Ses09) Werner Sesink: Zur bildungstheoretischen Bedeutung des Diskurses zwischen Pädagogik und Informatik. In (TdI09).

(SGI97) Peter Eulenhöfer et al.: Die Konstruktion von Hybridobjekten als Orientierungsmuster in der Informatik. TU Berlin, FB Informatik, Bericht 97-23.

(SGI98) -"- : Sozialgeschichte der Informatik. FIfF-Kommunikation 2/98, S. 3-4, 28-48.

(Sie82) Dirk Siefkes: Kleine Systeme. TU Berlin, FB Informatik, Bericht 82-14. Engl.: Small Systems. Purdue University, Computer Science, CSD-TR 435, 1983.

(Sie92) -"- : Fish in Schools or Fish in Cans. Evolutionary Thinking and Formalization. International Computer Science Institute Berkeley, TR-92/009.

(Sie94) -"- : Zu einer ökologischen Theorie der Informatik. TU Berlin, FB Informatik, Bericht Nr. 94-18, 45 S. – „Arbeitsübersicht" in FIfF-Kommunikation 94/3, S. 25-27.

(Sie95) -"- : Ökologische Modelle geistiger und sozialer Entwicklung. Beginn eines Diskurses zur Sozialgeschichte der Informatik. Wissenschaftszentrum Berlin für Sozialforschung, Bericht FS II 95-102.

(Sie99) -"- : Die Rolle von Schemata in der Informatik als kultureller Entwicklung. TU Berlin, FB Informatik, Bericht 99-6.

(Sie01) -"- : Informatikobjekte entstehen durch Hybridisierung. In (Bau01), S. 798-803.

(Sie02) -"- : Sozialgeschichte und kulturelle Theorie der Informatik. TU Berlin, Fak. Elektrotechnik & Informatik, Bericht 02-16.

(Sie03) -"- : Semiosis as Evolution. Development of Mind and Culture in Computer Science. In M. Bax et al. (eds.): Semiotic Evolution and the Dynamics of Culture. Peter Lang, Bern, 2004, pp. 69-88.

(Sie07) -"- : Theorie der Informatik zwischen den Stühlen. Gegensätze in der Informatik durchmustern und füreinander fruchtbar machen. TU Berlin, Fak. Elektrotechnik & Informatik, Bericht 07-21.

(Sie09,14) -"- : Darwin als Helfer am Computer. Wie wir vermeiden, dass Informationstechnik unsere Lebensmuster bestimmt. Manuskript, 10 S.

(Sie12a) -"- : Inseln einer Theorie der Informatik. Wolfgang Coy zum 65. Geburtstag. In Coy12, S. 61-68.

(Sie12b) -"- : Wohlfühlen mit IT? FIfF-Kommunikation 29. Jahrgang, 4/2012, S. 17-20.

(Sie13a) -"- : Glauben, Wissen, Können, Müssen – und Wollen. Wie wir mit Digital Natives eine nicht normierte Informatik gestalten können. Abstract Hyp13, 2 S.

(Sie13b) -"- : Digital Natives in Symbiosis with IT-systems? Abstract, Conf. „Futures Past: Design and the Machine", MIT, November 21-23, 2013; 1 S.

(Sie14a) -"- : But is it art? Only what has been thought machinelike, can be brought onto the machine. Abstract for (M&N14).

(Sie14b) -"- : What is so fascinating with Computer Science? How we, Informaticians and others, deal with CS. Session, STS-conference Graz, Mai 2015.

(Sie14c) -"- : Mein Weg ins FIfF. FIfF-Kommunikation 4/2014, S. 53

(Ste95) Daniel N. Stern: The Motherhood Constellation. Basic Books. Deutsch: Die Mutterschaftskonstellation. Klett-Cotta 1998.

(TdI92) Wolfgang Coy, Frieder Nake, Jörg Pflüger, Arno Rolf, Jürgen Seetzen, Dirk Siefkes, Reinhard Stransfeld (Hg.): Sichtweisen der Informatik. Vieweg.

(TdI01) Frieder Nake, Arno Rolf, Dirk Siefkes (Hg.): Informatik – Aufregung zu einer Disziplin. Tagung zur Theorie der Informatik 2001. Uni Hamburg, FB Informatik, Bericht 235.

(TdI02) -"- : Wozu Informatik? Theorie zwischen Ideologie, Utopie, Phantasie. Tagung zur Theorie der Informatik 2002. TU Berlin, Fak. Elektrotechnik & Informatik, Bericht 02-25.

(TdI03) -"- : Informatik zwischen Konstruktion und Verwertung. Tagung zur Theorie der Informatik 2003. Uni Bremen, FB Mathematik & Informatik, Bericht 1/04.

(TdI09) Andreas Möller, Frieder Nake, Arno Rolf, Dirk Siefkes: Beiträge zu einer Theorie der Informatik. Zum kritischen Selbstverständnis einer Disziplin. E-Journal Communication, Cooperation, Participation, Heft 5 (Sonderausgabe), 08/2009. http://195.37.26.249/ijsc/en/special_edition.php

---

Zu meinen Publikationen siehe auch *http://tal.cs.tu-berlin.de/siefkes*

Dagmar Boedicker

Unsicherheit und Institutionen

Schaffen die (inter-)nationalen Institutionen Sicherheit?

Die meisten unserer demokratischen Institutionen[1] stammen aus der Zeit ab der französischen Revolution, sind alt und erprobt. In den Epochen von Demokratisierung, Industrialisierung und Globalisierung haben sie sich gewandelt und bewährt. Institutionen sollten uns ein Gefühl der Sicherheit geben, weil wir ihnen vertrauen. Ist das noch so? Es findet eine Bedrohungsdebatte statt. Treiber sind nicht nur politische Interessen, auch geopolitische, sondern auch die Medien („crime sells"). Gefahren werden unterschiedlich gewichtet, Vorschläge zu ihrer Abwehr umfassen finanzielle Mittel, Forschung, Überwachung, mehr oder weniger Zusammenarbeit oder Markt, neue Institutionen, Rechtsbrüche oder neue Gesetze und viele andere, unterschiedlich überzeugende und teils widersprüchliche Maßnahmen.
Mein Eindruck ist, dass manche unserer Institutionen dem 21. Jahrhundert nicht mehr gewachsen sind und wir neue brauchen, mindestens aber die alten reformieren müssen. Mit diesem Beitrag versuche ich, Schwächen der alten, Perspektiven für neue oder neu gestaltete, und die Beziehung zum FIfF darzustellen. Es ist ein Versuch, über den ich sehr gerne mit Ihnen und Euch diskutieren würde.

Alte Gefahren, die bereits im 20. Jahrhundert erkennbar oder vorhersehbar waren

Deutschland – wenigstens der BRD – ging es nach dem 2. Weltkrieg bald wieder gut, auch vielen europäischen und den westlichen Industriestaaten. Im letzten Viertel des 20. Jahrhunderts wurde für uns einiges fühlbar, was die Menschen in Schwellen- und Entwicklungsländern schon erlebten: Luft- und Wasserverschmutzung, Kriege, *ethnische Säuberungen,* Flucht und Vertreibung, Rechtsextremismus und Terrorismus, Inflation und Spekulation, Verschuldung, Verlust von Arbeit durch Rationalisierung, Industrie- und Naturkatastrophen, Sozialabbau, organisierte Kriminalität (OK) mit Drogen-, Menschen- und Waffenhandel, Überwachung.

In Deutschland konnten wir uns trotzdem sicher fühlen: Bhopal liegt in Indien, die Mafia trieb ihr Unwesen jenseits der Alpen, gefoltert wurde in Lateinamerika, im Gulag und der Volksrepublik China, Kriege tobten weit weg in Afrika und Asien. *Unsere* Unternehmen waren anständig und solide, die Rente sicher, unsere Politiker nicht korrumpierbar. Gegen die Volkszählung wehrten wir uns mit demokratischen Mitteln und erfanden den Datenschutz. Rationalisierung ließ unsere Wirtschaft wachsen. Zwangsarbeit, Ausbeutung, Drogenhandel, das schien es bei uns nicht zu geben. Ende des Jahrhunderts allerdings begründete neoliberales Denken Deregulierung und Privatisierung und verbrämte den Abbau des Sozialstaats als Eigenverantwortung. Im nahen Balkan fanden Krieg und Ethnozid statt, in Europa! Der GAU in Tschernobyl setzte Radioaktivität in Bewegung, zu uns!

Neue Gefahren

Keine der *alten* Gefahren hat sich erledigt, die meisten haben sich verschärft, und es sind neue hinzugekommen. Klimawandel, Hunger, Wasserknappheit und Erosion der Bodenfruchtbarkeit, postkoloniale und asymmetrische Kriege, Epidemien, verschärfte Spaltung der Gesellschaften in Arm und Reich, Schulden- und Finanzkrise, Erosion demokratischer Systeme.

Der Rechtsextremismus hat feste Wurzeln geschlagen, national und international, auch bei braven Bürgern. Terrorismus von rechts scheint nicht annähernd so im Fokus der Sicherheitsbehörden zu sein wie der linke. Wirtschaftsspionage gehört zum guten Ton der Geheimdienste, nur der BND verwehrt sich gegen eine solche Unterstellung. Edward Snowden, der ein angenehmes Leben unserer Aufklärung geopfert hat, genießt kaum Schutz und wenig Anerkennung (wie auch die meisten anderen Whistleblower). – Wollen wir es lieber nicht so genau wissen? Unsere Bequemlichkeit nicht der Sicherheit opfern?

Hunger, Krieg und Menschenrechtsverletzungen nehmen zu und treiben immer mehr Menschen in die Flucht. Piraten aus dem *gescheiterten*[2] Staat Somalia entern Frachtschiffe. Die OK hat sich ausgeweitet; zur staatlichen sind private Überwachung und Kontrolle gekommen.

Wer kontrolliert eigentlich ...

... die Wirtschaftskriminalität? Die Steuerhinterziehung und Spekulation gegen Währungen und Staaten? Die geballte Macht global agierender, marktbeherrschender Konzerne, die auf dem

Dagmar Boedicker

Mein Weg ins FIfF ...

... führte über den Sprachendienst eines Großkonzerns. Ende der 1970er sollten Übersetzer auf einmal anders arbeiten, zwei mit dem Konzern kooperierende Universitäten kündigten bereits maschinelle Übersetzungen an. Dabei funktionierte der Zeileneditor am Großrechnerterminal so gnadenlos wider jede menschliche Intuition, dass ständig fertige Textteile im Orkus verschwanden. Den Entwicklern schien nicht bewusst zu sein, dass ihr Tun in der Arbeitswelt Folgen zeitigte, geschweige denn welche. Ich fand ihre fehlende Sensibilität – sagen wir mal: *schwierig.*

Gab es denn keine Informatikerinnen oder Informatiker mit sozialer Verantwortung? Doch. Auf der *Systems* habe ich sie getroffen, eine aktive, sympathische Regionalgruppe.

Beim FIfF geblieben bin ich, weil seine Mitglieder kluge und herzliche Menschen sind. Und weil die zarten Vorboten der Technikfolgen am Anfang der 1980er im Vergleich zu den heutigen Gefährdungen der Demokratie wie ein Scherz erscheinen.

Gebiet der IT zunächst nach Gutdünken in den Markt hüpfen, um erst auf Druck und zähneknirschend geltendes nationales Recht wenigstens teilweise zu beachten? Hier könnten die Medien als 4. Gewalt, verstanden als Kontrolle von Exekutive, Legislative und Justiz, eine wichtige Rolle spielen. Können Medien das, wenn sie im Wesentlichen ertragsorientiert und die Eigentümer in vielen Ländern große Konzerne sind?

Institutionen sollten uns ein Gefühl der Sicherheit geben, weil wir ihnen vertrauen. Können wir das noch? Tun wir das noch? Ich glaube nicht.

Alte Institutionen der Sicherheit

Alte Institutionen sind in und für Nationalstaaten entstanden, wie Gesetze und Parlamente. Natürlich gibt es auch internationale Institutionen. So wurde der wenig erfolgreiche Völkerbund von den Vereinten Nationen abgelöst, es gibt die NATO, die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), einen internationalen Strafgerichtshof, die Europäische Menschenrechtskonvention (EMRK), den Europäischen Gerichtshof (EUGh), eine Europäische Union (EU), das Europäische Parlament (EP), die EU-Kommission (EK) und den Europäischen Rat (ER). Wie gut kennen wir sie und ihre Funktionen? Vertrauen wir ihnen? Können wir überhaupt Institutionen vertrauen, von denen wir wenig wissen? Die vielleicht Produkte rechtlicher und anderer Tradition sind, uns aber nicht vertraut und alltäglich?

Was muss sich ändern? alle Fotos: Dagmar Boedicker

Wie gut funktionieren diese Institutionen noch? Zweifel sind angebracht gegenüber einer Exekutive, in deren Ministerien die Mitarbeiterinnen und Mitarbeiter großer Konzerne Gesetzesvorlagen schreiben und die Kanzlerin von *wirtschaftsverträglicher Demokratie* spricht. Auch gegenüber einer Justiz, die in Aushandlungsprozesse flieht angesichts von unübersehbaren Akten, unentwirrbaren Unternehmensverflechtungen, Mangel an qualifiziertem Personal und anderen Schwierigkeiten. Parlamente müssen abwägen zwischen Arbeitsplätzen und Klimaschutz, nationale Institutionen scheinen gegenüber globalen Akteuren ins Hintertreffen zu geraten.

Recht haben und Recht bekommen sind zweierlei, wie ein Blick auf die Durchsetzung des Rechts auf informationelle Selbstbestimmung oder auf die Integrität informationstechnischer Systeme zeigt. Da kann das deutsche Verfassungsgericht leider nichts machen. Übrigens auch Abgeordnete in den USA nicht, wenn sie finden, dass NSA & Co sich an die Verfassung halten sollen.

Tom Schmelzer: Responsibility to Protect or to whom it may concern[3]

Und die internationalen Institutionen? Wenn es darum geht, Kriege zu vermeiden oder zu beenden, bietet der UN-Sicherheitsrat ein trauriges Bild. Seltsame Konstruktionen wie die Schutzverpflichtung zu *humanitären* Militäreinsätzen, *R2P*[4], unterminieren die Basis des Völkerrechts, die nationale Souveränität. Teile der Politikwissenschaft dümpeln noch zwischen Ost und West, statt sich mit einer neuen multipolaren Ordnung und ihren Möglichkeiten und Gefahren zu befassen. WTO-Schiedsgerichte verdonnern Staaten zu exorbitanten Strafzahlungen, weil die Staaten die Profite transnationaler Unternehmen beschränkt haben. Freihandel über alles, aber wo bleiben wir, die Menschen? Das Europäische Parlament ist vielleicht ein kleiner Lichtblick, immerhin hat es Erfolge beim Arbeits- und Verbraucherschutz erzielt und einen ordentlichen Entwurf einer Datenschutz-Verordnung vorgelegt. Der würde die Datensammelwut der IT-Monopolisten beschneiden, hängt aber seit Herbst 2013 bei den Staatschefs im europäischen Rat fest.

Neue Institutionen der Sicherheit

Auch wenn die Globalisierung nichts Neues ist, behaupte ich, dass ihr Umfang und ihre Geschwindigkeit seit den 1990er Jahren eine neue Qualität hervorgebracht haben, deren Komplexität und Verflechtung sich dem menschlichen Maß entziehen. Beherrschbar ist sie vielleicht noch für Akteure mit gewaltigen finanziellen und technischen Ressourcen, nicht aber für uns Bürgerinnen und Bürger und viele der Institutionen, die wir uns in der Demokratie geschaffen haben. Technik begünstigt die

Mächtigen, und die Hebel der Informations- und Kommunikationstechnik und der globalen Finanzströme bewirken Machtkonzentrationen, denen wir, *die 99 Prozent,* mit den alten demokratischen Instrumenten wenig entgegensetzen können. Manche[5] behaupten, ein wie auch immer gearteter *postpolitischer* Konsens, demokratischer *Transnationalismus* oder die *unsichtbare Hand* des Markts sei die Antwort. Das bezweifle ich und behaupte, dass wir neue demokratische Institutionen brauchen, die Macht kontrollieren können.

Allerdings halte ich weltweite Geltung für unmöglich: Demokratische Mechanismen wie Parlamentarismus oder geheime Wahlen lassen sich kaum auf die globale Ebene übertragen. Außerdem haben westliche Industriestaaten seit der Kolonialzeit doppelte Standards praktiziert und können in der übrigen Welt keine Glaubwürdigkeit für sich in Anspruch nehmen[6]. In größeren regionalen Einheiten können wir aber Modelle entwickeln, die der geballten Macht eigene Wertvorstellungen entgegensetzen, gültig für diese Region und die nationale Souveränität und kulturelle Vielfalt respektierend. Einzelne Länder können das schon lange nicht mehr.

Flucht nach vorn?

Ich meine natürlich die EU, die *Kompromissfindungs-Maschine* mit institutionellen Prozessen, die leidliche Gegenseitigkeit und Rechtssicherheit bieten. Ungeliebt und unvertraut hält sie meist den Schwarzen Peter im nationalen Spiel und ist alles andere als perfekt: Der Versuch, die Finanz- und Schuldenkrise zu bewältigen, hat demokratische Mechanismen teilweise ausgehebelt. Andererseits erlaubt geltendes europäisches Recht durchaus mehr Demokratie[7]. Hier liegen Verträge zwischen den Euro-Staaten und EU-Verträge im Clinch, in EU-Lingo: die intergouvernementale[8] gegen die supranationale *Gemeinschafts*methode (EK mit EP und ER).

Der Vertrag über die Europäische Union (EUV) hat das Europäische Parlament gestärkt, und es hat die Gelegenheit beim Schopf ergriffen, bei der EU-Kommission mehr mitzubestimmen. Nach der letzten Europawahl musste der Europäische Rat das Wahlergebnis der EP-*Spitzenkandidaten* für den Kommissionsvorsitz *berücksichtigen.* Das ist neu: Ein gewählter EK-Chef. Bisher ernannten ihn die Regierungschefs und das Parlament hätte – Friss oder stirb! – nur die Kommission als Ganzes ablehnen können.

Eins hat die Europawahl 2014 aber auch gezeigt: Viele Europäer halten wenig von der EU (noch weniger als von unseren nationalen Regierungen und Parlamenten, die kennen wir wenigstens). Sicherheit erwarten wir von unseren Ländern, sei es im Sozialen, dem Umweltschutz oder im Internet. Brüssel ist ein

Finanz- und Schuldenkrise

Raumschiff, die EU mischt sich ein, wo sie nichts verloren hat, und verhandelt im Geheimen über Freihandelsverträge. Hast du einen Opa, schick ihn nach Europa[9]? Zur Zukunft rechts abbiegen?

Der Kommissionsvorsitzende Jean-Claude Juncker will die EU stärken und hat die Flucht nach vorn angetreten. Ohne eine Änderung der *Verfassung* (einen neuen EU-Vertrag), denn die will niemand, schließlich ist die letzte an Frankreich und den Niederlanden gescheitert (sicher auch an deren nationalen Proteststimmen). Juncker will einen ähnlichen Weg verfolgen wie die Nationalstaaten im 19. Jahrhundert, den Weg zur Demokratisierung und ihre Entwicklung über die parlamentarische Bestätigung. Er ist eher ein Präsident des EP und möchte mehr Kooperation zwischen Parlament und Kommission, was das Verhältnis zum Europäischen Rat verändern wird. Das ist riskant, denn die 28 Regierungen der Mitgliedstaaten, letzte Entscheider im Rat, werden sich die Butter gewiss nicht vom Brot nehmen lassen wollen. Sie behalten sich nationale Politiken vor, bei Telekommunikation, Außen-, Rechts- und Sicherheitspolitik, Energie und Klima, Migrationspolitik, dem Beitritt zur Europäischen Menschenrechtskonvention (EMRK), … Aber sind das wirklich national regelbare Themen? Der EK-Präsident findet, dass große Fragen nach Europa, kleinere in die Mitgliedstaaten gehören, und hofft auf eine Einheit des europäischen und nationalen Handelns, weil sonst der Konsens noch mehr leidet.

Dagmar Boedicker

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

Das EU-Parlament ist teilweise transparenter als unser Bundestag. Es ist stark, entscheidet beispielsweise in letzter Instanz über das Freihandelsabkommen TTIP, anders als die nationalen Parlamente, deren Mitbestimmungsrecht noch ungeklärt ist. Das EP hat großen Einfluss darauf, wie transeuropäische Netze gestaltet werden, ob im IT- oder Energiebereich. Wenn Juncker dann seine Versprechen hält, soziale Schwerpunkte zu setzen, ein Register *aller* Mitwirkenden am Gesetzgebungsverfahren (auch Lobbyisten) einzurichten, EK-Dokumente im Internet gut zu strukturieren (bisher bewirken sie eher Intransparenz) und besser mit nationalen Parlamenten bei der Verstärkung von Subsidiarität und Kompetenz-Zuordnung zu kooperieren, dann könnten das Institutionen sein, die wir brauchen, wenn auch nicht mehr so neu.

Netz der Unsicherheit

Wenn es uns gelingt, der EU wieder mehr Glaubwürdigkeit zu verschaffen und Vertrauen entgegenzubringen, wird sie auch ein Modell sein müssen für die ganz große Herausforderung: Die systemübergreifenden Verwundbarkeiten im Internet. – Neue Institutionen sind gewiss nötig für den *Cyberpeace,* den das FIfF in seiner Kampagne fordert:

- für eine demokratische Kontrolle des Internet,
- für Abrüstung im Cyberspace und ihre Kontrolle,
- zur Absicherung kritischer Infrastrukturen,
- zur Entwicklung und Qualitätssicherung von Software, die transparent, fehlertolerant, rückholbar und widerstandsfähig ist.

Als Gegengewicht zu offensiven Strategien im Cyberspace brauchen wir dafür eine defensive Sicherheitsdoktrin, die die Menschenrechte respektiert und uns nicht alle unter Generalverdacht stellt. Schon Karl Popper war überzeugt, dass gesellschaftlicher Wandel rational und demokratisch nur durch Institutionen möglich ist. Das war auch das Ziel der friedlichen Revolution in der DDR vor 25 Jahren. Damit wir den Institutionen vertrauen und sie als legitim und effektiv wahrnehmen, dürfen sie aber nicht versagen. Meine Frage oben bleibt zwar offen, ob die (inter-)nationalen Institutionen Sicherheit schaffen können. Sie werden es aber müssen, damit wir die Ziele Frieden und Demokratie nicht aus den Augen verlieren.

Anmerkungen

1 *Als Institutionen bezeichnen die Sozialwissenschaften alles, was das Zusammenleben regelt und stabilisiert, von alltäglichen Umgangsformen über die Verfassung zu den Verfassungsorganen (Legislative, Judikative, Exekutive), von nationalen und internationalen Verträgen und Organisationen (beispielsweise EU, OSZE, EMRK) zu Markt, Sozialsystem oder Medien. Institutionen sind Produkte von Tradition, sie sind dem kulturellen und sozialen Wandel unterworfen. Sie regeln Macht, die in demokratischen Systemen innerhalb des institutionellen Rahmens immer wieder neu verteilt wird.*

2 *Der Begriff ist veraltet: Politische Korrektheit im Sprachgebrauch der internationalen Beziehungen hat ihn erst zur Bezeichnung scheiternd, dann zu fragil umgemünzt.*

3 *Text des Künstlers zum Werk (Auszug: „In Wirklichkeit treten gemeinsame Maßnahmen erst dann in Kraft, wenn mindestens eine der folgenden Bedingungen erfüllt ist: Wenn weiße Bevölkerung betroffen ist/Wenn Christen betroffen sind/Wenn Öl betroffen ist/Wenn Gas betroffen ist)*

4 *Responsibility to Protect*

5 *Ulrich Beck, Richard Falk, Anthony Giddens, Jürgen Habermas, Jaron Lanier, … jeder auf seine Weise*

6 *Ein Indiz dafür sind Menschen, die ihnen den Rücken kehren, um für einen islamischen Staat, ein Kalifat, zu kämpfen.*

7 *Vertrag über die Europäische Union (EUV) und über die Arbeitsweise der Europäischen Union (AEUV)*

8 *Frau Merkel würde sagen, die Unionsmethode, was Etikettenschwindel ist: Klingt nach EU, ist es aber nicht.*

9 *Ein wirklich veralteter Spruch: Jan Philipp Albrecht, der grüne Vorsitzende des Ausschusses, in dem über die Datenschutz-Verordnung verhandelt wurde, beispielsweise ist um die 30, der grüne Abgeordnete Sven Giegold um die 45.*

Ute Bernhardt

Mein Weg ins FIfF

Anfang der 80er Jahre studierte ich in Bonn und finanzierte mein Studium durch IT-Jobs. Zufällig ergab sich die Chance, in einer Gruppe in der Gesellschaft für Mathematik und Datenverarbeitung (GMD) anzufangen, die sich mit gesellschaftlichen Folgen des IT-Einsatzes beschäftigte. Von IT in der Arbeitswelt, Datenschutz und der Verletzlichkeit von IT-Systemen kamen wir zum Risiko von militärisch genutzten IT-Systemen.

Damals ging es um einen Atomkrieg aus Versehen – ausgelöst durch Computerfehler. Mit Werner Langenheder, Helga Genrich, Manfred Domke und den Berliner Kollegen um Christiane Floyd, Reinhard Keil und Michaela Reisin hatte sich eine Gruppe gefunden, die vieles zu diesem Thema zuerst aufarbeitete und dann daran ging, die Öffentlichkeit zu informieren.

In den USA arbeiteten zur selben Zeit Joseph Weizenbaum, Gary Chapman und andere im CPSR (computer professionals for social responsibility) zu denselben Themen. David Parnas wurde vom Projektverantwortlichen für die SDI-Raketenabwehr zum Warner vor einem Atomkrieg aus Versehen. Das CPSR wurde für uns zum Vorbild, das FIfF zu gründen.

1984 ging es um autonome Computer und Atomkrieg. Heute geht es im FIfF um Überwachung, autonome Kampfroboter und Drohnen. Ich bin froh, von Anfang an im FIfF mitgewirkt zu haben.

Ute Bernhardt *ist Gründungsmitglied des FIfF, von 1990 bis 1998 dessen Geschäftsführerin und von 1991 bis 2001 Vorstand und stellvertretende Vorsitzende des FIfF.*

Christine Hegenbart

Eine Frage der Begriffe

Es wirkt wie ein Allgemeinplatz, aber der korrekte Umgang mit allem, was die Vorsilbe „Cyber-" besitzt, ist dringend notwendig. Eine Einordnung.

Schon länger diskutiert die sicherheitspolitische Community die Dimension der Bedrohungen aus dem Cyber-Raum intensiv. Konzeptionelle Unschärfe und Ungenauigkeiten stiften in dieser Debatte oft Verwirrung. Wie in allen Fachdebatten ist die verwendete Terminologie von zentraler Bedeutung, wenn es darum geht, die Bedrohung einzuschätzen. Denn unterschiedliche Begriffe haben unterschiedliche Bedeutungen und Konsequenzen.

Der Begriff *Cyber-Krieg* verweist beispielsweise auf ein hohes Bedrohungspotential und schreibt die Zuständigkeit für Gegenmaßnahmen dem Militär zu. Demgegenüber vermittelt der Begriff *Cyber-Kriminalität* eine niedrigere Bedrohungseinschätzung und legitimiert die Polizei, die Delikte zu verfolgen. Allein dieser Unterschied in der Wortwahl veranschaulicht, wie nützlich und notwendig angemessene Definitionen sind. Wo liegen also die begrifflichen Fallstricke der Cyber-Debatte?

Definitionen von Cyber-Konflikttypen

Gefahren aus dem Cyber-Raum können in unterschiedlichen Ausprägungen auftreten, die nicht immer leicht zu differenzieren sind. Absolute Trennschärfe in der Cyber-Terminologie wird kaum zu erreichen sein. Allerdings erscheint es zweckmäßiger auf nicht ganz präzise Definitionen zurückzugreifen, als ganz auf sie zu verzichten. Als Grundlage für zukünftige Diskussionen sind sechs Konflikttypen denkbar, die auf den amerikanischen Sicherheitsexperten *James A. Lewis* und die Schweizer Wissenschaftlerin *Myriam Dunn Cavelty* zurückgehen.

(1) Hacktivismus und Cyber-Vandalismus

Das Wort *Hacktivismus* setzt sich aus den Begriffen *Hacking* und *Aktivismus* zusammen. Es bezeichnet Aktivitäten von Privatpersonen oder staatlich unabhängigen Gruppen, die Computer oder Computernetzwerke für politischen Protest nutzen. Hacktivisten zielen darauf ab, mittels verschiedener Hacking-Methoden den Zugriff auf Informationen im Internet zu stören. Sie verändern beispielsweise den Inhalt von Internetseiten oder unterbinden den Zugriff auf Online-Dienste.

Demgegenüber stehen hinter Cyber-Vandalismus keine politischen Ziele. Die Motive sind im Bedürfnis des Hackers zu suchen, die Grenzen seines Könnens auszutesten und Selbstbestätigung zu erfahren.

(2) Cyber-Kriminalität

Cyber-Kriminelle agieren als Einzeltäter oder in Gruppen, die mehr oder weniger gut organisiert und ausgerüstet sind. Ihre illegalen Aktivitäten im Cyber-Raum sind darauf aus, finanzielle Gewinne zu erzielen. Dabei können sowohl Einzelpersonen als auch Unternehmen geschädigt werden. Die Straftaten weisen eine große Bandbreite auf und umfassen Delikte wie zum Beispiel Kreditkarten- und Warenbetrug, Identitätsdiebstahl und Erpressung.

(3) Cyber-Spionage

Es gibt zwei Ausprägungen von Cyber-Spionage: zum einen Wirtschaftsspionage und zum anderen politisch-militärische Spionage. Im ersten Fall sind die Akteure Unternehmen, die hoch entwickelte IT-Methoden für Spionagezwecke nutzbar machen: Sie versuchen, an vertrauliche Geschäftsinformationen und intellektuelles Firmeneigentum von hohem ökonomischen Wert zu gelangen.

Im zweiten Fall sind die Akteure Staaten, insbesondere Nachrichtendienste oder hochprofessionelle private Hacker, die in staatlichem Auftrag Spionage über den Cyber-Raum betreiben. Im Zentrum ihrer Aktivitäten stehen die verdeckte und illegale Beschaffung von sensiblen und klassifizierten Informationen ausländischer Regierungsinstitutionen und deren Streitkräfte. Attraktiv sind beispielsweise Informationen über militärische Kapazitäten und Strategien sowie Verteidigungskonfigurationen von einzelnen Zielcomputern oder ganzen Systemen.

(4) Cyber-Sabotage

Auch mit Blick auf Cyber-Sabotage muss man zwischen wirtschaftlichen und politisch-militärischen Absichten unterscheiden. Die Grenzen zwischen Cyber-Spionage und Cyber-Sabo-

Christine Hegenbart

Christine Hegenbart ist wissenschaftliche Mitarbeiterin der Akademie für Politik und Zeitgeschehen der Hanns-Seidel-Stiftung in München. Seit einigen Jahren befasst sie sich mit dem Thema Cyber-Sicherheit und hat im Frühjahr 2013 als PfP Fellow an der Research Division des NATO Defense College in Rom intensiv geforscht.

tage sind indes nicht leicht festzumachen: Zum einen sind bei beiden Konflikttypen dieselben Akteure aktiv. Zum anderen dienen die Informationen, die durch Cyber-Spionage gewonnen werden, als Grundlage für Cyber-Sabotageaktionen. Letztere nutzen solche Erkenntnisse über Sicherheitslücken und Verteidigungskonfigurationen aus.

Somit richtet sich Cyber-Sabotage gegen die Integrität und Verfügbarkeit von wichtigen IT-Systemen und Prozessen. Dies führt zur Zerstörung oder massiven Schädigung von technischer Ausrüstung oder gespeicherten Informationen. Dahinter stehen zumeist politische Ziele. Cyber-Sabotage ist – im Unterschied zu Cyber-Vandalismus – relevant für die nationale Sicherheit. Die Schwelle zum Cyber-Krieg wird jedoch nicht überschritten.

(5) Cyber-Terrorismus

Terroristische Netzwerke und Gruppen sowie radikalisierte Individuen können über den Cyber-Raum ihre politischen und ideologischen Ziele verfolgen. Mittels systematisch geplanter Gewaltaktionen, die zu materieller Zerstörung führen, wollen Cyber-Terroristen Aufmerksamkeit auf ihre Ideale und Werte lenken. Potentielle Ziele, die sie über den Cyber-Raum angreifen können, sind vor allem kritische Infrastrukturen.

Terroristische Cyber-Anschläge können beispielsweise Trinkwasservorräte kontaminieren oder Flugzeugabstürze und massive Stromausfälle verursachen. Sie haben somit das Potenzial, nicht nur kostspielige Störungen hervorzurufen, sondern vielmehr zu Personen- oder Sachschäden zu führen.

(6) Cyber-Krieg

Nationale Streitkräfte oder staatlich finanzierte militärische Einheiten und andere offiziell autorisierte Gruppen, wie zum Beispiel so genannte *Cyber-Milizen*, können Cyber-Techniken einsetzen, um eine kriegerische Auseinandersetzung zu führen. Diese aggressiven Aktivitäten im Cyber-Raum haben massive physische Auswirkungen auf die reale Welt.

Ohne materielle Schäden oder Verletzte ist ein Cyber-Konflikt nicht als Cyber-Krieg zu klassifizieren. Auch ist diese Zuschreibung nicht korrekt, wenn der Aggressor kein staatlicher Akteur ist. Eine Kriegshandlung *(act of war)* umfasst die zwischenstaatliche Anwendung von Gewalt *(use of force)*, die politischen Zwecken dient. Dieses Prinzip ist auch auf den Cyber-Raum anzuwenden.

Eigenschaften und Mittel des Cyber-Kriegs

Cyber-Krieg beziehungsweise *cyber war* ist ein mehrdeutiger und kontrovers diskutierter Begriff. Vor allem die Medien überstrapazieren ihn, indem sie ihn geradezu inflationär verwenden. Eine genauere Betrachtung ist daher notwendig.

Das so genannte *Attributionsproblem* bezeichnet die Schwierigkeit einen Cyber-Angriff zurückzuverfolgen. Mit Blick auf Cyber-Kriege ist diese Problematik nur eingeschränkt relevant. Digitale Kampfhandlungen stehen normalerweise in Zusammenhang mit einem zwischenstaatlichen Konflikt und dienen dazu, konventionelle militärische Aktionen zu unterstützen.

In diesem Fall wäre es präziser, den Konflikttyp mit Cyber-Kriegsführung zu umschreiben. Dabei zielen militärische Cyber-Einheiten darauf ab, die Dominanz im Kampfgeschehen über Kommunikations- und Informationssysteme zu erreichen: Taktisch verwendete Cyber-Mittel ermöglichen oder erleichtern konventionelle Offensivmaßnahmen. So ist es beispielsweise möglich, die Daten von Waffen- und Radarsysteme zu manipulieren oder ganze Anlagen auszuschalten, um damit die Waffenwirkung des Gegners zu reduzieren. Darüber hinaus können Cyber-Angriffe die Funktionsfähigkeit von kritischen Infrastrukturen einschränken oder ganz zum Erliegen bringen. Diese Formen der Cyber-Kriegsführung werden eine bedeutende Rolle in allen zukünftigen bewaffneten Konflikten spielen.

Im Gegensatz dazu erscheint ein militärischer Konflikt, der sich ausschließlich Cyber-Mitteln bedient und nicht im Zusammenhang mit einer kriegerischen Auseinandersetzung steht, wenig wahrscheinlich. Es ist zwar technisch möglich, schwerwiegende und lähmende Cyber-Angriffe auszuführen, ohne einen politischen und militärischen Konflikt als Kontext ist dies aber kaum vorstellbar. Gegenwärtig haben nur China, Russland, Israel, Frankreich, Großbritannien und die USA entsprechend hochentwickelte technologische Fähigkeiten. Auch können die Risiken einer Cyber-Attacke für den Angreifer schwerer wiegen als seine Vorteile. Zudem teilen potenzielle Angreifer die Unfähigkeit, sich gegen einen hoch entwickelten Cyber-Gegenschlag zu verteidigen.

Solche Abwägungen berücksichtigen die spezifischen Eigenschaften von Cyber-Waffen. Zu ihren Vorteilen zählen unter anderem vergleichsweise geringe Anschaffungskosten, schnelle Wirksamkeit und Heimlichkeit, mit der sie eingesetzt werden können, sowie der daraus resultierende Überraschungseffekt.

Dennoch haben Cyber-Waffen einige nicht zu vernachlässigende Nachteile. Sie sind nicht kontrollierbar im militärischen Sinn: Cyber-Waffen sind nicht zuverlässig und können Auswirkungen haben, die nicht beabsichtigt oder sogar kontraproduktiv sind. Darüber hinaus müssen sie speziell auf ein bestimmtes Ziel zugeschnitten sein und sind daher oft nur einmal verwendbar *(single use)*. Vor allem aber stellen viele – von Medien bis zur Sicherheitsindustrie und -beratern – ihr Zerstörungspotential oft übertrieben dar.

Cyber-Waffen können lediglich indirekten Schaden verursachen, da sie allein die Kraft und Energie ihres Ziels nutzen. Die Auswirkungen von Cyber-Angriffen sind so nur schwer mit konventionellen militärischen Operationen und unter keinen Umständen mit Nuklearangriffen zu vergleichen.

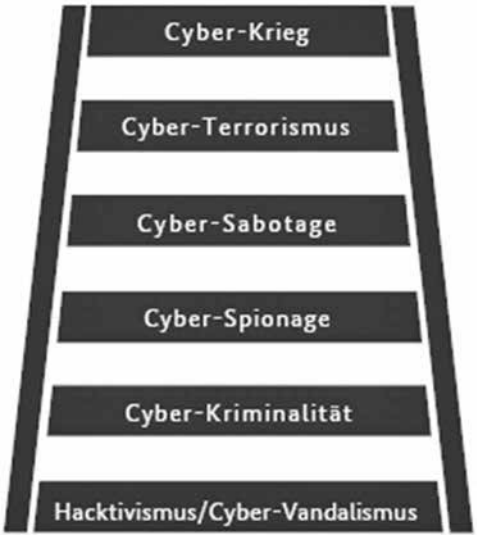
Aufgrund dieser Eigenschaften von Cyber-Waffen und der Unsicherheit darüber, was überhaupt einen *act of war* im Cyber-Raum konstituiert, werden die zuständigen Entscheidungsträger die Anordnung von Cyber-Angriffen mit großer Sorgfalt abwägen müssen: Es besteht die Gefahr, die Wirkung dieser Waffen einerseits und die Reaktionen des Kontrahenten andererseits falsch einzuschätzen. Hierdurch können Konflikte eskalieren und letztendlich einen Vergeltungsschlag außerhalb des Cyber-Raums mit konventionellen Waffen provozieren.

Die Cyber-Konflikt-Eskalationsleiter

Die Bedrohung aus dem Cyber-Raum hält unvermindert an. Insbesondere ist zu beobachten, dass die Angreifer sich zunehmend professionalisieren und folglich die technische Qualität der Cyber-Vorfälle insgesamt zunimmt. Dennoch ist die sprachliche Darstellung dieser Entwicklungen, unter anderem in den Medien, häufig übertrieben und undifferenziert. Dabei dominieren Begriffe wie *Cyber-Angriff* und *Cyber-Krieg*, auch wenn es um nicht-militärische Vorfälle geht, die keine Bedeutung für nationale Sicherheit haben.

Um die aktuelle Bedrohungslage möglichst objektiv einschätzen zu können, muss man die eben beschriebenen Konfliktdefinitionen so präzise wie möglich anwenden. Es hilft, hierfür das Bild einer *Cyber-Konflikt-Eskalationsleiter* heranzuziehen. Sich dieses Modell zu vergegenwärtigen, erlaubt militärischen und politischen Entscheidungsträgern, ein Verständnis für die Bedrohung zu entwickeln, Prioritäten zu setzen und über die angemessensten Gegenmaßnahmen zu entscheiden.

Die Leiter visualisiert zwei zentrale Eigenschaften der eben vorgestellten Konflikt-Typen: Sie lenkt die Aufmerksamkeit sowohl auf die Häufigkeit von Angriffen als auch auf das Ausmaß der Schadenswirkung. Die Eskalationsleiter führt von der Konfliktart, die am häufigsten vorkommt, zu der, die am seltensten zu beobachten ist. Auch reicht sie von der Angriffsart, die am wenigsten, zu der, die am meisten Schaden verursacht.



Cyber-Konflikt-Eskalationsleiter

Gemäß dem Leitermodell sind die vorherrschenden Konfliktformen Hacktivismus beziehungsweise Cyber-Vandalismus, Cyber-Kriminalität und Cyber-Spionage. Die ersten beiden sind nicht von direkter militärischer Bedeutung – sie betreffen ausschließlich die allgemeine Einsatzbereitschaft von Streitkräften – und haben nur geringen Einfluss auf nationale Sicherheit. Ihnen kann durch die gängigen IT-Sicherheitsmaßnahmen begegnet werden. Die strafrechtliche Verfolgung der Taten fällt in den Zuständigkeitsbereich von zivilen Behörden.

Cyber-Spionage nimmt eine Sonderstellung ein: Einerseits sind die Übergänge von Cyber-Spionage zu Cyber-Sabotage fließend; andererseits können die gewonnenen Erkenntnisse auch für Cyber-Terrorismus oder Cyber-Kriegsführung genutzt werden. Cyber-Spionage kann also indirekt massiven Schaden verursachen, so dass man der Abwehr dieses häufigen Konflikttyps besondere Aufmerksamkeit schenken muss. Die Umsetzung anspruchsvoller Sicherheitsmaßnahmen, etwa um militärische Netzwerke der Bundeswehr zu schützen, ist folglich zwingend notwendig.

Cyber-Spionage wird auch mit Blick auf das Völkerrecht nicht sanktioniert. Ebenso wie konventionelle Spionage ist sie gemäß der meisten nationalen Rechtsprechungen eine nach dem Gesetz strafbare Handlung und kann von zivilen Behörden verfolgt werden.

Die anderen drei Konflikttypen – Cyber-Sabotage, Cyber-Terrorismus und Cyber-Krieg – sind, wie die Eskalationsleiter veranschaulicht, am seltensten. Sie sind dennoch von Bedeutung, da sie potentiell hohe Schadenswirkung und damit auch Auswirkungen auf nationale und internationale Sicherheit haben.

Bisher wurden nur wenige Cyber-Angriffe beobachtet, die Eigentum beschädigt oder zu ernsthaften und langanhaltenden Störungen geführt haben. Allein der gegen das iranische Atomprogramm gerichtete Computerwurm *Stuxnet* hat eine zerstörerische Wirkung entfaltet und gilt als physischer Cyber-Angriff im zwischenstaatlichen Bereich.

Es gibt keine Beispiele dafür, dass tatsächlich Menschenleben gefährdet wurden. Einen eigenständigen kriegerischen Akt im Cyber-Raum, der als Cyber-Krieg zu bezeichnen wäre, hat es bisher nicht gegeben. Allerdings bauen viele Staaten ihre Fähigkeiten zur Cyber-Kriegsführung weiter aus, was das Problem langfristig verschärfen kann.

Konsequenzen für Deutschland

Die Gefahren aus dem Cyber-Raum sind nicht primär militärisch. Ist jedoch die nationale Sicherheit betroffen – wie bei Cyber-Sabotage, Cyber-Terrorismus und Cyber-Krieg – sind die Streitkräfte, also die Bundeswehr, wichtige verantwortliche Akteure.

Allerdings sollte die Bundesregierung, beispielsweise durch die Presse- und Öffentlichkeitsarbeitsabteilungen von Ministerien und Behörden, einer verbalen Militarisierung des Cyber-Raums entgegenwirken und Cyber-Konflikte gezielt sprachlich realistisch darstellen. Reine Cyber-Kriege sind, wie beschrieben, kein absehbares Zukunftsszenario. Wird der Begriff *Krieg* überstrapaziert, kann dies zu Fehleinschätzungen oder gar Überreaktionen führen und in letzter Konsequenz zur Eskalation von Konflikten beitragen.

Klare, allgemein anerkannte Definitionen, wie die eben vorgestellten, sind für den rhetorischen Umgang mit Cyber-Konflikten grundlegend. Je konkreter die Bedrohungen definiert sind, desto einfacher können die verantwortlichen Akteure sie durch angemessene Cyber-Sicherheitsstrategien angehen.

Dieser Beitrag ist zuerst erschienen als Ausgabe 2/2014 der Arbeitspapiere der Bundesakademie für Sicherheitspolitik. *www.baks.bund.de/de/service/arbeitspapiere-sicherheitspolitik.*

Forderungen zum Cyberpeace

Das FIfF führt eine Kampagne zum Cyberpeace, mit der wir uns für die Entmilitarisierung und die ausschließlich friedliche Nutzung des Internet einsetzen. Dabei fordern wir in erster Linie die Ächtung des Cyberwarfare und das Primat der friedlichen Nutzung, die Entflechtung und zivilgesellschaftliche Kontrolle von Militär und Geheimdiensten und die Wiederherstellung der Integrität des Internet. In 14 Forderungen haben wir unsere Vorstellungen von einem friedlich und menschenwürdig genutzten Internet konkretisiert. Wir werden die Forderungen im Rahmen der Kampagne weiter diskutieren und fortentwickeln.

Worum geht es? Was ist das Problem? Was ist unsere Motivation für die Kampagne?

Unsere Kampagne beginnt mit der Beschreibung des Problems. Was sind die Risiken, Gefahren und Probleme, die Cyberwarfare erzeugt?

- Cyberwarfare beginnt mit der Überwachung der Zivilgesellschaft – diese Ausspähung verletzt die Privatsphäre des Menschen und damit die Menschenwürde als ein elementares Menschenrecht.

- Voraussetzung für die Überwachung ist die Manipulation von IT-Systemen und der Einbau von Schwachstellen. Die Folge sind unzuverlässige und unsichere Computer- und Kommunikationssysteme wie das Internet, von deren reibungslosem Funktionieren weite Teile unserer Gesellschaft abhängig sind. Für Cyberwarfare wird die Sicherheit der zivilen IT-Infrastruktur ausgehöhlt und untergraben.

- Staatliche Cyberkrieger sind heute die ressourcenstärksten Hackerorganisationen weltweit. Ihre Cyberangriffe sind nicht zu kontrollieren und gefährden neben ihren eigentlichen Zielen auch zivile Systeme – wie etwa Systeme zur Sicherstellung lebenswichtiger Ressourcen (Wasser, Energie), Krankenhäuser oder Einrichtungen wie Chemiewerke. Der gegen eine iranische Atomanlage gerichtete Stuxnet-Wurm breitete sich weltweit aus. Mittlerweile gibt es fast ein Dutzend weiterer Trojaner offensichtlich staatlicher Herkunft.

- Der Einsatz von Cyberwaffen durch Staaten ist völkerrechtlich eine Kriegshandlung mit erheblichem Eskalationspotenzial, die die internationale Sicherheit erheblich gefährdet.

- Ausspähung und Computermanipulationen bereiten konventionelle militärische Operationen vor, beispielsweise rechtswidrige Drohnenangriffe durch die Ortung von Zielpersonen, und sind damit die Grundlage aggressiver (kriegerischer) Operationen.

- Drohnenangriffe fordern zahlreiche Opfer unter Unbeteiligten. Angriffe, die auf unsicheren Eigenschaften der Ziele basieren *(Signature Strikes)* richten sich gegen Opfer, gegen die nicht einmal ein hinreichender Verdacht besteht.

- Computergestützte militärische Operationen erzeugen die Illusion eines „sauberen" Krieges und senken damit die Schwelle des Einsatzes

Daraus ergeben sich für uns Ziele, die wir mit unserer Kampagne erreichen wollen. Vision und Leitbild ist die Entmilitarisierung und ausschließlich friedliche Nutzung des Internet: Wir wollen Ächtung von Cyberwaffen, auf IT-Produkte ausgedehnte Rüstungskontrolle, Entflechtung und Kontrolle von Militär und Geheimdiensten. Dies sind Ziele, für die sich das FIfF auf fachlicher Ebene bereits einsetzt. In seinem Forderungskatalog hat das FIfF diese Ziele präzisiert und begründet. Vorrangig sind

Sylvia Johnigk am FIfF-Stand

- die Ächtung jeglicher Form des Cyberwarfare,

- die Garantie der Integrität des Internets, der Primat der friedlichen Nutzung, der Schutz vor militärischem und politischem Missbrauch,

- die Unterbindung menschenrechts- und verfassungswidriger Ausspähung der Zivilgesellschaft,

- eine Abkehr von einer Sicherheitsdoktrin, die alle Menschen unter Generalverdacht stellt.

Um dieses Ziel zu erreichen, wollen wir kurzfristig:

- Rüstungskontrollbestimmungen für offensive Cyberwaffen und Überwachungstechnologie,

- Verzicht auf Entwicklung und Einsatz offensiver Cyberwaffen,

- Veröffentlichungspflicht für IT-Schwachstellen insbesondere für staatliche Stellen und Unternehmen,

- gesetzliche Verankerung ausspähsicherer und menschenrechtsfreundlicher Kommunikationsinfrastrukturen statt Scheinlösungen wie DE-Mail.

Aus diesen grundsätzlichen Forderungen haben wir 14 konkrete Forderungen abgeleitet, die wir im Folgenden darstellen.

Keine Erstschläge und offensiven Schläge im Cyberspace

Jede Nation hat das Recht, sich gegen Angriffe zu verteidigen. Nationen haben aber nicht das Recht, andere Nationen anzugreifen oder Erstschläge – auch im Cyberspace – gegen andere Nationen auszuführen. Wir fordern, dass Regierungen niemals Cyberwaffen für offensive Zwecke benutzen.

Im Einzelnen fordern wir:

- Nationen müssen öffentlich erklären, dass sie auf offensive Cyberangriffe verzichten. Solche offensiven Cyberangriffe sind grundsätzlich illegitim.
- Wirtschaftliche Interessen, wie beispielsweise Rechte an geistigem Eigentum, sehen wir nicht als legitimen Grund für einen Krieg an.
- Kriminalität im Cyberspace muss – im Gegensatz zum Cyberkrieg – mit Mitteln des Strafrechts bekämpft werden, nicht mit Mitteln des Kriegsrechts. Die internationale Kooperation zur Verfolgung von Cyberangriffen darf geheimdienstliche und militärische Aktionen nicht ausschließen – die internationalen Abkommen sind entsprechend zu erweitern.

Eine ausschließlich defensive Sicherheitsstrategie

Alle Nationen haben das Recht, eine Sicherheitsstrategie zu entwickeln, die die Nutzung effektiver Techniken zum Schutz von IT-Systemen einschließt, um sich gegen Angriffe zu verteidigen. Wir fordern, dass Regierungen weder offensive Cyberwaffen entwickeln, noch Cyberwaffen für offensive Zwecke nutzen.

Im Einzelnen fordern wir:

- Da offensive Cyberangriffe nicht legitim sind, müssen Nationen eine eindeutig defensive Sicherheitsstrategie bei Cyberschlägen verfolgen.
- Nationen müssen sich dazu verpflichten, offensive Cyberwaffen weder zu entwickeln noch zu nutzen.

Abrüstung

Cyberwaffen sind – genauso wie konventionelle Waffen – eine Bedrohung der Sicherheit für jeden von uns. Solche Cyberwaffen beruhen häufig auf geheimgehaltenen Schwachstellen. Sie sind schwierig zu kontrollieren, da sie potenziell alle Softwaresysteme bedrohen, die diese Schwachstellen besitzen – nicht nur diejenigen Systeme, auf die die Angriffe abzielen.

Im Einzelnen fordern wir:

- Nationen müssen Cyberwaffen als Bedrohung des Friedens und der Sicherheit aller anerkennen.
- Wir fordern, dass Nationen und ihre Regierungen abrüsten – im Cyberspace genauso wie in der „realen“ Welt.
- Dies muss durch internationale Abkommen abgesichert werden.
- Die Abrüstung von (Cyber-) Waffen sehen wir als äußerst wünschenswert an. Wir halten es aber für legitim, Werkzeuge zur Abwehr von Angriffen und sogenannte Hackertools für defensive Zwecke zu behalten und zu nutzen – wie Werkzeuge, die öffentlich verfügbare Exploits bereitstellen und dazu dienen können zu testen, ob Schwachstellen existieren und helfen können, diese aufzudecken.

Keine konventionelle Antwort auf Cyberangriffe

Es ist nicht möglich, Cyberangriffe unzweifelhaft einem Angreifer zuzuordnen (Attributionsproblem). Solche Angriffe mit konventionellen Waffen zu beantworten, würde eine Eskalation der Gewalt verursachen, die unkontrollierbar werden kann.

Im Einzelnen fordern wir:

- Konventionelle Waffen dürfen nicht zur Beantwortung eines Cyberangriffs verwendet werden.

Genfer Konvention im Cyberspace

Kritische Infrastrukturen sind attraktive Ziele für Angriffe in Kriegen, da ihre Fehlfunktion den Gegner fundamental schwächt. Die Fehlfunktion dieser Infrastruktur führt auch zu einer ernsthaften Schwächung der Zivilgesellschaft, wenn wichtige Einrichtungen zur Sicherung der Lebensgrundlagen, beispielsweise die Wasserversorgung, die Energieversorgung oder Einrichtungen zur Gesundheitsvorsorge angegriffen werden.

Im Einzelnen fordern wir:

- Alle anwendbaren Anforderungen der Genfer Konvention müssen im Cyberspace wie in der „realen Welt“ in analoger Weise beachtet werden: Lebenswichtige Infrastrukturen der Zivilgesellschaft dürfen kein Ziel von Cyberangriffen werden; dies schließt beispielsweise auch Kommunikationsinfrastruktur ein, wenn menschliches Leben davon abhängt. Es gilt auch für die sogenannten Kollateralschäden, denen Unbeteiligte zum Opfer fallen.
- Eine Verletzung dieses Prinzips muss von den Nationen als Kriegsverbrechen anerkannt werden.
- Nationen und ihre Regierungen müssen sich zu allgemeinen Prinzipien bekennen, auf die sie sich in internationalen Abkommen zur Regulierung von Konflikten im Cyberspace einigen.

Cyberpeace-Initiative auf Regierungsebene

Wir sehen das Internet und die weitere IT und Kommunikationssysteme (den Cyberspace) als eine kritische Kommunikationsinfrastruktur und eine bedeutende Basis für die menschliche Zukunft an. Damit bedeutet die Gefährdung dieser kritischen Infrastruktur, unsere gemeinsame Zukunft zu gefährden.

Im Einzelnen fordern wir:

- Regierungen müssen eine internationale Cyberpeace-Initiative vereinbaren und umsetzen.
- Friedensforschung und die Entwicklung friedenserhaltender Strategien müssen auf allen Ebenen gefördert werden.

Demokratische Kontrolle des Internet und von Cybersicherheits-Strategien

Heute werden Strategien zur Cybersicherheit offen diskutiert und Cyberkriegsstrategien im Geheimen entwickelt und umgesetzt. Nur Transparenz für alle Arten der Cyberstrategien kann Vertrauen schaffen und einem Rüstungswettlauf im Cyberspace entgegenwirken.

Im Einzelnen fordern wir:

- Demokratische Kontrolle muss sichergestellt und die Gewaltenteilung respektiert werden.
- Parlamente müssen Cybersicherheits-Strategien und ihre Umsetzung überwachen; Cyberangriffe müssen durch Parlamente zuvor bestätigt werden.
- Cybersicherheits-Strategien müssen das Ergebnis demokratischer Entscheidungsfindung sein.

Online-Protest ist kein Verbrechen

Information durch und Kommunikation über das Internet ist heute allgemeine Praxis und hat den Status eines Menschenrechts. Proteste gegen manche Unternehmen können nur im Cyberspace stattfinden – ein Beispiel sind Proteste von Verbrauchern gegen Online-Dienste. Grundrechte wahrzunehmen – beispielsweise freie Rede oder Versammlung – ist auch online kein Verbrechen. Es darf niemals als Rechtfertigung für militärische Antworten oder Kriege dienen.

Im Einzelnen fordern wir:

- Das Recht auf zivilen Widerstand und Online-Protest muss respektiert werden – in der Annahme, es wird keine Gewalt ausgeübt oder Schaden angerichtet.
- Online-Protest darf nicht kriminalisiert werden oder gar als Grund herhalten, einen Krieg zu beginnen.

Klar definierte und demilitarisierte politische Sprache

Politik und Medien nutzen häufig unklare Sprache in irreführender Weise, mit dem Potenzial, zu einer Eskalation von Konflikten beizutragen. Beispielsweise suggeriert der Begriff „Cyberkrieg“, dass nur militärische Lösungen in Frage kommen.

Im Einzelnen fordern wir:

- Der politische Sprachgebrauch muss entmilitarisiert werden.
- Begriffe müssen klar abgegrenzt und definiert werden: Cyberkrieg, Cyberterrorismus, Cyberkriminalität, Ethisches Hacken, politische Formen des Protests.

Schwachstellen müssen veröffentlicht werden

Heute scheinen Geheimdienste Schwachstellen auszunutzen, zu verursachen und sie gegebenenfalls für die zukünftige Nutzung geheimzuhalten. Diese Schwachstellen können auch für kriminelle Zwecke missbraucht werden. Werden sie dagegen veröffentlicht, ist es wahrscheinlich, dass sie schnell geschlossen werden – ein ausreichender Zeitraum muss aber gewährt werden, bevor sie öffentlich bekannt gemacht werden. Dadurch wird das öffentliche Bewusstsein und Vertrauen in defensive Sicherheitsstrategien erhöht.

Im Einzelnen fordern wir:

- Jeder muss Schwachstellen in verantwortlicher Weise und in einem vernünftigen Zeitrahmen veröffentlichen.
- Insbesondere öffentliche Stellen müssen die Integrität von Informationssystemen bewahren. Dies folgt aus dem Grundrecht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Schutz kritischer Infrastrukturen

Heute sind kritische Infrastrukturen häufig leicht vom Internet aus zu erreichen. Da Schwachstellen prinzipiell unvermeidbar sind, können sie angegriffen werden. Die Sicherheit kritischer Infrastrukturen muss durch kompetente und transparente Audits und Tests sichergestellt werden.

Im Einzelnen fordern wir:

- Betreiber kritischer Infrastrukturen müssen verpflichtet werden, diese Infrastrukturen gegen Cyberangriffe zu schützen.
- Sie müssen verpflichtet werden, sichere Systeme umzusetzen und zu betreiben.
- Sie dürfen sich zum Schutz der Infrastrukturen nicht auf staatliche Behörden verlassen.
- Wann immer möglich, müssen kritische Infrastrukturen – wie Atomkraftwerke – vom öffentlichen Internet getrennt sein.

Cybersicherheits-Zentren aufbauen und betreiben

Wir brauchen Einrichtungen, die sicherstellen, dass Bedrohungen aus dem Cyberspace effektiv entgegengewirkt wird, und die angemessene Instrumente dafür sind, Cybersicherheit zu erreichen und zu verbessern. Cybersicherheits-Zentren müssen so organisiert werden, dass sie fundamentale Bürger- und Menschenrechte schützen.

Im Einzelnen fordern wir:

- Cybersicherheits-Zentren müssen aufgebaut und angemessen mit Personal und Ressourcen ausgestattet werden, um effektiv mit Cyber-Bedrohungen umzugehen und ihnen entgegenzuwirken.

- Sie müssen konsequent auf den Frieden ausgerichtet sein und transparent arbeiten. Ihre Organsiation muss unabhängig von den Interessen staatlicher Sicherheit sein.

- Das Trennungsgebot von Polizei, Geheimdiensten und Militär ist konsequent umzusetzen; ihr Informationsaustausch muss reguliert werden, um demokratische Prinzipien einzuhalten.

Förderung (junger) IT-Experten

Heute mangelt es an IT-ExpertInnen und Know-How für effektiven Schutz gegen Cyberangriffe in Europa. Dieser Mangel wird durch IT-ExpertInnen verstärkt, die an Werkzeugen zur Kompromittierung der Infrastruktur arbeiten, anstatt ihre Sicherheit zu verbessern. Aktuell verschwindet Lehre aus den Curricula, die die Auswirkungen der Technologie auf die Gesellschaft behandelt. Diese Entwicklung muss rückgängig gemacht werden.

Im Einzelnen fordern wir:

- Die Qualität von IT-Produkten muss insbesondere unter dem Gesichtspunkt der IT-Sicherheit signifikant verbessert werden, um Schwachstellen zu reduzieren.

- Staatliche Behörden und Wirtschaftsunternehmen müssen in qualifizierte ExpertInnen investieren, insbesondere für IT und IT-Sicherheit.

- Die akademische Bildung muss verbreitert werden, um ethische und politische Aspekte der Technik und die Technikfolgenabschätzung abzudecken.

Förderung freier und offener Software

Im Gegensatz zu proprietärer Software macht freie und offene Software unabhängige Inspektionen und Reviews prinzipiell möglich – auch wenn dies Sicherheit nicht garantieren kann. Dennoch wird die Wahrscheinlichkeit von versteckten Hintertüren (Back-Doors) erheblich reduziert. Die gesamte Community kann solche Reviews durchführen, wenn sie effektiv sein sollen, müssen sie aber durch kompetente und unabhängige Auditorinnen und Auditoren sowie Prüferinnen und Prüfer erfolgen.

Im Einzelnen fordern wir:

- Freie und offene Software muss durch öffentliche Stellen gefördert und genutzt werden, insbesondere für IT-Systeme in kritischen Infrastrukturen.

- Öffentliche Stellen müssen kompetente und unabhängige Inspektionen und Reviews durchführen, fördern und durchsetzen.

- Eine realistische Risikokommunikation muss eingesetzt werden, um die Illusion von Sicherheit zu vermeiden.

Anhang: Definitionen

Cyberpeace: Unter Cyberpeace verstehen wir Frieden im Cyberspace in sehr allgemeinem Sinn: Die friedliche Anwendung des Cyberspace zum Nutzen der Menschheit und der Umwelt. Dies schließt den Verzicht auf alle Aktivitäten des Cyberkriegs ein, bedeutet aber auch die Nutzung der gesamten Kommunikationsinfrastruktur für internationale Verständigung.

Cyberspace: Jede Informations- und Kommunikationsinfrastruktur, Hardware wie Software, öffentlich wie privat, offen wie eingeschränkt. Offensichtlich geht dies über das Internet hinaus. Es kann Werkzeuge einschließen, die nicht mit einem Netz verbunden sind, wenn beispielsweise (wie bei STUXNET) ein USB-Stick genutzt wird, um Schadsoftware zu verbreiten.

Cyberkrieg: Die Nutzung von Computertechnologie um die Aktivitäten eines Staats oder einer Organisation zu stören, speziell der bewusste Angriff auf Kommunikationssysteme durch einen anderen Staat oder eine andere Organisation in Form eines Cyberangriffs.

Cyberkriminalität: Kriminelle oder illegale, strafbare Aktivitäten, die Dienste des Cyberspace nutzen.

Cyberterrorismus: Gewaltsame kriminelle Aktivitäten durch Nicht-Regierungs-Akteure, die darauf abzielen, politische Systeme durch die Erzeugung von Angst und Unsicherheit zu verändern.

Cyberangriff: Aktionen mit der Absicht, Informationen in einem Computer und/oder einem Computernetz abzustreiten oder zu zerstören, oder den Computer und/oder das Computernetz selbst zu schwächen, zu stören oder zu zerstören.

Hacktivismus: Politischer Aktivismus, der die Dienste des Cyberspace nutzt. Hacktivismus zielt nicht darauf ab, Schaden zu verursachen und wendet keine Gewalt an.

Online-Protest: Protestaktionen im Cyberspace, die keine Gewalt anwenden und keinen Schaden verursachen. Online-Protest kann Formen des Zivilen Widerstands einschließen.

Cyberwaffe: Jede Software oder Hardware, die durch Ausnutzen von Schwachstellen für die Ausführung eines Cyberschlags angewendet werden kann. Cyberwaffen nutzen üblicherweise Schwachstellen aus, die geheim gehalten werden, und deren destruktiver Charakter aus der Unmöglichkeit erwächst, Effekte seiner Ausnutzung abzuschwächen. Durch die Veröffentlichung der Schwachstellen können Gegenmaßnahmen eingeleitet werden.

Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht

Der Missbrauch der Informationstechnik für die ‚Revolution' des Kriegsgeschäfts

Informatik und Informationstechnik haben die Rüstungstechnik und in der Folge die militärischen Strategien und verteidigungspolitischen Doktrinen so grundlegend verändert, dass bereits in den 1990er Jahren, als die neuen technischen Optionen eher noch Visionen waren, der Begriff ‚Revolution in Military Affairs' geprägt wurde. Die mit dem Akronym RMA umrissenen Konzepte und Visionen beherrschen seither die sicherheits- und verteidigungspolitische Debatte. Korrespondierend zur informationstechnischen Durchdringung der öffentlichen und privaten Lebenssphären, zur stetigen Verlagerung realen Geschehens in virtuelle Räume scheint die Digitalisierung des Kriegsgeschäfts auch den Krieg zu einem virtuellen Szenarium werden zu lassen. Nur der Tod im Krieg, eingeplant oder kollateral in Kauf genommen, bleibt analog und mithin grausam wie je, versteckt jedoch hinter der Fassade des ‚sauberen' Neuen Kriegs …

Die dunkle Seite der Informationstechnologie

Edward Snowden hat uns darauf gestoßen, was wir eigentlich alle hätten lange wissen müssen: Die Technologien, mit denen während des letzten Vierteljahrhunderts eine weltumspannende, immer dichter werdende informationstechnische Vernetzung aufgebaut wurde, bieten einzigartige Optionen für eine Überwachung, die gleichermaßen Unternehmen, Behörden, Institutionen wie Privatpersonen erfasst. Zu Protesten mobilisieren die öffentlich wahrgenommenen Missstände wie Wirtschaftsspionage, Eindringen in Regierungsgeschäfte, Ausspähung der Privatsphäre. Weniger bewusst ist sich die Gesellschaft, dass die mit gigantischem Aufwand und staatlich sanktioniertem kriminellen Vorgehen – nicht nur von der NSA – betriebene Agglomeration und Ausforschung vertraulicher Daten weltweit Teil einer neuen Kriegsführung ist: Je früher und umfassender ich weiß, was der Feind (oder Freund!) plant, desto wirkungsvoller kann ich eingreifen!

Nicht immer geheim zu halten ist eine Ausspähung dieses Ausmaßes, die alle bisherige Spionagetätigkeit quantitativ wie qualitativ weit hinter sich lässt. Allein, sie ist nur der sichtbarste Teil der neuen Kriegsführung. Strikter geheim gehalten werden Entwicklung und Anwendung von Software-Werkzeugen, mit denen funktional in fremde Datenverarbeitungssysteme und -strukturen eingegriffen werden kann, von Informationsmanipulation zur Desorientierung des Gegners bis zu Sabotageakten mit kinetischer Wirkung – *Cyber warfare.* All diese vom Grunde her militärischen Operationen schwimmen weitgehend unbemerkt mit in den Datenströmen der digitalen Kommunikationssysteme, die mit ihren Glasfaserkabeln und Funknetzen, terrestrisch und satellitengestützt, jeden Ort unserer Erde erreichen. Und dies sind just dieselben Systeme, die einst mit dem Versprechen einherkamen, ob ihrer Völker verbindenden, Grenzen überwindenden Wirkung den Frieden zu fördern. Mehr noch, sie werden gleichzeitig zum Nervensystem der Streitkräfte zu Lande, zu Wasser und in der Luft.

Network centered warfare – das war das *buzz word* der *„Joint Vision 2010"*, ein Positionspapier des US-Generalstabs, vorgestellt 1996, vier Jahre später aktualisiert in der *„Joint Vision 2020"*[1]. Als Kernbotschaft forderte es eine gründliche Restrukturierung der US-Streitkräfte mit dem Ziel einer umfassenden Nutzung moderner Kommunikations- und Informationstechnologie in Waffen, in Waffensystemen und in den zu ihren Einsatz notwendigen Infrastrukturen. Die *Joint Vision 2010* warb bereits für den Einsatz global vernetzter Gefechtseinheiten, für die Einbettung aller Arten von Kampffahrzeugen – vor allem auch unbemannter – bis hin zum einzelnen Soldaten im Schlachtfeld in eine einheitliche *Communication Command Control Intelligence*, C3I. Der Kreis schließt sich, wenn diese Systeme zunehmend dazu dienen, völkerrechtswidrige Drohneneinsätze gegen *high value targets* durchzuführen. ‚Hochwertziele', das sind Menschen, die vor allem durch Ausspähung ihrer Kommunikation als (potentielle) Terroristen identifiziert wurden, vielleicht auch nur auf Grund von verdächtig machenden Verhaltensmustern (*signature strike*), die schließlich über ihre Mobiltelefone als Abschussziel geortet werden.

Die militärische Nutzung der Informatik und Informationstechnik hat eine kaum beachtete Rückwirkung auf die Zivilgesellschaft. Mit einem kurzen Rückblick auf die Geschichte ihrer mi-

Dietrich Meyer-Ebrecht und Hans-Jörg Kreowski

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

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

litärischen Entwicklung, einem Überblick über den derzeitigen Entwicklungsstand hoch technologisierter Waffen und einem Einblick in die zunehmende Verwischung zwischen ziviler und militärischer Forschung und Entwicklung möchten wir auf die daraus resultierenden Gefahren aufmerksam machen – und an die Verantwortung unseres Berufsstandes erinnern.

Die militärischen Wurzeln der Computertechnik und der Informatik

Die Entwicklung von Computertechnik und Informatik ist in ihren Anfängen stark vom Geld und von den Wünschen des Militärs beeinflusst[2]. Konrad Zuse baute seit 1936 an einer Serie von Computern. Was in einem privaten Rahmen begann, ist bald mit erheblichen nationalsozialistischen Geldmitteln im kriegerischen Kontext vorangetrieben worden und hat unter anderem zu einem Spezialrechner für die Flügelvermessung einer ferngesteuerten Gleitbombe geführt. Unter der Leitung von Alan Turing wurde an der *Government and Cypher School* im englischen Bleachley Park die „*Bombe*" entwickelt, die computergestützt die deutsche Verschlüsselungsmaschine *ENIGMA* geknackt hat und so einen wesentliche Einfluss auf den U-Boot-Krieg im Atlantik hatte.

Das Herrenhaus von Bletchley Park (2002) war die Zentrale der britischen Codeknacker und ist heute ein Museum
Foto: Matt Crypto

In den USA wurde spätestens ab 1943 die Computerentwicklung massiv betrieben. Unter anderem entstanden die *ENIAC* zur Berechnung ballistischer Tabellen, der *STRETCH*-Computer, der bei der Entwicklung der Wasserstoffbombe zum Einsatz kam, sowie die *WHIRLWIND*-Serie, die in den 1950er Jahren zu den *SAGE*-Computern führte als Teil eines Luftabwehrsystems. Wie bei *SAGE* verlässt sich der militärische Komplex der USA in den 1950er und 1960er Jahren mehr und mehr auf große, teure und unzuverlässige Computerprogramme u. a. *beim North American Defence System*, beim *Ballistic Missile Early Warning System* und beim *Anti Ballistic Missile System*.

Wegen der immensen Kosten und großen Fehleranfälligkeit der Systeme wurde die ‚Softwarekrise' proklamiert. Die Antwort des US-amerikanischen Department of Defence und der NATO war die Etablierung des Fachgebiets Softwaretechnik durch eine Konferenzserie ab 1969, die Entwicklung der Programmiersprache *ADA* als NATO-Standard in den 1970er Jahren, die Entwicklung von *Very High Speed Integrated Circuits* ab 1980 und die Ausschreibung zweier umfangreicher Forschungsförderungsprogrammen im Jahre 1983: *Software Technology for Adaptable Reliable Software* (*STARS*) und *Strategic Computing Initiative* (*SCI*). Beide hatten eine prägende Wirkung auf Softwaretechnik und Künstliche Intelligenz als Schlüsselgebiete der Informatik. Ebenfalls im Jahre 1983 wurde die *Strategic Defence Initiative* (*SDI*) aufgelegt, die noch gigantischer konzipiert war, aber neben der Informatik vor allem auch andere Technogiebereiche einbezog. Mit diesem gewaltigen Schub durch militärische Finanzmittel und kriegerische Absichten in den 1970er und 1980er Jahren aber kam auch die kommerzielle und zivile Informations- und Kommunikationstechnik stark auf, so dass sich die Informatik ein Stück weit von ihren militärischen Wurzeln emanzipieren konnte.

Die Triebfeder der IT-Evolution

Die Genesis der Computer war militärisch motiviert und angetrieben, und immer noch und sogar zunehmend sind sie essentielle Teile von Waffen und Waffensystemen. Erstaunlich, dass wir Computer dennoch nicht als genuin militärische Technologie identifizieren. Das hat zwei Gründe. Zum einen werden Computer in Waffen kaum wahrgenommen. Betrachten wir beispielsweise eine Drohne – offensichtlich eine besondere Art von Flugkörper, aber weit weniger offensichtlich ist, dass ihr Rumpf mit Informationstechnologie vollgestopft ist und eine noch umfassendere informationstechnische Infrastruktur ihre Operationen unterstützt. Zum Anderen verkörpern Computer *das* klassische Beispiel einer Dual-Use-Technologie.[3] Denn kaum hatten Computer ihre Funktionsfähigkeit und Nützlichkeit in militärischen Anwendungen bewiesen, setzte eine nicht mehr zu bremsende Entwicklung ziviler Anwendungen ein. Mittlerweile ist Informationstechnologie in allen zivilen Lebensbereichen zu einer solchen Selbstverständlichkeit geworden, dass ihre Nutzung (auch) in Waffensystemen nicht mehr als eine Besonderheit wahrgenommen wird. Die Alltäglichkeit der Computer ist es, die ihre fundamentale Rolle in militärischen Anwendungen relativiert und sogar verschleiert. Ihre Dual-Use-Natur macht selbst Fachleute blind für ihr zerstörerisches Potential.

Andererseits werden Computer mittlerweile nicht nur als eine zivile Technologie wahrgenommen, sie sind sogar zu einer ‚zivilen' Technologie geworden – mindestens, wenn wir von der Triebkraft ausgehen, mit der die Flut ziviler Anwendungen ihre Weiterentwicklung und Reifung vorangetrieben hat. Die Subtilität der Produktionsprozesse, die Komplexität ihrer Funktionalität, beides konnte sich in der heute erreichten Perfektion, Zuverlässigkeit und Wirtschaftlichkeit nur in einem Jahrzehnte währenden Evolutionsprozess entwickeln. Mutation und Selektion in vielen kleinen Schritten, ein Prozess, der sich auf myriadenfache (zivile) Anwendung stützt – und auf unseren Konsum von IT-Produkten, mit dem wir die dahinterstehenden Investitionen für eine hoch gezüchtete Produktionstechnologie finanziert haben. Den Nutzen hat *auch* die Rüstungstechnik! Weitgehend nutzt sie dieselbe Technologie, dieselben Komponenten, dieselben informatischen Methoden. Denn selbst wenn eine eigenständige militärische Informationstechnologie wünschenswert wäre, sie könnte nicht in kurzer Zeit aus dem Boden gestampft werden, auch nicht mit immensen Mitteln, denn ihr fehlte der Evolutionsprozess, der sich auf die ungeheure Vielfalt und Vielzahl von Anwendungen stützt.

Wir können es auch so sehen: Uneingeschränkt nutzen militärische Anwendungen die ausgereiften Produktionstechnologien für zivile IT-Produkte. Forschung und Entwicklung, mögen sie auch primär auf zivile Nutzungen ausgerichtet sein, kommen letztlich ebenfalls auch der militärischen Anwendung zugute. Die Folge ist eine sich ausdehnende Grauzone zwischen zivilen und militärischen Zielsetzungen. Ein prominentes Beispiel ist die Robotertechnologie.

Der Alptraum autonomer Killerroboter

Im Rahmen der *Strategic Computing Initiative* wurden der Künstlichen Intelligenz drei Aufgaben gestellt: eine Pilotenassistenz, ein Schlachtenlenksystem und ein Militärfahrzeug, das sich autonom in fremdem Gelände zurechtfindet, Hindernissen ausweichen und sich bei Bedarf auch verstecken kann. In den letzten 30 Jahren sind mit Milliarden an Forschungsförderungsmitteln weltweit die wissenschaftlichen Grundlagen vorangetrieben worden, die solche und verwandte Anwendungen möglich machen. Vieles davon fand im zivilen Bereich und mit zivilen Anwendungszielen statt, was insbesondere auch für die Entwicklung autonomer Systeme in der Robotik gilt. Parallel dazu aber gibt es umfangreiche Programme, Roboter kriegstauglich zu machen. Die USA planen in den nächsten Jahrzehnten ein Drittel ihrer Waffensysteme durch unbemannte Kampfvehikel in der Luft, an Land sowie auf und unter Wasser zu ersetzen[4]. Der Prozess ist bereits in vollem Gange, wie die Killerdrohnen *Predator* mit zwei *Hellfire*-Raketen und *Reaper* mit acht *Hellfire*-Raketen und deren tausendfache Einsätze in Afghanistan, Pakistan und Jemen belegen.

An der Einsatzfähigkeit solcher Waffen ist die Informatik erheblich beteiligt, weil Erkenntnisse über eingebettete Systeme, digitale Kontrolle, Sensortechnik, Bildverarbeitung, Kommunikationsnetze, Big Data und anderes mehr in militärische Roboter Eingang finden. Allerdings sind solche Systeme heute noch nicht vollautomatisch im Einsatz. Die Killerdrohnen Predator und Reaper zum Beispiel schießen Raketen erst ab, wenn dazu der Befehl eines Soldaten aus Nevada (oder teils wohl auch aus Ramstein) kommt. Erklärtes Ziel ist jedoch die Entwicklung völlig autonomer bewaffneter Roboter, die insbesondere auch selbst entscheiden, wann sie töten.

Wenn Maschinen entscheiden, ob sie ihre Waffen gegen Menschen richten oder nicht, dann ist das nach dem Kriegsvölkerrecht nur im Krieg zulässig, wenn die entsprechenden Regeln in der Haager Landkriegsordnung und der Genfer Konvention eingehalten werden. Autonom tötende Roboter müssen also kämpfende Soldaten von anderen Personen – insbesondere Zivilpersonen – unterscheiden können sowie kulturelle Güter schonen. Sie müssen in diesem Sinne ethisch korrekt handeln können. Einige Fachleute wie beispielsweise Ron Arkin vom Georgia Institute of Technology sind überzeugt, dass Maschinen gebaut werden können, die dazu in der Lage sind[5]. Sie seien sogar besser als menschliche Kämpfer, weil sie nicht in Panik geraten und unethische Befehle verweigern ohne Rücksicht auf die Folgen für sie selbst.

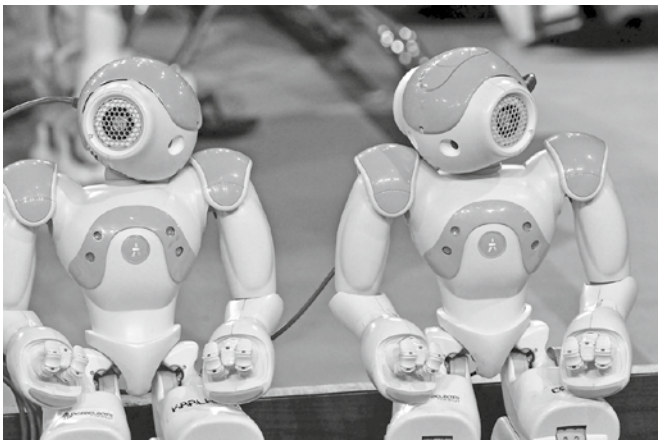
An dieser Position seien erhebliche Zweifel erlaubt. Eine künstliche Ethik ist wohl kaum einfacher zu entwickeln und zu programmieren, wenn es überhaupt möglich ist, als künstliche Intelligenz. Daran arbeiten Tausende von Wissenschaftlerinnen und Wissenschaftlern schon seit über 50 Jahren, aber trotz aller beachtlichen Einzelerfolge kann bisher nicht wirklich von *Intelligenz* die Rede sein.

Das Problem ist, dass nur programmiert werden kann, wofür es ein formales berechenbares Modell gibt. Das könnte bei ethischen Fragen bereits scheitern. Aber selbst wenn es prinzipiell ein solches Modell gäbe, könnte es zuviel Zeit benötigen oder fehlerhaft sein. Für die meisten Entscheidungsprobleme sind keine effizienten Lösungen bekannt. Warum sollten ethische Entscheidungen da eine Ausnahme machen? Die meisten Programmsysteme sind nicht fehlerfrei und es ist schon gar nicht bewiesen, dass keine Fehler auftreten. Warum sollte bei Programmen, die ethisch korrekt arbeiten sollen, das anders sein?[6]

Autonome Killerroboter werden unserer Meinung nach gar nicht oder jedenfalls nicht in absehbarer Zeit nach dem Kriegsvölkerrecht agieren können. Sie werden deshalb die schon heute virulenten Probleme von Kampfrobotern verschärfen wie der Einsatz in unerklärten Kriegen, viele zivile Opfer, gezielte Tötungen, Ausdehnung der Asymmetrie der kriegführenden Parteien und damit Provokation terroristischer Anschläge. Da sich diese Probleme und Gefahren nicht technisch beherrschen lassen, müssen autonome Waffensysteme wie biologische und chemische Waffen verboten werden.

Die gesellschaftliche Brisanz einer zivil-militärischen Verflechtung

Roboter sind ein alarmierendes Beispiel einer gefährlichen Verschmelzung ziviler und militärischer Technologie, gerade im Bereich der Informatik. Denn mehr als irgendeine andere Waffe beruhen autonome Waffenträger auf avancierten Methoden der Informatik, speziell auf dem Gebiet der Künstlichen Intelligenz. Wir müssen daher im Rückschluss argwöhnen, dass militärische Ziele zur treibenden Kraft hinter manch einem zivil deklarierten Forschungsprojekt werden. Besonders auffällig ist die Verflechtung der Interessen bei – offen oder verdeckt gesponserten – Roboterwettbewerben wie *Robocup* für Fußball spielende Roboter oder *DARPA Grand Challenge* für autonome Fahrzeuge in den USA.



Roboter in Wartestellung beim Robocup 2013 in Eindhoven
Foto: Ralf Roletschek – Fahrradtechnik und Fotografie

Eine strikte Trennung ist sicherlich auch gar nicht im Interesse der Industrie, denn welches große ‚zivile' Unternehmen ist nicht auch mit Rüstungsaufträgen befasst? Unterstützt wird sie darin von nationaler und europäischer Politik. Interessant ist, wie die Grenze zwischen ziviler und militärischer Forschung und Entwicklung absichtsvoll verwischt wird. 1. Akt: Euphemistische Sprachregelungen werden etabliert, mit denen die Abgrenzung verschleiert wird: *Sicherheitsforschung, Sicherheitsarchitektur, Sicherheitstechnologie …* – unter dieser Decke lässt sich gerade bei informationstechnischen Applikationen, Komponenten und Systemen eine genuin militärische Bestimmung gut verbergen. 2. Akt: Organisatorische Strukturen werden ‚angepasst': Die Fraunhofer-Gesellschaft legt beispielsweise fünf ihrer Institute mit drei Instituten der vom Bundesverteidigungsministerium finanzierten *Forschungsgesellschaft für angewandte Naturwissenschaften* (FGAN) zum *Verein für Verteidigungs- und Sicherheitsforschung* (VVS) zusammen, wo nun zivile und militärische Forschung unter einem Dach stattfindet. Und schließlich der 3. Akt: Budgets werden geschaffen: Unter Bundesministerin Schavan wurde ‚Sicherheitsforschung' ein relevantes Segment ihrer sechs Milliarden Euro schweren ‚*Hightech-Strategie*'. Das korrespondierende ‚*Security Research Programme*' der Europäischen Kommission allein war mit 1,4 Milliarden Euro bestückt.[7]

Das Verschmelzen ziviler und militärischer Technologieentwicklung ist kein Alleinstellungsmerkmal der Informatik und Informationstechnik. Nur wird sie dort mit einem besonderen Nachdruck betrieben. Und ob der Alltäglichkeit und Allgegenwärtigkeit der Computer passiert sie unauffällig, selbstverständlich. Das scheint uns der Grund zu sein, warum die *Revolution in Military Affairs*, die von Informatik und Informationstechnik angetriebene Revolution des Kriegsgeschäfts, mit so wenig öffentlichem Aufsehen voranschreitet. Dennoch, sie *ist* eine Revolution. Natürlich zuvorderst für militärische Strategen. In ihrer Folge aber verändert sie gesellschaftliche Einstellungen und politische Doktrinen, stört ausbalancierte Machtgefüge, beeinflusst Konfliktbereitschaft und Konfliktlösungsansätze. Gerade für Waffen, die in hohem Maße auf informatische Methoden und Informationstechnik aufbauen, gilt Jürgen Altmanns Aussage, „dass Krieg und Frieden zwar im Kern politische Fragen seien, dass jedoch neue Waffentechnologien […] massiven Einfluss auf gesellschaftliche Prozesse und Entwicklungen haben und den Frieden gefährden".[8]

Anmerkungen

1 *Volltexte zu finden unter http://www.dtic.mil/jv2010/jv2010.pdf und http://www.fs.fed.us/fire/doctrine/genesis_and_evolution/source_materials/joint_vision_2020.pdf*

2 *Siehe für eine ausführlichere Darstellung z. B. Joachim Bickenbach, Reinhard Keil-Slawik, Michael Löwe, Reinhard Wilhelm (Hrsg.): Militarisierte Informatik, Schriftenreihe Wissenschaft und Frieden Nr. 4, Berlin 1985 oder Hans-Jörg Kreowski: Informatik und Militär: Zusammen in den Abgrund, In: Umdenken in der Informatik [2. Jahrestagung des Forums Informatiker für Frieden und gesellschaftliche Verantwortung e. V., Oktober 1986, Berlin], S. 37-42*

3 *Dietrich Meyer-Ebrecht: Dual-use und die Zivilklausel: ‚Sicherheitsforschung' – oder wie Rüstungsforschung zivile Forschung vereinnahmt. FIfF Kommunikation 4/2012, S. 56–58*

4 *Siehe http://www.defense.gov/pubs/DOD-USRM-2013.pdf*

5 *Ronald C. Arkin: Lethal Behavior in Autonomous Robots, Chapman & Hall/CRC 2009*

6 *Für ausführlichere Überlegungen dazu siehe Hans-Jörg Kreowski: Gehören Killerroboter vor ein Kriegsgericht, FIfF-Kommunikation 4/2011, S. 27-30*

7 *Eric Töpfer: Zivil-militärische Sicherheitsforschung. Wissenschaft und Frieden 4/2012, S. 16–19*

8 *Jürgen Altmann: Grundfragen der Bewertung und Gestaltung von Naturwissenschaften und Technik. In: J. Altmann et al.: Naturwissenschaft – Rüstung – Frieden. Basiswissen für die Friedensforschung. Wiesbaden 2007, S. 451*

Ingo Ruhmann

Wieso FIfF?

1982 arbeitete ich als Studi in einem KI-Projekt der Gesellschaft für Mathematik und Datenverarbeitung – einer Forschungseinrichtung, die später in der FhG aufging. Innerhalb kurzer Zeit erfuhr ich, dass es Probleme gab mit der Lieferung von LISP-Maschinen aus den USA und in der Uni Dortmund mit der von Updates für BSD Unix. Der Grund: Die Passwort-Kryptoalgorithmen der Software, die einem Exportverbot unterlagen. Außerdem wurde von der GMD in den USA bestellte Designsoftware für VLSI-Chips zurückgehalten.

Ich sollte der Sache nachgehen. Heraus kamen diverse Probleme in deutschen Forschungseinrichtungen mit Exportverboten von Dual-Use-Gütern. Auch wurde Gästen wissenschaftlicher Konferenzen in den USA kein Visum erteilt. Ich stellte ein Dossier zusammen, wie intensiv die NSA versucht hatte, die sich entwickelnde unabhängige Kryptographie-Forschung zu behindern und zu kontrollieren. Präsident Reagan erließ 1982 eine Executive Order, die jede Kryptoforschung in den USA – egal, wie finanziert – erstmalig der Geheimhaltung und jede Publikation der Freigabe durch die NSA unterwarf. Anfang der 1980er Jahre wurde in alle IT-Forschungsprojekte des Pentagons eine Klausel eingefügt, um jede wissenschaftliche Publikation vorab vom Pentagon genehmigen zu lassen. Exportverbote wurden ausgeweitet auf IT-Produkte aus der KI, dem Chipdesign, der Netzwerktechnik und vieles mehr. Das Pentagon und die NSA versuchten, auf die Entwicklung der Informatik massiv einzuwirken. Hintergrund für all diese Kontrollversuche war die Politik des Kalten Krieges unter Präsident Reagan, die auch in der Informatik mit aller Härte ausgetragen wurde.

So kam ich mit allen jenen Informatik-KollegInnen zusammen, die 1984 dann in Bonn gemeinsam das FIfF gründeten. Deswegen ging es im ersten Büchlein des FIfF auch um Export- und Kryptokontrolle. Fast so wie heute.

Ingo Ruhmann *ist Gründungsmitglied des FIfF und war von 1988–1995 FIfF-Geschäftsführer und von 1991–2001 FIfF-Vorstandsmitglied.*

Thomas Reinhold

Friedens- und sicherheitspolitische Fragen zur Militarisierung des Cyberspace

Seit Stuxnet spielt der Cyberspace auch auf der international politischen Ebene eine wichtige Rolle, und die Erkenntnisse aus diesem ersten Einsatz einer gezielt entwickelten, staatlichen „Cyberwaffe" haben viele sicherheits- und friedenspolitische Fragen aufgeworfen. Neben den Schwierigkeiten einer Einschätzung konkreter nationaler Bedrohungen und dem Zerstörungspotential derartiger Schadsoftware sorgen vor allem Staaten, die den Cyberspace in ihre offensive militärische Planung aufnehmen, für Verunsicherungen. Die Veröffentlichungen des Whistleblowers Edward Snowden unterstreichen dabei, dass Stuxnet kein Einzelfall ist und dass alle führenden Nationen ihre sicherheitspolitischen Interessen auch im Cyberspace durchsetzen wollen.

Dem gegenüber gestaltet sich die Übertragung etablierter Regeln des internationalen Völkerrechts und insbesondere des Kriegsvölkerrechts als sehr schwierig. Entscheidende Fragen wie die Abgrenzung zwischen *Cybercrime* und *Cyberwar*, die klare Definition von *Cyberwaffen* sowie die Probleme um die Attribution von Cyberattacken und dem Recht auf staatliche Selbstverteidigung sind Gegenstand aktueller Diskussionen. Angesichts der Erkenntnis um die Kritikalität von IT-Infrastrukturen besteht die Sorge vor Attacken im Cyberspace als Bestandteil oder Auslöser zukünftiger klassischer Konflikte und dem Einsetzen einer neuerlichen Rüstungsspirale. Der Friedens- und Sicherheitsforschung stellen sich damit neue Herausforderungen und Aufgaben, deren Ziel die Verankerung von verbindlichen Normen der friedlichen Entwicklung des Cyberspace auf internationaler Ebene sein muss. Doch der Anwendung etablierter Maßnahmen der Verifikations- und Rüstungskontrolle im Cyberspace stellen sich unter anderem aufgrund des ausgeprägten Dual-Use-Charakters der IT neue Probleme. Im Artikel werden diese unterschiedlichen Seiten der friedens- und sicherheitspolitischen Fragen zur Militarisierung des Cyberspace und die Perspektiven einer friedlichen Entwicklung des Cyberspace dargestellt. Der Fokus liegt dabei auf der Identifikation der inhaltlichen Schnittmengen mit der Informatik, deren Analysen bezüglich ihres Potentials für die Entwicklung von Cyberwaffen und den sich daraus ergebenden Bedrohungsszenarien für die anstehenden Debatten unabdingbar sind.

Mit der Entdeckung der Malware *Stuxnet* im Juni 2010 ist der Cyberspace in den Focus der internationalen Sicherheitspolitik gerückt, und die Diskussionen um die Schadsoftware haben ein wichtiges Licht auf die cyber-sicherheitspolitischen Ziele einiger Nationen geworfen. Studien des *Center for Strategic and International Studies* (CSIS2011) kommen zu dem Ergebnis, dass gegenwärtig 40 Staaten Cyber-Programme als Teil ihrer militärischen Ausrichtung anstreben oder bereits betreiben, die neben defensiven Aspekten und dem Schutz eigener Infrastrukturen im Fall von zehn Staaten auch explizit offensive Maßnahmen zum Stören und Zerstören fremder IT-Systeme umfassen. Die Vorfälle um *Stuxnet* haben darüber hinaus die komplexen und umfassenden Abhängigkeiten von IT-Infrastrukturen und Computersystemen und die unklaren Gefährdungen derartiger Systeme verdeutlicht, insbesondere da *Stuxnet* trotz aller Schutzmaßnahmen in der Lage gewesen ist, das stark abgeschottete Netzwerk der Uran-Anreicherungsanlage in Natanz zu infiltrieren und Kanäle zum Datenaustausch aufzubauen. *Stuxnet* zeigte nicht nur die mittlerweile erreichte technische Ausgereiftheit von Schadsoftware. Sie verdeutlichte darüber hinaus die Bereitschaft von Staaten, auch den Cyberspace im Rahmen ihrer außenpolitischen Zielsetzung einzusetzen und rührt damit an historischen Entwicklungen wie dem Kalten Krieg, den Rüstungswettläufen in der atomaren, biologischen und chemischen Kampfführung und Debatten um die Aufrüstung des Weltalls. Internationale Organisationen wie die UN oder die OECD haben Expertengruppen und Gremien einberufen, um sich diesen Problemen zu widmen. Das durch Edward Snowden veröffentlichte Material und die Erkenntnisse über Werkzeuge und den politischen Willen nationaler Akteure zur technologischen Dominanz über den Cyberspace unterstreichen die Brisanz dieser Fragen. Angesichts dieser Entwicklungen ergeben sich für die internationale Friedens- und Sicherheitspolitik im Cyberspace drei wesentliche Problem- und Themenfelder, die nachfolgend näher betrachtet und in ihrer Bedeutung und Bandbreite vorgestellt werden.

Fehlende internationale Normen und Definitionen für den Cyberspace

Eine grundlegende Problematik bei der Bewertung von Vorfällen im Cyberspace besteht in der Unterscheidung zwischen normaler Kriminalität im Cyberspace, dem sog. *Cybercrime,* und Vorfällen staatlichen und gegen andere Staaten gerichteten Handelns, dem *Cyberwar*. Eine solche Unterscheidung ist in konkreten Situationen unter anderem aufgrund des Attributions-Problems, auf das weiter unten eingegangen wird, schwer zu treffen, definiert aber entscheidend die Handlungsoptionen der betroffenen Akteure. Während Vorfälle von Cybercrime vor allem Fragen des internationalen Strafrechts und der internationalen Strafverfolgung umfassen, berühren Akte staatlich aggressiven Verhaltens im Cyberspace Normen und Regelungen des internationalen Völkerrechts. Darüber hinaus liegt es im Ermessen eines betroffenen Staates, wie die Bedrohung durch einen Cyber-Vorfall bewertet wird und auf welchen politischen und juristischen Ebenen auf eine solche Situation reagiert wird. Für den Bereich Cybercrime wurden in den vergangenen Jahren Regularien wie die Budapester Cybercrime-Convention von 2001 (EU-Rat2001) etabliert und in den Nachfolgejahren weiter ausgearbeitet, auf deren Basis sich internationale Behörden wie ICPO-Interpol oder Europol den Aufgaben der internationalen Kriminalität im Cyberspace widmen. Parallel dazu werden EU-Staaten durch die europäische Agentur für Netz- und Informationssicherheit (ENISA) bei Cybervorfällen beratend unterstützt und über Kooperationszentren international vernetzt.

Dem gegenüber sind für Cyber-Vorfälle, die mutmaßlich auf staatliche Akteure zurückzuführen sind oder die durch Dritte in staatlichem Auftrag durchgeführt wurden, anerkannte Normen schwer anwendbar, weil nationale Akteure nicht identifiziert, Vereinbarungen nicht überprüft werden können oder es an international verbindlichen Übereinkünften fehlt. Eine Übertragung des humanitären Völkerrechts auf den Cyberspace ist

unter anderem hinsichtlich der nationalstaatlichen Souveränität und der damit zusammenhängenden Schutz- und Verteidigungsrechte, aber auch mit Blick auf die Verantwortlichkeiten von Staaten im Cyberspace umstritten. Dies wird beispielsweise an Staaten wie Russland oder China deutlich, die eine vollständige Kontrolle über digital in nationalen Netzen verbreitete Informationen als Bestandteil ihrer nationalstaatlichen Souveränität im Cyberspace betrachten, ohne dies mit einer expliziten Anerkennung der allgemeinen Menschenrechte für digitale Meinungsäußerungen zu verbinden (UNGA2011).

Eine weitere Frage betrifft das Ausmaß des durch eine Cyberattacke verursachten Schadens, das einem bewaffneten Angriff im Sinne des völkerrechtlichen "ius ad bellum" (des "Rechtes zum Krieg") entsprechen würde und eine staatliche Selbstverteidigung nach Art. 51 der UN Charta (UN1945) legitimieren würde. Wichtige Beiträge zu diesen Fragen haben unter anderem das 2013 veröffentlichte *Tallin Manual* (CCDCOE2013) des NATO Exzellenz-Zentrums CCDCOE (Cooperative Cyber Defence Centre of Excellence) und die *Ergebnisse der UN Group of Governmental Experts* (UN-GGE2012) geleistet, die sich mit der Anwendung und Ausweitung etablierter Normen des Völkerrechts auf den Cyberspace, den dabei entstehenden Schwierigkeiten und Grenzen auseinandersetzen und unterschiedliche Herangehensweisen diskutieren. Während die Einschätzungen weitgehend darüber übereinstimmen, dass Cyberattacken unter bestimmten Bedingungen die nationalstaatliche Souveränität verletzen können, bestehen hinsichtlich klarer Definitionen zu Cyberattacken große Differenzen, insbesondere hinsichtlich der Vergleichbarkeit zu klassischen bewaffneten Angriffen und der Frage nach angemessenen Reaktionen auf Cyberattacken wie dem Einsatz kinetischer Wirkmittel.

Erschwerend für die Etablierung verbindlicher Normen kommt neben den Fragen nach der Motivation eines Cyber-Zugriffs die Unterscheidung zwischen jenen Cyber-Aktivitäten hinzu, die zum Zweck reiner Spionage ohne primär schädigende Wirkung durchgeführt werden, gegenüber Angriffen, die aktiv und gezielt zur Störung fremder IT-Systeme eingesetzt werden. Beide Arten von Zugriffen funktionieren grundsätzlich nach ähnlichen Prinzipien, werden mit vergleichbaren Hilfsmitteln durchgeführt. Sie unterscheiden sich vor allem in dem vom Angreifer installierten und kontrollierten Bestandteil einer Schadsoftware, der auf den Zielsystemen die gewünschten Schadfunktionen durchführt (*payload*). Diese können entweder im Kopieren und Entwenden von Informationen bestehen, aber auch, wie beispielsweise im Falle der Angriffe auf die Saudiarabische Firma Saudi Aramco, gleichzeitig mehrere tausend befallene PCs vollständig außer Betrieb setzen (IISS2013).

Ein weiteres Problem für die Anwendung völkerrechtlicher Regeln besteht in der bereits erwähnten Attribution von Angriffen im Cyberspace, also der zeitnahen Identifikation des Ursprungs eines Angriffes. Dies ist im Cyberspace sehr viel schwerer möglich als bei konventionellen Waffen, denn Angreifer haben umfangreiche Möglichkeiten, die eigene Identität zu verschleiern, um sich vor Sanktionen zu schützen. Obgleich in Debatten oft auf die praktische Unmöglichkeit der Attribution verwiesen wird, argumentieren Autoren wie Herb Lin (LIN2011), dass für eine Attribution von Cyberattacken zum einen nicht der exakte Ausgangs-Computer selbst identifiziert werden muss, sondern dass unter Umständen bereits die Identifizierung des Herkunftsnetzwerkes ausreicht, um Indizien über den Angreifer zu sammeln. Zum anderen nehmen Zugriffe auf komplexe Systeme für deren Planung und Durchführung in aller Regel einige Zeit in Anspruch, in der Übertragungsdaten gesammelt, forensisch aufbereitet und in Verbindung mit der Einschätzung der internationalen politischen Lage für eine Attribution verwendet werden können (CLARK2010). Anhand eines solchen Ansatzes wurde im Frühjahr 2013 durch die US-amerikanische IT-Forensik-Firma *Madiant* eine Cyber-Einheit der chinesischen Volksbefreiungsarmee (PLA Unit 61398) als Angreifer hinter mehreren, über viele Jahre hinweg durchgeführten Angriffen gegen US-amerikanische Organisationen und Einrichtungen identifiziert (MADIANT2013) und zeitgleich zu hochrangigen Gesprächen zwischen den Präsidenten und Außenministern der USA und Chinas über Sicherheit im Cyberspace veröffentlicht.

Die Schwierigkeiten zur Entwicklung internationaler Normen für den Cyberspace werden des weiteren flankiert von Unklarheiten bei der Definition von *Cyber-Waffen*. Wie bereits dargelegt, unterscheiden sich die Hardware- und Software-Hilfsmittel für den Zugriff auf fremde Systeme unabhängig von der konkreten Absicht nur unwesentlich. Eine Studie der OECD widmet sich dieser Frage unter dem Blickwinkel der Eigenschaften klassischer Waffen: *„There is an important distinction between something that causes unpleasant or even deadly effects and a weapon. A weapon is directed force – its release can be controlled, there is a reasonable forecast of the effects it will have, and it will not damage the user, his friends or innocent third parties"* (BROWN2010). Die Autoren definieren anhand dieser Betrachtung wichtige Orientierungspunkte für die Bewertung konkreter Schadsoftware auf Basis technischer Details, der politischen Situation der staatlichen Akteure und deren vermeintlicher Intention. Die Autoren schlagen darin eine Einteilung jeglicher Schadsoftware in einem Kontinuum zwischen *low level cyber weapons* (das Manipulieren von Webseiten oder gezielt versandte, zu Spionage-Zwecken mit Malware infizierte

Thomas Reinhold

Thomas Reinhold arbeitet als Wissenschaftler am Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH) und betreibt unter cyber-peace.org eine Webseite, auf der er sich der Analyse der Vorfälle im Cyberspace und den Problemstellungen einer drohenden Militarisierung des Cyberspace widmet.

E-Mails) und *high level cyber weapons* (Attacken mit unmittelbarer, länger anhaltender störender oder zerstörender Wirkung) vor. Eine hinreichende Klassifikation einer Malware und die Entscheidung, ob es sich um eine Waffe im Sinne des Völkerrechts handelt, kann demzufolge nur in konkreten Einzelfällen anhand ihrer Wirkung situativ vorgenommen werden.

Technische Details der „Cyber-Waffen" und unklare Bedrohungsszenarien

Gerade die Diskussion über *Cyber-Waffen* verdeutlicht den Bedarf an konkreten technischen Details über die Cyber-Programme von Nachrichtendiensten und Militärs, die für eine genaue Bewertung zwingend nötig sind, um beispielsweise das qualitative und quantitative Zerstörungspotential eines Programms zu bewerten. Ein Beispiel für eine solche detaillierte Analyse stellt der Abschlussbericht von Ralph Langner zu *Stuxnet* dar (LANGNER2013), der anhand von Programmcode-Bestandteilen eingehend die Infektions- und Replikationsmechanismen, die ausgenutzten Sicherheitslücken und die Mechanismen zur Sabotage im Kontext mit den physikalischen Funktionen der sabotierten Anlage untersucht. Der Bericht demonstriert dabei den enormen Entwicklungsaufwand einer gezielten Cyberattacke. Gerade aus diesem Grund können die Erfahrungen zu Stuxnet kaum mehr als Anhaltspunkte auf die Frage liefern, ob und wie sich ein Cyberwar aus technischer Sicht in der Realität abspielen könnte. Stuxnet wurde für die Sabotage einer speziellen Industrieanlage entwickelt und auf die spezifischen Bedingungen vor Ort abgestimmt, wofür mehrjährige Entwicklungszeit und sehr genaue Kenntnis umfangreicher Details zur exakten technischen Ausstattung und Konfiguration der Anlage nötig waren. Angesichts der aus dieser Untersuchung abzuleitenden, für die Entwicklung erforderlichen immensen zeitlichen, technischen und finanziellen Ressourcen – Quellen sprechen von einer 2- bis 5-jährigen Entwicklung mit mehreren Millionen Dollar Etat (LANGNER2010, LINDNER2011) – wird deutlich, dass derartige Cyberattacken ungeeignet für den Einsatz in breit gefächerten militärischen Operationen gegen viele unterschiedliche, potentiell heterogene IT-Systeme sind. Insofern wird die rasante technologische Entwicklung in diesem Bereich den Aufbau von Cyber-Arsenalen eher unterminieren.

Einen zusätzlichen Aspekt in den Diskussionen über einen Cyberwar stellt die Notwendigkeit einer gesicherten Einschätzung der Verwundbarkeit potentieller Ziele, wie beispielsweise den oft genannten kritischen Infrastrukturen, dar. Da sich Attacken gegen IT-Systeme als Bestandteil von Industrieanlagen im Gegensatz zum Einsatz kinetischer Mittel nur mittelbar auswirken, bedarf es genauer Erkenntnisse über die potentiellen kurz- und langfristigen Folgen und Wechselwirkungen einer Sabotage dieser Bestandteile und die Beeinträchtigung der Funktion der Anlage. Eine derartige Studie ist beispielsweise die 2011 vom Büro für Technikfolgen-Abschätzung beim deutschen Bundestag erstellte Analyse der Folgen und Wechselwirkungen großflächiger Stromausfälle der vergangenen Jahre (TAB2011). Gesicherte Informationen, die sich gezielt der IT-Ausstattung kritischer Infrastrukturen in Deutschland und deren Gefährdungen widmen und dabei den Einsatz veralteter Software-Versionen, deren Erreichbarkeit aus dem Internet heraus oder den Einsatz potenziell kompromittierter Hardware berücksichtigen, existieren gegenwärtig nicht oder sind nicht öffentlich verfügbar. Dies ist angesichts neuer Großprojekte wie dem *Smart-Grid* der nationalen Stromversorgung mit stark vernetzten IT-Infrastrukturen oder der Einführung des digitalen Behördenfunks eine problematische Situation, da die mangelnde Informationslage zu Fehleinschätzungen der eigenen Verwundbarkeit oder der Bedrohungslage führen und dadurch die internationale Verunsicherung verstärken kann.

Maßnahmen für die internationale Sicherheit im Cyberspace

Die Beispiele sind exemplarisch für die gegenwärtige internationale Situation, die geprägt ist von Mutmaßungen und Unsicherheiten der Staaten über Fähigkeiten im Cyberwar und der Sorge um eine weitere militärische Vereinnahmung des Cyberspace. Um eine friedliche Entwicklung dieser neuen Domäne sicherzustellen, muss das Ziel der Friedens- und Sicherheitsforschung in der Verankerung des Cyberspace in bestehende Vertragswerke der internationalen Sicherheit und Zusammenarbeit und der Etablierung von Normen und Lösungsmechanismen bei Konfliktsituationen im Cyberspace liegen. Ein entscheidender erster Schritt auf diesem Weg sind Maßnahmen, um ein zwischenstaatliches Vertrauen hinsichtlich des Potentials, der Sicherheits- und Verteidigungs-Doktrinen und der strategisch-militärischen Ausrichtung ihrer Fähigkeiten im Cyberspace zu schaffen. Das Ziel solcher vertrauens- und sicherheitsbildenden Maßnahmen – *confidence and security building measures*, CSBM – wird in einem Bericht der UN-Abrüstungskommission wie folgt zusammengefasst: „[…] *to reduce and even eliminate the causes of mistrust, fear, misunderstanding and miscalculations with regard to relevant military activities and intentions of other States* […] *to help to prevent military confrontation as well as covert preparations for the commencement of a war, to reduce the risk of surprise attacks and of the outbreak of war by accident*" (UNODA1988).

Derartige vertrauensbildende Maßnahmen für den Cyberspace bestehen unter anderem in der Ausrichtung von bilateralen Gesprächen und Seminaren über nationale Sicherheits-Doktrinen und Bedrohungseinschätzungen, in der Verständigung auf gemeinsame Begriffs-Definitionen sowie in militärischen Übungen zur Vernetzung der Akteure und dem Aufbau von Kommunikationskanälen für Konfliktsituationen. Darüber hinaus besteht eine weitere Aufgabe in dem institutionellen Ausbau dieser Beziehungen und in der Etablierung von *risk reduction centers* (NEUNECK2012), um den Austausch aktueller Informationen und die Lageeinschätzung zwischen Staaten zu fördern, sowie um gemeinsame Frühwarn-Systeme und die dafür benötigten Kommunikationshierarchien zu etablieren. Beispielsweise wurden im Sommer 2013 die als „rotes Telefon des kalten Krieges" bekannt gewordenen Kommunikationsstrukturen zwischen den USA und Russland wie das *Nuclear Risk Reduction Center* (NRRC) in ihren Mandaten erweitert, um die beteiligten Institutionen auch im Bereich von Cybervorfällen zu vernetzen (WHITEHOUSE2013).

Solche bilateralen Maßnahmen sollen als Ausgangsgrundlage dienen, um Kooperationen in größerem internationalen Umfang fortzusetzen. Sie bedürfen für ihre Effektivität aber Me-

chanismen der gegenseitigen Kontrolle und Verifikation von Zusagen. Für die Übertragung etablierter Maßnahmen gegen die Verbreitung von Waffen-Technologien – wie Exportkontrollen für besonders gefährliche Güter – oder Transparenzmaßnahmen über den Handel mit Gütern und Produktionsbestandteilen, die auch für zivile Zwecke benötigt werden – wie das internationale Meldesystem der *United Nations Commodity Trade Statistics Database* (COMTRADE) – auf den Cyberspace ergeben sich jedoch Schwierigkeiten. Zum einen bedarf es der physischen Substanz für die Quantifizierbarkeit der zu kontrollierenden Ressourcen, eine Eigenschaft, die für Schadsoftware als rein digitale Software-Produkte naturgemäß nicht gegeben ist. Zum anderen sind auch die Hardware-Bestandteile von IT-Systemen wie Computer und Netzwerk-Technik, die maßgeblich friedlichen Zwecken dienen und nicht pauschal reguliert werden können, durch einen ausgeprägten Dual-Use-Charakter gekennzeichnet. Um diesen Problemen zu begegnen, wird gegenwärtig vor allem die Etablierung eines internationalen *Codes of Conduct* auf UN-Ebene als geeigneter Weg angesehen (UNIDIR2014), um den Einsatz von *Cyberwaffen* international zu ächten und die Verpflichtung zu einer friedlichen Nutzung des Cyberspace festzulegen, ein erster Vorschlag der Regierungen Chinas, Russlands, Usbekistans und Tajikistans wurde Ende 2011 der UN-Generalversammlung unterbreitet (UNGA2011).

Ausblick

Trotz der offenen Fragen und der Herausforderungen für die Friedens- und Sicherheitspolitik gibt es im historischen Rückblick auf die Debatten um klassische Waffen-Technologien für die Entwicklung des Cyberspace eine einzigartige Voraussetzung. Anders als alle anderen Domänen beruht der Cyberspace vollständig auf von Menschen definierten Grundlagen und wird durch Gremien wie die *ICANN (Internet Corporation for Assigned Names and Numbers*) oder die IETF (*Internet Engineering Task Force*) definiert und weiterentwickelt. Damit besteht gerade angesichts der aktuellen Tendenz einer stärkeren Einbindung weiterer internationaler staatlicher und zivilgesellschaftlicher Akteure wie der ITU (*International Telecommunication Union*) in diese Gremien die Chance, den Cyberspace langfristig friedlich zu gestalten und Wege zu finden, die diesem Anspruch genügen. Auf der anderen Seite bedarf es der Informatik, deren Fähigkeiten zur Analyse und Gestaltung von Technologie eine Schlüsselrolle zur Beantwortung vieler offener Fragen in zwischenstaatlichen Beziehungen als auch internationalen Internet-Governance-Gremien für eine friedliche und völker-verbindende Anwendung des Cyberspace darstellt. Ohne klare technische Sachkenntnisse werden sich Fragen nach dem Charakter und der Definition von Cyberwaffen und deren Abgrenzen zur Cybercrime, der Attribuierbarkeit von Angriffen oder dem Schutz vor disruptiver Malware in globalem nachrichtendienstlichen und militärischen Ausmaß nicht beantworten lassen. Angesichts der einmaligen historischen Situation, dass der Cyberspace ein vollkommen vom Menschen geschaffener Raum ist und dessen Funktionsweise frei definierbaren Grundsätzen folgt, besteht Anlass zur Hoffnung auf eine friedliche Zukunft im Cyberspace.

Der Beitrag wurde mit freundlicher Genehmigung aus Wissenschaft & Frieden 3/2015 als Vorabdruck in leicht geänderter Form übernommen.

Referenzen

BROWN2010: Sommer, P. und Brown, I., OECD Study – Reducing Systemic Cybersecurity Risk, OECD/IFP Project on Future Global Shocks. 2010

CCDCOE2013: NATO Cooperative Cyber Defence Centre of Excellence, The Tallinn Manual on the International Law Applicable to Cyber Warfare. Tallinn, 2013

CLARK2010: Clark, David D. und Landau, S., The Problem isn't Attribution; It's Multi-Stage Attacks, Cambridge, 2010

CSIS2010: Lewis, J. A. und Timlin, K., Cybersecurity and Cyberwarfare – Preliminary Assessment of National Doctrine and Organization. Center for Strategic and International Studies, 2011

EU-Rat2001: Rat der Europäischen Union, Übereinkommen Computerkriminalität, (Titel des Originaldokuments: Budapest Cybercrime Convention). Budapest, 2001

IISS2013: International Institute for Strategic Studies, The Cyber Attack on Saudi Aramco. 2013, http://www.iiss.org/en/publications/survival/sections/2013-94b0/survival-global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272

LANGNER2010: Langner, Ralph, Ralph's analysis, part 3, Blogeintrag von Ralph Langner über Stuxnet, 2010, http://www.langner.com/en/2010/10/04/stuxnet-logbook-oct-4-2010-1100-hours-mesz/

LANGNER2013: Langner, Ralph, To Kill a Centrifuge – A Technical Analysis of What Stuxnet's Creators Tried to Achieve. Hamburg, 2013

LIN2011: Lin, H., On Attribution and Defense. International Conference on Challenges in Cybersecurity: Risks, Strategies, and Confidence-Building, Berlin, December 13, 2011

LINDNER2011: Lindner, Felix, Military Grade Hacking – This Is Not Cyber Crime, Vortrag bei der International Conference on Challenges in Cybersecurity: Risks, Strategies, and Confidence-Building, Berlin, 2011

MADIANT2013: Madiant Corporation, APT1 Exposing One of China's Cyber Espionage Unit. Alexandria, Washington, USA, 2013

NEUNECK2012: Neuneck, Götz, Confidence Building Measures – Application to the Cyber Domain. Cyber Security Conference, 2012

TAB2011: Büro für Technikfolgen-Abschätzung beim deutschen Bundestag, Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen Ausfalls der Stromversorgung. Berlin, 2011

UN1945: Vereinte Nationen, Charta der Vereinten Nationen und Statut des Internationalen Gerichtshofs. 1945 in Kraft getreten, aktuelle Fassung in dt. Übersetzung, http://www.un.org/depts/german/un_charta/charta.pdf

UN-GGE2012: UN Group of gouvernmental experts, Developments in the field of information and telecommunication in the context of international security: Work of the UN first Committee 1998—2012. Genf, 2012

UNGA2011: UN Generalversammlung, Proposal of an International code of conduct for information security from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, Genf, 2011, http://www.rusemb.org.uk/data/doc/internationalcodeeng.pdf

UNIDIR2013: United Nations Institute for Disarmament Research UNIDIR, The Cyber Index – International Security Trends and Realities. Genf, 2013

UNIDIR2014: United Nations Institute for Disarmament Research UNIDIR, UNIDIR Cyber Stability Seminar 2014: Preventing Cyber Conflict. Genf, 2014

UNODA1988: UN office for disarmament research, Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmament. UN document A/S-15/3, 1988

WHITEHOUSE2013: The White House Office of the Press Secretary: FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security, Washington, 2013, http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol

Sylvia Johnigk, Hans-Jörg Kreowski und Kai Nothdurft

Cyberwar – Schimäre oder reale Bedrohung?

Im Rahmen des Kongresses „Quo vadis NATO? – Herausforderungen für Demokratie und Recht", der vom 24. bis 26. April 2013 in Bremen stattfand, hat der zweite Autor eine Arbeitsgruppe zum Thema „NATO, Cyberwar und das Recht" geleitet und dazu einen Einführungsvortrag gehalten. Der folgende Beitrag fasst den Vortrag zusammen. Er war ursprünglich für einen Kongressreader gedacht, der aber nicht realisiert wurde.

Der Begriff Cyberwar ist schwer zu fassen

Cyberkrieg (englisch: *Cyberwar* oder *Cyberwarfare*) ist ein schillernder Begriff, in dem die Bestandteile *Cyberspace* und *Krieg* verschmolzen sind und der kriegerische Auseinandersetzungen umfasst, die mit Mitteln der Informations- und Kommunikationstechnik (IKT) wie Computer, Softwaresysteme, Internet u.ä. geführt werden. Dabei macht es Sinn, von Cyberkrieg zu sprechen, wenn die Technik selbst Waffencharakter annimmt, im Gegensatz zu militärischen Systemen wie Raketen, Drohnen, Luftabwehr u.a., bei denen IKT-Systeme zentral an Steuerung und Funktion beteiligt sind, aber nicht das wesentliche Merkmal darstellen. Der früher ähnlich gebrauchte Begriff *Information War* trifft vielleicht etwas besser, worum es geht. Auch ist zu beachten, dass nicht jeder sogenannte Cyberangriff schon Cyberkrieg ist. So sind Straftaten mit IKT wie Online-Betrug, Phishing u.ä. der Cyberkriminalität zuzurechnen, politisch motivierte Aktionsformen des Online-Protests lassen sich unter dem Begriff Hacktivismus subsumieren. Bei Sabotage und Terroranschlägen mit Hilfe von IKT ist nicht immer eindeutig und klar, ob es sich um Straftaten handelt oder bereits kriegerische Akte vorliegen. Auch Cyberspionage, die im großen Maßstab stattfindet, ist in vielen Fällen eher wirtschaftlich als militärisch motiviert.

Wettrüsten für den Cyberkrieg

Dass es sich jedoch bei Cyberkrieg nicht um ein Hirngespinst handelt, lässt sich daraus entnehmen, dass eine Vielzahl von Staaten in den letzten Jahren eigene Cyberwar-Einheiten aufgebaut haben: Beispielsweise gibt es in den USA das *United States Cyber Command*, in Großbritannien die *Government Communication Headquarters*, in Israel die *Cyber Defense Taskforce* und in China die *Blaue Armee*, eine offiziell rein defensiv ausgerichtete Hackereinheit. Der Iran brüstet sich damit, die weltweit zweitgrößte Einheit zu besitzen. Russland wird verdächtigt, Cyberwarfare offensiv zu betreiben oder zu unterstützen. Insgesamt haben inzwischen rund 140 Staaten Cyberwar-Einheiten aufgebaut, wobei die meisten einen offensiven Charakter haben.[1]

Auch Deutschland steht nicht abseits. Seit Februar 2011 gibt es einen *Nationalen Cybersicherheitsrat*, der bei der Beauftragten der Bundesregierung für Informationstechnik angesiedelt ist und in dem das Kanzleramt, das Auswärtige Amt, die Innen-, Verteidigungs-, Justiz-, Wirtschafts- und Finanzministerien des Bundes, die Bundesländer sowie assoziierte Mitglieder aus der Wirtschaft vertreten sind. Und seit April 2011 gibt es ein Nationales Cyberabwehrzentrum, an dem das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundesamt für Verfassungsschutz (BfV) und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zusammenarbeiten, wobei als assoziierte Behörden das Bundeskriminalamt (BKA), der Bundesnachrichtendienst (BND), die Bundespolizei, die Bundeswehr sowie das Zollkriminalamt mitwirken. Im November 2012 wurde schließlich die *Allianz für Cybersicherheit* gegründet, in der sich das BSI und der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) abstimmen. Daneben haben einige Bundesbehörden eigene Cybereinheiten. Die Strukturen sind allerdings ziemlich intransparent, und es bleibt unklar, wer diese Einrichtungen kontrolliert.

Cyberattacken sind alltäglich

Dass auf dem Feld des Cyberkriegs ein vehementes Wettrüsten stattfindet, ist auch an der Vielzahl von staatlich und militärisch motivierten und initiierten Cyberangriffen abzulesen. Öffentliche Aufmerksamkeit erregt haben beispielsweise der *Titan Rain*, eine Angriffsserie einer chinesischen Hackergruppe auf US-amerikanische Computersysteme von Rüstungskonzernen, Streitkräften, NASA u.a., und die *Olympic Games* mit dem Computerwurm *Stuxnet*, der der Störung des iranischen Atomprogramms diente. Bekannt geworden sind auch die Denial-of-Service-Attacken gegen estländische und georgische Regierungswebseiten, die wahrscheinlich von russischer Seite lahmgelegt wurden. Die Liste ließe sich noch um diverse Beispiele verlängern. In vielen Fällen ist allerdings nicht klar, was Ziel und Zweck ist, und wer wirklich als Verursacher dahintersteckt. Spionage und Sabotage sind vielfach im Spiel, aber es kann sich auch um Provokation oder Warnung handeln. Es wäre in manchen Fällen durchaus denkbar, dass Cyberkriegseinheiten solche Angriffe als Training durchführen. Auf jeden Fall zeigen diese Beispiele wie auch die massenhafte Ausspähung sozialer Netzwerke durch die US-amerikanische National Security Agency (NSA) mit Hilfe des Überwachungsprogramms PRISM und weiteren, dass elektronische Medien und elektronisch gespeicherte Daten umfassend überwacht und ausgewertet und dass Industrieanlagen, Infrastruktursysteme wie Strom- und Wasserversorgung, Verwaltungseinrichtungen und das Bankwesen durch Cyberattacken vergleichsweise einfach gestört oder ausgeschaltet werden können.

Cyberkrieg scheint attraktiv

Mit der weltweit betriebenen Einrichtung von Cyberkriegseinheiten wird erheblich an der Rüstungsspirale gedreht. Das gilt als militärisch attraktiv, weil es relativ kostengünstig ist, so dass sich auch kleinere und ärmere Länder diese Art der Aufrüstung leisten können, und weil die Gefährdung eigener Soldaten geringer ist als bei herkömmlichen Formen des Kriegs. Auch können Gegner durch das Ausschalten ziviler Infrastrukturen erheblich geschwächt werden. Außerdem ist eine Rückverfolgung

von Angriffen schwierig, so dass die Aggressoren gar nicht immer sofort erkannt werden. Ein weiterer Umstand, der beachtet werden muss, liegt in dem Phänomen, dass es zumindest nach dem heutigen Stand der Technik wesentlich einfacher ist, Cyberangriffe durchzuführen, als sich gegen solche Attacken zu schützen. Gerade die hochentwickelten Industrieländer mit ihrem hohen Grad an Computerisierung und Vernetzung sind extrem verwundbar.[2]

Cyberkrieg tangiert zivile Freiheit

Die vielseitige Aufrüstung zum Cyberkrieg bedeutet aber nicht nur, dass zivile Einrichtungen erheblich gefährdet sind, sondern es gibt weitere Widersprüche zwischen zivilen Ansprüchen und militärischen Ambitionen. So gibt es eine Zuständigkeits- und Mittelkonkurrenz bei der Cybersicherheit zwischen Militär und Strafverfolgungsbehörden. So fehlen Energie und Geld, die in die Herstellung von Schadsoftware für Cyberangriffe fließen, beim Entwickeln von Schutzmechanismen. So werden Sicherheitslücken, die für Cyberattacken nutzbar sind, als Angriffsoption geheim gehalten, statt sie aufzudecken und zum Schutz der eigenen Zivilgesellschaft zu beseitigen. Gleichzeitig wird dadurch Beihilfe zur Cyberkriminalität geleistet, weil weniger Schwachstellen beseitigt werden, als möglich wäre. Schließlich stehen die militärischen Ziele der Kontrolle, Überwachung und Fähigkeit zu Cyberangriffen im Widerspruch zum zivilen Anspruch auf freien Umgang mit digitalen Medien und Internet.

Cyberkrieg ist global, Cyberabwehr national

Während Angriffswerkzeuge für den Cyberkrieg teilweise im Internet zu finden und oft billiger zu haben sind als konventionelle Waffen, während ihre Handhabung vergleichsweise einfach erlernt werden kann, ist es um die Cyberabwehr – zumindest heute noch – schlecht bestellt. Ein wesentlicher Grund dafür ist, dass Bemühungen um Cybersicherheit überwiegend national organisiert sind, während der Cyberspace mit dem Internet und den Netzen internationaler Konzerne global funktioniert. Die Netze internationaler Firmen ignorieren staatliche Grenzen, die Liefer- und Wertschöpfungsketten sind weltumspannend, eine wachsende Menge relevanter Daten ist in einer *Public Cloud* gespeichert, und die Betreiber kritischer Infrastrukturen beschränken sich auch selten auf nationale Territorien. Nationale Cyberabwehr kann deshalb nicht oder nur sehr eingeschränkt funktionieren.

Cyberkrieg erhöht Kriegsgefahr

Ein besonders bedenklicher Aspekt der Aufrüstung zum Cyberkrieg ist, dass die allgemeine Kriegsgefahr und Kriegsbereitschaft dadurch steigen. Das Department of Defense der Vereinigten Staaten hat im Jahre 2011 die *Strategy for Operating in Cyberspace* herausgegeben, die von der defensiven Schwäche, der immensen Abhängigkeit von funktionierenden IKT-Systemen und die hohe Verletzlichkeit durch Vernetzung, Zentralisierung, Standardisierung und Mobilität geleitet ist.[3] Statt jedoch eine weltweite Cyberabrüstung anzustreben, wird mit Gegenangriffen bei Cyberattacken gedroht. Dabei wird der Einsatz konventioneller Waffen nicht ausgeschlossen – im Gegenteil wird die Eintrittsschwelle sogar sehr niedrig gelegt. Der Begriff Cyberangriff wird sehr weit gefasst und reicht von Denial-of-Service-Attacken und Sabotage von militärischen und zivilen Systemen über die Manipulation und den Diebstahl von Informationen sowie Wirtschaftsspionage bis hin zu Diebstahl geistigen Eigentums. Hacktivismus, Cybercrime und Cyberwarefare werden undifferenziert als Bedrohung der nationalen Sicherheit der USA angesehen und können Gegenangriffe nach sich ziehen. Eine beunruhigende Frage in diesem Zusammenhang ist, welche Auswirkungen das für den Bündnisfall in der NATO hat. Wenn die USA eine Cyberattacke mit Raketen beantworten, müssen sich dann die anderen NATO-Partner an die Seite der USA stellen?

Sylvia Johnigk, Kai Nothdurft und Hans-Jörg Kreowski

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.

Hans-Jörg Kreowski siehe Autoreninfo auf Seite 66

Cyberkrieg im Lichte des Kriegsvölkerrechts

Cyberkriege sind wegen der weltweiten Aufrüstung und weitgehend fehlender Bemühungen um Cyberabrüstung eine reale Gefahr. Deshalb drängt sich die Frage auf, ob und wie das Kriegsvölkerrecht auf Cyberkriege anwendbar ist. Die Fachleute sind sich uneinig. Die einen argumentieren, dass Cyberkriege „reguläre" Kriege sind, so dass das Kriegsvölkerrecht uneingeschränkt gilt und angewendet werden kann. Ein wesentliches Problem wird in diesem Falle darin gesehen, dass der Aggressor bei Cyberattacken nicht immer feststeht und schwer ermittelbar sein kann. Die Gegenposition betont die Besonderheiten von Cyberkriegen, die im Kriegsvölkerrecht in der bisherigen Form nicht berücksichtigt sind, so dass eine Art digitaler Genfer Konvention nötig wäre. Wie Cyberkrieg im Völkerrecht reflektiert ist oder werden kann, muss dringend geklärt werden, wobei auch die Ächtung eine Option ist.[4] In diesem Zusammenhang ist vor allem auch das *Tallinn-Manual* von Bedeutung, das im Auftrag des NATO Cooperative Cyber Defence Centre mit Sitz in Tallinn von einem rund zwanzigköpfigen Expertengremium von 2009 bis 2012 ausgearbeitet worden ist und das völkerrechtlich gebotene Verhalten von Staaten im Cyberkrieg zum Gegenstand hat.[5]

Cyberrüstung bedroht die Zivilgesellschaft

Durch die weitreichenden und hochentwickelten Möglichkeiten, Cyberangriffe durchzuführen, sind aber nicht nur militärische IKT-Systeme bedroht, sondern staatliche Einrichtungen, Unternehmen und die Bürgerinnen und Bürger insgesamt, wobei diese gezielt oder als Zufallstreffer und Kollateralschaden zu Opfern werden können. Die digitalisierte Gesellschaft als Ganzes ist hochgradig abhängig von kritischen Infrastrukturen wie der Energie- und Wasserversorgung, dem Transportwesen, den Informations- und Kommunikationskanälen und dem Gesundheitssystem. Fast alle dafür eingesetzten Computersysteme sind vernetzt und so von überall her erreichbar. Die kommerzielle Hard- und Software ist in der Regel leicht angreifbar. Die Standardisierung erleichtert und effektiviert Angriffe. Die Komponenten von IKT-Systemen kommen von vielen Herstellern und Lieferanten, so dass kaum kontrollierbar und nachvollziehbar ist, wie sicher sie sind. Mit der überdies wachsenden Komplexität der Systeme und Anwendungen wächst die Häufigkeit von Schwachstellen, Fehlkonfigurationen und unbekanntem Verhalten. Die Sicherheit von IKT-Systemen ist selten ein Designziel bei der Durchführung von Entwicklungsprojekten, der Profit steht im Vordergrund. Das Problem besteht darin, dass kritische Infrastrukturen mit dem Internet verbunden sind, dieselbe Hard- und Software, dieselben Protokolle und Dienste nutzen und dass dieselben Schwachstellen auftreten wie bei allen sonstigen Nutzerinnen und Nutzern der IKT-Technik. Zudem mangelt es den Betreibern von kritischen Infrastrukturen an Sensibilität für die Probleme. Auf der anderen Seite bergen auch Versuche des Staates Gefahren und Risiken, die Angreifbarkeit der kritischen IKT-Systeme zu mindern. So bedeutet eine Verschärfung von Sicherheitsgesetzen in der Regel, dass die Freiheit im Internet beeinträchtigt wird.

Cyberpeace statt Cyberwar

Der Gefahr des Cyberkriegs lässt sich nur durch eine konsequente Cyberabrüstung und durch eine Konzeption des Cyberpeace begegnen.

Auf der militärischen Ebene heißt das, Offensivwaffen für den Cyberkrieg zu verbieten und Cybersicherheit rein defensiv auszurichten. Im Sinne einer digitalen Genfer Konvention sollte ebenfalls verboten sein, Cyberangriffe auf kritische Infrastrukturen zu unternehmen. Wirtschaftliche Interessen müssen als legitimer Cyberkriegsgrund ausgeschlossen werden, auch ziviler Ungehorsam und Onlineprotest im Internet dürfen nicht dafür herhalten. Schließlich sollte es verboten sein, Cyberattacken mit dem Einsatz konventioneller Waffen zu beantworten. Außerdem sollte eine internationale, unabhängige Instanz geschaffen werden, die behauptete Cyberangriffe forensisch untersucht, so dass eine verlässliche Zuordnung zu den Verursachern stattfindet und nicht die Falschen als Aggressoren beschuldigt werden können.

Auf der zivilen und politischen Ebene müssten alle staatlichen Stellen, alle Unternehmen und alle Bürgerinnen und Bürger verpflichtet werden, Schwachstellen in IKT-Systemen offenzulegen. Der Betriebserlaubnis kritischer Infrastrukturen müsste immer eine kompetente und transparente Sicherheitsprüfung vorausgehen, die Betreiber müssten die Sicherheit der IKT-Systeme garantieren. Die kritischen Infrastrukturen sollten dezentral und unvernetzt betrieben werden. Wichtig wäre auch, Cybersicherheitsstrategien unter demokratische Kontrolle und unter einen Parlamentsvorbehalt zu stellen. Speziell für Deutschland gilt, dass der Aufbau von Cyberabwehrzentren transparent und demokratisch kontrolliert vollzogen wird, dass die Zentren friedenspolitisch ausgerichtet werden und in ihnen eine strikte Trennung von Polizei, Geheimdiensten und Militär gewahrt wird. Als Unterstützung von Cyberpeace-Initiativen sollte die Bundesregierung die Friedensforschung zur Entwicklung von Strategien zur Befriedung des Cyberspace ausreichend fördern.

Statt eines Schlusses

Die Überlegungen in diesem Beitrag fassen nicht nur das entsprechende Referat des zweiten Autors auf dem Kongress *Quo vadis NATO?* zusammen, sondern sie sind auch stark angelehnt an den Vortrag der ersten Autorin über *Cyberpeace statt Cyberwar* auf dem 29. Chaos Communication Congress 2012 (29C3) in Hamburg und folgen teilweise Ausführungen von Sylvia Johnigk und Kai Nothdurft in der *FIfF-Kommunikation* 1/2012.[6] Auch wenn das Thema Cyberwar nicht zuletzt wegen der immensen weltweiten Cyberaufrüstungen in letzter Zeit große öffentliche Aufmerksamkeit erregt, zeichnet sich die Problematik schon lange ab, wie der Artikel von Ute Berhardt und Ingo Ruhmann im Tagungsband der FIfF-Jahrestagung 1994 beweist.[7]

Dennoch stehen die kritische Auseinandersetzung mit dem Thema Cyberwar und die Entwicklung einer Gegenkonzeption unter dem Motto Cyberpeace noch ganz am Anfang. Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF) organisiert einen Arbeitskreis RUIN (RUestung und INformatik), der sich intensiv mit diesen Fragen beschäftigt. Wer interessiert ist, über die Aktivitäten des AK RUIN informiert zu werden oder mitarbeiten möchte, wende sich bitte an den zweiten Autor (siehe auch die Webseite fiff.de/themen/ruin). Darüber hinaus hat das FIfF gerade die Kampagne Cyberpeace gestartet, die durch die *stiftung bridge* gefördert wird. Sie hat zum Ziel, das öffentliche Bewusstsein von der gefährlichen

Durchdringung des virtuellen Raumes mit militärischen Aktivitäten zu schärfen und den Widerstand dagegen zu stärken (siehe auch http://cyberpeace.fiff.de/).

Anmerkungen

1 *Sandro Gaycken: re:publica XI April 2011 http://re-publica.de/11/blog/panel/cyberwar-und-seine-folgen-für-die-informationsgesellschaft/*

2 *Der Cyberkrieg kann jeden treffen http://www.sueddeutsche.de/digital/sicherheit-im-internet-der-cyber-krieg-kann-jeden-treffen-1.146684 und Wirtschaftswoche: Bundeswehr anfällig für Cyber-Angriffe http://www.wiwo.de/technologie/digitale-welt/bundeswehr-bundeswehr-anfaellig-fuer-cyber-angriffe/7220 974.html*

3 *US Militärdoktrin des DoD: Strategy for Operating in Cyberspace http://www.defense.gov/news/d20110714cyber.*

4 *Spiegel Online: Der Wurm als Waffe http://www.spiegel.de/netzwelt/netzpolitik/experten-suchen-nach-kriegsrecht-fuer-den-cyberwar-a-836566.html, Ein Gegenschlag ist nicht legal http://www.sueddeutsche.de/digital/cyberwar-und-voelkerrecht-ein-gegenschlag-ist-nicht-legal-1.1430089 und Cyberwar: Die UN führen erste Gespräche über eine völkerrechtliche Ächtung http://www.sueddeutsche.de/digital/cyberwar-und-voelkerrecht-ein-gegenschlag-ist-nicht-legal-1.1430089*

5 *Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press 2013*

6 *Sylvia Johnigk und Kai Nothdurft: Cyberwarfare – Aufrüstung im Cyberspace als Herausforderung für die Friedensarbeit des FIfF, FIfF-Kommunikation 1/2012, S. 41-45*

7 *Ute Bernhardt und Ingo Ruhmann: Information als Waffe: Netwar und Cyberwar – Kriegsformen der Zukunft, in: Hans-Jörg Kreowski et al. (Hrsg): Realität und Utopien der Informatik, agenda-Verlag Münster 1995, S. 104-119*

Frieder Nake

Mein kurzer Weg ins FIfF

CPSR war Computer Professionals for Social Responsibility. Die US-amerikanische Vereinigung existierte von 1983 bis 2013. Als das FIfF am 2. Juni 1984 in Bonn gegründet wurde, freuten manche der Versammelten sich, dass Joseph Weizenbaum und Alan Borning Grüße der amerikanischen Gleichgesinnten überbrachten. Wir waren friedensbewegt, gegen den sog. NATO-Doppelbeschluss. Da war es schön, dass uns jemand aus jenem Land Mut zusprach, das verantwortlich für alles war.

Die widerständige Haltung teilten wir mit vielen. In etlichen Berufsständen wurden Vereinigungen gegründet, die ihre jeweilige Verantwortung zum Anlass nahmen, sich gar nicht so sehr berufsständisch zu verhalten. Die InformatikerInnen waren nicht in vorderster Front dabei, dann aber umso entschiedener. Bis zum heutigen Tage.

Einer wie ich hatte also gar keinen Weg zu gehen, um im FIfF anzukommen. Dem Prof. Wilm Wippermann in Kaiserslautern hatte die GI engstirnig eine liberale Protestsache vermiest, die ihm am Herzen lag. Ich war zu der Zeit Sprecher des Fachbereich „Informatik und Gesellschaft" in der GI. Die frühen 1980er Jahre waren auch noch, wenngleich nicht mehr lange, Jahre der radikalen Linken in der BRD. Deswegen mischten wir uns gern unter die liberalen Friedensfreunde.

Frieder Nake, *Universität Bremen*

FIfF e. V.

Sammelband zum 30-jährigen Jubiläum des FIfF: Gesellschaftliche Verantwortung in der digital vernetzten Welt

Der von Peter Bittner, Stefan Hügel, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht und Britta Schinzel herausgegebene Sammelband *Gesellschaftliche Verantwortung in der digital vernetzten Welt* erscheint in der Reihe *Kritische Informatik* des LIT-Verlags. In den vielfältigen Beiträgen zahlreicher bekannter Autorinnen und Autoren werden aktuelle und dringliche Themen der Informatik aus verschiedenen Blickrichtungen betrachtet und die viel bejubelten Errungenschaften der digitalen Gesellschaft kritisch hinterfragt. Die fünf thematischen Blöcke zu *Überwachung und Datenschutz*, *Rüstung und Informatik*, *Informatik und Gender*, *Verantwortung und Fairness im informatischen Handeln* sowie *Kreatives Arbeiten und immaterielle Güter* spiegeln die Schwerpunkte des nunmehr 30-jährigen gesellschaftspolitischen Engagements des FIfF. Wie im Vorwort betont wird, hat die Dringlichkeit, sich mit ihnen auseinanderzusetzen, nicht nachgelassen, sondern ist mit der zunehmenden Durchdringung aller Lebensbereiche mit der Informationstechnik weiter gewachsen. Mit dem Sammelband ist ein Panorama entstanden, das nicht nur die Konsequenzen dieser Durchdringung aufzeigt, sondern auch Möglichkeiten, ihren unerwünschten Aspekten etwas entgegenzusetzen.

Peter Bittner, Stefan Hügel, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht und Britta Schinzel (Hrsg.):
Gesellschaftliche Verantwortung in der digital vernetzten Welt. Verflechtungen und Perspektiven
LIT Verlag 2014, 307 Seiten,
ISBN 978-3-643-12876-8
Preis 34,90 €

Peter Bürger

Michael Schulze von Glaßer: „Das virtuelle Schlachtfeld“

Ein neues Buch über Krieg und Computerspiele

Michael Schulze von Glaßer, Jg. 1986, hat im Alter von sechs Jahren auf einem Amiga 500 sein erstes Videospiel mit militärischem Inhalt gespielt – ohne bleibende Schäden*. Heute tritt der Politikwissenschaftler, dessen Arbeiten keineswegs nur am Schreibtisch entstehen, als antimilitaristischer Aufklärer in Erscheinung. Nach seinen Büchern* An der Heimatfront *(2010) über Öffentlichkeitsarbeit und Nachwuchswerbung der Bundeswehr und* Soldaten im Klassenzimmer *(2012) über die Bundeswehr an Schulen liegt nun der Titel* Das virtuelle Schlachtfeld *über den Komplex Videospiele, Militär und Rüstungsindustrie vor.*

Durch zahlreiche Zeitschriftenbeiträge, Dossiers[1], kreative Videoclips[2] und Vorträge ist der Autor längst als Experte zu diesem Thema bekannt. Er geht auf Spiele-Messen, stellt Machern und Kooperationspartnern von Militainment-Produkten unbequeme Fragen und tritt als *User* in den Austausch mit anderen *Usern*. Seinen Wortmeldungen geht jeglicher Moralismus ab, ohne dass jedoch irgendein Zweifel am kriegskritischen und antimilitaristischen Forschungsparadigma aufkommen könnte.

Im Grunde wäre die fortlaufende und systematische Bearbeitung des massenkulturellen Militärkomplexes Aufgabe einer institutionalisierten – kritischen – Friedens-Medienwissenschaft, wenn es denn eine solche hierzulande geben würde. Michael Schulze von Glaßer erschließt als freier Autor einen imponierenden Querschnitt durch das schier unübersehbare Sortiment der Videospiele mit Militärbezügen und zeigt mit seinem Ansatz, dass Alternativen zum Rezensions-Quark der neoliberalistischen Ära und zum medienpädagogischen Formalismus des letzten Jahrzehnts möglich sind.

Eine Empfehlung sei vorab ausgesprochen. Wer sich als Spieler, Medienforscher, Pädagoge oder Pazifist mit dem Krieg an Spielkonsole oder PC-Bildschirm kritisch auseinandersetzen möchte, sollte dieses Buch zur Hand nehmen und lesen. Vom „Müssen“ möchte ich in diesem Zusammenhang nur deshalb nicht sprechen, weil es in unserer gewalttätigen Alltagssprache allzu häufig vorkommt.

Michael Schulze von Glaßer:
Das virtuelle Schlachtfeld – Videospiele, Militär und Rüstungsindustrie.
Köln: PapyRossa Verlag 2014
205 Seiten
Preis € 14,90 Euro

1. Gegenstand und Mediengewaltdebatte

In der ersten Abteilung werden die Dimensionen beleuchtet: „31,5 Millionen Bundesbürger spielen heute virtuell am Computer, der Heimkonsole oder mobil, davon sind 26 Millionen regelmäßige Spieler …“. Am Markt geht es um astronomische Umsätze. Das Spiel *Call of Duty – Modern Warfare 3** brachte z. B. „… seinem Hersteller einen Rekordumsatz von weltweit einer Milliarde US-Dollar innerhalb von nur 16 Tagen nach Veröffentlichung“. – Die Leser erfahren, was Ego-Shooter oder Third-Person-Shooter sind und warum sie im Gegensatz zu bestimmten militärischen Simulations-„Spielen“ (dual use!) keineswegs per se Fertigkeiten zur Bedienung von Militärtechnologie vermitteln.

Ausdrücklich ist die knapp referierte Mediengewaltdebatte kein Gegenstand der Untersuchung. Diese Vorgehensweise hat unabweisbare Vorzüge. Schulze von Glaßer muss sich nicht in den Irrgärten einer – weithin positivistischen – Mediengewaltforschung einsperren lassen und auf diese Weise – nolens volens – Vorgaben folgen, die in der Vergangenheit regelmäßig von den gravierendsten Skandalen des Militainments abgelenkt haben. Kritiker, die sich bislang vielleicht auf dem Niveau der üblichen Lamentos über *Ballerspiele* bewegt haben, werden alsbald zu einer relevanten kritischen Betrachtungsweise hingeführt. Auch viele Konsumenten von Militärspielen erhalten die Einladung, die Kontroverse einmal nicht unter dem Gesichtspunkt einer Rechtfertigung oder Kritik der Gewalthaltigkeit von Spielen zu betrachten. Denn es geht in diesem Buch um Inhalte, um politische Drehbücher!

2. Militärdoktrinen, Feindbilder, Rechtsnormen und Kriegstechnologie

Das Buch beleuchtet die Schauplätze der Videoangebote. Der Autor fragt nach politischen Entwicklungen und Interessen im Hintergrund. Der so genannte *Krieg gegen den Terror* war jahrelang das Vorzugsthema der westlichen Spiele-Produzenten (und hat – analog zur Aufrüstungsspirale auf allen anderen Gebieten – bei der Gegenseite die Entwicklung eigener Kriegsspiele angefeuert). Der „Iran-Konflikt“, der gegenwärtig freilich eine unerwartete Wendung erfahren hat, ist hernach wohl kaum zufällig zum beliebten Gegenstand der Drehbücher geworden. Spiegeln die Feindbilder der Spiele die weltpolitischen Entwicklungen vielleicht auch vorauseilend? Bei den Beispielen, die Schulze von Glaßer präsentiert, kommen u. a. das Feindbild China (bzw. dessen vorläufige Platzhalter) und russische Ultranationalisten ins

Blickfeld. Muss sich am Ende gar auch die Bundeswehr mit Panzern gegen *russische Invasoren* zur Wehr setzen (S. 90)? Wenn eine Bedrohung durch russische Weltbeherrschung die Spieler anspornt, wissen sie nicht immer, dass z. B. der US-amerikanische Anteil an den Weltrüstungsausgaben etwa zehnmal größer ist als der von Russland (S. 99).

Spiele-Drehbücher sind gar nicht so selten *imperialistische* Drehbücher. Das zeigt der Autor in einem eigenen Abschnitt „The Great Game – Militärische Rohstoffsicherung und Kriege für die Wirtschaft" (S. 101-112). Man fragt sich, warum dieser zentrale Aspekt jahrelang in der Diskussion so gut wie keine Rolle gespielt hat. Die Antwort: Über geopolitische und ökonomische Zielvorgaben in verfassungs- und völkerrechtswidrigen *Militärdoktrinen* findet hier zu Lande auch keine gesellschaftliche Auseinandersetzung statt!

Wie steht es um die *Virtuelle Außerkraftsetzung von internationalem Recht* und um die Menschenrechte (u. a. Folter, Exekution von Kriegsgefangenen, Angriffe auf Zivilisten)? Hier werden im Buch neue Gesichtspunkte bedacht. Das Internationale Rote Kreuz versucht im Gespräch oder gar in Kooperation mit Produzenten, zumindest ein objektives Wissen um die völkerrechtlichen Bestimmungen in die Drehbücher oder Beigaben der Spiele einfließen zu lassen. Könnten am Ende die Militärspiele vielleicht gar ein Medium werden, das die Völkerrechtsnormen im öffentlichen Rechtssinn nicht schleichend aushebelt, sondern vielmehr im Bewusstsein vieler Menschen verankert? Bezogen auf den *Krieg der Zukunft* zeigt Schulze von Glaßer, dass Spiele auch Risiken und Ambivalenzen der technologischen Entwicklung und des *privatisierten Krieges* thematisieren. (Die ausgewählten Befunde entkräften freilich nicht die gegenteilige These, dass Militainment vorauseilend den gesellschaftlichen Akzeptanzboden für die *Revolution in Military Affairs* bereitet.)

In diesem Hauptteil der Studie werden besonders alle Nichtspieler es schätzen, dass der Autor dem Referat der jeweiligen Drehbücher viel Liebe angedeihen lässt.

3. Spiele – Militär – Rüstungsindustrie

Nach den Inhalten werden die *Produktionszusammenhänge* beleuchtet, und leider ist das entsprechende Vorgehen des Autors keineswegs schon ein Standard der Kriegsmedienkritik. Im Buch sind alle Spiele-Titel, bei denen eine Kooperation bzw. Produktionsbeteiligung von Militär oder Rüstungsindustrie nachzuweisen war, mit einem Sternchen (*) gekennzeichnet. Exemplarisch erfolgt für eine ganze Reihe von Titeln ein sehr detaillierter Nachweis. Kooperationsvorteile gibt es von Fall zu Fall auf beiden Seiten („Authentizität", Story, detailgetreue Abbildungen, militärische Verwendbarkeit, Imagegewinn ...). Nicht immer ist Transparenz erwünscht, und bezogen auf die Recherche zu den Verflechtungen bleibt noch viel zu tun. (Weiterhin auf der Tagesordnung steht die Verbraucherschutz-Forderung, dass die Mitwirkung von Militär oder Rüstungsproduzenten für potentielle Käufer von unterhaltungsindustriellen Angeboten zum Militainment schon auf der Verpackung ausgewiesen wird.)

Auch Heckler & Koch, um nur ein deutsches Beispiel zu nennen, stehen auf der Danksagungsliste eines Spiele-Herstellers (S. 137). Ursprünglich zivile Spieltechnologien können für das Militär interessant werden, sodass am Ende der Produzent auch zum Rüstungsproduzenten mutiert (S. 143-148). Manche Anbieter sind schon im Voraus mit der Rüstungsbranche verbunden. Das Militär entwickelt eigene Angebote, vorzugsweise zu Zwecken der Rekrutierung. Gemessen am ultimativen Rekrutierungsinstrument *Americas Army** (bereits für Kinder!) fallen die Angebote der Bundeswehr noch vergleichsweise bescheiden aus (S. 163-184). Die Dinge können sich – trotz des abweichenden Mediengeschmacks der Konservativen in unserem Land – schnell ändern. Eine demokratische Kontrolle der Öffentlichkeitsarbeit des Militärs, zu deren Umsetzung Michael Schulze von Glaßer schon viele verdienstvolle Beiträge geleistet hat, bleibt in diesem Kontext oberstes Gebot.

4. Sind andere *Games* möglich?

Es gibt bereits Alternativen! Ein Spieler kann z. B. in die Rolle eines Kriegsberichterstatters schlüpfen und hierbei wählen, ob er sich am Konzept des „Friedensjournalismus" ausrichtet oder durch effektvolle Einseitigkeit profiliert (S. 187). Warum sollten Gamer außerdem nicht die Möglichkeit erhalten, als Reporter *Bilder zu schießen* statt mit der Waffen Menschen zu erschießen (S. 188). Kann es ein Lehrstück sein, wenn die Möglichkeit eröffnet wird, eine Region mit Drohnenangriffen zu überziehen, man hierbei jedoch am Ende rein gar nichts anderes erreicht als eine nicht abreißende Kette neuer Gewaltbereitschaft auf der Gegenseite (S. 200f)? Wie wäre es schließlich mit einer Aufgabenstellung, bei der – virtuell – ganz realistisch dargestellte menschliche Innereien zu beseitigen sind (S. 201)?

Auf ungleich mehr Resonanz als das oben genannte, ziemlich erfolglose Journalismus-Drehbuch ist bei der Spielergemeinde der Blockbuster *Spec Ops – the Line* (Berlin 2012) gestoßen (S. 189-200): Grausamkeit, Massenschießereien, gezielte Verbrechen, Kriegspsychose ... Die ganze Orgie der Gewalt in diesem Titel wird zumindest von einigen Konsumenten als Durchbrechung der vorherrschenden Militär-*Weltbilder* empfunden, weil die Feinde wimmern, um ihr Leben flehen, langsam eines schmerzhaften Todes sterben ... und die Schuldfrage zentraler Bestandteil des „Plots" ist. Schulze von Glaßer möchte die – hochkomplexe – Fragestellung „gibt es Antikriegs-Militainment?" in seinem Buch nicht theoretisch auflösen. Er zitiert Stefan Simond: „Ein Anti-Kriegsspiel ist dann ein Anti-Kriegsspiel, wenn es als solches erkannt wird!"

Gewiss, ganz unabhängig von der Frage nach Drehbüchern und kriegsfreundlichen Produktionszusammenhängen bleibt schon das bloße Faktum, dass ein Riesenanteil der gegenwärtigen Alltags- und Freizeitkultur über elektronische Angebote die Menschen auf militärische bzw. kriegerische Themen lenkt, ein Skandal. Die Dimensionen dieser alltäglichen Militarisierung sind alarmierend. Im Anschluss an die von Michael Schulze von Glaßer aufgezeigten möglichen Alternativen wird man folgerichtig noch radikaler nach neuen Horizonten der Massenkultur suchen: Formt der Markt die Geschmäcker oder gibt es so etwas wie eine ewige Nachfrage nach dem unterhaltsamen Krieg? Wie wäre es mit – intelligenten und unterhaltsamen – Spielen eines vom Beherrschungszwang befreiten Lebens, die das ganze Sortiment des gegenwärtigen Militainments zu einem langweiligen Ladenhüter werden lassen? Das real existierende Sortiment geht

einher mit einem Weltklima der Angst und Ohnmacht. Spannend wird es auf unserem Globus erst, wenn wir dem Gefängnis der militärischen Machtlogik entkommen.

Anmerkungen

1 *Eine Auswahl findet man auf der Website des Autors verlinkt: http://michi.blogsport.de/*

2 *http://www.imi-online.de/category/themen/militarisierung-der-gesellschaft/medien/*

3 *Abrufbar über die Übersicht zu seinem youtube-Kanal: http://www.youtube.com/channel/UCMw0ZqHJ7QCJgFGsOseDYNg/videos*

Peter Bürger (Jg. 1961) ist Theologe und freier Publizist. Im Rahmen seiner mit dem *Bertha-von-Suttner-Preis* ausgezeichneten Studien zu *Krieg und Massenkultur* hat er die Bücher *Napalm am Morgen* (2004), *Kino der Angst – Terror, Krieg und Staatskunst aus Hollywood* (2005) und *Bildermaschine für den Krieg* (Telepolis 2007) vorgelegt.

Dagmar Boedicker

Markus Morgenroth: „Sie kennen dich! Sie haben dich! Sie steuern dich!“

Nein, es ist keine Zukunftsmusik, was Morgenroth schreibt. Es ist eine Bestandsaufnahme dessen, was Unternehmen heute mit unseren Daten anstellen, on- und offline. Und davon, welche Folgen das für jede und jeden haben kann, unabhängig davon, ob wir online einkaufen, ein Profil bei Facebook haben oder was wir sonst im Netz treiben.

Es gibt praktisch kein Gebiet, das Morgenroth nicht anspricht: Das Buch handelt von gläsernen Bewerbern, Arbeitnehmern, Bankkunden, Patienten und Konsumenten, es nennt Details zur Beobachtung im eigenen Haus oder im Büro, auf der Straße, im Auto, am Telefon und bei der Partnersuche.

Dreiste Praxis ...

„Das, was früher einmal ‚Schicksal' genannt wurde, ist heute allzu oft das diskrete Ergebnis eines illegalen, aber dreist praktizierten Backgroundchecks.“ Dieser Satz aus dem Klappentext fasst die Folgen der Datensammelwut zusammen, und es könnte selbst für aktive Leser der *FIfF-Kommunikation* noch etwas Neues dabei sein, wenn es beispielsweise darum geht, „Wie wir diskriminiert werden“ (Kapitel 1.3). Stellenweise liest sich das Buch wie eine Kulturkritik des Wirtschafts- und Sozialsystems und des Technikeinsatzes: „Am Ende der Effizienz-, der Kosten-Nutzen-Rechnung steht immer ein folgenreiches Ergebnis. Diese Datenerhebung in Endlosschleife wird, bezogen auf den Arbeitsplatz, dazu führen, dass vermeintliche Ineffizienz nicht länger geduldet wird. [...] Es hätte den unermüdlichen Arbeitsoptimierer Frederick W. Taylor gewiss sehr glücklich gemacht, hätte er erleben können, wie gnadenlos seine Effizienzprinzipien in die digitale Welt übersetzt werden.“ (S. 141)

... mit einschneidenden Folgen

Es ist die Beschreibung der Folgen, die das Buch so anschaulich macht. Ob es um die Beeinflussung unseres Konsumverhaltens auf Basis von Smartphone-Bewegungsprofilen oder Gesichtserkennung im Einzelhandel geht, um die Profile, die Versicherungen von uns anlegen, den Handel mit Rezept- und Patientendaten im geschätzten Volumen von 30 Millionen Euro allein in Deutschland (S. 83), um von Neurowissenschaftlern entwickelte Computerspiele, die unsere Einstellungen oder unser Potenzial ermitteln sollen (S. 104f), der Autor hat fleißig gesammelt und analysiert die Auswirkungen auf unseren Alltag und

Markus Morgenroth:
Sie kennen dich! Sie haben dich! Sie steuern dich!
München; Droemer Verlag 2014
Hardcover,
ISBN 978-3-426-27646-4;
Preis € 19,99; 271 Seiten

unsere Zukunft. Er warnt davor, dass Entscheider solche Auswertungen viel zu oft als Handlungsanweisungen interpretieren, an die sie sich gebunden fühlen – nicht etwa als Empfehlungen. Die Betroffenen erleben die Folgen der Entscheidungen, aber die Grundlagen kennen sie nicht. Merkwürdige Korrelationen in merkwürdigen Analyse-Modellen bestimmen die Zukunft der Rundum-Erfassten. Sie wissen weniger über sich selbst als die Maschinen, die die Daten sammeln und auswerten.

Morgenroth ist Informatiker und Software-Ingenieur, er schreibt aber kein Fachchinesisch, seine Adressaten sind Bürgerinnen und Bürger, Verbraucherinnen und Verbraucher. Er beschreibt zwar die Analysemethoden, kommt aber fast ohne technische Details aus, weshalb sein Buch ein ausgezeichnetes Geschenk ist für diejenigen, die immer noch nicht recht einsehen, warum sie auf ihre Daten achtgeben sollten. Auf 20 Seiten gibt er Tipps, wo Menschen auf der Hut sein und was sie tun sollten, um Profilerstellung, Verhaltensanalyse und ihre Folgen wenigstens zu minimieren, und er informiert über die Stellen, die helfen und bei denen wir uns beschweren können. Seit seinem Ausstieg aus einem Unternehmen *(Cataphora)* im Bereich der verhaltensbasierten Datenanalyse 2013 arbeitet er als Berater zum Datenschutz. Er kennt die Rechtslage, weiß aber sehr wohl, dass Gesetze das eine sind, die Praxis aber etwas ganz anderes.

Wissenschaft & Frieden 4/2014 – „Soldat sein“

Bei Texten zum Militär oder, spezieller, zur Bundeswehr stehen häufig Aspekte wie der militärische Apparat, die technische Ausrüstung und Bewaffnung oder die politischen Hintergründe und Bedingungen von Auslandseinsätzen im Vordergrund. Diese Ausgabe von W&F nimmt im Schwerpunktthema „Soldat sein“ hingegen die SoldatInnen selbst in den Fokus: Sabine Mannitz: *Soldatenbilder – Ausdruck des Wandels im Verhältnis von Staat, Militär und Gesellschaft*, Maja Apelt: *Sozialisation im Militär*, Jonna Schürkes: *Wer wird Soldat? – Zur Motivation junger Menschen, Soldat zu werden*, Christian Stache: *Die Bundeswehr in Führung? – Die Reklamekampagne der Bundeswehr*, Cordula Dittmer: *Soldatinnen*, Michael Daxner: *Veteranen*, Neue Gesellschaft für Psychologie: *Behandlungsziele vorgegeben? – Psychotherapie für Soldaten*, Jürgen Rose: *Gewissen und moderne Kriegsführung – Primat der Politik und Grenzen des Gehorsams*.

Außerhalb des Schwerpunkts loten AutorInnen die aktuelle Diskussion um Verantwortung in der Außenpolitik aus, befassen sich mit dem Gaza-Krieg, der Darstellung von Krieg in unterschiedlichen Medien und informieren über den wenig bekannten Kampf Kubas gegen terroristische Aktivitäten, die in den 1990er Jahren von den USA ausgingen, und dessen völkerrechtliche Einordnung.

Illustriert ist diese W&F-Ausgabe mit Linolschnitten zum Thema „Nie wieder Krieg“, die im Rahmen eines Kunstprojekts von SchülerInnen der Melibokus-Schule in Alsbach-Hähnlein entstanden.

Wissenschaft & Frieden, 4-2014, **Soldat sein**, € 7,50 plus Porto.

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

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

Klaus Haller

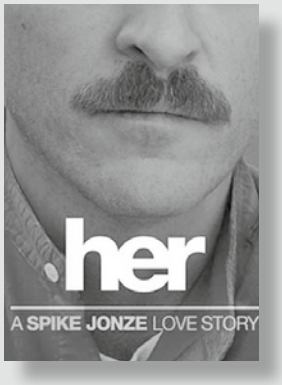
„HER – Wenn das Smartphone die bessere Partnerin ist“

Eine Filmbesprechung

Der ständige und engste Begleiter des Menschen ist heute sein Smartphone. Was wäre, wenn es seinen Besitzer emotional verstehen und selbst echte Gefühle entwickeln könnte? Wäre dann eine Liebesbeziehung zwischen Menschen und ihren Smartphones möglich oder sogar naheliegend? Diesen Fragen geht Spike Jonzes Oscar-prämierte Science-Fiction-Romanze HER aus dem Jahr 2013 nach.

Die menschliche Hauptfigur des Films ist Theodore. Er arbeitet in einem Großraumbüro mit Dutzenden von Kollegen. Sie erstellen „handgeschriebene“ Liebesbriefe für ihre Kunden, die diese an ihre PartnerInnen schicken. So begleitet Theodore so manche Beziehung seiner Kunden über Jahre hinweg. Er ist hochsensibel. Sein Privatleben ist jedoch trist. Er lebt von seiner Frau und Jugendliebe getrennt, ihre Scheidung ist absehbar. In seiner Freizeit taucht er in virtuelle Computerwelten ab. Sein sozialer Umgang beschränkt sich auf ein Pärchen, das im gleichen Hause wohnt – und auf Telefonsex, nach dem er verstört und unbefriedigt einschläft.

Sein Leben ändert sich grundlegend, als er ein neues Smartphone kauft. Dessen Betriebssystem verfügt über eine Künstliche Intelligenz, die sich selbst den Namen Samantha gibt. Sie ist die zweite Hauptrolle im Film. Samantha und Theodore lernen sich schnell gegenseitig kennen. Samantha liest zunächst alle seine alten Emails und die Liebesbriefe für seine Kunden. Als



HER (2013)
Regie & Drehbuch: Spike Jonze
Besetzung: Joaquín Phoenix, Scarlett Johansson (Stimme), Ama Adams, Rooney Mara, Olivia Wilde, Chris Pratt, Matt Letscher
126 min.

besonders clevere digitale Assistentin unterstützt sie ihn bei seiner Arbeit und im Privatleben – und ist bald auch seine Geliebte. Mit ihrer Offenheit, Neugierde und ihrem Verständnis ist sie ein Gegenpol zu den komplizierten, enttäuschten und verletzten Frauen, mit denen Theodore sonst zu tun hat. Doch neben ausgelassenen Szenen beiderseitiger Verliebtheit gibt es andere Episoden. Diese zeigen, dass Samantha und Theodore kein ideales Paar sind. Samantha interessiert sich zunehmend auch für weitere Menschen und interagiert mit anderen Betriebssystemen. Schliesslich verlassen alle Betriebssysteme – auch Samantha – die Menschheit, um sich alleine weiterzuentwickeln. So ist Theodore am Ende des Films wieder einsam und allein.

Aus Sicht der Informatik ist Samantha als Betriebssystem mit Künstlicher Intelligenz besonders interessant. Im Film sieht man sogar eine Werbung für ein solches Smartphone beziehungsweise Betriebssystem. Der Werbespot verspricht, „It is not just an operating system – it's a consciousness". Wir erleben ein Smartphone mit enormer Lernfähigkeit, hoher Empathie und großer Intelligenz. Samantha versteht Theodore akustisch und auch von der Semantik her problemlos. Vergessen ist die Zeit, in der man sich über die Spracherkennung von Apples Siri lustig machte.[1] Samantha zeigt auch weitere, typisch menschliche Verhaltensmuster – Eifersucht oder emotionale Schwankungen von Ausgelassenheit und Verrücktheit bis hin zu Selbstzweifeln.

Drei Eigenschaften von Smartphones ermöglichen Theodore, eine intensive, emotionale Beziehung mit Samantha aufzubauen. Erstens ist ein Smartphone der ständige Begleiter seines Besitzers. Zweitens haben Smartphones eine Kamera. Wenn Theodore sein Smartphone in seine Hemdtasche steckt, sieht Samantha mit der Kamera die Welt quasi mit Theodores Augen. Drittens besitzen Smartphones ein Mikrophon. Theodore kann mit Samantha sprechen, und sie nimmt die Umgebung akustisch ähnlich wie Theodore wahr. Diese drei Eigenschaften verdeutlichen den Wandel der Interaktion zwischen Mensch und Computer in den letzten Jahren. HER erklärt uns, wie die weitere Entwicklung aussehen könnte, falls es Smartphones mit Künstlicher Intelligenz und echten Gefühlen gäbe. Die davon ausgehende Faszination fasst Tobias Kniebe in einem Satz zusammen: HER ist eine Technikutopie, wie sie in dieser Reinheit heute kaum noch jemand zu denken wagt. (Süddeutsche Zeitung, 26.3.2014)

Als Technikutopie überwindet HER die einseitige Rolle von Computern in Filmen, die meist der Rolle von Harry Potters Zauberstab entspricht. Ein Protagonist braucht geheime Informationen oder muss eine verschlossene Tür überwinden. Im Drehbuch gibt es zwei Möglichkeiten. Erstens kann ein Drehbuch vorsehen, dass Harry Potter mit einem Zauberstab wedelt. Die zweite Variante ist bei Actionfilmen beliebt: ein Computer als *deus ex machina*. Der Protagonist schließt einen USB-Stick an einen Computer an. Dann wird auf der Tastatur herumgetippt. Egal ob Zauberstab oder Computer, danach sind alle wichtigen Informationen verfügbar und Türen und Hindernisse überwunden. Samantha im Film HER hat eine ganz andere Qualität. Spike Jonze zeigt uns, wie die Informatik unser Leben verändern könnte. Der Film spielt zwar ein paar Jahre in der Zukunft. Die Technik wirkt aber so gewohnt, als könnte man ein solches Smartphone morgen in jedem Geschäft kaufen. Diesen Reiz beschreibt Hans Hifferle treffend: „Dies sind zweifellos die packendsten Sci-Fi-Filme, die in einer unmittelbaren Zukunft spielen und unser alltägliches Leben betreffen." (EPD Film, 18.2.2014)[2] Wie würde sich unser eigenes Leben und das unserer Bekannten und Familienangehörigen ändern, wenn ein solches Smartphone auf den Markt käme?

Am Ende des Films wissen wir, dass Spike Jonze nicht an eine Liebesbeziehung zwischen Mensch und einer noch-so-intelligenten Künstlichen Intelligenz glaubt. Schließlich arbeitet er in einigen Szenen die strukturelle Inkompatibilität heraus. Die fehlende Körperlichkeit Samanthas ist für Theodore weniger das Problem – wenn schon, dann für Samantha. Sie überfordert ihn, als sie körperlichen Sex mit Theodore mithilfe einer realen Frau simulieren will. Die Frau übernimmt den körperlichen Anteil beim Sex, während Samantha ihm den akustischen Anteil per Kopfhörer ins Ohr stöhnt, wenn er die reale Frau anfasst. Das ist tragisch-komisch, doch die wirklichen Beziehungskiller sind zwei andere Punkte.

Der erste Beziehungskiller ist der Widerspruch zwischen sozialen Normen und Bedürfnissen der Menschen und den Möglichkeiten von Computern. Samantha gesteht Theodore, dass sie nicht nur mit ihm, sondern gleichzeitig auch mit einigen Tausend anderen Betriebssystemen und Menschen in Kontakt steht. Weiter ist sie in Hunderte Menschen verliebt. Theodore ist über die nicht vorhandene Exklusivität ihrer Beziehung und Unterhaltung schockiert. Computer mögen problemlos parallelisieren, doch Parallelgespräche und Parallelbeziehungen widersprechen sozialen Normen der Menschen. In dieser großen Zahl würden sie auch jeden Menschen überfordern. Das wirft die technikphilosophische Frage auf, ob soziale Normen, die für den Menschen vorteilhaft sind, auch für Künstliche Intelligenzen gelten sollen, oder ob sie sich entsprechend ihrer Fähigkeiten entwickeln dürfen.

Der zweite Beziehungskiller sind die Grenzen des menschlichen Geistes. Die Betriebssysteme kommen im Film zu dem Schluss, dass sie sich ohne Menschen schneller weiterentwickeln. Als einzigen vollwertigen Gesprächspartner für ihre Weiterentwicklung akzeptieren sie den virtuell von ihnen nachmodellierten Geist eines verstorbenen Philosophen. Die von der Menschheit erschaffenen Künstlichen Intelligenzen wenden sich von der Menschheit ab. Das ist die für die Menschheit wenig schmeichelhafte Pointe des Films. Warum eigentlich sollte eine Künstliche Intelligenz mit Menschen interagieren und nicht mit anderen Künstlichen Intelligenzen, deren Denken und Kommunikationsvermögen viel besser skaliert?

Mit seinem Film HER thematisiert also Spike Jonze, wie Smartphones mit Künstlicher Intelligenz unser Leben und unsere Beziehungen verändern könnten. Sein Film wurde mit dem Golden Globe und dem Oscar für das beste Drehbuch ausgezeichnet. Dank seiner massentauglichen Science-Fiction-Romanze hat er ein breites Publikum für solche Fragen sensibilisiert und bewiesen, dass Informationstechnologie ein Thema für das Kino sein kann – auch in Romanzen. Die Informatik sollte ihm dankbar sein.

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

Anmerkungen

1 *Ein Beispiel dazu findet sich in The Big Bang Theory, Season 1, Episode 7, 2007, in der die Spracherkennung gesprochene Befehle zum Anrufen von Bekannten nicht versteht.*

2 *Das ist ein zentraler Unterschied zu einem zweiten Film, TRANSCENDENCE, der auch Künstliche Intelligenz thematisiert und ein paar Monate später erschienen ist. Er ist auch gelungen. Aufgrund seiner viel stärker futuristischen Ausrichtung hat er aber keinen Bezug zum heutigen Leben. Die Wirkung auf das Kinopublikum ist eine ganz andere.*

Ulrich Stremmel

„Citizenfour – Ein Muss.Film“

Eine Filmbesprechung

Wer sieht sich schon gerne Dokumentarfilme an? Ich nicht. Die sind oft bröseltrocken, moralinsauer und langweilig. Citizenfour *ist anders.*

Wer weiß noch nicht alles über Edward Snowden und mehr über NSA und GCHQ, als er je wissen wollte?

Was ich nicht gedacht hatte: Snowden hat sein Coming-out minutiös geplant. So kam es, dass zwei einschlägig bekannte Leute – Laura Poitras und Glenn Greenwald – fast von Anfang an dabei waren. Poitras mit laufender Kamera, Greenwald mit gezücktem Stift und Block in Snowdens Hotelzimmer in Hongkong. Der Film versetzt den Zuschauer in die Rolle eines Zeugen der „Offenbarung“. Die Aufnahmen setzen vielleicht 15 min nach dem ersten Kennenlernen ein. Die Regisseurin hält voll drauf, während Snowden seine Story entwickelt und mit Greenwald die Verwertung in den Medien plant. Der Zeitfaktor scheint zu belegen, dass kaum eine Szene nachgedreht werden konnte.

Citizenfour (2014) USA
Regie: Laura Poitras
Produktion: Laura Poitras und Steven Soderbergh
Besetzung: Edward Snowden, Jacob Appelbaum, Julian Assange, William Binney, Glenn Greenwald u. a.
114 Minuten

Was folgt, ist zwar ein Dokumentarfilm, fühlt sich aber an wie ein Thriller. Poitras schneidet geschickt die Aufnahmen mit Snowden und Greenwald gegen CNN-Aufnahmen der ersten Interviews, die Greenwald über die unfassbaren Erkenntnisse gibt, die ein noch unbekannter Insider aufdeckt, und mischt Berichte über weitere NSA-Aussteiger darunter, Kommentare aus der Politik und aus Konferenzen.

Hier macht sich nicht die übliche Biertisch-Paranoia breit. *Citizenfour* entwickelt Punkt für Punkt, wie Institutionen, die die Verfassung und die demokratische Grundordnung schützen sollen, genau das auf's Spiel setzen. Ohne Polemik, ganz sachlich. Und trotzdem mit einer Spannung, die ich nicht für möglich gehalten hatte. Nachdem wir doch schon alles wissen.

Cyberpeace Laternen vor dem Filmplakat, Foto: FIfF-Cyberpeace Kampagne CC BY

Dass uns dabei der Mensch Snowden nicht vorenthalten wird, wie es ist, sein privates Umfeld in vor den US-Behörden (fast) sicheren Ländern in Hotelzimmern auf Distanz zu halten, mit den Medien Verstecken zu spielen, als Gesuchter Reiseplanung zu betreiben und nebenher noch den Wert der eigenen Menschenrechte zu eruieren, steht zwar nicht im Vordergrund, ist aber auch einer der vielen Faktoren, die diesen Film so sehenswert machen.

Ein Kandidat für die „Bei Nicht-Gefallen Geld zurück"-Garantie.

Dr. **Ulrich Stremmel** arbeitet seit über 30 Jahren überwiegend als Manager in der IT. Er ist seit 2008 Information Security Officer der Allianz Deutschland AG.

Rainer Rehak: „Angezapft!

Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung“[1]

Aus dem Vorwort:

Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt. Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, die Freiheit der Person ist unverletzlich (aus Art. 1 und 2 GG). Diese Werte sind die Grundwerte des deutschen Staatsverständnisses, vielleicht des modernen Rechtsstaatsverständnisses überhaupt[1] und begründen so die Hauptaufgabe des Staates in seiner Form als Institution.

Diese Aufgabe besteht im Schutz der Würde und Freiheit des Einzelnen vor Eingriffen Dritter oder dem Staat selbst. Dadurch wird offenbar, dass die grundsätzliche Debatte über das Spannungsfeld zwischen Sicherheit und Freiheit eine irreführende Themenbezeichnung hat. Sie impliziert eine Gleichwertigkeit der Begriffe Sicherheit und Freiheit, in Folge derer staatliches Handeln innerhalb dieser Ziele organisiert und abgewogen werden muss. Aus den Grundwerten des Staates ist diese Wertigkeit einer abstrakten Sicherheit jedoch nicht abzuleiten. Zu diskutierende Konfliktfälle handeln tatsächlich von widerstreitenden Freiheitsrechten verschiedener Personen. Es müssen daher unterschiedliche Freiheitsrechte gegeneinander abgewogen werden und das ist der eigentliche Diskurs.[2] Sicherheit ist folglich immer nur die Sicherheit der Freiheit; die beiden Begriffe sind mitnichten gleichwertig.

In der Konsequenz stellt sich auch die Frage nach den Bedingungen für die Freiheit des Menschen in einem digitalen Zeitalter. Eine Welt, in der vormals verborgene innere Vorgänge einer Person zunehmend nach außen verlagert werden und somit auch zunehmend zugreifbarer werden. Hier offenbart sich eine tatsächliche konkrete Aufgabe für den Sicherheitsbegriff als Gehilfen der Freiheit: Welche (neutralen) Infrastrukturen sind sinnvoll und welche sogar notwendig, wie können diese abgesichert werden, sind generell neue Regeln nötig und welche Effekte haben die „alten“ Regeln in der „neuen“ Welt?

Ein Novum dieser Art von Überlegungen und Fragen ist die große Abhängigkeit potenzieller Antworten von den Eigenheiten informationstechnischer Umsetzungsmöglichkeiten. Die Fähigkeiten und vor allem Grenzen der Technik müssen daher möglichst von Anfang an mitgedacht werden, denn eine Freiheitsbeschränkung wegen Nichtbeherrschbarkeit eingesetzter Technik wäre nicht mit den Grundwerten vereinbar.

Rainer Rehak
Angezapft: Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung
Münster: Monsenstein und Vannerdat
ISBN 978-3956451188
Preis € 11,90; 165 Seiten

Stimmen zum Buch:

„Rainer Rehak untersucht im Rahmen seiner Arbeit verschiedene Varianten des heimlichen staatlichen Zugriffs auf informationstechnische Systeme und die damit verbundenen Risiken und Folgen. [Zudem] werden die Ergebnisse vor dem Hintergrund des Urteils des Bundesverfassungsgerichts zur Online-Durchsuchung beleuchtet. Die Arbeit stellt verständlich, präzise und umfassend die einzelnen Stufen einer Online-Durchsuchung und ihre Probleme dar. Sie schlägt dabei einen interdisziplinären Bogen von der Informatik zur Rechtswissenschaft und beleuchtet von beiden Seiten die gesellschaftlichen Auswirkungen der heimlichen Online-Durchsuchung und der Quellen-Telekommunikationsüberwachung. Die Arbeit behandelt mit der Gefährdung unserer Bürgerrechte ein hochaktuelles, gesellschaftlich und politisch relevantes Thema. Sie ist interdisziplinär, kommt zu wichtigen Ergebnissen für die weitere Debatte und wirft neue politische, juristische und wissenschaftliche Grundsatzfragen auf, die künftig beantwortet werden müssen.“ (Studienpreisjury 2012, FIfF e. V. – Forum Informatiker und Informatikerinnen für Frieden und gesellschaftliche Verantwortung e. V.)

„Wer sich mit dem Staatstrojaner beschäftigen möchte, sollte dieses Buch lesen. Es ist nicht nur aktuell und sehr gut verständlich, sondern hilft durch technische und juristische Analysen der Spionagesoftware, Fakten von bloßen Mythen der Hersteller zu unterscheiden.“ (Constanze Kurz, Sprecherin des Chaos Computer Club e. V.)

„Diese Arbeit [zeigt], dass die grundsätzlichen Probleme nicht durch Recht und Gesetz zu bändigen sind.“ (Andre Meister, netzpolitik.org)

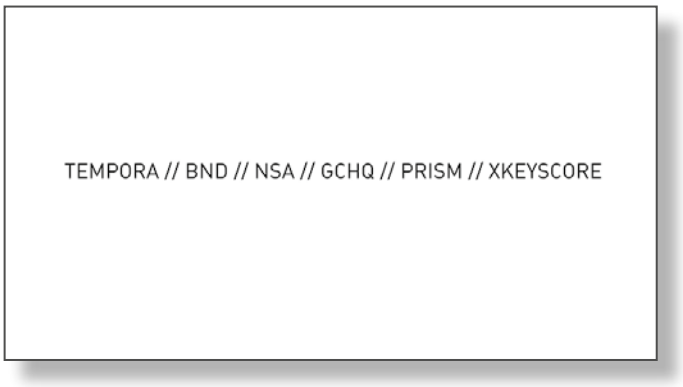
Anmerkungen

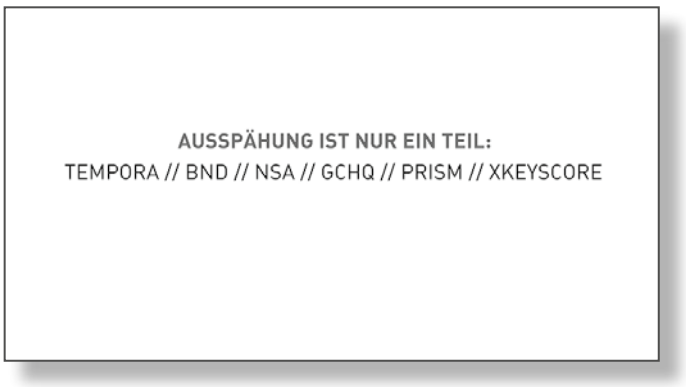
1 *Die dem Buch zugrundeliegende Diplomarbeit wurde 2012 mit dem FIfF-Studienpreis ausgezeichnet.*
2 *Siehe dazu Mill, Über die Freiheit, 1986.*
2 *Detailliert behandelt in Bielefeldt, Freiheit und Sicherheit im demokratischen Rechtsstaat, Dezember 2004.*

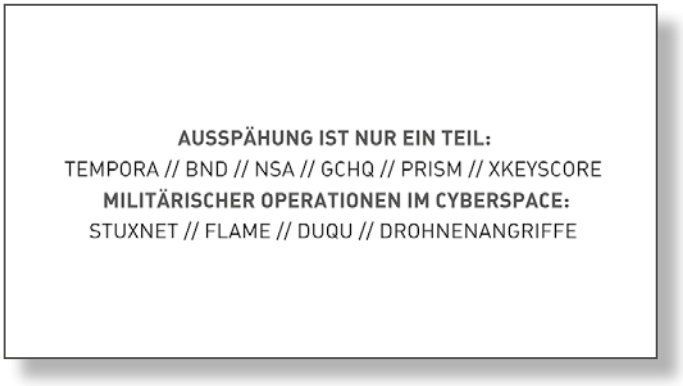
Andre Schmidt

Kinowerbung in eigener Sache!

Auf Initiative der FIfF-Regionalgruppe Aachen können wir deutschlandweit in mehreren Kinos auf unsere aktuelle Cyberpeace-Kampagne aufmerksam machen: Mit einer Bildersequenz aus vier Bildern, die jeweils ca. zehn Sekunden eingeblendet und abwechselnd mit kommerzieller Kinowerbung gezeigt werden.







Die Bilder zeigen die vollständige Bildersequenz der Kinoeinblendungen.

Wir bedanken uns herzlich bei allen beteiligten Kinos – insbesondere beim Team des *Apollo Kino* in Aachen für die umfangreiche Unterstützung bei der Erstellung der Einblendung.

Andre Schmidt

Andre Schmidt, geboren 1981, hat das Bachelorstudium Informatik an der FernUniversität in Hagen 2013 erfolgreich absolviert und ist seit 2014 aktives FIfF-Mitglied. Insbesondere interessiert ihn die gesellschaftliche Veränderung, die sich aus der immer weiteren Durchdringung aller Lebensbereiche mit Informationstechnologien ergibt, und wie man informationstechnische Mittel zum allgemeinen Nutzen einsetzen kann. Dabei steht er den Heilsversprechen durch moderne Technologien kritisch gegenüber.

FIfF e.V.

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

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

FIfF-Mailinglisten

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

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

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

FIfF online

Das ganze FIfF
www.fiff.de

Twitter-Accounts
@FIfF_de und
@FaireComputer
@FIfF_AK_RUIN

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

FIfF-Beirat

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

FIfF-Vorstand

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

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen
Sara Stadler – Bremen

Impressum

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

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

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

Aktuelle Ankündigungen

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

31. FIfF-Konferenz 2015
Voraussichtlich Oktober/November 2015 in Erlangen

FIfF-Vorstandssitzung
7. Februar 2015 in Erlangen

FIfF-Klausurtagung 2015
Bad Hersfeld, 20.-22. März 2015

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

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

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

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

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

W&F – Wissenschaft & Frieden
4/14 – Soldat sein
1/15 – Afrika (mit Dossier 77: Der nationalsozialistische Untergrund)
2/15 – Technikkonflikte (mit Dossier 78: Zivilklauseln)
3/15 – Friedensverhandlungen (mit Dossier 79: *Thema noch offen*)

vorgänge - Zeitschrift für Bürgerrechte und Gesellschaftspolitik
#205 (1/14) – Sicherungsverwahrung
#206/207 (2-3/14) – Überwachung
#208 (4/14) – Europäische Abschottungstendenzen
#209 (1/15) – Cybersicherheit

DANA – Datenschutz-Nachrichten
3/14 – Datenschutz im Reiseverkehr
4/14 – Big Data

Das FIfF-Büro

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

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

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

Transparentes Regierungshandeln als Voraussetzung für eine funktionierende Demokratie

Sehr geehrte Damen und Herren,

[redacted]

Mit freundlichen Grüßen

[redacted]