H 7625

FIfF-Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

31. Jahrgang 2014 Einzelpreis: 7 EUR

1/2014 – März 2014

ISSN 0938-3476

• Snowden – Held oder Verräter • FIfF-Studienpreis 2013 • AK RUIN •

Mit Dossier: Information Warfare und Informationsgesellschaft

FIfF Kommunikation

Titelbild: Sanne Grabisch *http://ideal.istik.de/* für die Cyberpeace-Kampagne des FIfF *http://www.fiff.de/* freigegeben, CC BY-SA 3.0

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Inhalt

Ausgabe 1/2014

inhaltt

03 Editorial
- *Stefan Hügel*

FIfF e.V.

04 Brief an das FIfF: 1984 + 30
- *Stefan Hügel*

05 Ausschreibung FIfF-Studienpreis 2014

06 AK RUIN – RUestung und INformatik

16 Ankündigung FIfF-Jahrestagung 2014

Retrospektive

55 Politik der Chiffren
- *Ingo Ruhmann*

Lesen & Sehen

59 „Computer Chess“: Ein Film von skurrilen InformatikerInnen und der Angst vor dem 3. Weltkrieg
- *Klaus Haller*

60 „Inside Wikileaks“
- *Dietrich Meyer-Ebrecht*

61 Mark Mazzetti: „Killing Business. Der geheime Krieg der CIA“
- *Dagmar Boedicker*

62 Christian Fuchs und John Goetz: „Geheimer Krieg – wie von Deutschland aus der Kampf gegen den Terror gesteuert wird“
- *Stefan Hügel*

64 Karin Harrasser: „Körper 2.0. Über die technische Erweiterbarkeit des Menschen“
- *Britta Schinzel*

Rubriken

67 Impressum/Aktuelle Ankündigungen

68 SchlussFIfF

Schwerpunkt FIfF-Jahrestagung 2013 – Cyberpeace

21 Datenschutz bei datenzentrischen Diensten Auslaufmodell oder nur 30 Jahre zurück?
- *Günter Müller*

25 „Das Imperium schlägt zurück“
- *Sebastian Schweda*

30 Die Grenzen des Systems sind die Grenzen der Person
- *Rainer Rehak*

32 Mitten im Cyberkrieg – Angriff auf die Zivilgesellschaft
- *Ute Bernhardt, Ingo Ruhmann*

34 Wer nicht kämpft, hat schon verloren
- *Karin Schuler*

37 Deutsche Sicherheitspolitik, Bundeswehr und CyberWarfare
- *Paul Schäfer*

Schwerpunkt FIfF-Studienpreis 2013

43 Einleitung
- *Stefan Hügel*

44 Too smart for you? – Anforderungen an den Einsatz von mobilen Informatiksystemen in der Schule
- *Daniel Spittank*

48 ‚Due To Legal Issues‘ – Packet Inspection
- *Agata Królikowski*

52 Zweckgebundener Datenbrief
- *Julia Hofmann*

Aktuelles

08 Edward Snowden – Held oder Verräter?
- *Christian Schrader*

12 Zum 30. Mal Chaos Communication Congress – 30C3
- *Sylvia Johnigk*

14 Vortrag *Dead Man Edition* auf dem 30C3
- *Sebastian Jekutsch*

15 Betrifft: Faire Computer
- *Sebastian Jekutsch*

16 Log 1/2014
- *Sara Stadler*

20 Ausbau der Internet-Polizei
- *Stephan Geelhaar*

Editorial

Cyberpeace – Frieden gestalten mit Informatik. Das war der Titel unserer Jahrestagung 2013 und das ist der Titel des Schwerpunkts in diesem Heft, der die Jahrestagung dokumentiert und aufarbeitet.

Dass diese Forderung sehr aktuell ist, zeigen die Ereignisse der letzten Monate: die weiterhin andauernde Ausspähung duch Nachrichtendienste, verbunden mit Angriffen auf die Integrität unserer Kommunikationsinfrastruktur – allein bereits eine Form des Cyberkriegs – und die Kriegführung durch Drohnen, die die Erkenntnisse der Ausspähung nutzt und Recherchen zufolge bereits den Tod tausender von Menschen verursacht hat – vermeintliche Terroristen ebenso wie Unschuldige –, praktisch immer ohne rechtsstaatliches Verfahren.

Dass ein unbegrenzter Cyberkrieg gegen Freund und Feind geführt wird, machen *Ingo Ruhmann* und *Ute Bernhardt* in ihrem umfassenden Dossier *Information Warfare und Informationsgesellschaft – Zivile und sicherheitspolitische Kosten des Informationskriegs* sehr deutlich. Das Dossier entstand in Zusammenarbeit mit der Zeitschrift *W&F – Wissenschaft und Frieden* und ist deren Ausgabe 1/2014 sowie dieser Ausgabe der *FIfF-Kommunikation* beigelegt.

Der Schwerpunkt der Ausgabe zur Jahrestagung besteht aus zwei Teilen: Der erste Teil dokumentiert Vorträge und Arbeitsgruppen der Tagung. In seinem im Umfeld des FIfF sicherlich Widerspruch provozierenden Beitrag *Datenschutz bei datenzentrischen Diensten: Auslaufmodell oder nur 30 Jahre zurück?* vertritt *Günter Müller* die Grundthese, Daten seien als handelbare Ware aufzufassen. Er schlägt einen wirtschaftlich basierten Datenschutz vor, der auf Transparenz in Verbindung mit Privatheitsregeln fußt. Heutige Datenschützer erscheinen ihm eher wie anachronistische Idealisten – ein frei bestimmtes *Opt-out* ohne soziale und wirtschaftliche Kosten sei über Regulierung nicht erreichbar.

Das Imperium schlägt zurück, so überschreibt *Sebastian Schweda* seinen Bericht *zur Lage der Menschenrechte im digitalen Zeitalter*. „*Cyberwar ist die Fortführung des kinetischen Kriegs mit anderen Mitteln*", stellt er fest. „*Der Kollateralschaden dieses virtuellen Krieges mit realen Folgen ist die weitgehende Vernichtung der unkörperlichen Integrität des Einzelnen: seiner Privatsphäre.*" Schweda arbeitet am Aufbau einer Koordinationsgruppe *Digitale Technologien und Menschenrechte* bei *amnesty international* und wünscht sich dazu Austausch und Kooperation mit dem FIfF.

„*Die Infrastruktur unserer digitalen Welt wird ganz bewusst unsicher, extern zugreifbar und flächendeckend überwacht gestaltet*", so *Rainer Rehak* in seinem Beitrag *Die Grenzen des Systems sind die Grenzen der Person*. Er fordert unter anderem die Beendigung der Zusammenarbeit des BSI mit Geheimdiensten, die Aufhebung der staatlichen Abhängigkeit deutscher Datenschutzkontrollinstanzen und den ausschließlichen Einsatz freier Software in staatlichen Stellen und Organen. Rainer Rehak bezweifelt, dass „*eine Demokratie überhaupt mit dem Prinzip des Geheimen (von unfreier Software bis hin zu Geheimdiensten) kompatibel ist.*"

Ausführlich wird die Arbeitsgruppe *Mitten im Cyberkrieg – Angriff auf die Zivilgesellschaft* behandelt. In ihrem einleitenden Beitrag stellen *Ute Bernhardt* und *Ingo Ruhmann* fest, dass durch die Ausspähung des NSA-Skandals nicht allein unsere Privatsphäre, sondern die gesamte Infrastruktur in Gefahr ist, deren Voraussetzung sichere IT-Systemen sind. Die Autoren vermissen jegliche politische Gestaltungsidee und erwarten von IT-Sicherheitsverantwortlichen in der Wirtschaft und von Bürgerinnen und Bürgern, notfalls ihre Interessen gegenüber Politik und Cyber-Kriegern durchzusetzen.

Ein erster Schritt dazu ist der Selbstdatenschutz. *Karin Schuler* gibt in ihrem Beitrag *Wer nicht kämpft, hat schon verloren* einen Überblick über dessen Möglichkeiten und Werkzeuge: „*Weder der Gesetzgeber noch Fatalismus bringen uns unsere Grundrechte zurück, wenn wir nicht auch die Möglichkeiten des Selbstdatenschutzes ausschöpfen.*" Eine umfassende Darstellung zur *deutschen Sicherheitspolitik, Bundeswehr und Cyber-Warfare* gibt der frühere Bundestagsabgeordnete *Paul Schäfer*. Zur Einhegung und Kontrolle fordert er mindestens die Beseitigung bestehender Sicherheitsmängel, die Durchsetzung des Grundwerts *Schutz der Privatsphäre* als Teil der Netzpolitik, Rüstungskontrolle und Abrüstung anstatt eines neuen Rüstungswettlaufs auch im Bereich der Cyberwarfare, und das ständige kritische Hinterfragen der Kriseninterventionen *out of area*.

Der zweite Teil des Schwerpunkts dokumentiert den *FIfF-Studienpreis 2013*. Nach einer einleitenden Übersicht folgen die Beiträge von *Daniel Spittank*: *Too smart for you? – Anforderungen an den Einsatz von mobilen Informatiksystemen in der Schule,* von *Agata Królikowski*: *‚Due to legal Issues' – Packet Inspection* und von *Julia Hofmann*: *Zweckgebundener Datenbrief für das Identitätsmanagementsystem mittels Web-basiertem Benutzerinterface*.

Der aktuelle Teil enthält eine Analyse von *Christian Schrader*: *Edward Snowden – Held oder Verräter*. „*Letztlich ist er ein Held*", stellt er darin fest, „*weil er uns hoffen lässt, dass die in ihrem Krieg gegen den Terror so verblendeten USA doch wieder das Land der Freiheit sein können.*" In der kurzen Fortsetzung seines Beitrags aus der *FIfF-Kommunikation* 4/2013 liefert *Stephan Geelhaar* ein Update zum *Ausbau der Internet-Polizei*. Ergänzt wird der aktuelle Teil durch Konferenzberichte von *Sylvia Johnigk* und *Sebastian Jekutsch* zum 30. *Chaos Communication Congress* und die bereits etablierten Kolumnen.

Die Retrospektive, erneut von *Ingo Ruhmann* zur immer noch aktuellen *Politik der Chiffren* aus Sicht von 1996 und unsere Rezensionen von Büchern und Filmen ergänzen diese Ausgabe der *FIfF-Kommunikation*.

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

Stefan Hügel
für die Redaktion

1984 + 30

War is Peace
Freedom is Slavery
Ignorance is Strength
(George Orwell, Nineteen eighty-four)

Liebe Mitglieder des FIfF, liebe Leserinnen und Leser,

im Jahr 1949 veröffentlichte George Orwell seinen dystopischen Roman *Nineteen eighty-four* – die Darstellung eines totalen Überwachungsstaats. Seither wird die Jahreszahl *1984* gerne als Symbol für Überwachung verwendet. Fast ebenso bekannt sind die Parolen der regierenden Partei des Romans:

„War is Peace"

Mit dem Ende des kalten Krieges hofften wir, nun endlich die Friedensdividende einfahren und ohne ständige Kriegsdrohung leben zu können. Und es scheint ja auch zu stimmen: Die Gefahr eines globalen Atomkriegs erscheint seit Jahren gebannt. Das Leben unter täglicher Kriegsdrohung ist in weite Ferne gerückt.

Doch die Bedrohung ist nicht verschwunden – sie hat nur Ort und Opfer gewechselt. Gleichzeitig soll die Bundeswehr – einst als reine Verteidigungsarmee gegründet – eine immer größere Rolle in der Welt spielen. „Die Sicherheit der Bundesrepublik Deutschland wird auch am Hindukusch verteidigt." begründete der damalige Verteidigungsminister Peter Struck bereits 2002 *Out-of-Area*-Einsätze, die zuvor undenkbar waren. Manche würden sich auf ein fragwürdiges „Recht auf Wegsehen" zurückziehen, kritisiert heute Bundespräsident Joachim Gauck, ein militärischer Einsatz sei als „äußerstes Mittel" möglich. Deutschland müsse mehr Verantwortung übernehmen, assistiert Verteidigungsministerin Ursula von der Leyen und kündigt an, das Engagement in Afrika zu verstärken. „Als eine bedeutende Volkswirtschaft und als ein Land von erheblicher Größe" habe die Bundesrepublik Deutschland „ein starkes Interesse an internationalem Frieden und Stabilität." Militärpolitik als Wirtschaftspolitik? Nachdem der damalige Bundespräsident Horst Köhler noch wegen eines solchen Statements und der darauf folgenden öffentlichen Empörung zurücktrat, sollen wir offenbar langsam daran gewöhnt werden.

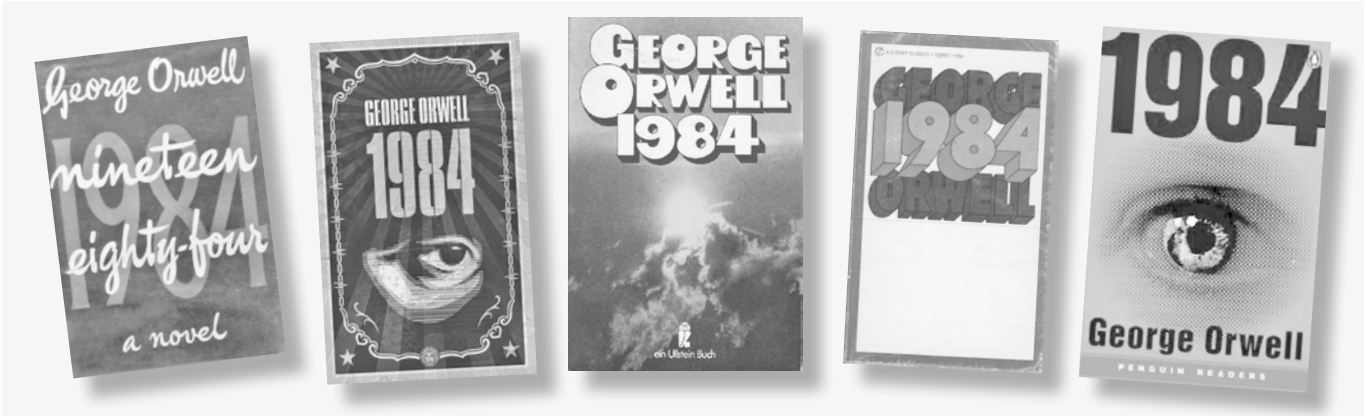
Gleichzeitig führen unsere Verbündeten, die Vereinigten Staaten, ihren *Krieg gegen den Terror* weiter – insbesondere mit Drohnenangriffen, denen Menschen mit einem als *terroristisch* wahrgenommenen Verhaltensprofil zum Opfer fallen. Von den weiteren, zynisch als *Kollateralschaden* verharmlosten, zivilen Opfern nicht zu reden. Müssen wir nach außen Krieg führen, um nach innen unseren Frieden – und unseren Wohlstand – zu bewahren?

„Freedom is Slavery"

„Wir wählen die Freiheit!" – so lautet ein vielzitierter Ausruf des damaligen Bundeskanzlers Konrad Adenauer. Auch Bundespräsident Joachim Gauck wird nicht müde, Freiheit als Wert in den Vordergrund zu rücken – dem ist zunächst ja auch zuzustimmen.

Nicht immer ist jedoch klar, was sie damit meinen. Der Umgang mit Andersdenkenden gerade in der Bundesrepublik Adenauers zeichnet bereits ein fragwürdiges Bild. Wie wir zudem mittlerweile wissen, steht die Bundesrepublik Deutschland seit Anbeginn unter umfassender Überwachung durch aus- und inländische Geheimdienste. Was seit nunmehr einem dreiviertel Jahr als *NSA-Skandal* die öffentliche Diskussion bestimmt, ist nur die Fortsetzung dieser Überwachung, die damit bis heute andauert. Sie ist eine Form des Cyberkriegs.

Als der aktuelle Ausspähskandal bekannt wurde, wurde von einigen politisch Verantwortlichen die angeblich wichtige Rolle betont, die die Informationen aus der Überwachung auch für den Schutz der deutschen Bevölkerung spielen. Überwachungsinitiativen wie die Vorratsdatenspeicherung werden parallel



65 Jahre 1984, Erstausgabe erschienen 1949 (ganz links)

dazu konsequent vorangetrieben, vorgeblich ebenfalls, um uns zu schützen – vor Terror, vor Kriminalität. Sicherlich kann man den damit verbundenen Verlust an Freiheit als *Sklaverei* versinnbildlichen.

Freiheit ist ein Menschenrecht – das schließt allerdings auch die wirtschaftlichen Voraussetzungen ein. Die Grenze ist dann überschritten, wenn die Freiheit der einen zur inakzeptablen Beeinträchtigung der Anderer führt. Hier gibt es dann auch Fälle, die wir tatsächlich als Sklaverei bezeichnen können. Ob aber die weltweite Ausspähung das richtige Mittel dagegen ist, ist zweifelhaft.

„Ignorance is Strength"

Transparentes Regierungshandeln bleibt immer noch hinter dem Möglichen und Notwendigen zurück. Häufig wird hinter geschlossenen Türen verhandelt. Soll die Bevölkerung uninformiert bleiben, um umstrittene Abkommen durchzusetzen?

Ein zweites Phänomen ist die überraschte öffentliche Reaktion politisch Verantwortlicher auf Enthüllungen, und die Beteuerung, davon nichts gewusst zu haben; so erlebt beim Ausspähskandal oder der Debatte um die Drohne *Eurohawk*. Wie glaubwürdig das im Einzelfall ist, muss jede/r für sich entscheiden – fraglich ist allerdings, ob Verantwortliche, die in ihrem eigenen Verantwortungsbereich keine Kenntnis von wesentlichen Vorgängen haben, dem Anspruch an ihr Amt gerecht werden. Ist Unwissenheit Stärke?

Orwells Roman fügt eine Reihe von Facetten zusammen, die eine Diktatur ausmachen. Keinesfalls will ich nun behaupten, dass wir bereits in einer derartigen Diktatur leben – die Behauptung wäre verstiegen. Dennoch lohnt es sich, die Realität mit den vielen Bausteinen abzugleichen, die Orwell in seinem Roman aufzählt. Um jedweden Anfängen zu *wehren* ...

Mit FIfFigen Grüßen

Stefan Hügel

Das FIfF verleiht 2014 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 2014 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 2014
Goetheplatz 4, 28203 Bremen
oder per E-Mail an *studienpreis@fiff.de*.
Weitere Details unter *http://www.fiff.de/studienpreis.*

Der Preis wird in einer Feierstunde im Rahmen der FIfF-Jahrestagung am 8. November 2014 in Berlin verliehen.

AK RUIN – RUestung und INformatik

Arbeitstreffen am 9. Februar 2014 in Berlin

Nach einer intensiven Vorstandssitzung am vorangegangenen Samstag traf sich am Sonntag, dem 9. Februar 2014, der Arbeitskreis Rüstung und Informatik *im* Haus der Demokratie und Menschenrechte *in Berlin. Dabei ging es vor allem um die Schwerpunktthemen des Arbeitskreises und zukünftige Aktivitäten. Wichtigstes Thema war die Planung einer Cyberpeace-Kampagne.*

Am Anfang jeder Kampagne steht die Eingrenzung des Kampagnenthemas. Die derzeitige öffentliche Debatte führt uns dabei unmittelbar zur *nachrichtendienstlichen Ausspähung* der Bevölkerung, der Wirtschaft und politischer Entscheidungsträger sowie, damit verbunden, zur Infiltration von IT- und Kommunikationssystemen weltweit mit schädlicher Software und Hardware. Aus Sicht des AK RUIN ist dies bereits eine Form des Cyberkrieges, der gegen Freund und Feind gleichermaßen geführt wird. Er kompromittiert die Integrität unserer Kommunikationsinfrastruktur insgesamt und gefährdet damit die demokratische Basis unserer Kommunikationsgesellschaft. Gleichzeitig bereiten derartige Angriffe weitergehende Operationen vor. *Signature Strikes* beispielsweise, eine spezielle Form der gezielten *Tötung von Menschen durch Drohnenangriffe*, bei der die Zielpersonen durch Abgleich von Verhaltensmustern, nicht aber zweifelsfreie Identifizierung durch Sichtprüfung bestimmt werden. Sie bauen auf Informationen auf, die durch die Ausspähung der Kommunikation geliefert werden.

Es gibt darüber hinaus mehrere weitere Themenfelder, die im Kontext *Cyberpeace* diskutiert werden und die im AK RUIN weiter bearbeitet werden sollten:

Rüstung und Informatik: Ein klassisches FIfF-Thema, FIfF-Kommunikation 2/2005

- **Regeln für den Cyberkrieg** – vergleichbar der Genfer Konvention –, wie sie durch das *Tallinn-Manual* vorgeschlagen werden. Solche Regeln legen fest, was als Angriff zu gelten hat und welche Reaktionen darauf legitim sind. Grundsätzlich ist ein solches Regelwerk zu befürworten – es muss aber diskutiert werden, welche konkreten Regeln gelten sollen. Problematisch ist beispielsweise die Legitimierung konventioneller Militärschläge als Antwort auf Cyberangriffe.

- **Militärroboter**. Dieses Themenfeld geht über den Einsatz von Drohnen, die bereits eine spezielle Form der Militärroboter darstellen, weit hinaus. In diesem Zusammenhang werden Fragen zur Künstlichen Intelligenz (KI), zur automatisierten Erkennung feindlicher Kräfte und zu Formen einer automatisierten Ethik diskutiert.

- **Zivilklausel**. Grundlage jeder Rüstung und Kriegführung ist die militärische Forschung, die nicht selten im zivilen *Schafspelz* daherkommt. Zivilklauseln zielen darauf ab, dem Militär – zumindest an den Hochschulen – durch die Verpflichtung auf ausschließlich zivile Forschung den Boden zu entziehen.

- Nicht zuletzt gibt es das Thema der **Proliferation**. Waffenexporte machen das bewaffnete Austragen von Konflikten häufig erst möglich. Unser Thema ist in dem Zusammenhang vor allem der Export von Cyberwaffen – dazu zählen wir beispielsweise auch Überwachungssoftware. Diese wird auch von deutschen Unternehmen an Diktaturen geliefert, die sie nachweislich gegen Regimekritiker und Aufständische einsetzen.

Die Teilnehmenden sind dennoch übereingekommen, die nachrichtendienstliche Ausspähung und Kompromittierung der IT-Infrastruktur in Verbindung mit Drohnen und *Signature Strikes* zum Thema einer Kampagne zu machen. Dabei wollen wir eine Reihe von Facetten einbeziehen und zu einem geschlossenen Kampagnenthema verdichten. Einige dieser Facetten sind:

- die Natur der Ausspähung und Kompromittierung als Cyberkrieg,

- die Missachtung der Grundrechte, insbesondere des Grundrechts auf Datenschutz – vom Bundesverfassungsgericht aus dem Persönlichkeitsrecht geschöpft als das Recht auf informationelle Selbstbestimmung – und das Grundrecht auf IT-Sicherheit – als das Recht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme,

- das offensichtliche Versagen – oder fehlender Wille? – staatlicher Institutionen, diese Rechte effektiv sicherzustellen,

- die Verknüpfung der Ausspähung und Kompromittierung mit dem Drohnenkrieg, wobei sowohl Drohnen als Mittel der Ausspähung eingesetzt werden, indem sie die Kommunikation in ihrem Umfeld *on the fly* erfassen, als auch die bei der Ausspähung gewonnen Informationen als Grundlage für Drohnenangriffe verwendet werden in Form der bereits genannten *Signature Strikes*. Das geschieht beispielsweise, indem Zielpersonen durch Ausspähung der Ortsinformationen ihres Mobiltelefons lokalisiert werden.

Wir können für diese Arbeit auf umfassenden Grundlagen aufbauen, die im FIfF bereits geschaffen wurden – so gibt es eine Fülle von Veröffentlichungen, die den Cyberkrieg oder einzelne Aspekte davon thematisieren. Auch wenn einige davon *vor Snowden* entstanden sind und unter den neuen Erkenntnissen aktualisiert werden müssen, bilden sie eine solide inhaltliche Basis. Eine weitere Grundlage ist unser Forderungskatalog zum Cyberpeace, der auf der FIfF-Jahrestagung 2013 von der Mitgliederversammlung verabschiedet wurde und den wir weiterentwickeln werden.

Gleichzeitig bleibt einiges zu tun: Planung, Kampagnenmaterial, Aktivitäten, Öffentlichkeitsarbeit, Mobilisierung und – nicht zuletzt – die Finanzierung. Dies werden in den kommenden Wochen unsere nächsten Schritte sein.

Interesse an Mitwirkung?

Wir freuen uns über jede Mitstreiterin und jeden Mitstreiter. Dazu wird es ein Auftakttreffen geben, das wir rechtzeitig ankündigen werden. Wenn Ihr nicht so lange warten wollt: In der Geschäftsstelle könnt Ihr weitere Informationen erhalten, oder schreibt uns an *ruin@lists.fiff.de.*

Wissenschaft & Frieden 1-2014: Konfliktdynamik im »Globalen Norden«

Gesellschaftspolitisch relevante Konflikte in Europa und den USA stehen im Mittelpunkt der Ausgabe 1-2014 von *Wissenschaft und Frieden*. Es geht um ihre Ursachen, ihre Dynamiken und ihre Akteure. Acht Beispiele aus einer Vielzahl von Konflikten: *Ulrich Wagner* und *Christoph Butenschön*: Zur Entwicklung des Gegenübers – Sozialpsychologische Ursachen von Intergruppenkonflikten / *Bernard Schmid*: Konflikt um Homoehe – Eine reaktionäre Massenbewegung in Frankreich / *Mario Becksteiner*: Griechenland – Krise und Streik / *Elena Vazquez Nuñez* und *César Amaya*: Zwangsräumungen in Spanien / *Christin Landgraf*: Ungarn unter Orbán – Rechtsruck in Gesellschaft und Politik / *William Durston*: Von Lobbyisten und Mythen – Schusswaffengebrauch in den USA / *Vincenz Leuschner* und *Nils Böckler*: School-Shootings – Der aktuelle Forschungsstand.

Außerhalb des Schwerpunkts kommentiert *Thomas Seibert* die aktuelle Situation in Afghanistan, informiert *Michelle Kerndl-Özcan* über das jüngste Abkommen der EU mit der Türkei zur Flüchtlingsabwehr und *Udo Buchholz* über die Pläne zum Verkauf der Urananreicherungsanlage im westfälischen Gronau. 100 Jahre nach dem Beginn des Ersten Weltkrieges befasst sich der aktuelle Träger des Alternativen Nobelpreises, *Paul Walker*, mit Chemiewaffen: Vom massenhaften Einsatz zur weltweiten Abschaffung. Um Künstler und Krieg geht es in dem Bericht von *Jürgen Nieth* über die Ausstellung in der Bundeskunsthalle »1914 – Die Avantgarden im Kampf«.

Im Dossier 74, das in dieser Ausgabe gemeinsam mit dem FIfF herausgegeben wird und ebenfalls der vorliegenden Ausgabe der *FIfF Kommunikation* beiliegt, befassen sich *Ingo Ruhmann* und *Ute Bernhardt* mit »Information Warfare und Informationsgesellschaft. Zivile und sicherheitspolitische Kosten des Informationskriegs«.

Wissenschaft & Frieden, Nr. 1-2014 Konfliktdynamik im »Globalen Norden«, € 7,50 plus Porto.

W&F erscheint vierteljährlich, mindestens dreimal im Jahr liegt W&F ein 12 bis 20seitiges Dossier bei. Jahresabo 30 €, ermäßigt 20 €, Ausland 35 €, ermäßigt 25 €. W&F erscheint seit der 1-2013 nicht nur gedruckt, sondern auch in digitaler Form – als PDF und ePub. Das Abo kostet für Bezieher der Printausgabe zusätzlich 5 € jährlich – als elektronisches Abo ohne Printausgabe 20 € jährlich. Fördermitglieder von Wissenschaft und Frieden (mindestens 60 € jährlich) erhalten auf Wunsch die gedruckte und die digitale Ausgabe. Bezug: W&F, Beringstr. 14, 53115 Bonn,
E-Mail: *buero-bonn@wissenschaft-und-frieden.de*,
www.wissenschaft-und-frieden.de

Christian Schrader

Edward Snowden – Held oder Verräter?

Dan Brown *schrieb vor seinem* Da-Vinci-Code *einen Thriller über ungesetzliche Machenschaften im US-Geheimdienst National Security Agency (NSA)[1]. Die seit dem 6. Juni 2013 bekannt gewordenen Aktivitäten der NSA[2] übersteigen das Szenario dieses Thrillers um ein Mehrfaches. Im Mittelpunkt dieses Beitrags steht die Quelle der Enthüllungen, der IT-Berater* Edward Snowden*. Die Öffentlichkeit schwankt, ob sie ihn als Helden oder als Verräter ansehen soll.*

NSA = Skandal neuer Dimension

Vier Aspekte heben den Skandal um die NSA[3] auf eine neue Dimension. Die übliche Dauer eines Medienhypes beträgt selten mehr als 14 Tage. Bei der NSA ist kein Ende absehbar. Dass eine Supermacht geheimdienstlich in aller Welt agiert, ist banal. Bereits 2001 wurde die Überwachung der Satellitenkommunikation *(Echolon)* aufgedeckt.[4] Selbst das Abhören des Mobiltelefons von Bundeskanzlerin Merkel kann noch als informationstechnische Fortsetzung des Abfangens von Regierungsbriefen gewertet werden. Neu ist, dass auch unbeteiligte Staatschefs wie Kriminelle behandelt werden. Boliviens Präsident Morales musste auf dem Rückflug von Moskau in Europa zum Tanken zwischenlanden. Mehrere Länder verweigerten die Landung, weil eventuell Snowden an Bord sein könnte. Morales strandete wie Treibgut im Wiener Flughafen.

Die Infrastruktur des Internet ist auf die USA ausgerichtet. Das war und ist solange kein Problem, wie die USA das Internet als freien Ort der Informationsverbreitung achten. Persönliche Entfaltung, politische Freiheit und wirtschaftliche Dynamik konnten sich im Internet entfalten – auch deswegen, weil die Treiber in den USA saßen. Jetzt zeigt sich: Die Vermutung, dass ein USA-abhängiges Internet deswegen kein Problem ist, weil die USA freiheitsliebend sind, hat sich als Trugschluss herausgestellt. Der egoistische Sicherheitswahn der USA gefährdet Freiheitsrechte gerade im Ausland, weil die Informationsbeschaffung im Ausland aus US-Sicht keine Einschränkungen kennt. Die USA nutzen die den Markt dominierenden US-IT-Firmen als zusätzliche Informationsquelle.

Am Ende ist selbst die Wirtschaft aufgeschreckt. Betriebswirtschaftliche Trends, wie *Cloud-Computing*, stellen sich als höchst riskantes Vorgehen heraus. Im Grund müsste über den *Big-Data*-Ansatz der NSA auch der aktuelle wirtschaftliche Trend zu *Big Data* in die Diskussion kommen. Die technischen Methoden der NSA sind nur ein Vorgeschmack davon, was *Google*, *Amazon* und Co. genauso vorhaben.

Die Person Edward Snowden[5]

Edward Snowden ist US-amerikanischer Staatsbürger, geboren 1983. Er wuchs auf als Sohn eines ehemaligen Beamten der US-Küstenwache und einer leitenden Gerichtsangestellten. Von 1999 bis 2001 und 2004 bis 2005 studierte Snowden Informatik in Maryland. Zwischen den beiden Phasen seines Studiums meldete er sich für die U.S. Army, um im Irak-Krieg zu dienen. 2005 brach er sein Informatikstudium ab und wechselte zum Geheimdienst CIA. Anschließend arbeitete er als freier technischer Mitarbeiter einer NSA-Einrichtung in Japan. Im Jahr 2009 wechselte Snowden zur Beratungsfirma *Booz Allen Hamilton*, für die er in einem NSA-Büro auf Hawaii als Systemadministrator tätig war.

2013 kopierte er umfangreiche, als *Top Secret* eingestufte Dokumente der NSA und flog nach Hongkong. Von dort aus verschickte er die geheimen Dokumente zunächst an die *Washington Post* und an den *Guardian*, die erste Details am 6. Juni 2013 veröffentlichten. Am 9. Juni ging Snowden an die Öffentlichkeit und gab sich in einem Interview als Informant zu erkennen.

Am 14. Juni 2013 erwirkte das FBI mit einer Strafanzeige u. a. wegen Spionage einen Haftbefehl gegen ihn. Snowden konnte Hongkong mit dem Ziel Ecuador verlassen. Als die USA seinen Reisepass für nichtig erklärten, strandete er beim Zwischenstopp in Moskau. Am 1. August 2013 erklärte Russland sich bereit, ihn für ein Jahr aufzunehmen.

Als Motiv gibt Snowden an, ihm seien bereits 2007 Zweifel an der Rechtmäßigkeit seiner Arbeit gekommen: *„Ich erkannte, dass ich Teil von etwas geworden war, das viel mehr Schaden anrichtete als Nutzen brachte. … Ich möchte nicht in einer Welt leben, in der alles, was ich tue und sage, aufgezeichnet wird."* Er könne es *„nicht mit meinem Gewissen vereinbaren, dass die US-Regierung die Privatsphäre, die Freiheit des Internets und grundlegende Freiheiten weltweit mit ihrem Überwachungsapparat zerstöre."*

Was ist ein Verräter?

Verrat ist in seiner Wortbedeutung ein *besonders schwerer Vertrauensbruch*[6] oder ein *treuloses Handeln* beziehungsweise „das Aufdecken von Geheimnissen"[7].Es gibt aber Unterschiede, wer oder was verraten wird. In der Bibel meint Verrat, dass der Mensch eine Vereinbarung nicht einhält, eine Ehe oder eine andere von Gott gegebene Ordnung bricht. Wegen der Abendmahlsworte „in der Nacht, in der er verraten ward" (1. Korinther 11,23) erscheint Judas als der Prototyp des Verräters. Als Verräter kennzeichnet das Grimmsche Wörterbuch jemanden, „der von seinem gesetz abtrünnig war, auch verflucht jn jedermann als einen verrheter und feind seines vaterlandes."[8] Hier kommen wir also zum Verrat am Vaterland.

Der Verrat ist ein traditioneller Straftatbestand. Schon die Peinliche Gerichtsordnung Kaiser Karls V. von 1532 nannte in Art. 124 als „straff der verreterey" die „viertheylung", bei Landesverrat verschärft durch „schleyffen oder zangenreissen". Die Strafen haben sich gemildert, die herausgehobene Stellung des Landesverrats blieb. Als allerersten Straftatbestrand definiert heute § 81 Strafgesetzbuch als Hochverrat,

> *„Wer es unternimmt, … die auf dem Grundgesetz der Bundesrepublik Deutschland beruhende verfassungsmäßige Ordnung zu ändern, wird mit lebenslanger Freiheitsstrafe oder mit Freiheitsstrafe nicht unter zehn Jahren bestraft."*

Aber: Das Wort Verrat ist aus dem Straftatbestand verschwunden. Das macht stutzig. Hochverrat ohne das Wort Verrat? Verrat ist für uns Deutsche eine fast ausgestorbene Kategorie. Verrat ist ein Kennzeichen nicht nur patriotischer, sondern vor allem autoritärer, totalitärer Staaten. Diktatoren, auch ideologisierte Gruppen versuchen, ihre Mitglieder über das Prinzip der Treue und Loyalität extrem an sich zu binden. Sie betonen den Begriff der Treue, um „die gemeinsame, hehre Sache“ nach vorne zu führen.

Verrat gab es nach dem Zweiten Weltkrieg auch in der Bundesrepublik – noch. Willy Brandt wurde als Herbert Frahm, als Emigrant in der NS-Zeit verhöhnt und in die Nähe des Verrats gestellt. Wer sich mit der Oder-Neiße-Grenze abfand, verriet die großdeutsche Sache. Später stürzte Willy Brandt als Bundeskanzler über einen echten Verräter: Günter Guillaume, der ihn zugunsten der DDR ausspionierte. Doch die 1968er-Zeit hat für die Deutschen den Staat entzaubert. Die Auflösung des Ost-West-Konflikts ließ den Anlass für scharfe Freund-Feind-Ansammlungen von Staaten vergessen. Das Nationale geriet in eine Sinnkrise. Der Staat ist heute eher angesehen als eine Zweckorganisation, die möglichst effektiv die großen Krisen von unserem privaten Leben abhalten soll.

PRISM-Demo der Piratenpartei zum Besuch des amerikanischen Präsidenten Barack Obama
Foto: Mike Herbst CC BY-SA 2.0

Sabine Rückert meinte am 2. April 2010 in der ZEIT, dass sich selbst Judas heute nicht mehr als Verräter darstellen ließe. *„Der Glaube verflüchtigt sich in tausend Möglichkeiten. Die Überzeugungen lösen sich auf im Mainstream politisch korrekter Allerweltsansichten. Die Psalmen des Alten Testaments gehen unter im Stimmengewirr des Internets, die Verse des Evangeliums konkurrieren mit den Texten von* Tokio Hotel. *Was gibt es da noch zu verraten?“*[9] Durch die Aufklärung, durch Individualismus und Pluralismus leben wir unsere persönlichen Werte und Überzeugungen. Es fehlen uns die großen gemeinschaftlichen Gewissheiten, deren Abweichung als Verrat gedeutet werden könnte.

Verrat bezieht sich nicht mehr auf Werte der Gesamtgesellschaft, sondern nur noch auf Illoyalität an einer Gruppe. Doch wo gibt es heute noch eine so hohe Gruppenidentifikation, dass an ihr ein Verrat geübt werden kann? Anhänger von Borussia Dortmund empfinden es als Verrat an der privaten Gemeinschaft, wenn Mario Götze zu Bayern München wechselt. Noch schlimmer wäre ein Wechsel zu Schalke 04. Aber Verrat war es nicht, dass einige Jahre zuvor der Nationalspieler Kevin Kuranyi zu Dynamo Moskau ging ...

Was ist ein Held?

Wikipedia nennt als Helden eine Person mit besonders herausragenden Fähigkeiten oder Eigenschaften, die sie zu besonders hervorragenden Leistungen, so genannten *Heldentaten*, treiben.[10] Die Bibel versteht unter Helden im engeren Sinne Personen, die vor allem in kriegerischen Kontexten andere Menschen übertreffen[11] – den *Kriegshelden*. Bisweilen dient das Substantiv auch zur Bezeichnung vornehmster oder führender Persönlichkeiten. In ähnlicher Weise versteht das Grimmsche Wörterbuch unter dem Helden den „wegen seiner tapferkeit und kriegsthaten gefeierten mann edler abkunft“[12] – König Artus und die Ritter der Tafelrunde. Hier begegnen die alten Vorstellungen von edler Abkunft dem Begriff des Nationalhelden. Über heldische Vorbilder wird eine neue Nation gestiftet, ein Beispiel aus neuerer Zeit ist der kürzlich verstorbene Nelson Mandela.

Die Beschäftigung mit Helden ist in Deutschland nicht mehr üblich. Wir haben als verspätete Nation eine Überdosis genommen. Für die Aufopferung für die Nation gab es den Status des Heldentods, um in Kriegs- und Notzeiten den Durchhaltewillen zu stärken. Heldendenkmäler wurden nach 1871 und nach 1918 allenthalben in Deutschland errichtet.

Nach dem Zweiten Weltkrieg blieb die Zuspitzung auf Helden ein Mittel des sozialistischen ostdeutschen Staates. In der DDR trug *Luise Ermisch*, Damenschneiderin aus Halle, als erste den Ehrentitel *Held der Arbeit*. Für ideologische Zwecke hob die DDR eher durchschnittliche Menschen ohne große Taten heraus. Als in der Sowjetunion der Atomreaktor von Tschernobyl explodierte und es Menschen brauchte, die unter härtester Strahlung die Trümmer mit bloßen Händen wegräumten, wurde ihr Einsatz als Heldentum verbrämt und ihr absehbares Opfer an Gesundheit und Leben verschwiegen.

Im Westen dagegen wurde die harte Arbeit des Wiederaufbaus nicht mehr über den Begriff *Heldentat*, sondern über genügendes Essen und materielle Werte entlohnt. Die Gesellschaft in Westdeutschland hatte von staatlich geprägten Helden die Nase voll und verwendete den Begriff kaum. Nur die Gewinner der Fußballweltmeisterschaft 1954 wurden begeistert als die *Helden von Bern* gefeiert. Sie halfen, das lädierte Selbstwertgefühl der Deutschen nach der Nazizeit wieder aufzurichten. Auf eher unverdächtigem Gebiet, dem Sport, diente der Heldenbegriff dem gleichen Zweck: der Selbstvergewisserung der eigenen Nation.[13]

Als Zwischenbilanz lässt sich ziehen: Es gibt aus deutscher Sicht fast keine Verräter mehr und kaum noch Helden. Die pluralistische, globalisierte Gesellschaft definiert sich nicht mehr über Helden oder Verräter.

Edward Snowden – Held oder Verräter?

Vom Äußeren her ist Edward Snowden unauffällig. Mit eher randloser Brille, mit korrektem Haar- und Bartschnitt und Jackett hebt ihn wenig heraus aus der Masse der beruflich erfolgreichen 30-Jährigen. Er hält sich selbst nicht für einen Menschen mit besonderen Begabungen. Er argumentiert äußerst rational. Er selbst tritt also weder heldisch noch verräterisch auf.

Edward Snowden – Ein Verräter

Dennoch hielten ihn laut einer Umfrage der *Quinnipiac University* vom 10. Juli 2013 34 % der US-Bürger für einen Verräter. Allerdings ist er für 55 % ein *Whistleblower* mit einem legitimen Anliegen.[14] Es gibt also auch in der Öffentlichkeit der USA eine geteilte Meinung. Was sind die Gründe?

In den USA entstand eine Sicht, die in eine gute und eine schlechte Weitergabe geheimer Informationen unterscheidet. Der Whistleblower ist ein Guter, der Verräter ein Schlechter. In den USA gab es einige sehr große Skandale, in denen skrupellose Praktiken Schäden für die Allgemeinheit verursachten. Manchmal halfen Whistleblower, auf Missstände in einer Organisation (beispielsweise einem Unternehmen) hinzuweisen und so für die Allgemeinheit wichtige Informationen aus einem geheimen Zusammenhang an die Öffentlichkeit zu bringen. *Daniel Ellsberg* brachte 1971 die geheimen *Pentagon-Papiere* an die Öffentlichkeit, die die Täuschung der Öffentlichkeit über den Vietnamkrieg durch mehrere US-Regierungen enthüllten. Der Einbruch beim Psychiater von *Daniel Ellsberg* hat mit zum Sturz des US-Präsidenten Nixon geführt. Die Aufdeckung von Korruption wird nach Skandalen wie bei *Enron* als so wichtig angesehen, dass die USA ein eigenes Gesetz erließen, den *Sabarnes-Oxley-Act*, das den großen US-Firmen Verfahren zur vertraulichen, anonymen Einreichung von Beschwerden vorschreibt. Beschäftigte, die Beweise für Betrug vorlegen, müssen vor Vergeltungsmaßnahmen geschützt werden.[15]

In den Augen großer Teile der US-Öffentlichkeit und der US-Geheimdienste ist Snowden aber kein Whistleblower sondern ein Verräter. Warum? Es ist erklärlich aus dem starken Nationalstolz der USA und der Reaktion auf den 11. September 2001. Durch die Anschläge am 11. September 2001 wurde die USA als Nation herausgefordert. Die Bevölkerung eines Staates, der sich patriotisch als God's own country begreift, schließt sich in solchen Bedrohungssituationen zusammen und greift zum alten Reflex.

Die USA haben die zurückgeflogenen Särge der Gefallenen mit Heldenbegräbnissen beerdigt. Auf der anderen Seite wurden Personen, die Kriegsverbrechen veröffentlichten, hart als Verräter verfolgt. Der damalige US-Gefreite *Bradley Manning* – heute *Chelsea Manning* – hatte über Wikileaks grausame Aktionen des US-Militärs offenbart. Die USA schickten Manning 35 Jahre in Haft und verfolgen den Wikileaks-Gründer *Julian Assange* so unnachgiebig, dass er jetzt seit über einem Jahr in der Ecuadorianischen Botschaft in London festsitzt.

Über den normalen Patriotismus hinaus verstehen sich Geheimdienste immer als letzte Bastion des Nationalismus. Jedes Mittel erscheint recht, den Zweck des Staatsschutzes zu erreichen. Diese Position ist in der patriotischen US-Gesellschaft stark anschlussfähig. Snowden kann in ihren Augen nur ein Verräter sein.

Außerhalb der USA ist Snowden kein Verräter. Ein Verrat muss von den Grundüberzeugungen der eigenen Gruppe abweichen. Snowden, der US-Praktiken öffentlich machte, ist aus chinesischer und russischer Sicht kein Verräter. In Deutschland ist er kein Verräter, weil wir keine Verräter mehr kennen.

Edward Snowden – kein Held

Edward Snowden könnte ein strahlender Held sein. Er wird mit Preisen überhäuft. *Transparency International* verleiht ihm den *Whistleblowerpreis 2013*. Die *Universität Rostock* will ihm einen Ehrendoktor verleihen usw. Momentan ist er eher ein tragischer Held. Er hat sich für die US-amerikanischen Werte eingesetzt und sitzt in Moskau fest. Doch wer will schon in Russland leben, im kalten Winter und ebenso kalten politischen Verhältnissen? Ein Mann wie Snowden, der gegen Geheimdienste und für Demokratie und freie Meinungsäußerung eintritt, muss sich in Moskau wie im Gefängnis fühlen. Ein Märtyrer im Namen der westlichen Werte.

Er ist auch kein Held im Sinne eines Vorbilds, dem wir tatsächlich nacheifern. Gelegenheit war dazu drei Monate nach seinen Enthüllungen, bei der Bundestagswahl am 22. September 2013. Mit den Piraten gab es eine Partei, die genau auf dieses Thema zugeschnitten ist.

Aber: Das Thema hatte keine Bedeutung im Wahlkampf, und es wirkte sich auf das Wahlergebnis nicht aus. Insofern ist die Bedeutung dieses Themas für Wahlentscheidungen ebenso gering wie anscheinend die Vorbildwirkung für eigenes Handeln.

Christian Schrader

Professor Dr. **Christian Schrader** ist Professor für das Recht der Technikentwicklung an der Hochschule Fulda. Zu seiner Person siehe *www.hs-fulda.de/index.php?id=2241*, Kontakt: *Christian.Schrader@sk.hs-fulda.de*.

Der Beitrag beruht auf einem Vortrag in der Evangelischen Studierendengemeinde Fulda am 18. November 2013.

Es gibt keine Massenbewegung weg von den großen US-Anbietern wie *Microsoft*, *Google* oder *Amazon*, die so bereitwillig mit der NSA zusammenarbeiteten. Wer verwendet nicht mehr Google als Suchmaschine, wer bestellt nicht mehr über Amazon? Es brächte uns raus aus den Fängen der Datenkraken und aus den Hintertüren der Geheimdienste. Aber fast niemand macht es.

Edward Snowden: Denoch ein Held!

Im Gegensatz zu anderen aktuellen Whistleblowern ist er ein Held, weil er persönlich und politisch authentisch ist. Persönlich ist er nicht schrill wie Julian Assange und kein Außenseiter wie Chelsea Manning. Er verkörpert den amerikanischen Traum, auch ohne Studienabschluss glänzenden Erfolg haben zu können. Ein Haus auf Hawaii, einen sicheren Job und ein Jahresgehalt von bis zu 200.000 US-Dollar gab er auf, weil die Arbeit seinen Überzeugungen zuwiderlief. Er verkörpert das Ideal eines aufgeklärten Informatikers, den auch die gesellschaftlichen Folgen des Technikeinsatzes interessieren.

Er ist ein Held, weil er es schaffte, einen absoluten Überraschungserfolg zu landen und durch gute Planung weiterhin in relativer Freiheit zu agieren und nicht im US-Gefängnis abgekocht zu werden. Die größten Sicherheitsbedrohungen sind immer: Die eigenen Mitarbeiter. Das lässt sich nicht nur an Chelsea Manning belegen, sondern auch an den Mitarbeitern von Schweizer Banken, die Steuerdaten stehlen und für ein paar Millionen Euro an deutsche Steuerbehörden verkaufen. Dennoch konnte sich Snowden die Informationen besorgen und dort hingehen, wo die USA ohnmächtig sind. Bei all dem setzte er sich nicht einem Selbstdarsteller wie Julian Assange aus, der die Informationen, die Chelsea Manning ihm zuspielte, auf einen Schlag im Internet veröffentlichte. Snowden wandte sich an die klassischen Printmedien und setzte auf die Erfahrung und die Qualität von investigativem Journalismus anstelle des schnellen Tageshypes. Insgesamt: Clever gemacht!

Und das nicht für einen banalen Inhalt. Er ist ein Held, weil er uns zwingt, uns die großen Grundwerte unserer Gesellschaft bewusst zu machen. Edward Snowden ist nach *Friedrich Schorlemmer* kein Spion, sondern ein mutiger Anwalt der Wahrheit, der den Abhörern auf die Schliche kam und deren Gigantismus öffentlich machte. Er schützt die Demokratie vor maßlosem Einsatz von Geheimdiensten, er lässt uns die Frage nach rechtsstaatlichen Reaktionen ebenso stellen wie nach dem Wert eines freiheitlichen Internet.[16]

Letztlich ist er ein Held, weil er uns hoffen lässt, dass die in ihrem Krieg gegen den Terror so verblendeten USA doch wieder das Land der Freiheit sein können. In einem Interview sagte Snowden, er sei *„weder ein Verräter noch ein Held. Ich bin Amerikaner"*.[17]

Nach *Wolfgang Büscher*[18] zieht Snowden *„seinen Schluss, er zieht in den Kampf, ein rechtschaffener Einzelner, und sein Kampf ist ein Verrat ebenso großen Stils wie es die Kontrolle der ganzen Welt und ihrer Nervenbahnen durch die Geheimdienste ist, an der er so lange mitgewirkt hat, … die einsame Tat eines einzelnen aufrechten Mannes ist uramerikanisch. Und oft sind es Geschichten vom Kampf des Einzelnen gegen einen übermächtigen, alles kontrollierenden Staat. Staatsfurcht und Staatsfeindschaft, auch sie sind in Amerika heimisch. Dass sich beides widerspricht, die Liebe zum eigenen Land und die Liebe zum Außenseiter, zum Outlaw, schwächt aber nicht etwa den amerikanischen Mythos. Es stärkt ihn."* So liegt in einem in den USA strafbaren Verrat eine Bestätigung der US-amerikanischen Werte.

Es bleibt nur für Edward Snowden zu hoffen, dass er nach der Beengtheit des Moskauer Zwischenasyls wieder mehr persönliche Freiheit und Sicherheit erhält, in Deutschland[19] oder anderswo.

Anmerkungen

1 *Dan Brown: Diabolus, 1998, Bastei Lübbe Taschenbuch 2007.*
2 *Dazu: Stadler, Sara: Telefon- und Internetüberwachung, FIfF-Kommunikation 3/13, 24 f.*
3 *Der Einfachheit halber wird nur die NSA genannt, auch wenn sie in der Realität mit anderen Geheimdiensten wie dem britischen GCHQ zusammenwirkt.*
4 *Europäisches Parlament, Bericht A5-0264/2001 Teil 1 vom 11.07.2011 über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON).*
5 *de.wikipedia.org/wiki/Edward_Snowden (03.12.2013); Der Spiegel 45/2013.*
6 *de.wikipedia.org/wiki/Verrat (30.11.2013).*
7 *Brockhaus, 19 Auflage, 1989.*
8 *woerterbuchnetz.de/DWB/?sigle=DWB&mode=Vernetzung&hitlist=&patternlist=&lemid=GV03263 (03.12.2013).*
9 *Rückert. Sabine: Judas. Unser nützlichster Verräter, Die Zeit 02.04.2010.*
10 *de.wikipedia.org/wiki/Held (03.12.2013)*
11 *www.bibelwissenschaft.de/wibilex/das-bibellexikon/lexikon/sachwort/anzeigen/details/helden-3/ch/4922ca33d90d8ef16f4074c310a35595/ (3.12.2013).*
12 *woerterbuchnetz.de/DWB/?sigle=DWB&mode=Vernetzung&lemid=GH05741(03.12.2013).*
13 *In selbstironischer Weise will heute eine Website gleichen Namens „Hartplatzhelden", jedem Amateurfußballer ermöglichen, seine Fußball-Videos hochzuladen. Der Held ist hier demokratisiert. Ein echter Held ist er damit noch nicht.*
14 *quinnipiac.edu/images/polling/us/us07102013.pdf/ (03.12.2013).*
15 *In Deutschland gibt es keinen gesetzlich festgelegten Schutz für Whistleblower. Whistleblowing als strafbarer Verrat von Geschäft- und Betriebsgeheimnissen wird nicht als solcher verfolgt, wenn die von der Rechtsprechung des Bundesverfassungs- und des Bundesarbeitsgerichts aufgestellten Grundsätze beachtet wurden, die vorrangig auf interne Abhilfesysteme und auf die Verhältnismäßigkeit setzen.*
16 *Schorlemmer, Friedrich: Snowden nach Deutschland, Publik-Forum 15/2013 vom 16.8.2013.*
17 *Zitiert nach die tageszeitung 13.6.2013, m.taz.de/!118049;m/ (03.12.2013).*
18 *Büscher, Wolfgang: Warum die ganze Welt einen Verräter verehrt, Die Welt 17.6.2013.*
19 *Dazu: Bräutigam, Frank: Kann Snowden auf Asyl hoffen? 2.11.2013, www.tagesschau.de/ausland/faq-snowden-asyl100.html (03.12.2013); Der Spiegel 45/2013.*

Sylvia Johnigk

Zum 30. Mal Chaos Communication Congress – 30C3

30 Jahre und kein bisschen greise, im Gegenteil, der Congress ist jung oder zumindest jung geblieben, interessiert, interaktiv und kommunikativ. Er fand zum zweiten Mal im Hamburger Congress Centrum CCH statt. Im Vorfeld hatte man sich glücklicherweise entschieden, räumlich erheblich aufzustocken, um mehr Platz für Menschen, Projekte, Vorträge und Kreativität zu haben. Insgesamt strömten ca. 9000 TeilnehmerInnen ins CCH, mehr als erwartet[1] . Mit 176 Vorträgen, vielen zusätzlichen Workshops, einem Kindertag, an dem Kinder eine Einführung in die Welt des Hackens bekamen, und vielen anderen schönen Ideen war das Programm des Congresses so groß und vielfältig wie nie zuvor.

Ein Motto wie in den letzten Jahren gab es diesmal allerdings nicht. Den Veranstaltern ist schlicht nichts eingefallen, was irgendwie zu den Geschehnissen des vergangenen Jahres passend war oder einen drauf setzen konnte, und zum Persiflieren war das letzte Jahr zu bitter. Neben echten Hackerthemen wurden wie jedes Jahr gesellschaftliche Aspekte der IT-Sicherheit und des Datenschutzes diskutiert. Thematisch standen wie erwartet das Thema Überwachung und die Enthüllungen *Edward Snowdens* im Vordergrund.

Fotohinweis am 30C3 – Foto: Ordercrazy

Die Keynote[2] hielt per Skype der ehemalige *Guardian*-Reporter *Glenn Greenwald*. Anfangs sichtlich verlegen – „*Ich bin doch weder für meine Kryptografie noch Hackerkenntnisse bekannt*" – appellierte er, dass man sich mehr für den Schutz seiner Privatsphäre einsetzen solle, da sich bisher trotz der Enthüllungen noch gar nichts geändert habe. Er bedankte sich bei Edward Snowden, Chelsea Manning und *(habe ich vergessen)* für ihre Courage, die Informationen für eine breite Öffentlichkeit verfügbar zu machen. Die Vernichtung der Datenträger im Keller des *Guardian* bezeichnete er als Einschüchterungsmaßnahme.

Annie Machon[3], eine ehemalige Offizierin des britischen Security-Service *MI5*, die nach Enthüllungen gemeinsam mit ihrem Partner eine Zeitlang im Exil leben musste, kündigte in ihrem Vortrag *The four Wars – Terror, whistleblowers, drugs, internet*[4] einen Hilfsfonds *Courage Fund* an, um Whistleblower unmittelbar nach der Veröffentlichung schützen zu können.

Jacob Applebaum wartete mit neuen NSA-Enthüllungen auf[5]. Die Überwachungsmaßnahmen der NSA und anderer Geheimdienste gehen demnach weit über das bisher Bekannte hinaus. Dass Hardware, die man beispielsweise bei *Amazon* bestellt, abfangen und verwanzt wird, dass Schadcode über mehrere Kilometer Entfernung ins WLAN eingeschleust werden kann, oder das Abfischen von Bildschirm und Tastatureingaben via Radar sind nur eine kleine Auswahl der perfiden Überwachungsinstrumente. Mit diesen und noch weiteren Maßnahmen strebe der Geheimdienst die totale Überwachung und Kontrolle an. Damit werden schlimmste Albträume wahr, proklamierte Appelbaum auf dem Congress.

Josef Foschepoth thematisierte in seinem Vortrag *Deutschland ist das am meisten überwachte Land in Europa*, dass der NSA-Skandal nur den bisherigen Höhepunkt der Überwachungsmaßnahmen auf dem Territorium der Bundesrepublik Deutschland darstelle, deren Geschichte schon nach dem Ende des zweiten Weltkrieges begann und und dass die Überwachungsmaßnahmen systematisch ausgeweitet werden. Dabei entstand ein deutsch-alliierter geheimdienstlicher Komplex, der sich jeglicher Kontrolle entzieht. Der Schlüssel stecke dabei in dem gegenseitig vereinbarten Geheimhaltungsgebot.

Andreas Lehners Vortrag *Der tiefe Staat*[6,7] zeigte dieses Konzept anhand der bundesrepublikanischen Geschichte auf. Dabei kamen unter anderem rechtliche Aspekte und insbesondere der hohe Grad der Militarisierung und das Ausmaß der Überwachung in der Bundesrepublik zur Sprache, die einen großen Teil des Fortbestands des tiefen Staats gewährleisten.

Der ehemalige Bundesdatenschutzbeauftragte *Peter Schaar* beschäftigte sich in seinem Vortrag *Amtliche Datenschützer: Kontrolleure oder Papiertiger?*[8] unter anderem mit der Frage, inwieweit Instrumente existieren, um die vorhandenen Gesetze durchzusetzen. Dabei wünschte er sich, dass amtliche Datenschützer nicht nur gesetzliche Forderungen an den Datenschutz stellen, sondern erweiterte Instrumente erhalten, um diese auch durchsetzen zu können.

FX alias *Felix Lindner* beschäftigte sich in seinem Vortrag *CounterStrike*[9] mit der gesetzmäßigen Internetüberwachung (*Lawful Interception*). Lindner hat Standards, Geräte und Implementierungen untersucht, die über gesetzmäßige Überwachungsschnittstellen verfügen. Grundsätzlich können solche Überwachungsschnittstellen aufgrund ihrer Komplexität die gesamte Systemsicherheit gefährden. Mehr noch: *Lawful Interception* untergrabe grundsätzlich das Designprinzip eines Routers. Allerdings lassen sich solche Überwachungstechniken genauso leicht umgehen wie eine Antivirensoftware. Für eine allumfassende Überwachung müsse das Internet neu designed werden.

Das FIfF war dieses Jahr mit einem Vortrag von *Sebastian Jekutsch* vertreten, hierzu gibt es einen separaten Bericht. Der FIfF-Stand war als *Assembly*[10] im neu geschaffenen *Noisy Square* platziert, der den Zweck hatte unterschiedliche NGOs

zusammenzuführen, und einen eigenen Raum zu schaffen, in dem man spontan miteinander Themen diskutieren kann. Der Stand war sehr gut besucht, und wir hatten viele Möglichkeiten, mit anderen zu diskutieren.

Die gute alte Rohrpost wurde auf dem Hackerkongress wiederbelebt und mit dem Namen *Seidenstraße*[11] versehen. Die Seidenstraße war eine Alternative zum WLAN und dem hauseignen Telefonnetzwerk, man konnte an einzelnen Spots Nachrichten oder andere Inhalte mit einem Gewicht bis 500 gr verschicken oder entgegen nehmen. Insgesamt wurden ca. 500 blinkende LED-Kapseln unfallfrei in zwei Kilometern Drainagerohren per Staubsaugerantrieb durch das CCH gejagt, einzig eine Mateflasche schoss aus einem Eckstück hinaus, verletzte aber niemanden.

30. Chaos Communication Congress in Hamburg, 2013
Foto: Wikipedia, Tobias Klenze CC-BY-SA 3.0

Die Kölner Theatergruppe NÖ[12] führte im vollbesetzten Hauptsaal das Theaterstück *V wie Verfassungsschutz* auf, bedauerlicherweise ohne Livestream und Videoaufnahmen.

Die Abschlussveranstaltung begann mit einer kurzen Theatereinlage, die zu Anfang nicht unmittelbar als solche erkennbar war. Ein Mann im Businessanzug stellte sich als Mitarbeiter einer Sicherheitsfirma vor und bedankte sich für die Möglichkeit, als Sponsor hier vor dem Publikum das Firmenprofil vorstellen zu können. Er war Teil eines Experiments: Während des Kongresses hatten als Recruiter verkleidete Schauspieler versucht, Kongressteilnehmer, insbesondere Hacker, für Spionage- und Überwachungstechnologieunternehmen anzuwerben. Zum Glück waren nur zwei der Angesprochenen mit in einen separaten Raum gegangen, alle anderen (ca. 150) Personen waren an einer Zusammenarbeit nicht interessiert.

Alles in Allem war der Congress eine gelungene Veranstaltung, die wir nächstes Jahr sicher wieder besuchen werden.

Anmerkungen

1 *Dies führte zu einem ungewöhnlichen Engpass: Die Quelle, der von den Hackern so geliebte Matebrause, versiegte bereits am zweiten Tag am Samstagabend. Im Großraum Hamburg (bis Bremen) war keine Mate mehr erhältlich.*
2 *http://media.ccc.de/browse/congress/2013/30C3_-_5622_-_en_-_saal_1_-_201312271930_-_30c3_keynote_-_glenn_greenwald_-_frank.html*
3 *http://de.wikipedia.org/wiki/Annie_Machon*
4 *http://media.ccc.de/browse/congress/2013/30C3_-_5295_-_en_-_saal_1_-_201312292030_-_the_four_wars_-_annie_machon.html*
5 *Insbesondere Teil 2 seines Vortrags http://media.ccc.de/browse/congress/2013/30C3_-_5713_-_en_-_saal_2_-_201312301130_-_to_protect_and_infect_part_2_-_jacob.html*
6 *Ursprünglich war damit die konspirative Verflechtung von Politik, Militär, Justiz, Rechtextremen und organisierter Kriminalität in der Türkei gemeint [Wikipedia] http://de.wikipedia.org/wiki/Tiefer_Staat*
7 *http://media.ccc.de/browse/congress/2013/30C3_-_5415_-_de_-_saal_g_-_201312271245_-_der_tiefe_staat_-_andreas_lehner.html*
8 *http://media.ccc.de/browse/congress/2013/30C3_-_5623_-_de_-_saal_1_-_201312301600_-_amtliche_datenschutzer_kontrolleure_oder_papiertiger_-_peter_schaar.html*
9 *http://media.ccc.de/browse/congress/2013/30C3_-_5304_-_en_-_saal_1_-_201312292315_-_counterstrike_-_fx.html*
10 *https://events.ccc.de/congress/2013/wiki/Static:Assemblies#Assemblies*
11 *https://events.ccc.de/congress/2013/wiki/Projects:Seidenstrasse*
12 *http://www.noetheater.de/?page_id=6*

Sylvia Johnigk

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

Sebastian Jekutsch

Vortrag *Dead Man Edition* auf dem 30C3

Nach mehreren hundert Zuhörern beim Überblicksvortrag auf dem 29C3 reduzierte sich das Randthema Faire Computer *nun auf das zu erwartende Maß an Interesse. Etwa 50 Zuhörer erfuhren etwas zu dem Thema Rohstoffe und deren Konfliktfreiheit.*

Zum Inhalt: *Dead Tree Edition* wird auf ironische Weise Ausgedrucktes genannt, das auch elektronisch verfügbar ist. Man ignoriert dabei, dass für die Online-Infrastruktur und all die Computer nicht nur Bäume, sondern gleich ganze Berge, auf denen sie gestanden haben, abgetragen werden. Und Menschen kommen auch zu Schaden (daher der Titel des Vortrags) – um die Jahrtausendwende hat die UN aufgedeckt, dass der Handel mit Metallerzen, wie sie zur Herstellung von Elektronikbauteilen benutzt werden, die Konfliktparteien in der D.R. Kongo finanziert und somit den Bürgerkrieg am Leben erhält. Der Begriff der Konfliktmineralien war geboren.

Zehn Jahre später hat ein engagiertes Bündnis von Nichtregierungsorganisationen eine Regelung in ein US-amerikanisches Börsengesetz (*Dodd-Frank-Act*) einbringen können, das die Hersteller verpflichtet, den Kauf gewisser Rohstoffe aus dem Kongo zu veröffentlichen. Die Folgen waren zunächst verheerend, später zukunftsweisend. Konfliktfreie Mineralien aus dem Gebiet sind nun dank einiger Hersteller erhältlich, Kondensatoren werden daraus hergestellt, Lötzinn produziert, das *Fairphone* macht daraus ein Produkt, *Intel* wollte bis Jahresende einen konfliktfreien Prozessor anbieten (was nicht geklappt hat).

Nun will die EU nachziehen und ebenfalls zur Transparenz beim Kauf von Rohstoffen aus Konflikt- und Risikogebieten verpflichten. Das könnte große Wirkung auf unsere Elektronikprodukte haben. Wir sollten Einfluss auf die Ausformulierung nehmen, es droht nämlich eine nur freiwillige, sanktionsfreie, nicht weit genug gehende Regelung im Sinne der Industrie. Was wir aber brauchen, ist eine Regelung, die den Minenarbeitern wirksam hilft. Übersteigerte Anforderungen an eine Konfliktfreiheit sind zu ersetzen durch einen risikoabschätzenden Ansatz. Die OECD-Leitlinien für multinationale Unternehmen geben eine gute Blaupause dafür. Sie sind aber freiwillig und daher nicht ordentlich einklagbar. Doch nur mit einer starken Gesetzgebung kann es uns gelingen, die Produktion von IT fairer zu gestalten.

Zum Vortrag: Er ist auf *YouTube* leicht zu finden. Leider musste ich zu Gunsten einer Fragerunde einige Aspekte während des Vortrags kürzen, z. B. die konkreten Forderungen einer Gruppe von NGOs, zu denen auch das FIfF gehört. Ebenfalls hätte ich gerne klar gemacht, dass ich einen Boykott als Reaktion auf unerwünschte Zustände für selten zielführend halte. Vieles andere blieb leider unerwähnt. In der eher uninteressanten und nur zögerlich zustande gekommenen Diskussion kamen dann Nachfragen zum Bezug konfliktfreien Zinns, zum Recycling und zum Fairphone.

Zum Erfolg: Von Bekannten habe ich positive Rückmeldung; einige, die sich wirklich auskennen, haben Lücken angemahnt. Ein kurzes Interview mit dem (gedruckten) *Spiegel* (2/2014) war auch ein Ergebnis dieses Vortrags, zudem einige Neuinteressierte an unserem *Faire-Computer*-Nachrichtenkanal *@Faire-Computer* per Twitter. Ich selbst habe einiges inhaltlich gelernt bei der wieder mal aufwändigen Vorbereitung dieses Termins.

Sebastian Jekutsch

Sebastian Jekutsch ist ist FIfF-Mitglied aus Hamburg und aktiv im AK *Faire Computer* des FIfF. Wer sich für die Quellen für die erwähnten Berichte und Nachrichten oder das Thema überhaupt interessiert, liest unter Twitter bei *@FaireComputer* nach oder kann Kontakt aufnehmen über *fairit@fiff.de*.

Sebastian Jekutsch

Betrifft: Faire Computer

Fair wie in Faire Bananen.

In den letzten drei Monaten wurde über die Fairness von Computern ungewöhnlich viel diskutiert. Das Thema ist inzwischen so weit, einen Schwerpunkt nicht nur in der FIfF-Kommunikation, sondern auch in der *c't* zu bekommen. Dort erschienen in der Ausgabe 4/2014 neben einem Überblick *Gibt es ethische Elektronik?* eine Produktvorstellung, ein Herstellervergleich in Sachen Transparenz, Berichte über Fertigung in Deutschland und für das TCO-Siegel.

Vor allem hat die Diskussion aber das *Fairphone* angefacht. Zunächst: Alle Käufer – sie wohnen vor allem in Deutschland – haben ihre Geräte inzwischen bekommen. Diskutiert wurde, wie fair das Gerät eigentlich ist. Fairphone hat einen Audit des Herstellers *A'Hong* veröffentlicht, der zwar schon erste Verbesserungen beim Schutz jugendlicher Arbeiter, den Arbeitszeiten und der Arbeitssicherheit auflistet, insgesamt jedoch enttäuschte, liest sich vieles doch wie bei den Großen der Branche auch. Ein *Apple*-Fan rechnete in seinem schnell verbreiteten Blog-Beitrag vor, dass man bei *Foxconn*, dem großen Fertiger im Auftrage u. a. von Apple, doppelt so viel verdiene wie beim weithin unbekannten Produzenten des Fairphone. Er vergaß dabei allerdings den *workers welfare fund,* in den durch den Verkauf der Fairphones reichlich Geld geflossen ist, über das ein Gremium unter Beteiligung der Arbeiterinnen und Arbeiter bestimmen kann. Auch der AK *Faire Computer* hat sich an der Diskussion beteiligt, denn: Viel Verbesserung in der Fairness kann das Fairphone tatsächlich nicht vorweisen, erst recht nicht so viel wie einige vermutet haben, und ein Vergleich mit den Multis der Branche ist durchaus berechtigt. Ein Anfang für ein *ethically sourced* Smartphone ist aber gemacht und der Erfolg des kleinen Unternehmens beachtlich. Es hat eine zweite Version in Aussicht gestellt.

Ein weiterer Aufreger war die öffentlichkeitswirksame Ankündigung auf der *CES* in Las Vegas von *Intel,* ab sofort nur noch Prozessoren mit ausschließlich konfliktfreien Rohstoffen herzustellen. Damit hat es das Thema nun endgültig in den Mainstream geschafft. Es bleibt aber zu bedenken: Der Begriff der *Konfliktmineralien* bezieht sich seit entsprechender US-amerikanischer Gesetzgebung lediglich auf die Metalle Zinn, Wolfram, Tantal und Gold, und es bedeutet leider nicht, dass durch bewaffnete Konflikte belastete Erzminengebiete nun befriedet worden wären, sondern in aller Regel letztlich, dass die Rohstoffe nun in Ländern gekauft werden, in denen kein Bürgerkrieg herrscht, etwa Australien, Brasilien oder Südafrika. Ab Mai müssen alle US-börsennotierten Hersteller offen legen, ob sie Konfliktmineralien in ihren Produkten haben könnten, und wenn ja, wie sie versucht haben, dies zu vermeiden. Gegen die Umsetzung des US-Gesetzes läuft übrigens noch ein Klageverfahren von Unternehmensverbänden. Und wer ist dort unter anderem Mitglied? Genau, Intel.

Das dritte große Thema war wieder mal *Apple,* genauer: die *Fair Labor Association (FLA),* die in Auftrag von Apple drei Betriebe des iPhone- und iPad-Zusammenbauers *Foxconn* untersucht hatte und nun ihren Abschlussbericht präsentierte. Die FLA berichtet dort von neuen Fortschritten, bemängelt aber weiterhin die langen Arbeitszeiten. Nahe liegende Fragen zu Gehalt, unbezahlter Arbeit und den versprochenen, aber nicht durchgeführten freien Betriebsratswahlen beantwortet der Bericht nicht. Und nicht nur Foxconn, sondern auch dessen Zulieferer haben etwas zu verbergen. So haben Initiativen rund um das neue NGO-Projekt *Electronics Watch* einen investigativen Bericht über einen der Touchscreen-Hersteller des iPhone veröffentlicht: *Biel Crystal,* mit Arbeitsrechtsverletzungen, die man hoffte schon überwunden zu haben.

Nager-IT, Hersteller der fairsten aller Computermäuse – bislang sind etwa 3000 Stück verkauft –, hat seinen Trip nach China beendet und Einblicke in die Herstellung des USB-Kabels bekommen. Die öffentlich dokumentierte Transparenz der Lieferkette ist damit noch mal erweitert worden, greifbare Folgen des Besuchs gibt es aber noch nicht. Derweil hat Nager-IT selbst herausbekommen, dass ein kleiner Teil des Zinns in der Maus aus *Bangka,* Indonesien kommt, ein Abbaugebiet mit dokumentierten Verletzungen von Arbeitnehmer- und Menschenrechten. Sie wollen nun nach anderen Quellen suchen. Man sollte ergänzen: Zinn aus Bangka ist potenziell in allen Geräten von Samsung, Apple und vielleicht sogar dem ach so fairen Fairphone. Konsequenzen hat bislang niemand gezogen.

Apropos *Samsung:* Der Marktführer verlässt das zunehmend teure China und baut eine große Fabrik in Vietnam. Auf der Baustelle gab es Ausschreitungen. *China Labor Watch* berichtet in einer Veröffentlichung über Samsungs Zulieferer *Samkwang* von unmenschlich hohem Leistungsdruck. Nach dem Selbstmord eines Kollegen kritisiert ein weltweiter Gewerkschaftsverbund Samsungs gewerkschaftsfeindliche Politik. Die Klagen gegen den Konzern in Brasilien über Arbeitsbedingungen und in Frankreich über Kinderarbeit dauern ohne neue Nachrichten an.

Warum gibt es hier immer nur *schlechte Nachrichten?* Die Szene ist noch sehr damit beschäftigt, unfaire Zustände aufzudecken. Ist es eine gute Nachricht, dass sich in China zunehmend Streiks formieren, im vergangenen Quartal auch bei *Nokia* und Chiphersteller *ASM,* bei letzterem mit einigem Verhandlungserfolg? Ist es beruhigend zu vernehmen, dass *TCO* Nägel mit Köpfen macht und dem Hersteller *SIS Display* ihr Siegel entzogen hat wegen fehlenden Nachweisen bei der Sozialverträglichkeit? Dass Foxconn in Tschechien zu sagenhaften 18.000 Euro verurteilt wurde wegen Verstößen gegen das Arbeitsgesetz? Wir sollten vielleicht zunehmend die positiven Beispiele hervorheben: die Ansätze von Nager-IT und Fairphone, die Verbesserungen die Apple immerhin eingeleitet hat, überhaupt, dass konfliktfreie Wege der Rohstoffe und die Auftragslage in der Kontraktfertigung die Lebenssituation mancher Menschen in Kongo und China doch schließlich verbessert haben.

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

FIfF-Jahrestagung 2014

Der Fall des Geheimen – Blick unter den eigenen Teppich

7. bis 9. November 2014 in Berlin (Mitte)

Themenumriss: Wir wollen die Rolle Deutschlands und insbesondere der deutschen Geheimdienste im Kontext der neueren Erkenntnisse (Snowden, Foschepoth) bearbeiten. Wie kommt es, dass Deutschland oft als *Datenschutzmekka* und *Demokratievorzeigestaat* bezeichnet wird, obwohl sich gerade hier einer der Dreh- und Angelpunkte von Folterflügen, Drohnenmordkoordination, Kriegslogistik und Infrastruktur für flächendeckende Überwachung innerhalb Europas zu befinden scheint. Inwiefern ist die Rolle Deutschlands keine widerwillig helfende, ja fast opferhafte, sondern ganz im Gegenteil eine rege, aktive, tragende Säule des sich immer weiter offenbarenden antidemokratischen Zustandes der Welt? Dabei mutete es fast schon als eine Plattitüde an, wenn gesagt wird, dass dieser Zustand auf das Werk einer Techniker-Gemeinde zurückführbar ist – aber wie sind diese Systeme gebaut und nach welchen normativen Weltauffassungen wurden sie konzipiert?

Dazu wollen wir das Thema in drei Dimensionen beleuchten: 1) mit historischem Blick auf die deutschen Geheimdienste und ihre technisch-organisatorische Entwicklung, 2) mit aktuellen Analysen der gegenwärtigen Lage der Geheimdienste, ihres technischen Apparats und ihrer rechtlichen Einhegung; gerade die Verflechtungen zwischen den Geheimdiensten, Telkos und der Techniker-Gemeinde bedürfen einer besonderen Aufmerksamkeit; 3) mit Erfahrungsberichten direkt Betroffener oder gar Erzählungen von Whistleblowern (wenn wir welche kriegen).

Kurzum: Von allem den fehlenden technischen Aspekten (Kompetenz des FIfF) soll in der Debatte um die deutschen Geheimdienste Rechnung getragen werden, aber für ein Verständnis der Lage ist natürlich mehr nötig, daher wollen wir auch Vortragende aus anderen Bereichen einladen und uns explizit von Verschwörungstheorien abgrenzen.

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

Sara Stadler

Log 1/2014

Ereignisse, Störungen und Probleme der digitalen Gesellschaft

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

Oktober 2013

31. Oktober 2013: Im Rahmen der Koalitionsverhandlungen sprechen Union und SPD über die Bedingungen für eine Wiedereinführung der Vorratsdatenspeicherung (Quelle: Heise).

31. Oktober 2013: Die Bundesregierung legt eine Unterrichtung zum großen Lauschangriff vor. 2012 wurden neun Wohnungen akustisch überwacht, die Maßnahmen wurden auf Bundesebene wegen Bildung einer kriminellen bzw. terroristischen Vereinigung und auf Landesebene in Bremen, Niedersachsen und Nordrhein-Westfalen meist im Zuge von Ermittlungen wegen Mord und Totschlag eingesetzt. Betroffen war von der Abhöraktion, die ausschließlich in Privatwohnungen vorgenommen wurde, auch eine große Zahl von Personen, „die sich nicht identifizieren ließen" und daher auch im Nachhinein nicht über die Maßnahme informiert wurden. In drei Fällen brachte die Maßnahme keinerlei Ergebnisse. Gegenüber 2011 haben die Zahlen abgenommen (Quelle: Heise).

November 2013

1. November 2013: Neue Quellen aus dem Fundus Edward Snowdens legen nahe, dass die weltweite Überwachung des Internetverkehrs noch umfangreicher ist, als bisher angenommen. Laut der *Washington Post* greifen diesen Dokumenten zufolge NSA und GCHQ im Rahmen des Programms ‚Muscular' auf die Server von Google und Yahoo auch durch die Hintertür zu, indem sie sich Zugriff auf die Datenleitungen zwischen den Rechenzentren verschafft haben. Auf diesen Wegen können KundInnendaten unverschlüsselt abgegriffen werden. Von einer solchen Abhörmaßnahme wären etwa sämtliche Google-Cloud-Dienste sowie die ohne Google-Dienste kaum zu betreibenden Android-Smartphones betroffen (Quelle: The Washington Post, Heise).

2. November 2013: Mit großer Wahrscheinlichkeit gibt es auch in Wien eine Abhörstation der NSA. Dies folgert zumindest der Whistleblower Thomas Drake aus dem *Spiegel* vorliegenden Snowden-Dokumenten (Quelle: Der Spiegel, Heise).

2. November 2013: Wie der *Guardian* berichtet, hat der GCHQ bei der Entwicklung von Technik zur Internetüberwachung eng mit dem Bundesnachrichtendienst (BND) zusammengearbeitet. Auch die Geheimdienste Frankreichs, Spaniens und Schwedens seien an der Entwicklungskooperation beteiligt gewesen (Quelle: The Guardian, Heise).

3. November 2013: Wie Frank Bsirske, Vorsitzender der Dienstleistungsgesellschaft ver.di, in einem Interview mit *heise online* berichtet, skizzieren InnenpolitikerInnen aus CDU und CSU in einem Forderungspapier Pläne zu einer umfassenden Internetüberwachung im Stil der NSA. In den Koalitionsverhandlungen mit der SPD möchten die konservativen PolitikerInnen gerne eine Ausleitung des Datenverkehrs an den Netzknoten, wie etwa dem zentralen Austauschpunkt DE-CIX in Frankfurt, beschließen. Die ausgeleiteten Daten sollen von Geheimdiensten und Polizeien ausgewertet werden können. CDU und CSU dementieren derart umfangreiche Pläne am Folgetag (Quelle: Heise).

5. November 2013: Die *Washington Post* kann den Vorwurf erhärten, dass die NSA Daten an den Leitungen zwischen den Rechenzentren von Google abgreift. In weiteren Folien aus dem Fundus Edward Snowdens seien Datenstrukturen enthalten, die unverschlüsselt das interne Netz von Google niemals verließen. Auch seien Datenformate aufgelistet, die bei Google nur intern Verwendung fänden (Quelle: The Washington Post, Heise).

5. November 2013: Der Geheimdienstexperte Duncan Campell legt in einem Artikel im britischen *Independent* nahe, dass auch von der britischen Botschaft aus die Kommunikation in Berlin abgehört wird. Dies folgert er aus einer auf deren Dach angebrachten Struktur, die an die Anlagen der ehemaligen US-Abhörstation auf dem Teufelsberg in Berlin erinnere (Quelle: The Independent, Heise).

6. November 2013: Nachdem die SPD den von Innenminister Friedrich geforderten Zugriff auf Mautdaten zunächst abgelehnt hatte, weicht sie einem Bericht von *heise online* zufolge in neuen Koalitionsverhandlungen von dieser Haltung ab. In zukünftigen Koalitionsverhandlungen soll definiert werden, unter welchen Bedingungen die strikte Zweckbindung der Daten zu LKW-Maut aufzuheben und ihr Einsatz zu Fahndungszwecken gerechtfertigt werden soll (Quelle: Heise).

7. November 2013: Angeregt durch eine entsprechende Aussage Jacob Applebaums spekulieren verschiedene Kryptografie-Experten darüber, ob es der NSA möglich ist, die RC4-Verschlüsselung, mit der mehr als die Hälfte der verschlüsselt im Web übertragenen Daten gesichert werden, in Echtzeit zu knacken. Das Ergebnis: durchaus möglich! (Quelle: Heise)

12. November 2013: Auf der Herbsttagung des Bundeskriminalamtes (BKA) zeichnet sich ab, in welchem Ausmaß Internetüberwachung zukünftig zu erwarten ist. So hat BKA-Chef Jörg Ziercke dort den Aufbau einer kriminaltechnischen Servicestelle ‚Cyberlab' vorgestellt, in deren Rahmen sich über 100 Cyber-SpezialistInnen der „Kryptoanalyse und Dekryptierung von Verschlüsselung" widmen sollen. Zudem ist der Aufbau eines Bereichs Cyberspionage in der Abteilung *Polizeilicher Staatsschutz* geplant. Quellen-TKÜ und Onlinedurchsuchung sollen zukünftig mit einer selbst entwickelten Software betrieben werden, durch die das Einhalten des rechtlichen Rahmens – erinnert sei hier an dessen Überschreitung durch den von DigiTask für das bayrische LKA entwickelten Staatstrojaner – gewährleistet werden solle. Als Voraussetzung für die erfolgreiche Arbeit der neu geschaffenen Stellen sieht er die schnelle Einführung einer umfassenden Telekommunikationsüberwachung mit einer ausreichend langen Speicherung der IP-Adressen bei den Providern an. Klaus-Dietrich Fritsche, Staatssekretär im Bundesinnenministerium, möchte sich dabei nicht allein auf IP-Adressen beschränken, sondern plädiert für eine „technikoffene Lösung". Zudem möchte er die internationale geheimdienstliche Zusammenarbeit, etwa im Rahmen des EC3-Centers, bei Europol forcieren (Quelle: Heise).

13. November 2013: Der Internetkonzern Google schaltet in den USA eine offene Warteliste zum Test der Datenbrille Google Glass frei. Nicht thematisiert werden die schweren Eingriffe in die Privatsphäre, die durch die Brille möglich gemacht werden. So kann die Brille alle Personen im Blickfeld aufnehmen, ohne dass diese es bemerken und leitet die Daten automatisch an einen Server weiter. Dass Apps zur Gesichts- und Spracherkennung der gefilmten Personen entwickelt würden hat Google zwar zunächst ausgeschlossen aber eben nur „at this time" (Quelle: Heise).

14. November 2013: In einer Bund-Länder-Arbeitsgruppe hat die Bundesagentur für Arbeit den Vorschlag unterbreitet, die Internet-Daten von Hartz-IV-EmpfängerInnen zu überwachen, um möglicherweise nicht gemeldete Nebeneinkünfte aus dem Online-Handel aufzudecken. Auch ein erweiterter Datenabgleich mit anderen Stellen, wie Versicherungsunternehmen, wurde angeregt. Diese Vorschläge zur verdachtsunabhängigen Überwachung stießen allerdings bislang nur auf eingeschränkt positive Resonanz (Quelle: Der Spiegel, Heise).

14. November 2013: Berichten der *Süddeutschen Zeitung* und des *NDR* zufolge haben die USA von Deutschland aus unter anderem Drohneneinsätze organisiert. Auch seien deutsche Behörden aktiv an der Umsetzung des „Krieges gegen den Terror" beteiligt (Quelle: NDR, Süddeutsche Zeitung).

15. November 2013: Wie die *New York Times* und das *Wall Street Journa*l berichten, sammelt die CIA Daten zu grenzüberschreitenden Bargeld-Transfers. Nach Vorgaben des Intelligence Surveilliance Courts müssten dabei lediglich die Identitätsangaben von US-BürgerInnen anonymisiert werden (Quelle: New York Times, Wall Street Journal, Heise).

Sara Stadler

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

19. November 2013: Aus Medienberichten geht hervor, dass auch der norwegische Geheimdienst in großem Stil Daten sammelt und diese auch an die NSA weitergibt. Ziel der Datensammlung sei die Unterstützung norwegischer Militäroperationen sowie des „Krieges gegen den Terror" (Quelle: Heise, Wall Street Journal).

Dezember 2013

2. Dezember 2013: Wie niederländische Medien berichten, verschafft sich auch der dortige In- und Auslandsgeheimdienst AIVD Zugriff auf NutzerInnendaten aus Internetforen (Quelle: Heise).

3. Dezember 2013: Apple erhält ein Patent für Gerätesteuerung durch Gesichtserkennung. Benannter Zweck des Geräts ist die Autorisierung der NutzerInnen. Dass sich eine solche Technologie vielfältig einsetzen lässt, steht außer Frage (Quelle: Heise).

5. Dezember 2013: Neue Snowden-Dokumente geben Aufschluss über das Ausmaß der Erfassung von Handy-Standortdaten durch die NSA. Bereits 2012 seien den der *Washington Post* vorliegenden Dokumenten zufolge weltweit täglich knapp 5 Milliarden Standortdaten gesammelt worden. Die Daten flössen in eine riesige Datenbank, wo sie mit dem Analysewerkzeug Co-Traveler ausgewertet würden. Ziel sei es, Kontakte von Zielpersonen über Bewegungsprofile zu erkennen (Quelle: The Washington Post, Heise).

9. Dezember 2013: Die französische Sicherheitsbehörde ANSSI hat durch einen Man-in-the-Middle-Angriff SSL-verschlüsselte Verbindungen ausspioniert. Das entdeckte der Konzern Google, da die Behörde dazu gefälschte Google-Zertifikate nutzte. Entsprechende Zertifikate wurden im Anschluss auch bei Mozilla und Microsoft erkannt und aus den Zertifikatslisten entfernt (Quelle: Heise).

9. Dezember 2013: Der *Guardian* veröffentlicht gemeinsam mit der *New York Times* und *ProPublica* neue Dokumente aus dem Snowden-Fundus. Daraus geht hervor, dass auch Multiplayer-Spielwelten und Xbox-Live-Netzwerke von NSA und GCHQ angezapft werden. Zudem seien auch Agenten der Geheimdienste in den virtuellen Welten unterwegs (Quelle: The Guardian, Heise).

9. Dezember 2013: Wie die *Süddeutsche Zeitung* berichtet hat die Bundesregierung Millionenaufträge an private Sicherheitsdienstleister vergeben, die für die NSA Abhörprogramme entwickelt haben, darunter der ehemalige Arbeitgeber Edward Snowdens, Booz Allen Hamilton (BAH). Ebenfalls auf der Gehaltsliste stünden Unternehmen, die bei CIA-Verschleppungen halfen, wie die CSC oder über Tochterunternehmen an Misshandlungen in Abu Ghuraib beteiligt waren, hier namentlich L-3 Communications. Gegenstand der Aufträge sei etwa die „Analyse von kritischen Infrastrukturbereichen in Deutschland" gewesen (Quelle: Süddeutsche Zeitung).

9. Dezember 2013: Eine Abmahnwelle wegen Streaming-Konsums beim Pornovideoportal *Redtube* sorgt für öffentliches Aufsehen. Vieles spricht dafür, dass die den abgemahnten Personen vorgeworfenen Urheberrechtsverletzung von den RechteinhaberInnen mittels der Umleitung des Traffics über einen Proxy selbst generiert wurde. Dabei wurden offensichtlich auch die IP-Adressen geloggt. Die AbmahnerInnen selbst äußern sich sich nicht über das genutzte Verfahren zur IP-Ermittlung. Die Herausgabe der Namen zu den IP-Adressen durch die Provider hatte das Landgericht Köln bewilligt. Dies führte zu zahlreichen Beschwerden, denen das Landgericht schließlich stattgeben musste (Quelle: Heise).

10. Dezember 2013: Die Hessische Polizei testet den Einsatz sogenannter Body-Cams. Die am Körper der Beamten angebrachten Kameras sollen diese nach eigenem Ermessen nutzen können, um Übergriffe zu verhindern. Dass dadurch auch Übergriffe durch PolizistInnen dokumentiert werden, wie ein Sprecher des hessischen Innenministeriums behauptet, ist erfahrungsgemäß eher unwahrscheinlich (Quelle: Heise).

11. Dezember 2013: Die Kassenärztliche Vereinigung weist darauf hin, dass entgegen ursprünglich anders lautender Behauptungen die alten Versicherungskarten bis zum aufgedruckten Verfallsdatum ihre Gültigkeit behalten. An der Einführung der Elektronischen Gesundheitskarte ändert das prinzipiell jedoch nichts (Quelle: Heise).

11. Dezember 2013: Aus neueren Snowden-Dokumenten geht dem kanadischen TV-Sender *CBC* zufolge hervor, das der kanadische Geheimdienst CSEC in 20 Staaten Abhörstationen für die NSA betrieben habe (Quelle: CBC, Heise).

12. Dezember 2013: In einem Rechtsgutachten stellt der Generalanwalt am Europäischen Gerichtshof Pedro Cruz Villalón fest, dass die umstrittenen Richtlinien zur Vorratsdatenspeicherung in der aktuellen Form nicht mit den Europäischen Grundrechten vereinbar sind. Grundsätzlich erachtet der Gutachter die Vorratsdatenspeicherung jedoch für legitim (Quelle: Der Spiegel, Heise).

12. Dezember 2013: In Frankreich stimmt nach der Nationalversammlung auch der Senat einer erweiterten Klausel zur Internetüberwachung zu. Danach dürfen nicht mehr nur französische Geheimdienste, sondern auch zahlreiche Behörden Verbindungs- und Standortdaten bei Providern sowie Inhaltsdaten bei Dienstanbietern zukünftig in Echtzeit abgreifen. Statt einer richterlichen Genehmigung ist zukünftig nur noch ein Gesuch bei einem nationalen Konsortium erforderlich (Quelle: Heise).

14. Dezember 2013: Wie die *Washington Post* unter Berufung auf Snowden-Dokumente berichtet, kann die NSA massenhaft Handy-Gespräche unter Ausnutzung der unsicheren Verschlüsselung des Mobikfunk-Standards GSM abhören. Auch neuere Verschlüsselungs-Mechanismen seien für die NSA möglicherweise knackbar (Quelle: The Washington Post, Heise).

14. Dezember 2013: Der Apple-Zulieferer Foxconn verstößt in seinen chinesischen Werken weiterhin gegen geltende Arbeitszeitregeln. Die geht aus dem Abschlussbericht der Fair Labor Association (FLA) hervor (Quelle: FLA).

14. Dezember 2013: Google übernimmt das unter anderem für seine Militärroboter bekannte Unternehmen Boston Dynamics, zu dessen Auftraggebern auch das Pentagon gehört. Zu-

vor hatte der Konzern bereits sieben andere auf Robotik spezialisierte Unternehmen übernommen (Quelle: Der Spiegel).

21. Dezember 2013: Aus neu veröffentlichten Snowden-Unterlagen geht hervor, dass sich der Sicherheitssoftware-Anbieter RAS Security mit zehn Millionen Dollar von der NSA für eine Hintertür in der Krypto-Bibliothek BeSafe bezahlen lies. Konkret wurde hier der von der NSA entwickelte trojanische Zufallsgenerator Dual_EC_DRBG eingebaut. Im Effekt wurde dadurch – auch von nichts ahnenden EntwicklerInnen – Sicherheitssoftware erstellt, deren Krypto-Schlüssel einfach zu knacken sind (Quelle Heise).

29. Dezember 2013: NSA und GCHQ greifen in massivem Umfang Daten an der transkontinentalen Netzinfrastruktur ab. Wie *Spiegel Online* berichtet, hat die NSA auch Zugriff auf ein Unterseekabel zwischen Europa und Asien (Quelle: Der Spiegel, Heise).

Januar 2014

2. Januar 2014: Mit Unterstützung des Wehrbeauftragten des Bundestages fordert die Bundeswehr die schnelle Anschaffung bewaffneter Kampfdrohnen (Quelle: Der Spiegel, Heise).

3. Januar 2014: Es häufen sich Berichte über Backdoors bei diversen Routermodellen namenhafter Hersteller wie Cisco, Linksys und Netgear, mittels derer die Router über das Internet ausspioniert und manipuliert werden können (Quelle: Heise).

8. Januar 2014: Wie aus der Antwort des Bundesinnenministeriums auf eine Anfrage der Linksfraktion im Bundestag hervorgeht, will die Bundesregierung die polizeiliche Zusammenarbeit und den Datentransfer auf EU-Ebene ausbauen. Konkret geht es unter anderem um den Bereich Cyber-Sicherheit sowie den Ausbau des europäischen Grenzsystems. Derartige Äußerungen lassen vermuten, dass nachfolgende Regelungen das für den Zeitraum von 2010-2014 gültige *Stockholm-Programm*, das bereits eine Echtzeitüberwachung digitaler Kommunikation vorsieht, noch übertreffen werden (Quelle: Heise).

9. Januar 2014: Wie aus einer Antwort des Innenministeriums auf eine Anfrage der Linksfraktion hervorgeht, plant die Bundesregierung die Einrichtung einer Datenbank über „reisende Gewalttäter". „Gewaltbereite Störer" sollen im Vorfeld von Veranstaltungen aus den Bereichen Freizeit, Politik oder Umwelt besonders beobachtet werden (Quelle: Heise).

10. Januar 2014: Wie aus den nun veröffentlichten Jahresbericht des parlamentarischen Kontrollgremiums des Bundestages für die Geheimdienste (PKGr) hervorgeht, haben das Bundesamt für Verfassungsschutz (BfV) und der Bundesnachrichtendienst (BND) im Jahr 2012 ihre Anti-Terror-Befugnisse noch eifriger ausgeschöpft als 2011. Insgesamt 176 Personen, die im Nachhinein nur teilweise informiert wurden, waren von der geheimdienstlichen Ausspähung mittels Auskunftverlangen bei Telekommunikations- und Luftfahrtfirmen sowie Kreditinstituten oder von IMSI-Catcher-Einsätzen betroffen. In das Post- und Fernmeldegeheimnis haben Geheimdienste im gleichen Jahr 157 mal eingegriffen (Quelle: Heise).

14. Januar 2014: In den USA hat ein Bundesberufungsgericht die Auflagen der Federal Communications Commission (FCC) zur Netzneutralität für rechtswidrig erklärt (Quelle: Heise).

14. Januar 2014: Google kauft das Unternehmen Nest Labs, das vernetzte Haushaltstechnik wie Thermostate und Rauchmelder entwickelt. Damit fließen zukünftig auch private Daten aus Haushalten zu Google (Quelle: Heise).

15. Januar 2014: Als Reaktion auf eine Kampagne des *Every Day Sexism Project* nehmen Apple und Google Spiele aus ihren Stores, in denen die SpielerInnen Schönheits-Operationen an vermeintlich übergewichtigen Mädchen durchführen sollen (Quelle: Heise).

15. Januar 2014: Die *New York Times* berichtet unter Berufung auf einen anonymen Geheimdienst-Informanten, dass die NSA aktuell fast 100.000 Computer und Netzwerke weltweit mit Spähsoftware infiziert habe (Quelle: The New York Times, Heise).

16. Januar 2014: Wie der *Guardian* berichtet, greift die NSA täglich bis zu 200 Millionen SMS ab (Quelle: The Guardian, Heise).

21. Januar 2014: Wie der *Guardian* berichtet, sollen in Großbritannien zukünftig PatientInnendaten zentral gesammelt und gegen Entgelt an Universitäten, Versicherungskonzerne oder Pharmafirmen weitergegeben werden. Zwar sollen die Daten pseudonymisiert werden, mit ein bisschen Aufwand lassen sich daraus aber theoretisch die psychischen Erkrankungen oder Trinkgewohnheiten konkreter Personen ermitteln (Quelle: The Guardian, Heise).

22. Januar 2014: In einer Anhörung des NSA-Untersuchungsausschusses spricht der russische Journalist und Geheimdienst-Experte Andrej Soldatow über das Abhörprogramm SOROM, mit dem der russische FSB die gleichen Ziele verfolge wie die NSA mit dem Programm PRISM, auch wenn ihm dafür nicht die gleichen Möglichkeiten zur Verfügung stünden (Quelle: Heise).

24. Januar 2014: *Heise Online* gibt einen Bericht des Fachblattes *Defense News* wieder, demzufolge die US-Army ihre Streitkräfte zukünftig verstärkt auf autonome Roboter umstellen möchte. Zunächst sollen diese einem Sprecher der Armee zufolge jedoch nur für Hilfsarbeiten wie Transporte eingesetzt werden (Quelle: Heise).

24. Januar 2014: Thomas de Maizière, der deutsche Innenminister, möchte weiter am Ausbau der Festung Europa mithilfe eines elektronischen Grenzsystems nach US-amerikanischem Vorbild arbeiten. Dies geht aus den Äußerungen des CDU-Politikers anlässlich des Treffens der europäischen Justiz- und Innenminister in Athen hervor (Quelle. Heise).

27. Januar 2014: Über ein von der britischen Bürgerrechtsorganisation *Statewatch* veröffentlichtes Arbeitsprogramm des EU-Polizeinetzwerks ENLETS (European Network of Law Enforcement Technology Services) werden dessen Pläne bekannt, in in der EU zugelassenen Fahrzeugen eine Technologie einzubauen, die deren Anhalten per Funk ermöglicht. Zudem will ENLETS die polizeilichen Kompetenzen in der „Funkaufklärung" in Telekommunikationsnetzen erweitern und damit die Grenze zur geheimdienstlicher Tätigkeit weiter verwischen (Quelle: Heise).

27. Januar 2014: Google kauft mit DeepMind eine Firma, die sich führend mit künstlicher Intelligenz beschäftigt. Deren Technologien können unter anderem zur Auswertung großer Datenbestände genutzt werden (Quelle: Heise).

28. Januar 2014: Aus neu veröffentlichten Snowden-Dokumenten geht hervor, dass der GCHQ die massenhaft an den Glasfaserkabeln abgegriffenen Daten von Facebook, Google, Youtube und Co. unter anderem dazu nutzen möchte, Proteste vorherzusagen und gesellschaftliche Entwicklungen berechenbar zu machen (Quelle: Heise).

28. Januar 2014: Der *Guardian*, die *New York Times* und *ProPublica* berichten von neuen Snowden-Dokumenten, denen zufolge NSA und GCHQ auch über Smartphone-Apps ins Internet übertragene Daten abgreifen. Auch aus den Daten von Spielen wie *Angry Birds*, lassen sich den Medien zufolge Einzelheiten über die Geräte und ihre NutzerInnen gewinnen (Quelle: The Guardian, The New York Times, Heise).

Stephan Geelhaar

Ausbau der Internet-Polizei

Nachschlag zur Bestandsdatenauskunft

Während sich die FIfF-Kommunikation noch im Druck befand, stand die Zeit nicht still. An dieser Stelle daher ein kurzes Update zur Neuregelung der Bestandsdatenauskunft, die in der letzten Ausgabe, Seite 27, ausführlich betrachtet wurde.
Inzwischen hat das Bundesland Sachsen mit einer Novellierung seines Polizei- und Verfassungsschutzgesetzes im Eiltempo nachgezogen. Ein entsprechender Gesetzesentwurf wurde erst am 27. September 2013 bekannt gegeben und schon am 17. Dezember mit den Stimmen der Regierungskoalition im Sächsischen Landtag verabschiedet.

Die verabschiedeten Inhalte gleichen denen der anderen Bundesländer und auch die Vorbehalte und Einschränkungen für die Datenabfrage weisen nur graduelle Unterschiede zu denen auf, die im vorigen Heft betrachtet wurden. Vertauscht sind lediglich die Rollen im Landtag. Während zur Regierungskoalition neben der CDU auch die FDP gehört, gönnten sich die Sozialdemokraten – als Teil der Opposition – den Luxus, mal gegen Gesetzesverschärfungen zu argumentieren.

In Sachsen wurde erneut das Argument ausgespielt, man brauche den Zugriff auf Passwörter und andere *Zugangscodes,* um Suizid-gefährdete Personen oder Amokläufer zu lokalisieren. Bereits im Vorfeld stellten die Grünen eine *Kleine Anfrage* an die Staatsregierung, um zu erfahren, ob denn Informationen darüber vorliegen, wie viele Suizide und Amokläufe per Telefon oder Internet angekündigt wurden. Die Antwort war denkbar knapp. Es gebe keine entsprechenden Statistiken und dies sei auch nicht „automatisiert recherchierbar". In der Landtagsdebatte selbst wurde dann deutlich, dass keine Evaluation vorliegt, die einen sinnvollen Einsatz der Auskunftsersuchen in solchen Fällen nahelegt.

Dennoch sind es solche extremen Beispiele, welche die Debatte bestimmen, während sich der weitaus wahrscheinlichere Anwendungsfall erst auf dem zweiten Blick offenbart. So nennt der Abgeordnete Christian Hartmann (CDU) auf Nachfrage folgendes Szenario:

> *Sie stellen zum Beispiel fest, dass es eine Veranstaltungsankündigung für ein Konzert im Naturschutzgebiet gibt. Nun können Sie darüber lachen, doch Naturschutz sollte Ihnen wichtig sein. Im Übrigen haben wir in der Dresdner Heide so etwas gehabt. Es gab Informationen, die zu einer Party im Naturschutzgebiet aufriefen, und es wurde angegeben, dass man zu einem bestimmten Zeitpunkt eine Handynummer anrufen soll. Hier haben Sie eine Ordnungsmaßnahme, an der Sie entsprechend Zugriff gewährleisten.*[1]

Dass solche Ordnungsmaßnahmen der eigentliche Grund für das große Interesse der Sicherheitspolitiker an den neuen Regeln zur Datenabfrage sind, gerät bei der emotional geführten Diskussion um Beispiele von Selbstmorddrohungen oft in den Hintergrund.

Dabei hat das Bundesland bereits einen eigenen Skandal um die massenhafte Abfrage von Handydaten hinter sich. Im Februar 2011 wurden während der Proteste gegen einen Neonazi-Aufmarsch in der Dresdner Innenstadt innerhalb von zwei Tagen insgesamt 1.034.000 Verbindungsdaten von Handybenutzern abgefragt. Darunter alle 20.000 Gegendemonstranten und viele Anwohnerinnen und Anwohner. Erst im vergangenen Jahr hatte ein Gericht die Rechtswidrigkeit der Maßnahme festgestellt.

Angesichts der nun verabschiedeten Gesetze steht zu befürchten, dass wir auch in Zukunft nicht von ähnlich bösen Überraschungen verschont bleiben werden. Die neu gewählte Bundesregierung (hier wiederum ohne FDP und mit SPD) hat bereits eine Gesetzesinitiative zur Vorratsdatenspeicherung angekündigt, zum *Großen Bruder* der Bestandsdatenauskunft.

Anmerkung

1 *Zitiert nach dem Protokoll der 88. Sitzung des Sächsischen Landtags (Plenarprotokoll 5/88), S. 67.*

Stephan Geelhaar studiert Informatik an der Universität Rostock und ist Neumitglied des FIfF.

Günter Müller

Datenschutz bei datenzentrischen Diensten: Auslaufmodell oder nur 30 Jahre zurück?

Das Geheimnis des Erfolgs von Google und Facebook und anderen liegt in der Fülle ihrer heute unverzichtbaren, scheinbar kostenfreien Dienste, für deren Nutzung die Anwender aber mit persönlichen Daten bezahlen. „Daten sind das Öl des 21ten Jahrhunderts" [16] ist zu einem gängigen Schlagwort geworden. Die allgemeine Akzeptanz solcher Aussagen scheint die Privatheit zum Auslaufmodell zu degradieren. Nachfolgend werden daher die Nutzer von datenzentrischen Diensten etwas unüblich als die Datenanbieter *und die Anbieter der Dienste als die* Datenkonsumenten *bezeichnet [11,18]. Der Vorschlag, Daten als Ware zu sehen, die gehandelt werden kann, ist die Grundthese dieses Beitrags für einen wirksamen Datenschutz auf der Höhe der Zeit.*

Privatheit ist im Deutschen ein Kunstwort und basiert auf der Institution der informationellen Selbstbestimmung. Dies ist im anglo-sächsischen Rechtsraum anders. Dort ist *Privacy* im Amendment 4 der Verfassung der USA geregelt und hat eine räumliche Dimension – Privatheit im öffentlichen Internet ist unmöglich –, während in Europa die Privatsphäre an die Person gebunden ist und auch im Internet gilt. Ökonomisch ergibt sich aus der Datensammlung der datenzentrischen Dienste die Gefahr der informationellen Asymmetrie zwischen Anbieter und Konsument. Wirtschaftlich würden die Datenanbieter *enteignet*, wenn dies das Prinzip des Datenschutzes wäre. Miller und Poscher zeigen, dass gerade die informationelle Selbstbestimmung in Europa und Deutschland einen wirtschaftlichen „Wertansatz" impliziert [17]. Die Kontrolle erfolgt über Privatheitsmechanismen, die in *PET (Privacy Enabling Technology)* und *TET (Transpareny Enabling Technology)* aufgeteilt werden können. Zwar scheint Transparenz das Gegenteil von Privatheit zu sein, dennoch, in Verbindung mit Privatheitsregeln ermöglichen sie eine aushandelbare Privatheit zwischen den Kommunikationspartnern [9,20] und könnten so zur Voraussetzung eines wirtschaftlich basierten Datenschutzes werden. Trotz großer technischer Fortschritte wirken bislang die kleinen Grüppchen der Datenschützer wie anachronistische Idealisten, die vergeblich vor immer neuen Gespenstern warnen. Auch die Enthüllungen von Snowden haben nur aufgedeckt, was man schon vorher wusste, aber letztlich nicht wissen wollte. Mit einem omnipotenten Geheimdienst ist Privatheit weder im amerikanischen noch im deutschen Rechtssystem möglich [21].

Datensparsamkeit und Transparenz

Datenzentrische Dienste verstoßen dem Geiste nach – nicht de facto – gegen das Bundesdatenschutzgesetz (BDSG), da sie weder die Zustimmung, die Korrektur noch die Kontrolle der gespeicherten Daten durch den Nutzer in Betracht ziehen und schon gar nicht der Zweck der Datenspeicherung vor der Datenerhebung genannt wird. Daten werden auf Vorrat mit der Absicht der wirtschaftlichen Verwertung erhoben, bei Nachfrage aufbereitet und dann veräußert. Dies alles geschieht ohne Kenntnis der Nutzer, die zuvor allerdings zumeist ihre Zustimmung durch entsprechende Markierungen auf der Webseite gegeben haben. Gegenwärtig übergeben nahezu 100 % aller Nutzer ihre wirtschaftlich vertretbaren Rechte ohne Gegenleistung an den Datenkonsumenten, da sie mit Recht befürchten, sonst nicht am gewünschten Dienst teilhaben zu können [21]. Heutige datenschutzrechtliche Konzepte lassen dem *Datenanbieter* – also dem Nutzer der Dienste – keinerlei Möglichkeit, diese Weitergabe zu verfolgen oder evtl. falsche Informationen zu korrigieren. Die zunehmend *unwissenden* Nutzer benötigen Schutz vor den immer *wissen-*

der werdenden Diensteanbietern. Das aktuelle Prinzip der Datensparsamkeit setzt am falschen Punkt an. Es geht davon aus, dass nicht gegebene Daten auch nicht missbraucht werden können. Wird hingegen das *Datensammeln* zu Gunsten der Privatheit verteuert, dann ist der Datenkonsument dem Datenanbieter Rechenschaft schuldig, um die Lizenzgebühren zu entrichten.

Eine Analyse des Wertes von Web-Diensten in Bezug auf die Aktienkursentwicklung zeigt einen eindeutigen Zusammenhang zu der Datenverfügbarkeit [10]. Das *Privacy Paradox* beschreibt die empirisch oft zu beobachtende Tatsache [5], dass private Akteure einerseits dem Schutz der Privatheit eine hohe Wertschätzung zuerkennen, jedoch andererseits in konkreten Entscheidungssituationen sehr freigiebig persönliche Daten anbieten [23]. Bislang gibt es zwar zahlreiche kasuistisch nachgewiesene Evidenzen [6], aber theoriebegründete Erklärungen dieses Phänomens gibt es nicht [4]. Ebenso fehlen Theorien für die Relevanz der Regulierung des Datenschutzes auf beispielsweise die volkswirtschaftliche Wohlfahrt [21,24].

Die *Ökonomisierung* hat aber noch viele weitere *weiße Flecken*. Die Auswirkungen auf Innovationen und das Erzeugen der dafür *Anreiz schaffenden* Kräfte sind nicht bekannt. *Aquisti* und *Varian* schlussfolgern, Datenschutz könne Innovationen behindern und damit das volkswirtschaftliche Wachstum langfristig bremsen [3]. *Berendt et al.* kommen zum Schluss, dass für Datenschutz ein höherer Preis durchsetzbar wäre, wenn er als Qualitätseigenschaft gesehen würde [6].

Auswirkungen von Verstößen gegen Datenschutz untersuchen Acquisti et al., indem sie die Veränderung des Aktienkurses des betroffenen Unternehmens nach datenschutzrelevanten Vorkommnissen als einen Indikator vorschlagen [3]. Festgestellt werden konnte ein potenziell negativer Effekt auf den Marktwert, welcher jedoch nur sehr kurzlebig war. Langfristig kommen sie zum Ergebnis, dass Unternehmen von Verletzungen des Datenschutzes sogar profitieren könnten. Andere Untersuchungen gehen davon aus, dass die Wirkung des Datenschutzes am ehesten durch den Risikoanteil beschrieben werden kann, der mit der Enttäuschung des Vertrauens verbunden ist [2].

Technikmodell und Privatheit

Seit der kommerziellen Nutzung von Rechnern erleben wir einen ständigen Wandel in der Art und Weise, wie Computing angeboten und genutzt wird, d.h. das Technikmodell ändert sich.

In den 60er und 70er Jahren hat – dominiert durch die Technologie der IBM – die Datenverarbeitung in geschlossenen Räumen stattgefunden. Es brauchte schon eine gewisse kriminelle Energie, um überhaupt an Daten zu gelangen. Das Aufkommen des Internet, verbunden mit dem Personal Computing (PC) und der zunehmenden Mobilität digitaler Endgeräte, machte den Missbrauch leichter und addierte die ständige Kontrolle der Bewegungsdaten zu den Profilen eines Nutzers. Wer wollte schon auf die Bequemlichkeit der Nutzung eines Mobiltelefons nur deswegen verzichten, weil dafür die Ortsdaten bekannt wurden? Die datenzentrischen Dienste gehen nun einen Schritt weiter. Informationen, abgeleitet aus den Daten der sich stetig vermehrenden *Big Data,* dienen der *Geschäftsintelligenz* der Kunden datenzentrischer Dienste. Big Data sind lebende oder ständig mit der Nutzung wachsende *Datensammlungen*, die sich vor allem auf verbesserte, bislang nicht gesammelte Daten konzentrieren. Die Bildung von Korrelationen ist das Ziel [22]: Inferenzen sind Korrelationen zwischen beliebigen Größen. Ein Datenanbieter mag dennoch die Freiheit besitzen zu entscheiden, welche Informationen er oder sie preisgibt; hat aber doch keine Möglichkeit zu erahnen, wozu die Daten in welcher Aggregation in Zukunft dienen sollen. Abgeleitete Daten sind datenschutzrechtlich nicht geschützt, da es sich um verarbeitete Daten handelt.

Informationssicherheit wird in der Regel über die Einhaltung von vier Schutzzielen definiert: Vertraulichkeit, Integrität, Zurechenbarkeit und Verfügbarkeit [18]. Das vorrangige Ziel der IT-Sicherheit ist der Schutz der gespeicherten und verarbeiteten Informationen und der Kommunikation zwischen Partnern, die sich gegenseitig vertrauen und sich vor Angriffen durch Dritte schützen wollen. Bei der Privatsphäre misstrauen sich die Kommunikationspartner untereinander. Schutzziele – wie bei der Sicherheit – sind unbekannt.

Privatheit und Interaktion

Informationelle Selbstbestimmung setzt voraus, dass man sich über die Folgen der Datenweitergabe im Klaren ist. Aus den nachfolgenden technischen Annahmen der PET-Technologien, ist zu erkennen, dass sie in keinem Aspekt für die aktuellen sozialen Netze erfüllt sind [1,19]:

- Das Identitätsmanagement: Alle Teilnehmer sind eindeutig identifizierbar.
- Jeder Nutzer ist in der Lage, selbstbestimmt zu entscheiden, welche Daten freizugeben sind und welche Folgen dies haben kann.
- Die miteinander kommunizierenden Instanzen einigen sich auf vorher festgelegte Regeln, wie mit Daten verfahren wird.

Die Bedienbarkeit

Whitten und *Tygar* untersuchen beispielhaft das Sicherheitswerkzeug PGP 5.0 und zeigen, dass dieses durch Normalbenutzer nicht bzw. nur unzulänglich bedienbar ist und dadurch unsicher wird [25]. Mit dem Ziel der Entwicklung eines objektiven Maßes für die Nutzbarkeit eines Sicherheitsmechanismus befassen sich *Kaiser* und *Reichenbach* 2002 [13]. Sie identifizierten dazu die möglichen Fehler im Umgang mit einem Dienst und zeigen die Folgen für die Sicherheit. Es stellt sich heraus, dass sich 75 % aller Nennungen den sicherheitskritischen Benutzbarkeitsproblemen zuordnen lassen. Kaiser untersucht mittels einer zweiten empirischen Studie, warum heutige Internet-Nutzer Sicherheitsmechanismen in IT-Anwendungen nicht oder nur eingeschränkt nutzen [14]. Die Sicherheitslaien, obwohl schon die größte Gruppe, können danach weiter unterteilt werden:

1. Sicherheitslaie 1: „Die gefährdeten Gutgläubigen“
2. Sicherheitslaie 2: „Die Bereitwilligen, aber Ungeduldigen“
3. Sicherheitslaie 3: „Die risikofreudigen Könner“

Mit 65 % sind die Gutgläubigen am stärksten vertreten, ca. 20 % der Laien sind Bereitwillige, die Sicherheitsgefahren zwar erkennen, aber nur wenig Zeit auf sie verwenden. Die risikofreudigen Kenner nehmen die Gefahren wissend in Kauf.

Privatheits-Paradox

Darunter wird verstanden, dass für Nutzen Privatheit eingetauscht wird, obwohl man über die Folgen des Handelns keine Informationen hat. *Culnan* und *Armstrong* [8] analysieren eine zwischen 1990-1994 erhobene Studie von *Louis Harris* [12] über die Haltung von Konsumenten bezüglich Privatheitsfragen, um eine detaillierte Klassifikation der beobachteten Verhaltensweisen zu schaffen. Sie unterscheiden zwischen (a) Der Angst vor einem unauthorisierten Zugriff aufgrund von Sicherheitslücken bzw. dem Mangel an internen Kontrollen sowie (b) der Sorge vor einer missbräuchlichen, nicht zweckgebundenen (Weiter-) Verwendung der Daten wie bspw. der Weitergabe an Dritte. Mittels einer breiten Meta-Analyse von Privatheits-betreffenden Studien können Smith, Milberg und Burke zusätzlich (c) die generelle Sorge um Datensammlung sowie (d) die Angst vor möglicher Unfähigkeit zur Berichtigung von Fehlern identifizieren [24].

Berendt, *Günther* und *Spiekermann* verdeutlichen die Risikostreuung mittels eines Laborexperiments mit Probanden, deren Online-Shopping-Verhalten untersucht wurde [6]. Es wird die latente Bereitschaft zur Herausgabe persönlicher Informationen abgefragt, wobei die Bereitschaft zur Preisgabe von persönlichen Daten und die individuelle Wertung der Privatheit analysiert wurden. Die Autoren zeigen, dass sich Endverbraucher bezüglich der Ausprägung ihrer Privatheitsinteressen in 3 Klassen unterteilen lassen: (1) Die *marginally concerned* (24 %), die sich durch Gleichgültigkeit bzgl. ihrer Privatheit auszeichnen; (2) die *privacy fundamentalists* (30 %), die enormen Wert auf die Wahrung ihrer Privatheit legen sowie (3) die *pragmatic majority*, die einerseits das Interesse verfolgt, ihre Privatheit zu wahren, diese aber andererseits für die Erlangung eines Nutzens bereit ist, aufzugeben. *Beresford, Kübler* und *Preibusch* [7] zeigen, dass Privatheit schon für eine relativ geringe Vergütung eingetauscht wird. Diese Studie verdeutlicht eindrucksvoll, dass der Privatheit in konkreten Entscheidungssituationen oft ein sehr geringer Stellenwert zugeordnet wird, wenn der Preisgabe der Information ein (wenn auch noch so geringer) Nutzen gegenübersteht. Eine mögliche Erklärung für dieses Verhalten ist, dass mit dem Nutzen im Jetzt eine Delegation der (möglichen) Kosten in die Zukunft in Kauf genommen wird. Acquisti und *Grossklags* bezeichnen diese Handlungsgrundlage als *hyperbolische Diskontierung* [5]: Die mit einem exponentiell ansteigenden Diskontierungssatz gewichteten, zukünftig möglichen Kosten unterliegen dem Vorteil der sofortigen Nutzung. Verdeutlicht an einem Beispiel: Der Nutzen einer Zigarette im Jetzt spielt für den Raucher eine viel stärkere Rolle als der nicht notwendigerweise auf den Konsum zurückzuführende zukünftige Tod. Die ursprüngliche hohe Wertung der Privatheit des Konsumenten wird in konkreten Entscheidungssituation verworfen, um sie durch die Preisgabe von Informationen in die Lage zu versetzen, entsprechende Vorteile daraus zu ziehen. Acquisti vertritt die Ansicht, dass dieses paradoxe Verhalten nicht als Irrationalität seitens der Datenanbieter gelten kann, sondern auf den Einfluss verschiedener Faktoren wie inkonsistente Präferenzen, gegenläufige Bedürfnisse, unvollständige Informationen über mögliche Risiken, begrenzte kognitive Fähigkeiten sowie unterschiedliche systematische Abweichungen vom abstrakten rationalen Entscheidungsprozess zurückzuführen ist [3].

Eine Bestätigung des *Privacy-Paradoxons* zeigt sich auch bei der Nutzung von Facebook. Acquisti und Gross untersuchten das Offenbarungsverhalten von College-Studenten [4]. Die Auswertung beweist, dass von einem höheren Privatheitsempfinden nicht direkt auf eine geringere Nutzungshäufigkeit von Facebook geschlossen werden kann. Dem Wissen über mögliche Privatheitskonsequenzen steht der Wille entgegen, den Dienst trotz bestehender Gefahren zu nutzen. Die stärkste Triebkraft zur Nutzung von Facebook liegt in der Pflege von bereits bestehenden Kontakten bzw. Freundschaften durch bessere Kontaktmöglichkeit sowie bessere Informationsgewinnung. Dieser generelle Nutzen wird immer höher bewertet als einzelne Privatheitskompromisse.

Die Grundmythen der Datenschutzmechanismen

Grundsätzlich ist davon auszugehen, dass eine Kontrolle der Privatheit durch Dienste oder automatisierte Mechanismen bewirkt wird, die eine leichte Einschätzung der Folgen einer Datenfreigabe ermöglichen [20]. Die scheinbare Erlangung der Privatheit beruht auf zumindest vier Mythen:

1. **Die größte Gefahr für die Privatheit kommt von einem nicht autorisierten Zugang zu Informationen.**

   Die Krypotologie als die Königsdisziplin der Sicherheit hält Informationen vor Unberechtigten geheim. Nur dazu müssen sich die Kommunizierenden über den Austausch von Schlüsseln vertrauen, während sie sich bei Privatheit eben nicht vertrauen.

Günter Müller

Prof. Dr. Dr. h. c. **Günter Müller,** 1987 Direktor der IBM, Rechnernetze. Juli 1990 Telematik an der Universität Freiburg. 1993-1999 Kollegleiter „Sicherheit in der Kommunikationstechnik“, Gottlieb Daimler- und Karl Benz-Stiftung, 1995 Enquêtekommission des Landtages Baden-Württemberg, 1999 Sprecher des Schwerpunktprogramms der DFG „Sicherheit in der Informations- und Kommunikationstechnik“. 2000 Experte der Bundesregierung bei der Konferenz „Modernes Regieren im 21. Jahrhundert“, 2010 Ehrenkreuz des österreichischen Bundespräsidenten, 2011 ACM Fellow und Ehrenpromotion TU Darmstadt sowie Freund der Universität Zagreb und Ehrenmedaille der WU Wien.

2. **Privatheit ist dann gegeben, wenn man keine Personen identifizierenden Informationen (PII) erfasst.**

   Die Dienste von sozialen Netzwerken sind das Lockmittel, die privaten Daten der Preis. Es geht darum, das Verhalten der Massen zu berechnen. Statistisches Rechnen des E-Commerce, auch unter den Namen *Data Mining* oder *Business Intelligence* bekannt, braucht diese Exaktheit und Nutzung von PII nicht, um Profile abzuleiten.

3. **Mitteilung und Optionen zur Wahl sind die Grundpfeiler des Datenschutzes.**

   Die Annahme dieses *Mythos* ist, dass man zum Erhebungszeitpunkt erfährt, was mit den Daten in einem sich ändernden Kontext gemacht werden kann (Optionen). Die Nutzer entscheiden sich überwiegend aus Bequemlichkeitsgründen, bzw. aus kurzfristigen Optimierungsgründen heraus für die Weitergabe persönlicher Daten.

4. **Datenschutz ist eine Sache über Individuen.**

   Das Credo zur Privatheit in Europa heißt, dass jeder in die Lage versetzt werden solle, sich um den Schutz und die Herausgabe persönlicher Daten selbst zu kümmern, und dass ihm dazu auch die nötigen Mittel zur Verfügung gestellt werden, damit diese Freiheit *gelebt* werden kann. Dennoch, nicht einmal die Banken können die Folgen kalkulieren, wie beispielsweise der Fall *Kerviel* bei der Bank National de Paris gezeigt hat [26]. Informationelle Selbstbestimmung überfordert gegenwärtig die Nutzer, und es ist zu befürchten, dass dieser Trend sich verstärkt.

Datenschutz: Datenverfügbarkeit und Eigentum

Datenschutz ist ein ambivalentes Ziel. Er hat einen zuvorderst regulatorischen Ansatz und meint dennoch individuelle Freiheit, eben auch in der Vernachlässigung des Datenschutzes. Solche Konflikte jedoch könnten über eine quantifizierte Wertzuordnung aufgelöst werden. Zum einen muss man dazu zur Einsicht gelangen, dass die Datenanbieter, also Nutzer am besten dadurch geschützt werden, dass dem Datenkonsumenten Transparenz auferlegt wird, die als Grundlage zur Zahlung einer Lizenzgebühr an den Datenanbieter dient. Danach – so ist die Hoffnung – wird sich das Verhalten des Datenanbieters zu Gunsten der Privatheit verändern. Die Vorstellung, ohne soziale und wirtschaftliche Kosten zu einem freibestimmten *Opt-out* zu gelangen, ist über Regulierung nicht erreichbar.

Anmerkungen

1 *Accorsi. R.: A secure log architecture to support remote auditing. Mathematical and Computer Modelling, Elsevier, doi:10.1016/j. mcm.2012.06.35, 2012.*

2 *Ackerman, M., Cranor, L., & Reagle, J. (1999). Privacy in e-commerce: examining user scenarios and privacy preferences. Proceedings of the 1st ACM conference on Electronic commerce.*

3 *Acquisti, A. (2009). Nudging Privacy The Behavioral Economics of Personal Information. IEEE Security & Privacy Vol 7 No. 6 , S. 72-75.*

4 *Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing and privacy on the Facebook. PET 2006.*

5 *Acquisti, A., & Grossklags, J. (2003). Losses, gains and hyperbolic discounting: An experimental approach to information security attitudes and behaviour. 2nd Annual Workshop on Economics and Information Security.*

6 *Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in E-Commerce: Stated Preferences vs. Actual Behaviour. Communications of the ACM Vol. 48 No. 4, S. 101-106.*

7 *Beresford, A., Kübler, D., & Preibusch, S. (2010). Unwillingness to Pay for Privacy: A Field Experiment. IZA Discussion Paper No. 5017.*

8 *Culnan, M., & Armstrong, P. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science Vol. 10 No. 10 , S. 104-115.*

9 *Dolev, A., Yao, A.C (1983). On the Security of Public Key Protocols. IEEE Transactions on Information Theory 2(29), IEEE Press, 198—208, 1983.*

10 *Grossklags, J., & Acquisti, A. (2007). When 25 Cent is too much: An experiment on willingness-to-sell and willingness-to-protect personal information. Proceedings of the 6th Workshop on the Economics of Information Security (WEIS) .*

11 *Haas, S. Wohlgemuth, S., Echizen,I., Sonehara, N., Müller G. (2011). Aspects of Privacy for Electronic Health Records. Int. Journal of Medical Informatics, Special Issue: Security in Health Information Systems 80(2), Elsevier, e26-e31, 2011.*

12 *Harris, L. a. (1990-1994). Harris-Equifax Consumer Privacy Surveys, 1990-1994. Atlanta, GA: Equifax, Inc.*

13 *Kaiser, J. (2003). Besteht eine Beziehung zwischen Nutzbarkeit und Sicherheit? Praxis der Informationsverarbeitung und Kommunikation Vol. 26 No. 1 , S. 48-51.*

14 *Kaiser, J., & Reichenbach, M. (2002). Evaluating security tools towards usable security. Proceedings of the IFIP 17th World Computer Congress – TC13 Stream on Usability: Gaining a Competitive Edge.*

15 *Kumaraguru, P., & Cranor, L. (2005). Privacy Indexes: A Survey of Westin's Studies. ISRI Technical Report.*

16 *Maydorn, D. (2014). Daten sind das Öl des 21. Jahrhunderts, www. deraktionaer.de, http://www.shs-viveon.com / abgerufen 31.1.2014*

17 *Miller, R., Poscher, R. (2013) Informationelle Selbstbestimmung in Europa und Deutschland, in: FAZ, Nr. 278, S. 7.*

18 *Müller G., Rannenberg, K. (eds.) (1999). Multilateral Security in Communications – Technology, Infrastructure, Economy. Addison-Wesley, 1999.*

19 *Müller, G., et.al. (2003). Telematik und Kommunikationssysteme in der vernetzten Wirtschaft, München 2003.*

20 *Müller, G. (2014). Mythen der Privatheitsmechanismen, Vortrag anlässlich der Verleihung des Dr. h.c. an der TU Darmstadt http://www. telematik.uni-freiburg.de/ehrungen (1.2.2014).*

21 *Müller, G., Flender, C., Peters M. (2012). Vertrauensinfrastruktur und Privatheit als ökonomische Fragestellung, in Buchmann J. (Hrsg.), Internet Privacy: Eine multidisziplinäre Bestandsaufnahme (Acatech Studie), September 2012, Springer Verlag 2012, S. 143-183.*

22 *Müller, G., Wahlster, W. (2013). Placing Humans in the Feedback Loop of Social Infrastructures, in. Informatik Spektrum, 36-6-2013.*

23 *Sayre, S., Horne, D. (2000). Trading Secrets for Savings: How concerned are Consumers about Club Cards as a Privacy Threat? Advances in Consumer Research Vol 27 , S. 151-155.*

24 *Smith, H., Milberg, S., Burke, S. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. MIS Quarterly Vol. 20 No. 2 , S. 167-196.*

25 *Whitten, A., & Tygar, J. (1999). Why Johnny Can`t Encrypt: A Usability Evaluation of PGP 5.0. Proceedings of the 8th USENIX Secutity Symposium.*

26 *http://www.bfmtv.com/actualite/laffaire-jerome-kerviel/ abgerufen 1.2.2014*

Sebastian Schweda

„Das Imperium schlägt zurück“

Zur Lage der Menschenrechte im digitalen Zeitalter

Dieser Beitrag basiert auf meinem Vortrag auf der FIfF-Jahrestagung, berücksichtigt aber auch neuere Entwicklungen. Er gibt meine persönliche Meinung wieder, die nicht notwendigerweise mit der Position von Amnesty International *übereinstimmen muss.*

„Mir ist nicht bekannt, dass ich abgehört werde.“
„Ich warte da lieber ab.“
„Es ist nicht meine Aufgabe, mich in die Details von PRISM einzuarbeiten.“

Zitate, die so manchem die Zornesröte ob der Untätigkeit der Bundesregierung im *NSA*-Spähskandal ins Gesicht getrieben haben. Es waren die Worte Angela Merkels im Sommer des vergangenen Jahres, als immer weitere Details zu den Überwachungsprogrammen der US-amerikanischen und britischen Geheimdienste *NSA* und *GCHQ* bekannt wurden. Die Kanzlerin, so die Botschaft, sieht keinen Handlungsbedarf.

Foto: Benjamin Kees

Im Oktober dann plötzlich ganz andere Töne: „Ausspähen unter Freunden, das geht gar nicht.“ Die Kanzlerin spricht von einem „gravierenden Vertrauensbruch“, die Überwachung sei „völlig inakzeptabel“ und müsse unverzüglich unterbunden werden. Botschafter werden einbestellt (im Fall der USA) oder jedenfalls *zum Gespräch geladen* (im Fall des Vereinigten Königreichs). Die Minister, die zuvor noch tönten, Sicherheit sei ein „Supergrundrecht“ und „Die Vorwürfe sind vom Tisch“, fordern auf einmal eine Entschuldigung der USA, misstrauen allen früheren Zusicherungen der *amerikanischen Freunde* und versprechen eine lückenlose Aufklärung aller Vorwürfe. Das politische Berlin ist in Aufruhr.

Was war passiert? Ein Handy wurde abgehört. Nichts Neues? Doch. Denn es war das Handy der Bundeskanzlerin. Die Frage, weshalb das Menschenrecht auf Privatleben der Bundeskanzlerin soviel wichtiger und dringlicher sein soll als das der übrigen Menschen in Deutschland, blieb bei alledem unbeantwortet.

Das Online-Satiremagazin *Der Postillon* titelte: *„Innenminister Friedrich erklärt Abhörsicherheit von Kanzlerinnenhandy zum Superdupergrundrecht“*[1] – vor dem das Supergrundrecht auf Sicherheit natürlich zurücktreten muss. Und: *„Angela Merkel empört, dass sie von USA behandelt wird, als wäre sie ein deutscher Bürger“*.[2] Regierungssprecher *Seibert* wurde in dem Artikel der Satz in den Mund gelegt: *„Sie fragt sich sogar, wozu sie eigentlich Kanzlerin geworden ist, wenn ihre Privatsphäre genauso mit Füßen getreten wird wie die ihrer Wähler.“*

Galgenhumor ist eine gesunde, aber nicht unbedingt die effektivste Strategie, dem Spähskandal und den Reaktionen der deutschen Politik zu begegnen. Denn es geht bei den Enthüllungen um die Zukunft eines Menschenrechts, das schon lange angezählt war, und im jetzigen Umfeld um seine nackte Existenz bangen muss.

Menschenrechte im digitalen Zeitalter

Die Geschichte der Menschenrechte im Umfeld der IKT ist ambivalent.

Einerseits hat die Digitalisierung die Wahrnehmung von Menschenrechten vereinfacht, die Menschenrechtsarbeit effizienter gemacht:

> *„2010 wird möglicherweise als ein Jahr der Zeitenwende in die Geschichte der Menschenrechte eingehen: Menschenrechtsverteidiger und Journalisten bedienten sich zunehmend neuer Technologien, um die Mächtigen mit der Wahrheit zu konfrontieren und auf diese Weise auf eine stärkere Einhaltung der Menschenrechte zu dringen. Es war auch das Jahr, in dem einige repressive Regierungen damit rechnen mussten, dass ihre Tage gezählt sind.“*[3] (Salil Shetty, Generalsekretär von *Amnesty International*, am Anfang des Amnesty Reports 2011)

Es war die Zeit der – zunächst friedlichen – Revolutionen in zahlreichen arabischen Ländern. Tunesien, Ägypten, Libyen, Bahrain, Syrien: Überall manifestierte sich Widerstand auf der Straße. Doch woher kam er? Die klassischen Medien berichteten kaum unabhängig. Wie konnten sich die Menschen so schnell organisieren? Die Machthaber waren überrascht von der Geschwindigkeit, mit der sich die Proteste verbreiteten. Zunächst schien alles nach Plan zu laufen: Eine Regierung nach der anderen stürzte. Das Internet hatte daran einen wesentlichen Anteil: Einfache Bürger konnten etwa in Blogs mit der Weltöffentlichkeit kommunizieren, in sozialen Netzwerken Aktivitäten planen und rechtswidriges Handeln der Konfliktparteien durch selbstgedrehte Clips auf Video-Plattformen belegen. Repressive Maßnahmen wie die zeitweise Kappung der Internet- und Mobilfunkanbindung Ägyptens konnten die Proteste nicht dauerhaft behindern – auch dank der Hilfe von Aktivisten aus dem Ausland, die alternative Kommunikationswege bereitstellten.

2010 war auch das Jahr von *WikiLeaks*: Die Enthüllungsplattform veröffentlichte binnen weniger Monate Hunderttausende Dokumente, die erstmals Menschenrechtsverletzungen und Verstöße gegen humanitäres Völkerrecht in den Kriegen in Afghanistan und im Irak belegten. Die US-Botschaftsdepeschen zeigten, wie wenig einigen westlichen Regierungen an Veränderung in den arabischen Staaten gelegen war, obwohl sie von den repressiven Methoden der dortigen Regierungen wussten.

Die Ereignisse vermittelten eine neue Hoffnung: dass das Internet die Kräfteverteilung nachhaltig zugunsten der Menschenrechte und ihrer Verteidiger verändern könnte.

Drei Jahre später scheint diese Hoffnung vergebens – die andere Lehre, die wir aus der technischen Entwicklung für die Menschenrechte ziehen müssen: *Julian Assange,* der Gründer von *WikiLeaks*, sitzt im ecuadorianischen Botschaftsasyl. Er befürchtet, das Strafverfahren in Schweden wegen Sexualdelikten diene als Vorwand, ihn wegen seiner Tätigkeit für *WikiLeaks* an die USA auszuliefern. *Chelsea Manning,* die *WikiLeaks* einen Großteil des oben beschriebenen Materials zur Verfügung gestellt hatte, war in den USA nach ihrer Festnahme zunächst zu Bedingungen inhaftiert, die nach Ansicht von *Amnesty* internationale Standards für die menschliche Behandlung von Untersuchungshäftlingen verletzten. Im August 2013 wurde sie von einem US-Militärgericht zu einer Freiheitsstrafe von 35 Jahren verurteilt, wegen der Weitergabe von eingestuften Dokumenten und der Übergabe von Informationen über die nationale Verteidigung an nicht autorisierte Quellen. *Amnesty* hat sich mittlerweile für die Begnadigung *Mannings* ausgesprochen. Statt ein Exempel an ihr zu statuieren, solle die US-Regierung Menschenrechtsverletzungen im Zusammenhang mit ihrem *Krieg gegen Terror* untersuchen.[4]

Auch die Revolutionen des *Arabischen Frühlings* sind in vielen dieser Staaten – wie Ägypten oder Libyen – von schweren Rückschlägen bedroht. In Syrien haben sie zu einem jahrelangen Bürgerkrieg mit beiderseitigen Menschenrechtsverletzungen zwischen Regierungstruppen und einer zunehmend diffusen Gegenseite geführt, deren einziges gemeinsames Ziel der Sturz Assads zu sein scheint.

Die Enthüllungen *Edward Snowdens* schließlich zeigen, dass nicht nur bekannt repressive Regierungen wie die chinesische – die *ihren Teil* des Internet mit Hilfe der *Great Firewall of China* von kritischen Meinungsäußerungen freizuhalten sucht – die neuen Freiheiten der Menschen einschränken.

Wie sind diese Enthüllungen aus menschenrechtlicher Sicht zu bewerten, und welchen Schutz genießt der Enthüller?

Das verschwundene Menschenrecht

In einer Resolution vom 5. Juli 2012 stellte der UN-Menschenrechtsrat fest, was vor dem Hintergrund der Universalität der Menschenrechte selbstverständlich sein sollte, aber offenbar einer Bekräftigung in diesem Gremium bedurfte: dass *„die gleichen Rechte, die Menschen offline haben, auch online geschützt werden müssen"*.[5] Dies gelte insbesondere für das Recht auf freie Meinungsäußerung, aber auch für die übrigen Menschenrechte.

Heute dürfte kein vernünftiger Zweifel daran bestehen, dass die Massenüberwachungsprogramme der *NSA* und des *GCHQ* – insbesondere *PRISM,* die *Upstream*-Programme, *Muscular* und *Tempora* –, jedenfalls so, wie sie in den Unterlagen *Snowdens* erscheinen, massiv eingreifen in das Menschenrecht auf Schutz des Privatlebens, wie es unter anderem in Artikel 12 der Allgemeinen Erklärung der Menschenrechte und Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte garantiert ist. Ein umfassenderer Eingriff als die nahezu vollständige Aufhebung des Privaten im Bereich der Telekommunikation erscheint kaum vorstellbar.

Wie jedes Menschenrecht ist auch das Recht auf Schutz des Privatlebens nicht schrankenlos gewährleistet. Voraussetzung für einen rechtmäßigen Eingriff ist eine gesetzliche Grundlage, mit der ein legitimer Zweck verfolgt wird, zu dem die gewählte Maßnahme nicht außer Verhältnis steht. Bei einigen bekannt gewordenen Programmen ist die gesetzliche Grundlage zweifelhaft; sie basieren teils auf einer eigenwillig weiten Interpretation des *FISA Amendment Act 2008,* die die Grenzen der Auslegung zu überschreiten scheint. Auch daran, dass der Zweck in allen Fällen ein legitimer ist, sind Zweifel angebracht. Mit nationaler Sicherheit oder dem Krieg gegen den Terror lassen sich die Bespitzelungen von diplomatischen Vertretungen und Unternehmen oder die Überwachung des Kanzlerinnenhandys kaum begründen.

Ganz sicher wird eine Rechtfertigung zumindest der Massenüberwachungsprogramme an der Verhältnismäßigkeitsprüfung scheitern. Die unterschiedslose Speicherung und Analyse sämtlicher Kommunikation, derer ein Nachrichtendienst mit seinen technischen Mitteln habhaft werden kann, ohne effektives rechtsstaatliches Verfahren, zeigt, dass hier keine ernsthafte Abwägung der beteiligten Interessen stattgefunden hat. Statt dessen wurde durch die Enthüllungen offenbar, dass die US-amerikanische und die britische Regierung nationalen Sicherheitsinteressen im Bereich der Telekommunikation absoluten Vorrang eingeräumt haben gegenüber einem Menschenrecht, dessen Bedeutung für die Würde und die Identität des Einzelnen im digitalen Zeitalter kaum überschätzt werden kann.

In einer von Brasilien und Deutschland initiierten, einstimmig verabschiedeten Resolution der UN-Generalversammlung[6] werden die Staaten aufgefordert, das Recht auf Privatleben zu achten und Verletzungen zu beenden, ihre Überwachungsmaßnahmen auf die Vereinbarkeit mit diesem Recht zu überprüfen und eine unabhängige Aufsicht über diese Maßnahmen sicherzustellen. Die gleichzeitige Bitte an die UN-Hochkommissarin für Menschenrechte, bis zum kommenden Herbst einen Bericht über die Lage des Menschenrechts auf Privatleben im Kontext staatlicher Kommunikationsüberwachung und -datensammlung vorzulegen, wird dafür sorgen, dass das Thema auf der internationalen Agenda bleibt.

Amnesty hat Menschenrechtsbeschwerde vor dem britischen *Investigatory Powers Tribunal* erhoben.[7] Sie richtet sich gegen das Überwachungsprogramm *Tempora* des *GCHQ* und dessen unzureichende Regulierung sowie gegen die Nutzung von *NSA*-Daten aus *PRISM* und den *Upstream*-Programmen durch das Vereinigte Königreich. Das Verfahren läuft parallel zu einer ähnlich lautenden Beschwerde mehrerer Organisationen vor dem *Europäischen Gerichtshof für Menschenrechte (EGMR)* in Straßburg.[8]

Beide Verfahren machen neben einer Verletzung des Rechts auf Privatheit auch einen Verstoß gegen das Recht auf Meinungsfreiheit geltend. Welch abschreckende Wirkung *(chilling effect)* das Wissen um eine Überwachung des eigenen Handelns auf die Wahrnehmung dieses Rechts haben kann, hat erst kürzlich eine Umfrage des Schriftstellerverbandes *PEN America* gezeigt: 24 % der befragten Schriftsteller vermieden es als Folge der *Snowden*-Enthüllungen, bestimmte Themen in Telefongesprächen oder E-Mails anzusprechen; weitere neun Prozent dächten ernsthaft darüber nach.[9]

Schutz als Whistleblower?

Die öffentliche Bekanntgabe von Staatsgeheimnissen muss nicht zwangsläufig von der Meinungs- und Informationsfreiheit gedeckt sein. So ist anerkannt, dass nationale Sicherheitsinteressen einer Veröffentlichung im Einzelfall entgegenstehen können. Das bedeutet indes nicht, dass Staaten diesen Einschränkungsgrund missbrauchen dürfen, um die Veröffentlichung unliebsamer oder für sie unangenehmer Informationen zu verhindern. Geht es um Missstände, deren Bekanntgabe im öffentlichen Interesse liegt, wird eine Abwägung oft zugunsten der Veröffentlichung ausfallen, zumal wenn die aufgedeckten Handlungen gegen geltendes Recht verstoßen. In keinem Fall sollten Menschen dafür verfolgt werden, dass sie Informationen ans Licht bringen, die Menschenrechtsverletzungen belegen.

Die Rechtsprechung internationaler Gerichte zum *Whistleblower*-Schutz ist bislang dürftig. Der EGMR stützt die Beurteilung der Verhältnismäßigkeit einer Veröffentlichung interner Informationen (und damit die Frage, ob ein Verstoß gegen das Recht auf Meinungs- und Informationsfreiheit vorliegt) auf eine Reihe von Faktoren, die gegeneinander abzuwägen seien. Dazu zählen die Frage, ob alternative Wege bestanden und genutzt wurden, die Informationen bekannt zu machen (etwa auf dem internen Weg), das öffentliche Interesse an der Information, ihre Glaubwürdigkeit, der Schaden, den die staatliche Behörde durch die Veröffentlichung erleidet, und das Motiv des Whistleblowers. Aber auch die Schwere der gegen den Whistleblower verhängten Strafe kann eine Rolle spielen.[10]

All diese Kriterien scheinen für *Snowden* zu sprechen: Zumindest nach eigener Aussage hat er sich vor dem Gang an die Öffentlichkeit erfolglos an Vorgesetzte gewandt. An der Aufdeckung von Menschenrechtsverletzungen dürfte immer ein überragendes öffentliches Interesse bestehen, da es hier um gravierende Fehlentwicklungen und Völkerrechtsverstöße geht, so dass auch ein möglicher Schaden für den Staat im Verhältnis dazu in aller Regel zurücktreten muss. Die Authentizität der Informationen lässt sich angesichts der Menge und Detailgenauigkeit kaum bezweifeln. Ihr wurde auch von staatlichen Stellen bisher nicht grundsätzlich widersprochen. *Snowdens* Motivlage lässt die Anklageschrift[11] durchscheinen: Die Tatsache, dass *Snowden* nicht die „Übermittlung von Verteidigungsinformationen zum Nutzen einer ausländischen Regierung" (18 U.S.C. § 794(a)) vorgeworfen wird, zeigt, dass zur Zeit nicht einmal die Strafverfolger davon ausgehen, dass *Snowden* dem Feind helfen wollte. (Dieser Tatbestand setzt voraus, dass der Täter in der Absicht oder begründeten Annahme gehandelt hat, die Informationen könnten zum Schaden der USA oder zum Vorteil eines anderen Staates verwendet werden.) *Snowden* selbst hat eine entsprechende Motivation stets bestritten, seine bisherige Veröffentlichungsstrategie stützt dies.

Artikel 8
Recht auf Achtung des Privat- und Familienlebens

(1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

(2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

Artikel 10
Freiheit der Meinungsäußerung

(1) Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben. Dieser Artikel hindert die Staaten nicht, für Hörfunk-, Fernseh- oder Kinounternehmen eine Genehmigung vorzuschreiben.

(2) Die Ausübung dieser Freiheiten ist mit Pflichten und Verantwortung verbunden; sie kann daher Formvorschriften, Bedingungen, Einschränkungen oder Strafdrohungen unterworfen werden, die gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sind für die nationale Sicherheit, die territoriale Unversehrtheit oder die öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung oder zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral, zum Schutz des guten Rufes oder der Rechte anderer, zur Verhinderung der Verbreitung vertraulicher Informationen oder zur Wahrung der Autorität und der Unparteilichkeit der Rechtsprechung.

Europäische Menschenrechtskonvention

Amnesty hat nach den ersten Berichten über die *NSA*-Dokumente betont, dass die Veröffentlichung von Informationen über Menschenrechtsverletzungen vom Recht auf Meinungsfreiheit geschützt sind, und dass ein Gerichtsverfahren gegen *Snowden* wegen dieser Enthüllungen politischer Verfolgung gleichkäme. Er dürfe nicht an die USA ausgeliefert werden, da er dort dem Risiko unmenschlicher Behandlung in Haft ausgesetzt wäre (wie der Fall *Manning* belegt). Auch dass er sich nach dem US-Spionagegesetz im Verfahren nicht auf das öffentliche Interesse berufen dürfe, sei ein Auslieferungshindernis. Daneben werde sein Recht auf Bewegungsfreiheit und sein Recht, Asyl zu beantragen, durch die Ungültigerklärung seines Reisepasses verletzt.[12]

Nichts zu verbergen?

„Wer nichts zu verbergen hat, hat auch nichts zu befürchten" – so lautet ein gängiges Argument von Sicherheitspolitikern, mit dem Bedenken gegen den Totalüberwachungsansatz hinter den Aktivitäten von *NSA* und *GCHQ* zerstreut werden sol-

len.[13] Auf die damit unterschwellig formulierte Frage beeilen sich auch hierzulande solchermaßen beruhigte Bürger zu versichern: „Ich habe nichts zu verbergen." Können solche erzwungenen (Selbst-)Beschwichtigungen der Maßstab in einer freiheitlichen Gesellschaft sein, die sich den Menschenrechten verpflichtet fühlt? Kann der Fortbestand von grundlegenden Rechten davon abhängig gemacht werden, ob der Einzelne durch ihre Beseitigung etwas zu befürchten hat?

Selbst für den abwegigen Fall, dass wir alle tatsächlich nichts zu verbergen hätten: Wer kann heute sagen, dass das auch morgen noch gilt? Wer kann sagen, dass die Daten, die sie oder er heute preisgibt, nicht morgen gegen sie oder ihn verwendet werden? Wer kann sagen, was die heute preisgegebenen Daten in Verbindung mit den morgen preisgegebenen Daten übermorgen vielleicht einmal über sie oder ihn aussagen werden?

Ein Staat, der im Geheimen abhorcht, was ihn nichts angeht, ohne wirksam von Gerichten oder vom Parlament kontrolliert zu werden, der ist schon heute keine Demokratie mehr. Was wird er morgen sein? Und wie werden die Daten vielleicht schon heute in diesen „postdemokratischen Zuständen",[14] wie *Hans Magnus Enzensberger* es ausdrückt, gegen die Betroffenen verwendet? Wir werden das ganze Ausmaß wohl nie erfahren.

Erste Bedenken sind aber angebracht, wenn der deutsche Schriftsteller *Ilja Trojanow,* über den nicht bekannt ist, dass er sich irgendwelcher terroristischen Umtriebe verdächtig gemacht hat, der sich nichts zuschulden hat kommen lassen, außer sich kritisch über die Überwachungsaktivitäten der *NSA* zu äußern, trotz Visum ohne Angabe von Gründen nicht mehr in die USA einreisen darf.[15] Alarmiert sollte man sein, wenn Menschen aus Drittstaaten die Einreise in die USA verweigert wird, weil den US-Zoll- und Grenzschutzbehörden Gesundheitsinformationen vorlägen, die auf eine psychische Erkrankung hinwiesen.[16]

Nichts zu verbergen? So einfach ist es eben nicht. Für eine Woche, für ein Jahr, vielleicht für immer wird in großen Datensilos das Leben von Milliarden Menschen aufgezeichnet und analysiert, um es ihnen bei Bedarf vorhalten zu können. Jedenfalls dann, wenn sie sich in einem der Staaten aufhalten, die diese Überwachungsprogramme betreiben, oder dort einreisen wollen. Oder in ein Land, das mit diesen Staaten Daten austauscht – wie nach den Unterlagen von *Snowden* wohl die Mehrheit der EU-Mitgliedstaaten.

Vielleicht aber ist selbst das nicht einmal notwendig.

Wie ein Amnesty-Bericht vom Oktober 2013 belegt, führen die USA in einem strikt geheimgehaltenen Drohnenprogramm extralegale Hinrichtungen in pakistanischem Stammesgebiet durch.[17] Der Bericht untersucht neun der insgesamt 45 Drohnenangriffe, die die USA in der Zeit zwischen Januar 2012 und August 2013 in Pakistan durchgeführt haben und die zu zahlreichen zivilen Opfern geführt haben. Besonders verwerflich erscheinen dabei einerseits *secondary strikes* oder *rescuer attacks*, die sich gegen diejenigen zu richten scheinen, die Opfern vorangegangener Drohnenangriffe zu Hilfe eilen. Angriffe werden auch gegen Personen unbekannter Identität geflogen, deren Verhalten den die Stammesgebiete überwachenden US-Sicherheitsbehörden verdächtig erscheint *(signature strikes).* Doch auch in den übrigen Fällen außergerichtlicher Tötungen durch Drohnen operieren die USA nach Ansicht von *Amnesty* an menschenrechtlichen Standards und am Völkerrecht vorbei und begehen dabei unter Umständen sogar Kriegsverbrechen. Wie Berichte belegen, ist Pakistan nicht das einzige Land, in dem US-Kampfdrohnen Angriffe fliegen: Auch im Jemen oder in Somalia finden solche völkerrechtswidrigen Tötungen statt.[18] Die Daten für die Identifizierung und Lokalisierung der Zielpersonen stammen dabei häufig aus den Datenspeichern der *NSA* und *GCHQ*. Deren Personenprofile können direkt für Drohnenangriffe gegen den Betroffenen genutzt werden.[19] Auch der BND soll in mindestens einem Fall Telefondaten an die USA weitergegeben haben, die zur Tötung eines deutschen Staatsbürgers in Waziristan führten.[20]

Speicherung und Analyse der personenbezogenen Daten durch die Nachrichtendienste dienen zudem nicht nur dem Kampf gegen Terrorismus und organisierte Kriminalität, sondern auch dem *Cyberwar* um die Kontrolle über Gesellschaften und die Sicherung staatlicher Hegemonialstellungen.[21] Seitdem 2007 ein ganzes Land – Estland – lahmgelegt wurde, basteln die Militärstrategen an immer ausgefeilteren Cyber-Waffen, von denen *Stuxnet* die bekannteste sein dürfte.[22] Die Überwachungsprogramme der *Five Eyes*-Staaten und ihrer Partner verschaffen den Diensten dabei einen Informationsvorsprung, mit dem sie gesellschaftliche Entwicklungen weltweit früher als andere erkennen und im eigenen Sinne steuern können.

Carl von Clausewitz würde seinen bekannten Ausspruch vom *Krieg als Fortsetzung der Politik mit anderen Mitteln* heute vielleicht ergänzen um einen weiteren Satz: Cyberwar ist die Fortführung des kinetischen Kriegs mit anderen Mitteln. Der Kollateralschaden dieses virtuellen Krieges mit realen Folgen ist die weitgehende Vernichtung der unkörperlichen Integrität des Einzelnen: seiner Privatsphäre.

Kooperation ist wichtig!

Tim Berners-Lee, der Erfinder des World Wide Web, wandte sich im Sommer 2013 an alle Amnesty-Mitglieder mit den Worten:

> *„I believe we have reached a critical juncture where if we do not unite and fight for our rights to privacy, freedom of information, freedom of association, and freedom of expression in this new digital world, they will be taken away. […] [H]uman rights defenders like Amnesty are critical to win the battle."*[23]

In der deutschen Sektion nähern wir uns diesem Ziel: Die 2012 informell gegründete Arbeitsgruppe *Digital@Amnesty* will die bisherigen Aktivitäten von *Amnesty* zusammentragen, analysieren und eine Strategie für das weitere Vorgehen entwickeln. Mittelfristiges Ziel ist es, den Interessentenkreis zu einer *vollwertigen* Themenkoordinationsgruppe mit dem Fokus *Digitale Technologien und Menschenrechte* auszubauen. Auf dem Weg dahin suchen wir den Austausch mit auf diesem Gebiet bereits seit langem aktiven Bürger- und Menschenrechtsorganisationen wie dem FIfF. Der Spähskandal zeigt, wie eng westliche Geheimdienste in ihrem Bemühen kooperieren, auch ihre eigenen Bürger zu überwachen und zu kontrollieren. Wer diesem massiven Völkerrechtsbruch etwas entgegensetzen will, muss bereit sein,

sich ebenfalls mit Gleichgesinnten zu verbünden. Ich bin zuversichtlich, dass *Amnesty* als globale Bewegung ihren Teil dazu beitragen wird, gemeinsam mit anderen eine internationale Koalition der Verteidiger grundlegender Menschenrechte im digitalen Zeitalter zu bilden, und wünsche mir, dass die bereits geknüpften Kontakte zum FIfF nicht abreißen werden.

Anmerkungen

1 *http://www.der-postillon.com/2013/10/innenminister-friedrich-erklart.html*
2 *http://www.der-postillon.com/2013/10/angela-merkel-empört-dass-sie-von-usa.html*
3 *Amnesty International Report 2011: Zur weltweiten Lage der Menschenrechte, S. 7.*
4 *Amnesty International, USA: Commute Bradley Manning's sentence and investigate the abuses he exposed, 21.8.2013, https://www.amnesty.org/en/news/usa-commute-bradley-manning-s-sentence-and-investigate-abuses-he-exposed-2013-08-21*
5 *UN Human Rights Council, Resolution: The promotion, protection and enjoyment of human rights on the Internet, A/HRC/20/L.13, 29.6.2012 (angenommen am 5.7.2012), http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement*
6 *UN General Assembly, Resolution: The right to privacy in the digital age, A/RES/68/167, abgedruckt in A/68/456/Add.2, 10.12.2013 (angenommen am 18.12.2013), https://www.un.org/ga/search/view_doc.asp?symbol=A/68/456/Add.2, S. 139 f.*
7 *Amnesty International, Amnesty International brings claim against UK over state surveillance, 9.12.2013, https://www.amnesty.org/en/for-media/press-releases/amnesty-international-brings-claim-against-uk-over-state-surveillance-2013-*
8 *Beschwerdeführer in dem EGMR-Verfahren sind Big Brother Watch, English PEN, Open Government Partnership, und Constanze Kurz vom CCC; https://www.privacynotprism.org.uk/news/2013/10/03/gchq-to-face-european-court-over-mass-surveillance/*
9 *PEN America, Chilling effects: NSA Surveillance Drives U.S. Writers to Self-Censor, 12.11.2013, http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf*
10 *So etwa in: EGMR, Guja gegen Moldawien, Appl. No. 14277/04, Urteil vom 12.2.2008, §§ 73 ff., http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-85016*
11 *US District Court for the Eastern District of Virginia, USA v. Edward J. Snowden, Criminal Complaint, Case No. 1:13 CR 265 (CMH), 14.6.2013, http://s3.documentcloud.org/documents/716865/snowden-complaint.pdf*
12 *Amnesty International, USA must not persecute whistleblower Edward Snowden , 2.7.2013, https://www.amnesty.org/en/news/usa-must-not-persecute-whistleblower-edward-snowden-2013-07-02*
13 *Vgl. den britischen Außenminister William Hague wenige Tage nach der Veröffentlichung der ersten Snowden-Dokumente: https://www.youtube.com/watch?v=lWam4EWI48M*
14 *http://www.daserste.de/information/wissen-kultur/ttt/sendung/hr/sendung_vom_18082013-102.html*
15 *Spiegel Online, NSA-Kritiker Ilija Trojanow: Deutscher Schriftsteller darf nicht in die USA einreisen, 1.10.2013, http://www.spiegel.de/kultur/gesellschaft/ilija-trojanow-nach-nsa-protest-einreise-in-die-usa-verweigert-a-925467.html*
16 *Disabled woman denied entry to U.S. after agent cites supposedly private medical details, 28.11.2013, http://www.thestar.com/news/gta/2013/11/28/disabled_woman_denied_entry_to_us_after_agent_cites_supposedly_private_medical_details.html*
17 *Amnesty International, Will I Be Next? US Drone Strikes in Pakistan, 2013, http://www.amnesty.org/en/library/asset/ASA33/013/2013/en/041c08cb-fb54-47b3-b3fe-a72c9169e487/asa330132013en.pdf. Auf der englischsprachigen Sonderseite zum Bericht, http://dronespakistan.amnesty.org, hat Amnesty International Satellitenbilder, Videos und ausführliche Hintergrundinformationen zusammengestellt.*
18 *Vgl. „Schmutzige Kriege", ARD-Dokumentation, gesendet im Programm Das Erste am 28.11.2013. Siehe auch den Bericht zur Geolokalisierung von Angriffszielen für Drohnenangriffe von CIA und JSOC, einer Kommandoeinheit der US-Armee, durch Handy-Metadaten aus dem NSA-Datenbestand: Jeremy Scahill/Glenn Greenwald, The NSA's Secret Role in the U.S. Assassination Program, 10.2.2014, https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role/*
19 *Greg Miller/Julie Tate/Barton Gellman, Documents reveal NSA's extensive involvement in targeted killing program, 17.10.2013, http://www.washingtonpost.com/world/national-security/documents-reveal-nsas-extensive-involvement-in-targeted-killing-program/2013/10/16/29775278-3674-11e3-8a0e-4e2cf80831fc_story.html*
20 *Stefan Bucher/Hans Leyendecker, Unmut über BND-Chef Schindler, 10.8.2013, http://www.sueddeutsche.de/politik/kooperation-mit-us-geheimdiensten-unmut-ueber-bnd-chef-schindler-1.1743505*
21 *So auch „World Wide War: Der geheime Kampf um die Daten", ZDF Zoom, Sendung vom 9.10.2013.*
22 *Vgl. die Veröffentlichungen zu den Aktivitäten der NSA-Abteilung Tailored Access Operations (TAO) u. a. in: Inside TAO: Documents Reveal Top NSA Hacking Unit, Spiegel Online, 29.12.2013, http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html; Jacob Appelbaum/Judith Horchert/Christian Stöcker, Shopping for Spy Gear: Catalog Advertises NSA Toolbox, Spiegel Online, 29.12.2013, www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html*
23 *http://amnestyicm2013.wordpress.com/2013/08/22/the-greatest-threat-to-the-future-of-the-internet/*

Sebastian Schweda

Sebastian Schweda ist Rechtsanwalt mit Schwerpunkten im Datenschutz-, Telekommunikations- und Medienrecht und seit 2007 am Institut für Europäisches Medienrecht (EMR) in Saarbrücken tätig. Er ist aktives Mitglied bei Amnesty International und arbeitet derzeit am Aufbau einer neuen Koordinationsgruppe zum Themenkreis *Digitale Technologien und Menschenrechte* innerhalb der deutschen Sektion von Amnesty International. Die Gruppe ist erreichbar unter: *digital@amnesty.de*.

Rainer Rehak

Die Grenzen des Systems sind die Grenzen der Person

Die Infrastruktur unserer digitalen Welt wird ganz bewusst unsicher, extern zugreifbar und flächendeckend überwacht gestaltet. Dieser Umstand betrifft Privatpersonen genauso wie Behörden, Unternehmen genauso wie andere Organisationen; in Deutschland und weltweit. Wie verträgt sich die aktuelle IT- und Überwachungssituation aber damit, dass das Bundesverfassungsgericht im Jahre 2008 das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme *(IT-Grundrecht) formuliert hat und was muss daraus folgen?*

Im Kontext der Enthüllungen des ehemaligen NSA-Mitarbeiters *Edward Snowden* kam unter anderem ans Tageslicht, dass sicherheitskritische Schwachstellen im weit verbreiteten Betriebssystem *Microsoft Windows* absichtlich von Microsoft geheimgehalten und nicht – oder nur verzögert – behoben werden (Projektname MAPP). Einziger Grund sind die US-amerikanischen Geheimdienste: sie erhalten diese Informationen umgehend, um die offenen Sicherheitslücken für ihre Zwecke ausnutzen zu können. Darüber hinaus werden Verschlüsselungsstandards absichtlich von ihnen abgeschwächt (*Edgehill, Bullrun*), Zertifikate von Technologiefirmen gestohlen und dubios erlangte *Exploits* – also Programme, die Sicherheitslücken eines Computersystems ausnutzen – für alle gängigen Systeme gehortet, um im Zweifelsfall direkt zugreifen zu können (*TAO*). Doch auch intakte und sichere Endsysteme können die allumfassende globale Überwachung der Internet-Infrastruktur an ihren Knotenpunkten und Glasfaserkabeln (*Tempora, Upstream*) sowie direkt in den Rechenzentren großer Internetunternehmen (*PRISM*) nicht verhindern.

Die Deutschen machen mit

Auch die deutschen Geheimdienste freuen sich über derartig erlange Informationen, auf die sie mittels des *XKeyscore* genannten NSA-Suchwerkzeugs zugreifen können, ohne Widerspruch, Kritik oder Bedenken zu äußern. Sie helfen dieser Maschinerie sogar aktiv, indem sie eigene Daten in das Großsystem einfließen lassen und in regem Austausch stehen.[1]

Dabei muss immer erwähnt werden, dass beispielsweise die explizite Ausspähung der deutschen, türkischen, französischen und brasilianischen Regierungen, von UN- und EU-Dependancen, des G20-Gipfels, des Klimagipfels COP15 und der Internationale Atomenergie-Organisation (IAEA) natürlich keiner irgendwie gearteten *Terrorabwehr* dienen sollen.

Die Infrastruktur unserer digitalen Welt wird also ganz bewusst unsicher, extern zugreifbar und flächendeckend überwacht gestaltet.

Sicherlich können die Menschen in Deutschland keinen großen Einfluss auf ausländische Regierungen und anderer Länder Gesetze ausüben, aber das müssen sie auch gar nicht, denn zumindest in Deutschland sind sie – zumindest theoretisch – der Souverän.

Wie verträgt sich aber die aktuelle IT- und Überwachungssituation damit, dass das Bundesverfassungsgericht im Jahre 2008 das Grundrecht auf *Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* (IT-Grundrecht) formuliert hat? Das Grundrecht wurde damals aus dem allgemeinen Persönlichkeitsrecht abgeleitet, weil das Gericht die Bedeutung solcher Systeme für den Menschen und die Gesellschaft erkannte und dem Rechnung tragen wollte.[2]

Die Person im Mittelpunkt

Vertraulichkeit kann man sich technisch etwas vereinfacht als *Leseverbot* und *Integrität* etwa als *Schreibverbot* begreiflich machen, was aber ist mit *informationstechnisches System* gemeint? Das Gericht setzt bei der Definition die *Person* in den Mittelpunkt, die ein technisches System verwendet und mittelbar durch die Gewährleistung der Vertraulichkeit und Integrität geschützt werden soll. Das geschützte System ist also abstrakt und entsteht dadurch, dass es von der nutzenden Person als funktional zusammenhängend wahrgenommen und verwendet wird. Dabei ist es unerheblich, ob technisch gesehen ein Einzelgerät oder vielfach vernetze Rechnerverbünde genutzt werden. Das informationstechnische System einer Person bezeichnet daher die Menge aller Komponenten, die von der Person zur Datenverarbeitung verwendet werden, und dieses System wird grundrechtlich geschützt.

Wenn man also einen E-Mailanbieter nutzt, bei dem E-Mails hauptsächlich über ein Webinterface gelesen und geschrieben werden, sind nicht nur die E-Mails geschützt, sondern der genutzte Rechner, die Internetverbindung bis hin zum Rechenzentrum des E-Mailanbieters und natürlich auch die involvierten Server dort. Gleiches gilt für Online-Adressbücher oder -Kalender. Auch bei der Nutzung verteilter Ordner oder sonstiger Online-Speicherdienste gilt dieser umfassende Schutz durch das Recht auf Gewährleistung der Vertraulichkeit und Integrität. Grundrechtlich geschützt werden folglich nicht konkrete Daten sondern ganze Systeme.

Die übergeordnete Aussage des Urteils lautet demnach, dass die Grenzen des Systems gewissermaßen auch die Grenzen der Person sind. Mit der Verletzung des einen geht immer auch eine Verletzung des anderen einher. Denn nicht die unerwünschte Kenntnisnahme oder Veränderung liegt hier im Fokus – dafür gab es schon Gesetze – sondern der *Kontrollverlust* der Person durch die (unbemerkbare) *Möglichkeit* solcher Verletzungen.

Flächendeckende Verletzung

Alle eingangs erwähnten Programme der Geheimdienste betreffen den Großteil der Deutschen – natürlich auch auf deutschem Boden – und ergeben folglich eine flächendeckende, massive Verletzung des IT-Grundrechts, zumal das Grundrecht sich explizit nicht auf die Vertraulichkeit und Integrität sondern deren Ge-

währleistung – auch gegenüber Dritten – bezieht. Der Staat ist somit sogar explizit in der Bringschuld, wovon seit Jahren noch nirgends etwas zu sehen ist.

Um eine frühere Vorhersage von Prof. *Andreas Pfitzmann* auf die aktuelle Situation anzuwenden: Wir sehen gerade eine Entwicklung, die uns zu „*eine[r] sukzessive[r] Einschränkung und schließlich Auflösung dessen, was wir als Grundwert des Schutzes der Person, ihrer Autonomie, Freiheit und Würde kennen*“ führt.[3]

Nach vorn gedacht – Theorie

Das Bundesverfassungsgericht kann selbst keine Gesetze erlassen oder entwerfen, aber es kann den Gesetzgeber auffordern, etwas zu tun. Dies wird nur mit großer Zurückhaltung praktiziert, weil einerseits die Grundrechte konzeptionell zunächst Abwehrrechte gegen staatliches Wirken sind *(status negativus)* und andererseits die Gewaltenteilung es eigentlich verbietet, dass ein Gericht den Gesetzgeber anweist, bestimmte Regelungen zu treffen.

Allerdings ist es dem Gericht möglich, aus dem *Ermöglichungsaspekt* der Grundrechte *(status positivus)* in gewissem Umfang auch staatliche Handlungspflichten abzuleiten. Die Voraussetzungen und die Reichweite dieser Verpflichtung sind nicht sehr klar. Als Beispiel kann das Grundrecht auf körperliche Unversehrtheit (Art. 2 Abs. 2 GG) dienen: Es ist nicht nur subjektives Abwehrrecht gegen staatliche Eingriffe, denn aus dem objektivrechtlichen Gehalt erwächst auch die staatliche Pflicht, die genannten Rechtsgüter zu schützen und auch zu fördern. Zwar ist dadurch nicht die *Gesundheit* insgesamt geschützt, aber aus den körperlichen Aspekten können Leistungsansprüche für die staatliche Gesundheitsversorgung abgeleitet werden.

Aus der klaren Formulierung, dass das IT-Grundrecht in einer *Gewährleistung* besteht, mag man die Anwendbarkeit des sogenannten Untermaßverbotes annehmen, zu der das Gericht im Jahre 1993 schrieb: „*Der Staat muss zur Erfüllung seiner Schutzpflicht ausreichende Maßnahmen normativer und tatsächlicher Art ergreifen, die dazu führen, dass ein – unter Berücksichtigung entgegenstehender Rechtsgüter – angemessener und als solcher wirksamer Schutz erreichbar wird.*“[4] Vertiefende Ausführungen und die praktische Nutzbarmachung der eben angerissenen Aspekte sind jedoch den Juristen vorbehalten. Diese müssen nun mit Hilfe der Zivilgesellschaft durchdenken und vorantreiben, was Gewährleistung in diesem Kontext bedeuten kann und muss.

Nach vorn gedacht – Praxis

Doch auch ganz praktisch gibt es viele Forderungen, die man im Geiste des Urteils verfolgen muss. Auf politischer Ebene müssen endlich Maßnahmen zur Aufklärung der Sachlage ergriffen werden. Einerseits bezüglich des Ausmaßes der Auswirkungen der bekannt gewordenen Geheimdienstprogramme in Deutschland, andererseits aber auch bezüglich der Mitwirkung deutscher Organe. Insbesondere muss aber die rechtliche Lage geklärt werden, denn es mehren sich die Hinweise, dass seit Jahrzehnten u. a. mit Hilfe von Geheimabkommen und des G10-Gesetzes jegliche Überwachungstätigkeit der USA und Großbritanniens legalisiert wird.[5]

Der Ausbau der *Stiftung Datenschutz* sollte vorangetrieben werden, jedoch zur Abwechslung einmal unter Ausschluss von Lobbyisten und mit fachkundiger neutraler Besetzung. Sie könnte auch aktiv werden, um beispielsweise E-Mail-Anbieter auf ihre Verschlüsselung hin zu überprüfen.

Die Beendigung der direkten und indirekten Zusammenarbeit des *Bundesamtes für Sicherheit in der Informationstechnik* (BSI) mit Geheimdiensten ist unumgänglich. Der Interessenkonflikt *für die Nutzer – gegen die Nutzer* muss beendet werden. Auch in der digitalen Welt ist die Währung Vertrauen.

Die staatliche Abhängigkeit deutscher Datenschutz-Kontrollinstanzen muss endlich beendet werden (siehe Rechtssache Europäische Kommission gegen Bundesrepublik Deutschland, EuGH Az. C-518/07).

Der ausschließliche Einsatz von freier Software muss in staatlichen Stellen und Organen selbstverständlich werden, auch hier kann nur *verteiltes Vertrauen* eine Grundsicherheit bringen. Die Hersteller von Produkten sind doch selten ihre eigenen Kritiker. Freie Hardware muss zudem der nächste Schritt sein.

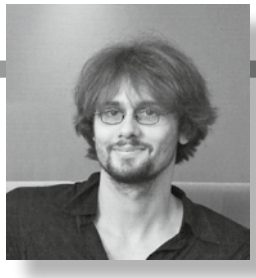
Der (endlich) in einem Koalitionsvertrag enthaltene Passus, dass IT-Hersteller und -Diensteanbieter für Datenschutz- und IT-Sicherheitsmängel ihrer Produkte haften sollen[6], muss zügig weiter ausgearbeitet werden, insbesondere für freie Software und Community-Projekte müssen Lösungen gefunden werden. Diese mehr als eine Dekade alte Idee muss Einzug halten.

Staatlich geförderte Ende-zu-Ende-Verschlüsselung muss großflächig ausgerollt und in Behördenkommunikation zur Pflicht werden, ob unter Einbeziehung der Funktionen des Neuen Personalausweises oder anderer Konzepte ist dabei zweitrangig.

Zu Letzt

Gerade Informatikerinnen und Informatiker als Architekten der digitalen Gesellschaft sollten nie vergessen: auch die beste Technologie kann keine politischen Probleme lösen. Es bleibt die grundsätzliche Frage, ob Institutionen einer Demokratie im Kern

Rainer Rehak



Rainer Rehak, Informatiker, Preisträger des FIfF-Studienpreises 2012.

überhaupt mit dem Prinzip des Geheimen kompatibel sind, von unfreier/closed-source Software über Geschäftsgeheimnisse bis hin zu Geheimdiensten). Ich denke, die Antwort lautet sowohl aktuell betrachtet als auch historisch begründet eindeutig *Nein*.

Anmerkungen

1 *T. Schwarze und A. Gruber, Darf der BND das?, http://www.zeit.de/politik/deutschland/2013-08/bnd-nsadatenweitergabegesetz/komplettansicht, 5. August 2013.*

2 *BVerfG, 1 BvR 370/07, https://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html, 27.2.2008.*

3 *In einer Rede vor dem Bundesverfassungsgericht als Sachverständiger zur Online-Durchsuchung, Karlsruhe, 10.10.2007.*

4 *BVerfGE 88,203, http://www.servat.unibe.ch/dfr/bv088203.html, 28.05.1993.*

5 *Josef Foschepoth, Überwachtes Deutschland: Post- und Telefonüberwachung in der alten Bundesrepublik, 2013.*

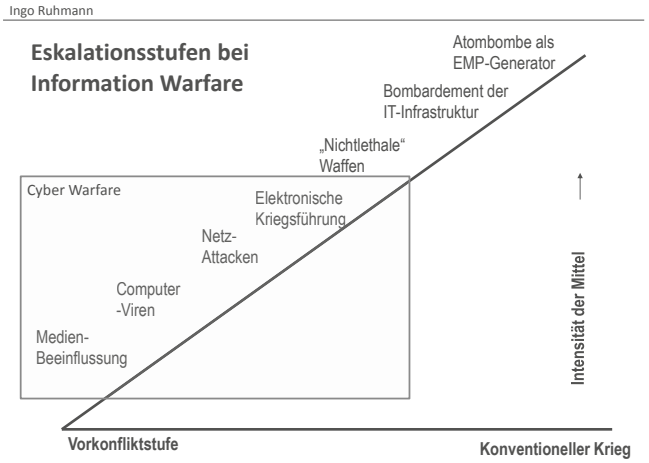
6 *Koalitionsvertrag zwischen CDU, CSU und SPD , 18. Legislaturperiode, S. 148, 2013.*

Ute Bernhardt, Ingo Ruhmann

Mitten im Cyberkrieg – Angriff auf die Zivilgesellschaft

Der seit dem Frühjahr 2013 weiter andauernde NSA-Skandal macht den Stellenwert staatlicher Hacker heute deutlich. Die bekannt gewordenen Dokumente lassen als Schluss nur zu, dass kein anderer als die NSA die leistungsfähigste und finanzstärkste Hackertruppe der Welt darstellt. Seit den 70er Jahren führt sie immer intensiver Cyberkrieg *gegen Freund und Feind. Nicht allein unsere Privatsphäre ist in Gefahr, sondern die gesamte Infrastruktur, die sichere IT-Systemen voraussetzt. Die Zivilgesellschaft, die das Internet zu ihrem Nervensystem gemacht hat, muss sich den Konsequenzen dieser Entwicklung stellen und staatlicher Computerspionage und -sabotage Einhalt gebieten. Wie dies möglich ist, war Thema der Arbeitsgruppe* Mitten im Cyberkrieg *auf der FIfF-Jahrestagung 2013.*

Zu Beginn des Workshops stellte *Ingo Ruhmann* eine Aufarbeitung der vom FIfF seit fast 30 Jahren bearbeiteten militärisch-geheimdienstlichen Überwachungsaktivitäten vor, die durch die beeindruckende Sammlung der mit Hilfe von Edward Snowden veröffentlichten Dokumente umfassend ergänzt und wesentlich konkreter fassbar wurden. Ausführlich ist dies auch in dem dieser Ausgabe beigelegten Dossier *Information Warfare und Informationsgesellschaft* (*Wissenschaft & Frieden*, Dossier Nr. 74) nachzulesen. Der erste Vortrag konzentrierte sich aber nicht auf Fragen der Überwachung, sondern der IT-Sicherheit. Dargestellt wurde, in welcher Weise Information Warfare und Cyberkrieg den Rahmen bilden für die Aktivitäten der amerikanischen und britischen Geheimdienste, die sich in jede Art von Kommunikation eingeklinkt haben.



Kommunikationsüberwachung war seit dem 19. Jahrhundert Aufgabe von Polizei und später Nachrichtendiensten. In allen Staaten ist gesetzlich geregelt, welche Unterstützung die Netzbetreiber für diese Überwachung leisten müssen. Neu an den NSA-Aktivitäten ist jedoch, dass die NSA seit den 1980er Jahren mit Cyber-Angriffswerkzeugen experimentiert hat – wozu interessante Presseberichte aus der Zeit von 1982 bis 2009 zu sehen waren –, und heute mit automatisierten Angriffswerkzeugen Trojaner und andere Schadsoftware auf IT-Systemen ihrer Opfer installiert. Wo diese Mittel nicht ausreichen, arbeitet seit Ende der 1990er Jahre eine spezielle Hackergruppe an gezielt durchgeführten Angriffen.

Die aufgrund der Medienberichte der NSA zuzurechnenden Trojaner wurden in einem Ausmaß nachgewiesen, das vergleichbar ist mit der am weitesten verbreiteten Schadsoftware, die konventionellen *Cyber-Kriminellen* zugeschrieben wird. Die Aufwände der NSA für das Aushebeln von Schutzmechanismen, von Verschlüsselungswerkzeugen und zur Sammlung von Kommunikationsdaten ist allerdings mit keinem anderen Akteur weltweit vergleichbar: Mit ca. 12 Mrd. US-Dollar pro Jahr ist die NSA zweifellos die mit den umfangreichsten Ressourcen ausgestattete Hackertruppe der Welt. Dass sich die NSA gegen Verbündete ebenso wie vermutete Gegner wendet, ist mittlerweile medial ausgiebig berichtet worden. Nach eigener Definition führen also die USA uneingeschränkten Cyberkrieg gegen Freund und Feind.

Fazit dieser Einführung war, dass die NSA wesentliche IT-Sicherheitsmittel umfassend kompromittiert hat. Gewissheit über die Zuverlässigkeit von IT-Sicherheitswerkzeugen kann es derzeit nicht geben. In einem *Cyberwar unter Freunden* kann Datenschutz daher nur ein Teil der Debatte sein. Sicherheit in der IT-Welt muss heute neu bewertet, viele lieb gewonnene Abläufe müssen mit neuen Sicherheitsmechanismen neu gestaltet werden. Dies, so das Ergebnis der Diskussion im Anschluss, ist ebenso Aufgabe für kritische IT-Experten unter anderem aus dem FIfF wie auch der Wirtschaft.

In seinem anschließenden Vortrag, der in diesem Heft in einem eigenen Beitrag dargestellt ist, konzentrierte sich der ehemalige MdB *Paul Schäfer* auf die sicherheitspolitische Rolle der Bundeswehr und deren Interessen an Aufklärungstechnik und -inhalten.

Die Auslandseinsätze vor allem in Afghanistan machen die Truppe abhängig von Aufklärungsdaten, die zumeist von anderen Alliierten gesammelt werden, da die eigenen Mittel begrenzt sind. Das Debakel um die Beschaffung von Überwachungsdrohnen, für die es zwar keine Flugzulassung gibt, aber eine ausgereifte Überwachungssensorik, die nun anderweitig genutzt werden soll, wird in Gänze nur im Zusammenhang mit früheren Beschaffungszielen und neuen Aufgaben nachvollziehbar. Auch die Aufgaben der im *Kommando Strategische Aufklärung (KSA)* zusammengezogenen Bundeswehr-Truppenteile für die elektronische, psychologische und die Cyber-Kriegsführung lassen einerseits erwarten, dass zusätzliche Aufgaben den Bedarf an neuer Technik nach sich ziehen werden. Andererseits sind die bestehenden Fähigkeiten nur äußerst schwer zu bewerten. Diese nur durch die besonderen Möglichkeiten eines Parlamentariers zu gewinnenden Einblicke leiteten über zu der Frage, welche Handlungsoptionen auch auf politischer Ebene aussichtsreich sein können.

Zur Systematisierung der Diskussion differenzierte *Ute Bernhardt* die Reaktionsmöglichkeiten und die potentiellen Akteure. Klar ist: Unbeobachtete Telekommunikation ist *das* strategische Grundrecht des Internet-Zeitalters. Vom Schutz einer einzigen Technik und einer einzigen Grundrechtsvorschrift hängen prinzipiell alle Aktivitäten im Internetzeitalter ab. Wenn alle Äußerungen und Aktivitäten durch Überwachung sichtbar werden, sind politische Willens- und Meinungsbildung, Entfaltung der Persönlichkeit, politische Teilhabe, Handlungsfreiheit unmöglich, sind Demokratie und Rechtsstaat verloren.

Allerdings geht es eben nicht allein um Überwachung. Ausgehend von den von NATO-Juristen gewählten Definitionen eines Cyberkrieges und deren Klassifikation von möglichen Angriffsformen im *Tallinn-Manual*[1] und den bekannten Fakten zum NSA-Skandal sind die Aktionen von NSA und GCHQ nach internationalem Recht als Cyberangriff zu werten. Ob es klug ist, diesen wiederum militärisch zu beantworten, darf bezweifelt werden. Allerdings ließe sich eine solche Attacke als Spionage und Sabotage oder staatlicher Cyber-Terrorismus begreifen. Dafür zuständig sind nun keine Datenschützer, sondern Strafverfolger. Nicht umsonst gibt es im Strafrecht Straftatbestände wie Computerspionage und Computersabotage. Das ist kein Novum: Auch im Kalten Krieg wurde mit der Staatsanwaltschaft gegen Großmächte und deren Spionageapparate vorgegangen.

Die Zurückhaltung der staatlichen Seite, hier tätig zu werden, macht allerdings andere Ansätze nötig. Die großflächige Kompromittierung der IT-Sicherheit zwingt die Wirtschaft dazu, technische und organisatorische Maßnahmen zu treffen, um IT und Geschäftsprozesse sicher und zuverlässig zu gestalten. Um interne und kundenbezogene Prozesse sicherer zu machen, müssen die Unternehmen kompromittierte IT ersetzen durch neue Kryptoverfahren und andere sichere IT-Lösungen. Erhebliche Entwicklungsaufgaben sind zu leisten, die Ressourcen binden und einen erheblichen Kostenfaktor darstellen werden. Der Aufwand dürfte ähnlich groß sein wie der beim Jahr-2000-Problem.

Hinzu kommen muss der klassische politische Protest, der aus Medienarbeit, der Arbeit von NGOs und deren Beratung des politischen Raumes, der Medien und Öffentlichkeit bestehen sollte, um Cyberkrieg und IT-Sicherheit zum politischen Thema zu machen. Die Unterstützung beginnt damit, konkrete Schutzwerkzeuge zu nutzen und – etwa mit PGP-Partys – bekannter zu machen. Der Beitrag von *Karin Schuler* in diesem Heft gibt dazu einen guten Überblick.

Fazit dieser Analyse und der Diskussion der Arbeitsgruppe war, dass weder die rechtlichen Grundlagen und Erfordernisse eines Cyberkrieges durch Geheimdienste noch die technischen Möglichkeiten für Reaktionen auch nur ansatzweise analysiert sind, jede politische Gestaltungsidee fehlt. Diese Defizite im Problembewusstsein haben leider zur Vernachlässigung von Lösungsansätzen und Visionen geführt. Visionen aber sind überfällig: Schließlich hat die brutale Realität des Krieges Abkommen wie die Genfer Konvention oder die Biowaffen- und Chemiewaffen-Konventionen nicht verhindert, sondern erst dazu geführt. Wenn es von staatlicher Seite kein Einsehen und keine Lösungen gibt, werden IT-Sicherheitsverantwortliche aus der Wirtschaft ebenso wie Bürgerinnen und Bürger genötigt sein, ihre Interessen gegenüber Politik und *Cyber-Kriegern* zu organisieren und umzusetzen. Aufgabe von kritischen Experten wie dem FIfF ist es, hier mitzuwirken.

Anmerkung

1 *Michael N. Schmitt (ed.): The Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge, 2013*

Ingo Ruhmann und Ute Bernhardt

Ingo Ruhmann ist Informatiker, wissenschaftlicher Referent und Lehrbeauftragter an der FH Brandenburg.
Ute Bernhardt ist Informatikerin, wissenschaftliche Referentin und Lehrbeauftragte. Beide sind ehemalige Vorstandsmitglieder im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. und arbeiten zu Datenschutz, IT-Sicherheit sowie Informatik und Militär.

Karin Schuler

Wer nicht kämpft, hat schon verloren

Dieses Zitat von Bert Brecht, besser gesagt: sein zweiter Teil, kommt mir in letzter Zeit häufiger in den Sinn, wenn ich Diskussionen über die Auswirkungen der geheimdienstlichen Ausspähskandale führe. Was kann man angesichts immer neuer Erkenntnisse über das Ausmaß der Überwachungsmaßnahmen überhaupt noch tun? Welche Chancen hat man gegenüber einer offensichtlich mit unbegrenzten Finanzmitteln ausgestatteten Hydra, die sich Rechenzentren, Supercomputer und Energie mit beliebigem Potenzial leisten kann? Welche Hoffnung kann man angesichts einer hilflos bis devot agierenden politischen Klasse noch haben, dass unseren Vorstellungen von Grundrechtsschutz wieder Geltung verschafft wird?

Was an politischer Einflussnahme nötig ist, soll hier nicht erörtert werden. Vielmehr ein Aspekt, der in der Diskussion immer noch sehr knapp wegkommt: nämlich die Einflussmöglichkeiten jedes und jeder Einzelnen. Wir dürfen uns nicht erschreckt zurücklehnen: weder der Gesetzgeber noch Fatalismus bringen uns unsere Grundrechte zurück, wenn wir nicht auch die Möglichkeiten des Selbstdatenschutzes ausschöpfen.

Ohne Ölspur durchs Internet

Natürlich ist es einfach, den neuen Laptop oder das schöne Tablet einfach mit den Voreinstellungen zu nutzen, die es von zu Hause aus mitbringt. Es funktioniert ja auch alles. Leider sind die Endgeräte bei der Hatz durchs Internet aber ziemlich undicht. Eine breite Spur zieht sich hinter uns her, wenn wir Seiten besuchen, Suchmaschinen abfragen oder Waren bestellen. Wen interessiert, welche Spuren man auf dem virtuellen Asphalt hinterlässt, dem sei das Firefox-Plug-In *Lightbeam*[1] empfohlen. Dieses Tool zeigt, grafisch aufbereitet, welche Seiten man besucht hat – und, viel aufschlussreicher, welche davon man gar nicht selbst aufgerufen hat, sondern die über eine besuchte Website unbemerkt dazugeschaltet wurden. Lässt man Lightbeam ein paar Tage mitlaufen, erreicht der visualisierende Graph eine beeindruckende Größe. Für Aha-Effekte sorgt auch das Plug-In *Ghostery*[2], das anzeigt, welche Tracking-Programme auf der jeweils aktuellen Seite *versteckt* sind. Es erlaubt sehr komfortabel per Schiebeschalter das Ein- und Ausschalten jedes Trackingdienstes. Achtung: von der Aktivierung von *Ghostrank* sollte abgesehen werden, da nicht hinreichend geklärt ist, wer die resultierenden Nutzungsdaten von *Evidon*, der Firma hinter Ghostery erhält.

Wem bei den gewonnenen Erkenntnissen mulmig wird, der kann sich der Hilfe diverser Tools bedienen, die die Geschwätzigkeit des eigenen Browsers zumindest eindämmen. *NoScript*[3] ermöglicht das gezielte, seitenbezogene An- und Ausschalten von JavaScript und Java und schützt so nicht nur vor unerwünschten Skripten sondern auch vor den Auswirkungen von Sicherheitslücken der Skriptsprachen. *BetterPrivacy*[4] schützt vor den umgangssprachlich als *Super-Cookies* bezeichneten *local shared objects (LSO)*, einer besonders unerfreulichen Form der Dateninvasion auf der Festplatte: der Flashplayer legt dabei kleine Infodateien in zentralen Ordnern des Rechners ab, ohne dass sie in der Standard-Browserverwaltung als Cookie erkannt werden. Ein Plug-In, das ursprünglich für Webentwickler gedacht war, ist *Counterpixel*[5]. Es sollte die Platzierung von Zählpixeln auf Webseiten erleichtern, indem erkannt wird, welche Tracking- oder Statistiksoftware eingesetzt wird. Auch wenn, dem ursprünglichen Zweck entsprechend, kein Blockieren von Zählpixeln angeboten wird, bringt das Tool einen Transparenzgewinn: Von *eTracker* über *Google Analytics* und *IVW* zu *PIWIK* und vielen weiteren wird angezeigt, welche Dienste Zählpixel versteckt haben.

Wen die Erkenntnisse aus dem Lightbeam-Graphen erschrecken, der sollte sich einen Überblick über domainübergreifende Anfragen verschaffen. Meist bleibt man nicht auf der Seite *xyz.de*, wenn man diese aufgerufen hat. So genannte *cross-site-requests* sind zu einem massenhaft auftretenden Phänomen geworden, seit Schriften, Medien und andere Objekte von Drittseiten nachgeladen werden. Wer lieber selbst kontrolliert, welchen Seiten er die Unterverweisung erlauben will und welchen nicht, der sollte sich das sehr mächtige Plug-In *RequestPolicy*[6] ansehen. Dessen Einsatz ermöglicht die vollständige Kontrolle über Nachladevorgänge und schützt bei restriktiver Einstellung vor *Cross-Site-Scripting*-Angriffen, bei denen durch untergeschobenen Aufruf einer URL Schadcode auf dem Rechner des Nutzers ausgeführt wird.

Eine gute Informationsquelle zum Thema Tracking findet sich auf den Seiten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein.[7]

Nur Max Mustermann war da

Wem auch die beschriebenen Maßnahmen nicht ausreichen, kann auf die verfügbaren Anonymisierungsdienste zurückgreifen und sich so weitgehend unsichtbar machen. Auch wenn es Grenzen der durch diese Dienste gewährten Anonymität gibt, wirkt die Vermeidung von profilgebenden, personenbezogenen Daten grundsätzlich persönlichkeitsschützend.

Da man dem Anbieter des Anonymisierungsdienstes vertrauen muss, fühlt sich wahrscheinlich nicht jede/r mit allen auf dem Markt befindlichen Produkten gleichermaßen wohl. Zwei kostenlose Angebote, die sich in der Netzgemeinde großen Vertrauens erfreuen, sollen beispielhaft genannt werden.

JAP[8], eine kostenlose Softwarelösung, die im Rahmen des Projekts *AN.ON (Anonymity Online)* entwickelt wurde, ist leider nicht die schnellste, genießt aber einen untadeligen Ruf. Hat man die Software installiert, führen eigene Webseitenaufrufe nicht mehr zu einer direkten Anfrage beim zugehörigen Server. Stattdessen wird der Aufruf in ein Netzwerk teilnehmender Verteilserver (Mixe) geschickt und darin mehrfach weitergeleitet, ehe die Anfrage beim eigentlich angefragten Server landet. Dieser sieht jedoch nur noch die IP-Adresse des letzten Verteilservers und kann keine Rückschlüsse auf den anfragenden Nutzer

mehr ziehen. Schöner Effekt: Keiner der beteiligten Mixe kann Rückschlüsse auf einzelne Nutzer ziehen, da er jeweils nur weiß, von welchem vorigen Mix die Anfrage kam und wohin er sie weiterleiten soll. Die Nutzer können die zur Verfügung stehenden Mixe bzw. deren Betreiber einsehen und gezielt eigene Mixkaskaden auswählen.

Eine weitere gut beleumundete Open-Source-Lösung bietet das *TOR-Netzwerk*[9], das grundsätzlich ähnlich wie JAP arbeitet, die Anfragen von Nutzern aber mittels *onion routing* aufteilt und weiterleitet. Hierbei werden keine festen Routen über Mixe verwendet (Mix-Kaskaden) sondern die Route wird jeweils individuell neu festgelegt.

Beide Verfahren haben aus Sicherheitssicht Vor- und Nachteile: der Zentralismus der Mix-Kaskaden schützt besser vor schleichender Übernahme von Verteilservern durch Anbieter, die als Maulwurf agieren. Andererseits bietet die größere Verteilung und Verschleierung der Übertragungswege beim *onion routing* weniger Angriffsfläche, falls einzelne Server angegriffen werden.

Googlen ohne Google

Was haben *Tempo*, *Knirps*, *Uhu*, *Maggi* und *Google* gemeinsam? Bei allen handelt es sich um so genannte generalisierte Markennamen: der Markenbegriff wird als Bezeichnung für eine ganze Produktgruppe verwendet. Nun weiß jeder, dass es Konkurrenzprodukte für Taschentücher, Taschenschirme und Suppenwürze gibt. Dass man jedoch auch ohne Googles Suchmaschine *googlen* kann, hat sich noch nicht weit genug herumgesprochen.

Dabei gibt es schon seit vielen Jahren datenschutzfreundliche Alternativen zu datenhungrigen Suchdiensten wie Google, Bing, Yahoo und Co.

Zu den Pionieren auf diesem Gebiet zählen die Dienste der Firma IxQuick, die zweierlei Suchmaschinen anbietet: *Ixquick*[10], eine Metasuchmaschine und *Startpage*[11], ein Proxydienst für die Suche über Google. Beide speichern keine IP-Adressen und vermeiden so die Profilbildung anhand der durchgeführten Suchanfragen.

Die Dienste sind gut in Browser integrierbar und bieten hohe Qualität. Es gibt also keinen Grund, sich weiterhin beim Namensgeber Google aushorchen zu lassen.

Passworte gehören in den Tresor

Wie viele unterschiedliche Passworte benötigt man als Nutzer?

Schätzungsweise hat ein durchschnittlicher Nutzer zwischen 50 und 200 Zugänge, wovon einige vielleicht nur ein einziges Mal genutzt werden (weil man z. B. kein zweites Mal in einem Online-Shop einkauft). Kommt in Diskussionen die Rede auf die Anzahl verwendeter Passwörter, hat man jedoch meist schnell das Gefühl, dass vielen Leuten vier bis fünf unterschiedliche ausreichen, um eine große Anzahl von Zugängen zu schützen.

Alternative zum Kämpfen? Foto: Benjamin Kees

Die jüngste Alarmmeldung des BSI[12], dass eine Datenbank mit Zugangsdaten entdeckt wurde, die 16 Mio. Einträge enthält, ist da nur ein besonders eindrucksvoller Fall.

Die Antwort auf die Eingangsfrage muss daher lauten: So viele, wie man persönliche Zugänge hat. Seien es Zugänge zu Rechnern, Online-Shops, Bank-Portalen, Online-Netzwerken, Cloud-Anwendungen, Providern, Nutzerportalen oder sonstigen Dienstleistungen: Jeder sollte ein eigenes Passwort haben. Denn sobald ein Zugang kompromittiert und das Passwort bekannt wurde, ist dieses *verbrannt*. Insbesondere in Fällen, in denen der Benutzername aus einer E-Mail-Adresse besteht, kann der Besitzer geknackter Passwörter auf die Person rückschließen und so deren weitere Zugänge ausprobieren. Wurde dann mehrfach das gleiche Passwort verwendet, sind auch alle anderen Zugänge mit diesem Schlüssel kompromittiert.

Aber wie schafft man den Spagat, einerseits gute Passworte zu verwenden (größer als 8 Stellen, Ziffern, Sonderzeichen, Groß- und Kleinschreibung), die in keinem Wörterbuch stehen (damit man sie nicht mittels *Wörterbuch-brute force*-Angriff errechnen kann) und sich andererseits diese Passworte so zu merken, dass man sie im Bedarfsfalle kennt, ohne sie auf gelbe Zettel an den Bildschirm zu kleben?

Die Helfer, die einem zur Lösung dieses Problems dienen, nennen sich Passworttresore. Die Idee ist recht einfach: man legt seine Benutzername/Passwort-Kombinationen im Regal eines durch starke kryptografische Verfahren gesicherten Containers ab und sorgt dafür, dass der einzige Schlüssel zum Container einen hohen Sicherheitsstandard hat. Diesen Schlüssel trägt man nur bei sich und nutzt ihn ausschließlich kurzzeitig um den Container zu öffnen, ein Passwort in einer Schublade des Regals nachzuschlagen und dieses zu verwenden. Der Container hat eine Türe, die sofort nach Verlassen automatisch zurück ins Schloss fällt. Noch besser: im Container befindet sich ein Generator, der einem gute Passworte im obigen Sinne erzeugt und sofort in die Schublade für einen neuen Zugang legt.

Eines der Programme, die so funktionieren, wurde von *Bruce Schneider* entwickelt, einem der bekanntesten Kryptografie-Experten. Er ist außerdem seit vielen Jahren bürgerrechtlich im Vorstand der *Electronic Frontier Foundation* engagiert und ist bei der Zeitung *The Guardian* Mitglied des Redaktionsteams, das Ed Snowdens Unterlagen sichtet und beurteilt.

Passwordsafe[13] bietet einem die Möglichkeit, komfortabel für jeden Zugang ein eigenes, gutes Passwort zu generieren und sicher abzulegen. Der Generalschlüssel, der den Zugang zum Safe ermöglicht, sollte lang und komplex sein. Aber da man sich nur diesen einen Schlüssel merken muss, sind sowohl Sicherheits- als auch Komfortgewinn enorm.

Keine Postkarten für die Späher

Jeder hat den Spruch schon mal gehört: „Eine E-Mail ist einer mit Bleistift geschriebenen Postkarte vergleichbar." Obwohl vermutlich niemand seiner Freundin heikle Krankheiten auf Postkarte mitteilen würde, haben viele Menschen keinerlei Skrupel, dies in aller Ausführlichkeit per E-Mail zu tun. Das Gefühl, dass man selbst nicht durchblickt, wie die Mail vom eigenen Rechner auf den Rechner des Freundes gelangt, führt anscheinend zur trügerischen, unreflektierten Überzeugung, dass das auch sonst niemandem gelingt. In IT-Fachkreisen wiederum begegnet man teilweise einer Art von Fatalismus, der in der Ansicht „ist doch eh alles knackbar" gipfelt. Beiden Haltungen ist gemein, dass sie passiv und uninformiert vermeiden, das Heft in die eigene Hand zu nehmen. Selbstdatenschutz sieht anders aus!

Zugegeben: die ergonomische Güte von E-Mail-Verschlüsselungsprogrammen ist noch immer ausbaufähig, aber die Zeiten unbedienbarer Produkte sind vorbei. Unabhängig von Betriebssystem und Mailprogramm stehen Verschlüsselungsmöglichkeiten zur Verfügung, die durch gewissenhaften Gebrauch durchaus Sicherheit vor unerwünschten Lauschern bieten.

Beispielhaft sei auf das gut zu handhabende und kostenlose Distributionspaket *GnuPG-Pack*[14] für Windows hingewiesen, das die offene Version der Verschlüsselungstechnik *pretty good privacy (pgp)* ermöglicht und Schlüssel größer als 4096 bit erzeugen kann. Ein Plug-In für die Mail-Software Thunderbird ist ebenfalls enthalten, so dass per Mausklick ver- und entschlüsselt werden kann.

Für Outlook-Nutzer bietet das Distributionspaket *Gpg4win*[15] ein Plug-In für die Mailsoftware Outlook.

My computer is my castle

Ergänzend zu den asymmetrischen (*public-key*-)Verfahren, bei denen jeder Teilnehmer zunächst ein Schlüsselpaar erzeugen muss, um am verschlüsselten Datenaustausch teilzunehmen, gibt es auch Verfahren der symmetrischen Verschlüsselung. Symmetrische Verfahren kommen aufgrund der Sensibilität ihrer Schlüssel meist in anderen Einsatzbereichen zum Einsatz, zum Beispiel bei der Sicherung von Daten auf der eigenen Festplatte. Gerade bei Laptops oder anderen mobilen Geräten oder Medien (USB-Sticks!), die jährlich in großer Zahl verloren gehen, ist die Sicherung der darauf enthaltenen Daten durch Verschlüsselung sehr zu empfehlen. Nicht nur bei Verlust des Rechners muss man sich so wenigstens keine Sorgen um die Vertraulichkeit der Daten machen, sondern auch beim Bewegen im Internet lassen sich definierte Bereiche der Festplatte so für die Dauer der Online-Verbindung vor unberechtigtem Zugriff schützen.

Eines der Programme, die kostenlose Festplatten-, Container- oder Ordnerverschlüsselung anbieten, ist **Truecrypt**[16], ein Tool, dessen Quellcode verfügbar ist (auch wenn es nicht vollständig der open-source-Definition entspricht).

Was bringt's?

Wer die vorstehend skizzierten Möglichkeiten nutzt, um sich und seine Daten nicht mehr auf dem Präsentierteller anzubieten, hat schon einiges in Sachen Selbstdatenschutz getan. Weitere Schritte können folgen, indem Chats gesichert, sichere Cloud-Austauschdienste verwendet oder Webcams deaktiviert werden.

Natürlich stellen die beschriebenen Maßnahmen und Mechanismen alleine kein Allheilmittel dar, um uns vor der Datengier von Geheimdiensten und profitierenden Wirtschaftsunternehmen zu schützen. Aber umgekehrt reicht der Weg über politische Einflussnahme alleine dazu auch nicht aus. Und vor allem sind die darauf erzielten Schritte sehr kurz, schwerfällig, und nicht immer auf das Ziel des Grundrechtsschutzes ausgerichtet. Wir müssen daher Eigenverantwortung übernehmen, uns aus dem Status des *blinden Nutzers* befreien, lernen, was wir tun, wie wir es tun und wie wir uns dabei bestmöglich selbst schützen können. Für diejenigen, die in der IT arbeiten, gilt es, das Wissen über Schutzmöglichkeiten möglichst breit unter nicht-fachkundigen Nutzern zu verbreiten – und selber mit gutem Beispiel voranzugehen.

Natürlich gibt es keine Garantie, dass wir uns auf diese Weise vor den Zudringlichkeiten selbst ernannter *Bedarfsträger* schützen und natürlich kann ohne wirksame staatliche Durchsetzung von Grundrechten kein vollkommener Schutz entstehen. Aber wo man sich selbst helfen kann, sollte man es auch tun, und für den Rest sollte es so schwer wie möglich sein, jedermanns Daten *einfach so* abzuzapfen. Getreu Brechts Motto: *Wer kämpft, kann verlieren. Wer nicht kämpft, hat schon verloren*.

Karin Schuler

Karin Schuler ist Vorsitzende der Deutschen Vereinigung für Datenschutz e.V., langjähriges FIfF-Mitglied, Beraterin für Datenschutz und IT-Sicherheit und vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannte Sachverständige für IT-Produkte.
Kontakt: *buero@schuler-ds.de · www.schuler-ds.de*

Anmerkungen

1 *https://www.mozilla.org/de/lightbeam/*
2 *https://www.ghostery.com*
3 *https://addons.mozilla.org/de/firefox/addon/noscript/*
4 *https://addons.mozilla.org/de/firefox/addon/betterprivacy/*
5 *https://addons.mozilla.org/de/firefox/addon/counterpixel/*
6 *https://addons.mozilla.org/de/firefox/addon/requestpolicy/*
7 *https://www.datenschutzzentrum.de/tracking/*
8 *http://anon.inf.tu-dresden.de*
9 *https://www.torproject.org*
10 *https://ixquick.com/deu/*
11 *https://startpage.com/deu/*
12 *https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Mailtest_21012014.html*
13 *http://passwordsafe.sourceforge.net*
14 *http://home.arcor.de/rose-indorf/*
15 *http://www.gpg4win.org*
16 *http://www.truecrypt.org*

Paul Schäfer

Deutsche Sicherheitspolitik, Bundeswehr und Cyber Warfare

In der jüngsten Vergangenheit hatten wir es im Zusammenhang mit der NSA-Abhöraffäre insbesondere mit drei Aufregern zu tun:

1. Dem Ausspionieren des Handys der Bundeskanzlerin.

2. Der Kooperation deutscher Dienste wie Verfassungsschutz und Bundesnachrichtendienst mit dem US-amerikanischen Geheimdienst NSA, bei der große Datenmengen weitergegeben wurden, was vorgeblich im Rahmen des Anti-Terrorkampfes dringend nötig gewesen sei.

3. Und in diesem Rahmen insbesondere der Weitergabe von Daten, um Drohnenangriffe gegen vermeintliche Terroristen (v.a. in Pakistan) optimieren zu können. Damit war unweigerlich die Frage verknüpft, inwieweit zumindest von einer indirekten Beteiligung deutscher Behörden an extralegalen „gezielten Tötungen" ausgegangen werden müsse.

Die Aufregung war nachvollziehbar, war aber – sofern von offiziellen Stellen die Rede ist, aber auch von Teilen der Medien – nicht frei von Bigotterie. Dass Deutschland am *Krieg gegen den Terror*, den der damalige US-Präsident George W. Bush nach den Terroranschlägen 2001 ausgerufen hatte, nicht unbeträchtlich beteiligt war, war doch bekannt. Es war die böse, aber konsequente Folge des Kanzler-Wortes von der „uneingeschränkten Solidarität". Dass aus Kreisen der US-Administration lapidar auf Übereinkünfte in diesem Rahmen hingewiesen wurde, war daher nur folgerichtig. Denn man konnte, ja musste davon ausgehen, dass zwischen den *Nachrichtendiensten* Vereinbarungen getroffen worden waren, die weit über die in diesem Milieu üblichen Deals (*Do ut des*; Gib und dir wird gegeben) hinausgingen.

Inwieweit ist Deutschland am Anti-Terror-Krieg beteiligt?

Die Beteiligung an dem von den USA geführten Anti-Terrorkrieg hatte immer verschiedene Seiten: Gesetzgeberisch, und damit in der Politik nach innen, wurden die empfindlichen Einschränkungen demokratischer Freiheitsrechte, die in den USA mit dem *US Patriot Act* vorgemacht wurden, *cum grano salis* hier übernommen. Nach außen war die Bundesrepublik bereit, sich an bestimmten Formen der Terrorbekämpfung zu beteiligen, beispielsweise am Krieg in Afghanistan, auch durch den Einsatz militärischer Spezialkräfte. Insgesamt war man bereit, das militärische und geheimdienstliche Zusammenwirken bei der Bekämpfung der Terroristen (bzw. derjenigen, die man entsprechend zuordnete) intensiv zu betreiben.

Dabei bewegte man sich gerne in Grauzonen und bevorzugte doppelbödiges Agieren: Von manchen Exzessen des *War On Terror* setzte man sich rhetorisch ab und erklärte im Zweifelsfalle auch, dass man sich nicht überall beteiligen müsse. Aber auf lauteren Widerspruch wurde bewusst verzichtet und das Mitmachen bei den diversen Unternehmungen wollte man nicht aufgeben. Die heutigen Absetzbewegungen von den NSA-Abhöraktionen entbehren daher nicht der Scheinheiligkeit.

Die illegalen Praktiken des *War On Terror*, wie die geheimen Verschleppungen (*rendition flights*) und Folterungen, hat man lange Zeit stillschweigend hingenommen, bestenfalls zwischen den Zeilen kritisiert, sich aber auch, wie im Falle des Bremers *Murat Kurnaz*, direkt in schlimme Dinge verstrickt. Den USgeführten Irak-Krieg hat man offiziell nicht mitgetragen, hinter den Kulissen aber Unterstützungsleistungen erbracht. Während man sich rhetorisch mehr und mehr vom Anti-Terrorkrieg absetzte, hat man sich noch bis ins Jahr 2010 an der völkerrechtlich unhaltbaren Mission *Enduring Freedom* in Afghanistan beteiligt. An der maritimen Anti-Terror-Mission *Active Endeavour* im Mittelmeer ist man trotz öffentlich immer wieder bekundeten Unbehagens bis heute beteiligt. Bei den Verhandlungen vorm Bundesverfassungsgericht über den Einsatz der Tornado-Aufklärungsflugzeuge, legte die Bundesregierung größten Wert auf die Feststellung, diese Flugzeuge kämen nur im Rahmen des völkerrechtlich gesicherten ISAF-Mandats zum Einsatz, und ISAF und *Enduring Freedom* blieben streng getrennt. Wie sich eine solche Trennung vor Ort *on the ground* tatsächlich aufrechterhalten ließ, bleibt bis heute ein Buch mit sieben Siegeln.

Vor allem in Afghanistan operierten bestimmte deutsche Militär-Einheiten auch im Grauzonenbereich. Was die speziellen *Task Forces* im Einzelnen getan haben, woran sie sich beteiligten, woran nicht, ist nicht restlos aufzuklären. Denn diese Spezialeinheiten haben ihrerseits immer eng mit den *US Special Forces* agiert. Tatsache ist zum Beispiel, dass sich die Bundesrepublik an der Erstellung von Listen besonders übler und gefährlicher Feinde in

Afghanistan beteiligt hat. Diese *JPALS-Listen* waren die Grundlagen für Militäroperationen, in denen vermeintliche Terroristen gefangengenommen (*capture*) oder getötet (*kill*) wurden. Bis heute steht die Aussage der politischen und militärischen Führung der Bundeswehr, dass man sich nicht an Aktionen beteiligt habe, bei denen es darum gegangen sei, Terroristenführer vorsätzlich und gewaltsam auszuschalten. Die Bundeswehr nehme nur fest und überstelle die Gefangengenommenen an die afghanischen Autoritäten, so die offizielle Lesart. Diese Version wird hier auch gar nicht bestritten (sofern nicht andere Beweise auftauchen), aber die offene Frage ist, wie weit die Kooperation mit den US-Akteuren reichte und damit die indirekte Verantwortung für illegale Praktiken? Was bedeuten die indirekten Hilfe- und Unterstützungsleistungen, wie die De-facto-Absicherung eines Operationsraumes, die Weitergabe von Daten über mögliche Gegner und deren Aufenthalte, konkret? Reicht es, dann die Hände in Unschuld zu waschen?

Bis heute ist ungeklärt, ob an der Durchführung von Killeroperationen mittels Kampfdrohnen US-Militärkommandos auf deutschem Boden involviert waren und sind. Es fällt schon auf, dass die verschiedenen Bundesregierungen dieser Art der Kriegführung, insbesondere in Pakistan, keinen nennenswerten politischen Widerstand entgegengesetzt haben. Immerhin äußerten zu Beginn des Jahres 2013 die Bundestagsfraktionen der SPD und Grünen, neben den bereits früher aktiven LINKEN, schwerste völkerrechtliche Bedenken gegen die *Targeted-killing*-Operationen und forderten die Regierung auf, sich für die sofortige Beendigung dieser Einsätze zu verwenden.

Dies führt zu Punkt Zwei:

Was ist nach dem NATO-Truppenstatut erlaubt?

In der Öffentlichkeit wurde vor einiger Zeit thematisiert, ob die Einsätze mit bewaffneten Drohnen zur gezielten Ausschaltung vermeintlicher oder tatsächlicher Terror-Anführer auch von deutschem Boden aus koordiniert werden, und inwieweit eine solche Praxis, so sie denn belegbar ist, mit internationalem und nationalem Recht vereinbar sei.

Was die Sachlage betrifft, ist zumindest davon auszugehen, dass das zur Zeit in Stuttgart angesiedelte Afrika-Kommando der US-Streitkräfte – *AFRICOM* – an den Drohnen-Einsätzen (Djibouti, Niger) in welcher Form auch immer beteiligt ist. Auch dürften Militärstrukturen im pfälzischen Ramstein bei der Datenübermittlung involviert sein.

Die Bundesregierung hat auf entsprechende Anfragen der Bundestagsfraktion der LINKEN in der vergangenen Legislaturperiode eher ausweichend geantwortet.

Ja, die Einrichtung des entsprechenden Regionalkommandos sei 2007/2008 mit dem Einverständnis der Bundesregierung erfolgt. Die rechtlichen Grundlagen dafür lägen im Vertrag über den Aufenthalt ausländischer Streitkräfte aus dem Jahre 1954; die Rechte und Pflichten der Streitkräfte aus NATO-Staaten ergäben sich aus dem NATO-Truppenstatut aus dem Jahre 1951 bzw. dem Zusatzabkommen zum Truppenstatut aus dem Jahre 1959.[1] Im übrigen träfe es zu, dass die Bundeswehr Verbindungskommandos zu den jeweiligen US-Führungsstrukturen unterhalte, so auch zum AFRICOM. Aber Zugang zu klassifizierten US-Informationen habe man darüber nicht. Dieses Eingeständnis, dass man eigentlich keine ausreichende Informationsgrundlage habe, hindert die Bundesregierung nicht daran, festzustellen, dass ihr „*keine Anhaltspunkte*" dafür vorliegen, „*dass sich die Vereinigten Staaten auf deutschem Staatsgebiet völkerrechtswidrig verhalten hätten*."[2] Über diesen Blankoscheck dürfte man sich in Washington freuen.

Nach Darstellung der US-Regierung habe es keinen Einsatz bewaffneter Drohnen von deutschem Boden aus gegeben, sagt die Bundesregierung. Aber genau darum ging es nie. Sondern darum, inwieweit auf deutschem Boden befindliche militärische Infrastruktur der *US Army* an ungesetzlichen Drohnenangriffen in Angriffe beteiligt war oder nicht. Und der blauäugige Hinweis der Bundesregierung, dass sich die US-amerikanische Bündnispartner und deren Streitkräfte jederzeit an die bestehenden völkerrechtlichen Normen und Gesetze halten würden, ist vor dem Hintergrund von Guantanamo, *rendition flights* und *waterboarding* mehr als überraschend.

Richtig ist zumindest, dass sich das NATO-Truppenstatut auf die strikte Beachtung völkerrechtlicher Normen und Regeln bezieht und sich dem auch die US-Streitkräfte in der Bundesrepublik unterwerfen müssten. Und richtig ist auch, dass die USA im Rahmen des NATO-Truppenstatuts und einschlägiger Zusatzabkommen militärische Strukturen wie die Kommandozentrale zur Raketenabwehr in Ramstein aufbauen dürfen – solange man sich in der Praxis ans Völkerrecht hält. Noch Fragen? Der offene Punkt bleibt, inwieweit diese Einrichtungen noch im Rahmen des NATO-Verteidigungsauftrages oder ohne entsprechende rechtliche Grundlagen tätig sind.

Leider wurde eine entsprechende Klage von Bürgern aus dem Raum Kaiserslautern jüngst vom Verwaltungsgericht Köln zurückgewiesen, vor allem, weil es keine besondere Interessenbetroffenheit des Klägers meinte erkennen zu können. Immerhin führte das Gericht aus:

> *„Dementsprechend sind völkerrechtlich sehr bedenklich wissentliche Unterstützungsleistungen seitens der Bundesrepublik zugunsten der USA durch Gewährung von Überflugrechten und der Nutzung von im Inland gelegenen Militärstützpunkten. Soweit die USA diese nicht innerhalb des NATO-Rahmens und des Völkerrechts, sondern für völkerrechtswidrige Handlungen nutzen sollten."*[3]

Und demzufolge müssten deutsche Behörden genau prüfen, ob bei solchen Militäreinsätzen von deutschem Boden aus gegen Völkerrecht verstoßen würde. In diesem Fall müsste die Benutzung deutschen Luftraums untersagt werden. Diese möglichst abstrakt gehaltenen und daher windelweichen Formulierungen besagen zumindest eines: Hier ist dringender weiterer (rechtlicher) Klärungsbedarf. Und: Die Auseinandersetzung muss politisch weitergeführt werden, auch weil die Drohnenattacken weitergehen.

Spionage nur Sache der US-Amerikaner?

In der aufgeregten öffentlichen Debatte wurde bisweilen so getan, als seien die Abhör- und Spionageaktionen der NSA ein exklusives US-amerikanisches Betätigungsfeld. Rechtfertigende Stimmen wiesen dagegen lapidar darauf hin, dass Spionage schließlich von nahezu allen Staaten der Welt betrieben würde. Dies gelte für den wirtschaftlichen wie den militärischen Bereich gleichermaßen. Dem ist auch so. Aber man darf dennoch nicht die Augen davor zu verschließen, dass die Abhör- und Spionageaktivitäten der US-Geheimdienste eine eigene Qualität hatten und haben. Schon allein der Umfang der bei der US-Regierung angesiedelten Behörden, die ihnen zur Verfügung stehenden Ressourcen, übersteigen die Möglichkeiten der anderen Industriestaaten zur Spionage um ein Vielfaches – von den Entwicklungsländern ganz abgesehen.

In dem von mir zu behandelnden militärischen Kontext ist wichtig, dass der ganze Bereich der *Information Warfare* seit über zwanzig Jahren gravierend an Bedeutung gewonnen hat. Spätestens Ende der 90er Jahre entwickelte sich eine intensive Diskussion innerhalb der NATO-Community – Streitkräfte, Militärplaner, Sicherheitsstrategen – welcher Stellenwert Informations- und Kommunikationstechnologien in der Zukunft zukommen werde. Dabei geht es um Kriegführung und die Zeit z*wischen den Kriegen* gleichermaßen. *Informationsüberlegenheit* ist dabei das Schlüsselwort. Die moderne Informationstechnik wird dabei als entscheidender *Force Multiplier*[4] angesehen. Wer potenziellen Gegnern immer Schritte voraus sei, diesen jederzeit in die Karten schauen und umgekehrt solche Einblicke verweigern könne, der habe maximale Handlungsfreiheit und den strategischen Vorteil auf seiner Seite. Diese Annahme wurde insbesondere vor dem Hintergrund der Thesen von den asymmetrischen Bedrohungen und Kriegen durchbuchstabiert. Der Versuch von Terrornetzwerken oder übel wollenden Regierungen in der vormaligen Dritten Welt, ihre rüstungstechnischen Nachteile durch unkonventionelle und den völkerrechtlichen Rahmen sprengende Kriegführung (Guerillakrieg, Terrorattacken etc.) auszugleichen, müsse quasi durch die weitere Revolutionierung der Waffentechnik unterlaufen werden. Die Entwicklung unbemannter Waffensysteme und die Forcierung destruktiver Fähigkeiten im Cyber-Raum stehen dabei obenan. In beiden Fällen geht es darum, effizienteste Störungs- bzw. Zerstörungswirkung auf der gegnerischen Seite bei größtmöglicher Schonung eigener Kräfte zu erreichen. Und in beiden Fällen geht es nicht zuletzt um *verdeckte Operationen*, mit denen auch Souveränitätsrechte anderer Länder ausgehebelt werden können und sollen!

Für die US-Streitkräfte wurden die entsprechenden Ziele und Vorgaben in einem *National Defense Panel* unter dem Titel *Transforming Defense. National Security in the 21st Century* ausgearbeitet und 1997 vorgelegt.

Im Bereich der Bundeswehr wurde bereits 1996 eine ausführliche Studie *Streitkräfteeinsatz (SKE) 2020* vorgelegt.[5]

Neue Informationstechnologien werden in der Folgezeit innerhalb der NATO als entscheidende neue Machtressource angesehen, mit der die Führungsüberlegenheit und damit die Durchsetzungsfähigkeit der eigenen Streitkräfte in der Zukunft gesichert werden könne.

EuroHawk nach der Landung am 21.07.2011 bei der WTD61 in Manching nach 20 stündigen Flug von EAFB in USA. Foto: Rekke

Die Bundeswehr war in den neunziger Jahren bereits im Bereich der Satellitenaufklärung aktiv geworden, kooperierte dabei eng mit den französischen Streitkräften (*Helios 2*), entwickelte aber auch eigenständige Kapazitäten und verfügt seitdem mit dem Satellitensystem *SAR Lupe* über die Möglichkeit strategischer Aufklärung mittels Radar. Daneben verfügte man über boden- und seegestützte signalerfassende Aufklärungssysteme (wie die Flottendienstboote), die aber nur begrenzte Fähigkeitsprofile aufweisen konnten (tageszeit- und wetterabhängig, unzulängliche Reichweite usw.). In den Erörterungen über Einsätze der Bundeswehr außerhalb des NATO-Gebietes *(out of area)* wurde daher betont, dass die Truppe bei der Ausrüstung in jeglicher Hinsicht nachlegen müsse. Das Spektrum reichte dabei von Transportflugzeugen mit großer Reichweite über besser geschützte Panzerfahrzeuge bis zu den neuartigen Informations- und Kommunikationssystemen, die für die Beurteilung der Lage vor Ort und die Führung der Militäroperationen essenziell erschienen.

Eine besondere *Fähigkeitslücke* entdeckte man sehr rasch. Die Bundeswehr würde nach der unumgänglichen Außerdienststellung alter Flugzeuge der Marine *(Breguet Atlantic)* spätestens 2010 nicht mehr über signalerfassende Aufklärungssysteme *(SIGINT)* verfügen. Und hier begann die Geschichte von *Eurohawk*, eines Drohnenflugzeugs, das in einer Höhe von etwa 15 km stationiert werden sollte und einen großen Radius von ca. 400 km abdecken könnte. Die Superdrohne wäre dort rund um die Uhr (24 Stunden, 7 Tage) aktiv und könnte nahezu ungefährdet alle telefonischen Daten abgreifen (Handy-Telefonate, Mail-Verkehr), die man zu Aufklärungszwecken für nötig erachtet.

In der Beschaffungsplanung wurde kein Hehl daraus gemacht, dass die *Eurohawk* oder vergleichbare Flugzeuge dafür gedacht waren (und sind), eine deutsche Beteiligung am militärischen Kriseninterventionismus zu gewährleisten und zu *optimieren*. Eine beliebte Rechtfertigungsformel dafür lautet: „Schutz der eigenen Truppen“ bei ihrem (selbstverständlich) friedensstiftenden Einsatz. Man kann es auch anders, präziser formulieren: Es geht um die Herstellung militärischer Dominanz, die die Freiheit des eigenen Handelns (*freedom of action*) garantieren und damit den Gegner in die Knie zwingen soll.

Vor dem *Eurohawk*-Untersuchungsausschuss des Deutschen Bundestages hat der frühere Generalinspekteur der Bundeswehr, General *Schneiderhan*, die Anforderung der Streitkräfte an die Aufklärungs- bzw. Spionagesysteme recht exakt benannt: Es gehe um kontinuierliche, verzugsarme strategische Lageinformation für die politische Leitung und die militärische Führung – im Spektrum von Krisenfrüherkennung, Krisenvorsorge, Krisenmanagement einschließlich der Planung und Vorbereitung von militärischen Einsätzen.[6]

Dass er dabei die Begriffe Krisen- und Interessensgebiete nahezu synonym verwendete, ist kein Zufall. Sein Nachfolger, General *Wieker*, konnte in der Ausspähung fremder Territorien durch Drohnen/Flugzeuge auch nichts Bedrohliches erkennen. Es scheint so zu sein, dass diejenigen, die sich immer auf der Seite des Guten wähnen, Schwierigkeiten haben, wahrzunehmen, dass solche Spionagehandlungen von den observierten Regierungen bzw. Bevölkerungen zumindest als unfreundlicher Akt empfunden werden könnten.

Umso mehr waren die Herren Generäle, neben den Industrievertretern, im Untersuchungsausschuss *Eurohawk* darum bemüht, die Drohnen auch als zivil nützliche Instrumente darzustellen. Sie könnten auch bei der Bekämpfung von Umweltkatastrophen helfen. (Ob dies für mit optischen- oder Infrarotsensoren ausgerüsteten Systeme zutrifft, könnte diskutiert werden. Aber dass man dafür den Telefon- und Funkverkehr abhören müsse, erscheint wenig plausibel.) Immerhin haben die Untersuchungen des Ausschusses auch zutage gefördert, wofür solch umfassende *Datenstaubsauger* auch nützlich sein könnten: Die Herstellungsfirma wollte die Drohnen der EU für die Flüchtlingsabwehr *FRONTEX* andienen. *Eurohawk* sollte der Bundesregierung *ressortübergreifend* offeriert werden, also auch für die *innere Sicherheit*. Zu denken ist an Ausspähungsmaßnahmen im Vorfeld von Großdemonstrationen, Streiks usw.

Wie wir wissen, wurde die Beschaffung von fünf Trägersystemen *Eurohawk* gestoppt, die Entwicklung des Aufklärungssystems *ISIS* allerdings konsequent zu Ende geführt. Diese Apparatur muss jetzt in eine andere Trägerplattform eingebaut werden. Was letzten Endes daraus werden wird, wissen wir zur Zeit noch nicht; fest steht jedoch, dass die Bundeswehr in wenigen Jahren über solche HighTech-Spionage-Instrumente verfügen wird. Ob dabei auch schon mal ein Handy einer ausländischen Regierungschefin abgehört werden wird?

Dass diese Entwicklungen – Kampfdrohnen wie ungehinderte Ausspähung durch Spionagesatelliten – strikt abgewiesen werden müssen, versteht sich. Aber machen wir es uns nicht zu einfach: Ist eine umfassende Aufklärung, die nicht zuletzt auch militärische Fakten einbeziehen muss, nicht eine wichtige Grundlage staatlichen Handelns? Brauchen nicht gerade internationale Einrichtungen wie die UNO oder die OSZE solche Aufklärungsmöglichkeiten, um politische und sonstige Entwicklungen überhaupt adäquat beurteilen zu können? Und kann der Hinweis auf Fälle, in denen mit sogenannten Aufklärungs- oder Spionage-Erkenntnissen Kriege bzw. bewaffnete Konflikte ausgelöst wurden, oder auch Krisen verschärft wurden, nicht umgedreht werden? Wenn man genauer wüsste, ob ein abgestürztes Flugzeug abgeschossen wurde und auch noch von wem, wenn man genau wüsste, wer in einem Krieg/Bürgerkrieg bestimmte Waffentypen eingesetzt hat (Beispiel C-Waffen), hätte man damit nicht eine Handhabe, um Provokationen zu entlarven und damit ins Leere laufen zu lassen? Kann so verstandene Aufklärung auch für Verhandlungsprozesse von Nutzen sein? Das wird man schwerlich pauschal abweisen können.

Das Grundproblem liegt in dem Wort *geheim*. Wer kontrolliert die sogenannten Nachrichtendienste? Wie viel Transparenz ist erforderlich, damit eine solche öffentliche, parlamentarisch-demokratische Kontrolle überhaupt möglich erscheint?

Was die Satellitensysteme der EU-Staaten, darunter auch das Beobachtungszentrum in Torrejon, anbetrifft, so schlugen Friedensforscher/-innen schon vor geraumer Zeit vor, dass die Daten, die dort gesammelt werden, *internationalisiert*, d.h. zum Beispiel der OSZE zur Verfügung gestellt werden sollten. Damit würden diese Informationen nicht mehr zu Herrschaftszwecken missbraucht werden und könnten von Allen nutzbringend eingesetzt werden. Ob ein solches Herangehen möglich, ob es sinnvoll ist, ob es überhaupt wahrscheinlich ist, und ob man es auf den Bereich der Drohnen-Aufklärung übertragen kann, muss weiter diskutiert werden.

Was die weitere Perspektive der *Dienste* betrifft, wird man mit einer pauschalen Forderung nach deren Auflösung in der heutigen Welt nicht weit kommen. Keine Regierung wird sich auf *Spiegel online*, *Breaking News* von CNN, *al Jazeera* – oder welches Medium auch immer – verlassen, um daraus Schlüsse für Regierungshandeln abzuleiten. Man wird auf Primärinformationen, auf authentischen Quellen bestehen, um sich ein eigenes Lagebild zu verschaffen. Das große Problem beginnt vor allem dort, wo die Nachrichtendienste operative Politik machen und dabei meinen, weil im Verborgenen, auch schlimme, verbotene Dinge tun zu dürfen. Die Überlegungen und Vorschläge sollten sich ergo darauf richten, wie aus Geheimdiensten parlamentarisch zu kontrollierende Nachrichtendienste werden können!

Es wird auch darauf ankommen, sich der unbegrenzten Durchsetzung der Drohnen-Aufrüstungsprogramme entgegenzustellen und dringliche Forderungen zu deren Regulierung zu entwickeln. Dass die Entwicklung der Drohnentechnologie und damit die Robotisierung des Krieges unaufhaltsam seien, muss man nicht glauben. Noch muss und kann alles dafür getan werden, den Einsatz der Kampfdrohnen durch internationale Abkommen zu ächten und die Verwendung von unbewaffneten Drohnen sehr genau zu regeln und einzuhegen. Hier ist internationale Rüstungskontrolle und Abrüstung gefragt. Und die Bundeswehr kann einseitig auf die Beschaffung der Kampfdrohnen verzichten. Das wäre eine friedensstiftende Maßnahme.

Wie ist das militärische Nachrichtenwesen in Deutschland organisiert?

Der Bedeutungszuwachs der Informationsbeschaffung und -auswertung für das Militär hat dazu geführt, dass der Gesamtbereich des militärischen Nachrichtenwesens 2007/2008 umorganisiert wurde.

Das *Zentrum für Nachrichtenwesen der Bundeswehr (ZNBW)* wurde am 31. Dezember 2007 aufgelöst. Die *Lagebearbeitung*

für das Bundesministerium der Verteidigung und die Bundeswehr erfolgt seitdem durch den Bundesnachrichtendienst, der jetzt das Monopol für die *Auslandsaufklärung* hat. Dies machte die Umsetzung hunderter Dienstposten erforderlich. Mitarbeiter der sogenannten Feldnachrichtenkräfte der Truppe wurden in den BND eingegliedert. Sie erfüllen inzwischen die Aufgabe, die Streitkräfte bei den Kriseninterventionen mit den erforderlichen Nachrichten zu versorgen; zugleich soll der BND die politische Führung in die Lage versetzen, angemessen auf die zahlreichen Krisenprozesse zu reagieren.

Der übrig gebliebene *Rest* ist bei der Bundeswehr geblieben: Dazu zählen die Satelliten-Aufklärung (SAR Lupe, Helios 2) und die signalerfassenden Systeme (wie die Flottendienstboote), die vom Kommando *Strategische Aufklärung* in Rheinbach bei Bonn geführt werden. Dort laufen dann die Informationen zusammen, die an die zuständigen Regierungsbehörden, den BND und andere weitergeleitet werden. Während der BND über eine MitarbeiterInnen-Zahl von ca. 5000 Personen verfügt, weist das Kommando *Strategische Aufklärung* auch einen Beschäftigten-Umfang von 5300 Menschen (= 4729 militärische und 579 zivile Dienstposten) aus. Das ist schon eine nicht gering zu schätzende Arbeitskapazität, lässt sich mit den Größenordnungen der US-Dienste allerdings nicht vergleichen (allein die NSA soll über 40000 Mitarbeiter verfügen).

Die Drohnen, die die Bundeswehr auf den Einsatz-Schauplätzen benutzt, werden bisher von den Teilstreitkräften (Heer, Luftwaffe) eingesetzt und geführt. Im Falle der *Eurohawk* war die Unterstellung noch nicht festgelegt; die Verschiebung der Beschaffung hat diese Frage bis heute offen gelassen. Von einer künftigen Zentralisierung der Drohnen-Systeme ist jedoch auszugehen.

Steigt auch die Bundeswehr in die Cyber Warfare ein?

Das neueste Spielfeld der Informationskriegführung heißt *Cyber Space*. Hierbei geht es um alles, was mit Computern, der Einwirkung auf Computer, Software etc. und dem Internet zu tun hat. Spätestens seit der Einschleusung der Schadsoftware *Stuxnet* in die iranischen Atomanlagen (über USB-Sticks), um diese zu zerstören oder zu schädigen und damit den Fortgang des dortigen Atomprogrammes zumindest beträchtlich zurückzuwerfen, ist auch einer größeren Öffentlichkeit bewusst geworden, dass sich hier ein neuer konfliktträchtiger Raum auftut. Stuxnet wird inzwischen eindeutig US-amerikanischen Urhebern zugeschrieben. Paradoxerweise muss dieser Trojaner in NATO-Debatten immer wieder herhalten, um die Dringlichkeit der Abwehr neuer Bedrohungen hervorzuheben.

Die NATO hat in ihrem Strategischen Konzept von 2010 erstmals das Thema *Cyber Security* prominent erwähnt; im Juni 2011 wurde ein weitreichender Beschluss über eine *Cyber Defense Policy* gefasst. Ein umfangreicher Maßnahmekatalog wurde verabschiedet.[7]

Natürlich war auch die Bundeswehr schon länger dabei, allerdings – wie wir heute wissen – nicht auf hohem Niveau.

Einen ersten, wenig aussagekräftigen Bericht übersandte das *Bundesministerium der Verteidigung (BMVg)* dem Verteidigungsausschuss im Juni 2011, der aber weiter keine Beachtung fand. Als Abgeordneter und Mitglied des Verteidigungsausschusses habe ich nachgefragt, darauf gedrängt, dieses Thema im Ausschuss zu behandeln. Zunächst ohne Wirkung. Im April 2012 folgte ein weiterer, immer noch recht dürftiger Bericht des BMVg, der viele Fragen unbeantwortet ließ. Ich sah mich dadurch herausgefordert und begab mich am 19. September 2012 direkt ins zuständige Kommando nach Rheinbach, um mich vor Ort briefen zu lassen. Auch andere Mitglieder des Ausschusses taten dies.

Der Verteidigungs-Ausschuss befasste sich erstmals eingehender mit dem Cyber-Thema auf seiner Sitzung am 30. Januar 2013. Dort trug ein Vertreter des *Bundesministers des Inneren* über die Maßnahmen im zivilen Bereich vor und berichtete über den Aufbau eines Nationalen Cyber-Abwehrzentrums. Der Ausschuss erfuhr erstmals durch BMVg-Vertreter einiges über den Aufbau einer *Cyber Unit* beim Kommando *Strategische Aufklärung* der Bundeswehr.

In einem ausführlicheren Bericht vom 16. April 2013 konnten die Abgeordneten mehr über die im Aufbau befindliche Abteilung *ComputerNetzwerk-Operationen* beim KSA erfahren. Die Debatte darüber erfolgte am 13. Juni 2013.

Zum damaligen Zeitpunkt verfügte diese spezielle Abteilung über 59 Dienstposten (die Zahl derer, die sich mit Cyber-Sicherheit beschäftigen, ist natürlich viel größer), ein rapider Aufwuchs war nicht vorgesehen, die Ausstattung wirkte eher bescheiden. Man habe eine „Anfangsbefähigung zum Wirken in gegnerischen Netzen" inzwischen erreicht, lautete die Botschaft des Berichts an den Ausschuss und des Briefings vor Ort. Was dies im Einzelnen bedeutet, blieb zunächst unklar. Die Simulation bestätigte nur, dass man im Prinzip mittels auf dem Markt vorfindlicher Werkzeuge in der Lage ist, die Luftabwehr eines potenziell gegnerischen Landes empfindlich lahm zu legen. Ob man aber auch tatsächlich schon in „gegnerischen Netzen" operiert, oder sich nur die Option verschafft hat, bleibt weiter offen.

Paul Schäfer

Paul Schäfer: Jg. 1949, Diplom-Soziologe, Publizist, lebt in Köln, von 1983 bis 1990 Redakteur der Zeitschrift *Wissenschaft und Frieden*, von 2005 bis 2013 Mitglied des Deutschen Bundestages und verteidigungspolitischer Sprecher der Fraktion Die LINKE.

Zumindest wissen wir jetzt mehr über die Cyber-Philosophie der deutschen Streitkräfte:

- Man vermeidet den Ausdruck *Cyber-Krieg*, sondern spricht stattdessen von *Cyber-Verteidigung*.

- Der *Cyber-Raum* wird – neben Luft, Land, See – schlicht als neue Dimension möglicher Auseinandersetzungen angesehen. Daher sei dieser Raum eine eigenständige operative Domäne, aber in der Sache gehe es *nur* um die Fortsetzung früherer militärischer Kampfoptionen mit neuen Mitteln (wenn man so will, als *ELoKa 2.0*). Im Bericht vom 13. April 2013 heißt es daher lapidar, bei den Aktivitäten im Cyber-Raum handele es sich um ein „weiteres Wirkmittel der Streitkräfte".

- Dass in diesem Bereich Defensive und Offensive nicht strikt zu trennen sind, stellt der Bericht nicht völlig in Abrede. Offensive Operationen werden als probates Mittel betrachtet, um Cyber-Attacken auf die eigenen Netze abzuschrecken. Die Grenzen sind zudem fließend: Schon bei der Vorfeldaufklärung über mögliche Cyber-Attacken kann es passieren, dass man in gegnerisches Systeme *eindringt*. Schließlich und am wichtigsten: Immer geht es bei der sogenannten Cyber-Abwehr auch um Aktionsspielräume der eigenen militärischen Kräfte bei Kriseninterventionen. Und ob es dabei immer um legitime Selbstverteidigung geht, darf bezweifelt werden.

- Die Bundeswehr zeichnet ein ziemliches diffuses Bild einer gegebenen Bedrohungslage, Das kennen wir auch aus der grundsätzlichen Bedrohungsanalyse der Streitkräfte. Aus dem eigenen *Lager* hervorgebrachte Bedrohungen, wie die Angriffe durch Stuxnet, werden umstandslos als Beleg aufgeführt; die Gesamtsumme der Angriffe im Netz, also auch und gerade im zivilen Bereich, muss als Beweis dafür herhalten, dass man die eigenen Anstrengungen erheblich steigern müsse. Und dazu gehört es eben auch (s.o.), die eigenen Fähigkeiten zum Eindringen in fremde Netze voranzutreiben.

- Dass nicht alle rechtlichen Fragen geklärt, wird eingeräumt. Eine der zu beantwortenden Fragen: Wann muss eine Cyber-Attacke auf Einrichtungen eines NATO-Mitgliedslandes als Angriff gewertet werden, der den Bündnisfall mit entsprechenden Beistandsverpflichtungen auslöst? Klärungsbedürftig sind auch Fragen im Zusammenhang des Parlamentsvorbehalts bei bewaffneten Einsätzen: Bedürfen aggressive Operationen in gegnerischen Netzen der Zustimmung des Parlaments? Muss darüber nicht zumindest im Vorfeld informiert werden? Muss das Parlamentsbeteiligungsgesetz hier weiterentwickelt werden? Immerhin scheint sich die Bundesregierung im internationalen Rahmen daran zu beteiligen, einen Verhaltenskodex für den Umgang mit empfindlichen Daten in den jeweiligen Netzwerken entwickeln zu wollen. In der entsprechenden Arbeitsgruppe der OSZE ist man aktiv.

Natürlich spielte in jüngster Zeit auch die Frage eine Rolle, welche Kooperationsbeziehungen die Bundesrepublik auf diesem Gebiet mit den USA oder anderen NATO-Staaten eingegangen ist und wie diese Zusammenarbeit künftig gestaltet werden sollte.

Die alte Bundesregierung hat dazu lediglich mitgeteilt, dass man sich in puncto Risikomanagement und Bedrohungsanalyse selbstverständlich mit den Bündnispartnern austausche (zuständig dafür ist auf deutscher Seite das *Computer Emergency Response Team der Bundeswehr (CERTBw))*. Aber das hätte man gerne genauer gewusst.

Fazit: Auch auf diesem Feld gilt es, unter kritischen Vorzeichen weiterführende Vorschläge zur Einhegung, Kontrolle usw. zu erarbeiten. Zumindest lässt sich sagen:

- Gegen Cyberterror hilft nicht zuletzt die Beseitigung der Sicherheitsmängel bestehender IT-Systeme. Da ist gewiss einiges in der jüngeren Vergangenheit geschehen, aber es kann noch mehr getan werden.

- Für den Gesamtbereich der *Netzpolitik* – ob es sich da um kommerzielle Nutzer, um Privatpersonen oder Regierungseinrichtungen handelt – gilt, dass der Grundwert *Schutz der Privatsphäre jedes Einzelnen/jeder Einzelnen* neu bekräftigt und durchgesetzt werden muss. Weder die ungehemmte Ausspähung Anderer noch das verdeckte Eindringen in *fremde Netze* sind statthaft.

- Eine neue Art Rüstungswettlauf im Bereich Cyber (Warfare) ist der falsche Weg; stattdessen muss auch hier der Weg in internationalen Regimen der Rüstungskontrolle und der Abrüstung gesucht werden:

- Da es innerhalb der NATO einen unabweisbaren Nexus zwischen Militäreinsätzen *out of area* und der Informations-/Cyber-Kriegsführung gibt, müssen diese Kriseninterventionen immer wieder kritisch hinterfragt werden. Die Stärkung der Friedens- und Konfliktforschung und der weitere Ausbau der zivilen Konfliktbearbeitung wären da eine prima Alternative.

Anmerkungen

1 *Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion Die LINKE, Zur Rolle des in Deutschland stationierten United States Command bei gezielten Tötungen durch US-Streitkräfte in Afrika, Dt. Bundestag, Drs. 17/14401 vom 18.07.2013*

2 *Ebd., S. 4*

3 *zitiert nach Berliner Umschau vom 25.10. 2013*

4 *Ruhmann, Ingo, Cyberterrorismus – Das Internet unter Kriegsrecht? in: S+F 2/2000, S. 144-149*

5 *Amt für Studien und Übungen (G.W. Meyer), Streitkräfteeinsatz 2020, 1996*

6 *Wer Näheres wissen will: Deutscher Bundestag, Drucksache 17/14650, oder: EURO HAWK Untersuchungsausschussbericht, Bundesanzeiger Verlag 2013*

7 *Mehr unter: NATO and Cyber Defense, s. www.nato.int/cps/en/natolive*

FIfF e.V.

FIfF-Studienpreis 2013

Beiträge der Preisträgerinnen und Preisträger

Im Rahmen der FIfF-Jahrestagung 2013, deren Beiträge in diesem Heft versammelt sind, haben wir – wie in den Jahren zuvor – den FIfF-Studienpreis verliehen. In der letzten Ausgabe haben wir bereits die Laudationes der Preisverleihung abgedruckt; diesmal stellen die Preisträgerinnen und Preisträger selbst ihre Arbeiten und Ergebnisse vor.

Daniel Spittank untersucht in seinem Beitrag *Too smart for you? – Anforderungen an den Einsatz von mobilen Informatiksystemen in der Schule* die Kriterien, nach denen mobile Systeme wie Tablets und Smartphones im Unterricht ausgewählt und eingesetzt werden sollten. Er stellt die Frage in den gesellschaftlichen Kontext der mobilen Kommunikation: Ziel ist die mündige Teilhabe an der digitalen Gesellschaft. Dazu fordert er, dass diese gesellschaftsverändernden Systeme in der Schule berücksichtigt werden – am ehesten in einem verpflichtenden Informatikunterricht, der seinem Namen gerecht wird. Dafür darf er sich nicht nur auf die reine Anwendungsperspektive beschränken, sondern muss auch die Analyse und Veränderung der Wirklichkeit thematisieren.

Agata Królikowski behandelt in Ihrem Artikel *‚Due to legal Issues' – Packet Inspection* die Anwendung von Packet Inspection zur Analyse von Verkehrsdaten, deren Auswertung die Erstellung von Sozialbeziehungs- und Bewegungsprofilen erlaubt. Sie untersucht, ob und mittels welcher technischer oder rechtlicher Maßnahmen sich Nutzerinnen und Nutzer vor Angriffen auf ihre Kommunikation schützen können. Auch wenn sie dabei zu dem Schluss kommt, dass es letztlich keinen Schutz gegen PI-Angriffe gibt, ist das Sichtbarmachen der Problematik ein erster Schritt in Richtung einer umfassenden Aufklärung und Sensibilisierung.

Julia Hofmann stellt in ihrem Beitrag *Zweckgebundener Datenbrief für das Identitätsmanagementsystem mittels Web-basiertem Benutzerinterface* eine Implementierung vor, mit der sich Nutzerinnen und Nutzer an der TU Darmstadt selbstständig über ihre gespeicherten und verarbeiteten personenbezogenen Daten informieren können. Dadurch wird die in §34 BDSG geforderte Auskunftspflicht realisiert und dabei die Schutzziele des technischen Datenschutzes nach dem Grundsatz *Privacy by Design* erreicht. Die Arbeit zeigt, dass Befürchtungen, die praktische Umsetzung eines Verfahrens zur Erfüllung der Auskunftspflicht sei mit zu hohem Aufwand verbunden, unbegründet sind.

Der geplante Beitrag von *Helge Peters* zu seiner Arbeit *Biopolitical Simulations: Governing Life in FuturICT,* die sich mit vorausschauender Simulation globaler sozialer und ökonomischer Systeme durch die Nutzung von *Big-Data*-Techniken kritisch auseinandersetzt, konnte leider nicht bis zum Redaktionsschluss fertiggestellt werden und erscheint voraussichtlich in der nächsten Ausgabe.

1. Preis	***Daniel Spittank*** ***Bergische Universität Wuppertal*** *Auswahl und Gestaltung mobiler Informatiksysteme für den Einsatz im Informatikunterricht*	Seite 43
2. Preis	***Agata Królikowski*** ***Humboldt-Universität zu Berlin*** *‚Due to legal Issues' – Packet Inspection*	Seite 48
3. Preis	***Julia Hofmann*** ***Technische Universität Darmstadt*** *Zweckgebundener Datenbrief für das Identitätsmanagementsystem mittels Web-basiertem Benutzerinterface*	Seite 52
Sonderpreis	***Helge Peters*** ***University of London*** *Biopolitical Simulations: Governing Live in FuturICT*	Geplant für die nächste Ausgabe

FIfF-Studienpreis 2013
1. Preis

Daniel Spittank

Too smart for you? – Anforderungen an den Einsatz von mobilen Informatiksystemen in der Schule

An dieser Stelle möchte ich mich noch einmal beim FIfF für die Auszeichnung meiner Examensarbeit[1] bedanken. Im Folgenden möchte ich die Chance ergreifen, die gesellschaftlichen Veränderungen näher zu charakterisieren, die ich in meiner Arbeit im Wesentlichen aus der informatisch-didaktischen Perspektive betrachtet habe. Auf die tatsächliche Umsetzung, die Wahl der Programmiersprache, die Python-Klassenbibliothek und deren didaktische Begründungen gehe ich hier nicht weiter ein.

Ein dominierendes Thema des Jahres 2013 war die von Edward Snowden losgetretene Debatte, die dessen Enthüllung der globalen, digitalen Spionagetätigkeiten der NSA[2] folgte. Plötzlich wurde einer breiten Öffentlichkeit bewusst, dass flächendeckende Überwachung weder eine wirre Idee von seltsamen Nerds mit Aluhüten auf dem Kopf, noch eine eher theoretische Möglichkeit ist. Vielmehr ist dies – nicht nur seitens der NSA und des britischen GCHQ[3] – inzwischen Alltag.

Auch private Akteure strecken beinahe wie gierige Kraken ihre Arme nach den privaten Daten nahezu aller Internetnutzer aus. So weiß nicht nur *Amazon*, was einem gefallen könnte, und kann so in naher Zukunft die Waren absenden, bevor der Kunde überhaupt weiß, dass er sie bestellen will[4], auch *Google Now* kann dem Smartphonenutzer sofort mitteilen, was dieser als Nächstes zu tun gedenkt und wo er sich voraussichtlich in der nächsten Stunde aufhalten wird.

Die diversen Internetdienste und Apps bringen allesamt nützliche Funktionen mit, die den Anwendern das Leben einfacher machen können. Durch die sich immer weiter verbreitenden mobilen Informatiksysteme (u. a. Smartphones und Tablets) und die nahezu flächendeckende Verfügbarkeit von mobilem Internet sind diese Dienste nicht nur immer verfügbar; vielmehr verliert die Frage ihren Sinn, ob man gerade online ist. Schlagwörter wie *Always-On* oder das „Internet der Dinge" machen deutlich, wohin die Reise geht.

Dass neben diesen nützlichen Funktionen perfekte, digitale Wanzen in unseren Alltag einzogen, die die flächendeckende Überwachung erst möglich machten, beginnt vielen Menschen erst heute, nach den Veröffentlichungen von Edward Snowden, klar zu werden.

Allgegenwärtige Informatik

In allen modernen Gesellschaften nehmen Informatiksysteme inzwischen einen wichtigen Platz ein. Man findet kaum ein elektrisches Gerät, das ohne Mikroprozessoren und Software auskommt. Selbst Kühlschränke, Toaster und Bügeleisen erfüllen heute die Definition von Informatiksystemen. Mal transparent für den Anwender, indem etwa der Teekessel per WLAN an das Smartphone meldet, wenn das Wasser kocht. Mal weniger transparent, wenn das Bügeleisen das Notebook mit einem Trojaner infiziert[5].

Unsere Welt ist durchdrungen von Informatik. Überall finden sich Informatiksysteme, ständig sind um uns herum informatische Prinzipien am Werk, laufen Algorithmen ab, die unser Leben für uns – und für Dritte – auswerten und berechenbar machen. Viele davon füttern wir selbst mit Daten, doch noch mehr sind uns im Alltag oft gar nicht bewusst. Die informatischen Systeme werden immer kleiner und unscheinbarer. Wo vor wenigen Jahrzehnten eine Fabrikhalle und noch vor wenigen Jahren ein Desktopcomputer notwendig waren, reicht heute für dieselbe Rechenleistung ein einfaches Smartphone.

Besonders stark sind die Veränderungen an den mobilen Informatiksystemen zu erkennen. Kaum jemand hat heute noch kein Mobiltelefon in der Tasche, die meisten verwenden sogar ein Smartphone, das beständig mit dem Internet verbunden ist. Mobile Datenflatrates machen dies möglich und erschwinglich.

Die sichtbarste gesellschaftliche Veränderung ist die der Kommunikation. Immerwährende Erreichbarkeit und ständig verfügbare globale Kommunikationskanäle haben direkten Einfluss auf das menschliche Verhalten. Sei es die von manchen Sprachforschern gescholtene Veränderung der Sprache (SMS-Sprache), die Hoffnung auf friedlicheres, demokratischeres Zusammenleben oder die Zunahme von Stress, da Beruf und Privatleben durch die ständige Erreichbarkeit nicht mehr klar zu trennen sind[6].

Ebenso offensichtlich ist der potenzielle Nutzen als universelles Werkzeug. Diese mobilen, digitalen *Schweizer Taschenmesser* sind inzwischen so mit Sensoren vollgestopft, dass es für viele Nutzer eine Freude ist, damit herumzuspielen – dank *Gamification*[7] im wahrsten Sinne des Wortes. Erweitert werden die Datenerfassungsmöglichkeiten dabei noch um externe Sensoren. Besonders beliebt sind derzeit diverse Fitness- und Gesundheitsgadgets wie Pulsmesser und Schrittzähler.

Die schiere Menge der verfügbaren Daten macht die mobilen Informatiksysteme dank – mal mehr, mal weniger – ausgeklügelter Software zu den persönlichen Assistenten, die schon vor Jahren mit den ersten Generationen der PDAs versprochen wurden. Durch GPS und andere Methoden der Positionsbestimmung, den Abgleich mit Kartenmaterial und den Daten aus dem persönlichen Kalender kennen diese Assistenten uns und unsere Verhaltensweisen und Gewohnheiten teilweise besser als wir uns selbst. Dabei hören sie dank *Siri*, *Google Voice* oder *S-Voice* auf's Wort und das mit verblüffender Genauigkeit. Die nächste Generation der mobilen Geräte steht mit Datenbrillen wie *Google Glass* bereits in den Startlöchern – noch unscheinbarer, nützlicher, allgegenwärtiger und datenhungriger als bisherige Systeme. In Zukunft werden sie wohl direkt Personen, mit denen wir reden, identifizieren können und uns live mit Zusatz-

informationen zu diesen und zu den Gesprächsinhalten versorgen können. Smart, fast magisch.

Doch auf wessen Wort hören die klugen Helferlein eigentlich? Mit wem reden sie? Diese und andere Fragen sind durch die reine Anwendungsperspektive nicht zu klären, sie stellen sich mitunter gar nicht erst. Von außen erscheinen die Systeme als Blackboxen, die mehr oder weniger das tun, was wir von ihnen erwarten. Dass unsere braven Assistenten sich jedoch stetig im Hintergrund mit ihrer jeweiligen Assistentenzentrale beraten, wird erst deutlich, wenn man sich mit dem informatischen Hintergrund beschäftigt. Für den normalen Nutzer wird selten ersichtlich, was die Geräte tatsächlich anstellen, da dies meist alles andere als offensichtlich ist.

Es ist sogar so, dass sich die Hersteller alle Mühe geben durch fortschreitende Simplifizierung entscheidende Aspekte der Funktionsweise vor den Anwendern zu verbergen. Denn schließlich wollen diese doch eigentlich gar nicht wissen, wie es funktioniert! Oder etwa doch? Nein, denn sie haben es nicht zu wollen. Neugierige Blicke werden durch technische und juristische Kunstgriffe gezielt abgelenkt. Bei Verstößen drohen Verlust von Garantie oder Benutzerkonten, inklusive gekaufter Inhalte.

So würde man für gewöhnlich kaum vermuten, dass das Verschönern eines Fotos mit lustigen Effekten voraussetzt, dass dieses Foto zunächst auf den Server des Anbieters geladen wird und sich dieser in seinen AGBs sämtliche Nutzungsrechte dafür einräumen lässt. Ebenso zeigen sich viele Nutzer überrascht, dass die elektronische Kommunikation mit ihren Freunden und Bekannten auf den Servern der Anbieter landet und von diesen ausgewertet werden kann, da dies den bekannten und erprobten Kommunikationskonzepten aus dem Alltag nicht entspricht. Mögliche Risiken lassen sich dabei durch die Nutzer selten richtig einschätzen, da die notwendigen informatischen Grundlagen fehlen. Fordert ein kostenloses Spiel für ein Smartphone den Zugriff auf Kalender- und Kontaktdaten und gleichzeitig vollen Internetzugriff an, so reagieren viele Anwender nicht skeptisch, sondern mit einem Klick auf ‚Ok'. Skepsis tritt höchstens im Nachhinein auf, wenn man feststellt, dass die smarten Gadgets in der Grundkonfiguration bereits alle Daten in die Cloud synchronisiert haben.

Die Hersteller der Geräte bzw. die Betreiber der zugrunde liegenden Dienste erhalten also einen Informationsvorsprung gegenüber den Anwendern. Zusätzlich geraten letztere in eine Abhängigkeitsfalle gegenüber ersteren. Dies sieht man am Lock-In bei den verschiedenen Smartphone-Plattformen: Wer die Plattform wechselt, verliert alle Investitionen, die bisher getätigt wurden. Gekaufte Apps sind nicht mehr nutzbar, kopiergeschützte Medien auf der anderen Plattform nicht mehr verfügbar und gekaufte Zusatzhardware ist oft schlicht nicht kompatibel. Noch deutlicher wird dies bei sozialen Kommunikationsplattformen: Man muss eine Plattform nicht nutzen, doch wenn die sozialen Kontakte zum Beispiel *Facebook* oder *Whatsapp* verwenden, verliert man beim Verzicht auf diese Dienste den Anschluss.

Es droht also ein Verlust an Selbstbestimmung zugunsten nützlicher Unterstützung. Ein Teil unseres Denkens geben wir an smarte Gadgets ab, die dies doch soviel effizienter erledigen als wir. Zusätzlich bezahlen wir diesen Service mit unseren privaten Daten. Dies geht natürlich mit dem Verlust von Freiheit einher, was durch die Möglichkeit zur Totalüberwachung durch die Anbieter der entsprechenden Plattformen und aller anderen, die Zugriff auf die anfallenden Daten erlangen, verstärkt wird.

Sind diese mobilen Informatiksysteme somit vielleicht sogar zu smart für uns? Oder stellt sich die Frage nach einer mündigen, aufgeklärten Teilhabe an der Gesellschaft gar nicht mehr, wenn mein Smartphone doch genau weiß, was ich wo und auf welche Weise als Nächstes tun sollte?

Ein – notwendiger – breiter gesellschaftlicher Diskurs, der den gesellschaftlichen Veränderungen Rechnung trägt, findet hier jedenfalls nicht statt. Bestenfalls werden Teilaspekte wie einzelne Facetten des Datenschutzes erörtert.

Notwendigkeit informatischer Bildung

Aus meiner Sicht ist es zwingend erforderlich, sich über die reine Anwendungsperspektive hinaus zu erheben, will man nicht Jahrhunderte gesellschaftlicher Entwicklung und Aufklärung verwerfen. Die reine Anwendungssicht wird der Realität der allgegenwärtigen Informatik nicht gerecht. Vielmehr kostet sie letztlich die Selbstbestimmtheit der handelnden Akteure. Wie schon Goethe schrieb: „Was man nicht versteht besitzt man nicht."

Es ist zwingend notwendig, Menschen in die Lage zu versetzen, moderne Informatiksysteme selbstbestimmt und verantwortungsbewusst zu verwenden und die mit Ihnen verbundenen Risiken und Nebenwirkungen einschätzen zu können, ohne zunächst den Informatiker ihres Vertrauens zu befragen, will man die mündige Teilhabe in demokratischen Gesellschaften sicherstellen.

Aktueller Stand in der Schule

Besonders bei Kindern und Jugendlichen sind die gesellschaftlichen Veränderungen längst angekommen[8]. Es findet sich kaum eine Klasse, in der nicht die große Mehrheit der Schülerinnen und Schüler über Smartphones verfügt. Doch von bewusster und mündiger Nutzung kann hier nur selten die Rede sein. Das ist natürlich nur logisch, denn nirgendwo wird dieser bewusste Umgang tatsächlich vermittelt.

Jeder Mensch müsste heute über eine grundlegende informatische Vernunft[9] verfügen, die weit über reines Anwendungswissen hinausgeht. Natürlich fällt diese nicht vom Himmel, sondern muss sich zunächst entwickeln. Hier sind die bestehenden Bildungsinstitutionen gefragt, allen voran die allgemeinbildenden Schulen. Doch leider findet an vielen Schulen kein geregelter und zielgerichteter Informatikunterricht statt, der die notwendigen Anforderungen zur Entwicklung informatischer Vernunft erfüllen kann. Informatik ist nur in wenigen Bundesländern ein Pflichtfach und es mangelt an ausgebildeten Lehrkräften. Wenn überhaupt Informatik unterrichtet wird, handelt es sich oft um einseitige Computernutzungs- oder Programmierkurse. Erstere verharren wiederum in der reinen Anwendungsperspektive, letztere verlieren viel zu häufig den Anspruch der allgemeinen Bildung aus den Augen und beschränken sich darauf, gute

Programmierer hervorzubringen[10]. Beide sind damit zu einseitig aufgestellt, um dem Ziel der Entwicklung informatischer Vernunft zu dienen.

Nebenbei vermittelt der Informatikunterricht häufig ein falsches Bild von Informatik, da die exklusive Nutzung von Computerräumen den Eindruck zementiert, dass sich die Informatik nur mit Computern beschäftigen würde. Außerdem stehen die räumlich festgelegten Computerarbeitsplätze moderneren Unterrichtsformen im Weg und erschweren oftmals die wichtige Kommunikation zwischen den Schülerinnen und Schülern.

Die Nutzung mobiler Informatiksysteme verspricht hier Abhilfe zu schaffen und den Informatikunterricht zu flexibilisieren sowie Fehlvorstellungen entgegenzuwirken. Die häufigste Reaktion auf die gesellschaftlichen Veränderungen durch die Verfügbarkeit mobiler Informatiksysteme ist jedoch – keine. Die zweithäufigste ist die Einführung von Verboten. Natürlich ist es nicht die Aufgabe der Schule, Modetrends hinterherzulaufen, jedoch zeichnet sich deutlich ab, dass klassische Informatiksysteme an Bedeutung verlieren[11].

Erfolgt die Nutzung von mobilen Informatiksystemen im Unterricht, wie es in Leuchtturmprojekten und an einzelnen Schulen geschieht, so wird diese häufig von überbordendem Enthusiasmus und größtenteils unkritisch begleitet. Dies wird von den Herstellern von Konsumgeräten vorangetrieben, so strebt etwa Apple an die Schulen[12] und umwirbt diese mit speziellen Angeboten und Inhalten. Das Verlassen der Anwendungsperspektive unterbleibt.

Bisherige Ansätze

Jenseits der Informatik beschränkt sich die Beschäftigung mit den mobilen Informatiksystemen leider allzu häufig auf reine Klickanleitungen, begrenzte, künstliche Lernumgebungen[13] oder Informationsbroschüren für Eltern, Lehrer und Schüler, die oft sehr einseitig auf die möglichen Gefahren ausgerichtet sind und kaum hilfreiche Handlungsalternativen anbieten. Natürlich kann man Schülerinnen und Schülern raten, bei der Nutzung sozialer Kommunikationsplattformen besonders zurückhaltend zu sein. Besonders sinnvoll ist dies jedoch nicht, denn hier wirkt sich der oben beschriebene Lock-In-Effekt besonders deutlich aus: Wer online nicht dabei ist, verpasst den Anschluss.

Hilfreiche Handlungsalternativen zu geben, ist auf einer anwendungsorientierten Ebene nur schwer möglich, da – wie bereits erwähnt – der notwendige informatische Hintergrund fehlt. Doch was man nicht versteht, kann man nicht sinnvoll anwenden.

Es gibt einige Beiträge aus der Informatik-Fachdidaktik, die den Einsatz von mobilen Informatiksystemen untersuchen. Hervorzuheben sind besonders die Arbeiten von Ralph Carrie[14], Matthias Heming[15] sowie die Beiträge und Pilotkurse von Ludger Humbert[16].

Matthias Heming zeigte in seiner Arbeit, dass ein Informatikunterricht, der auf Mobiltelefone als einzige Informatiksysteme setzt, nicht nur möglich ist, sondern auch den Bildungsstandards der Gesellschaft für Informatik (GI) für die Sekundarstufe I als auch den Vorgaben und Anforderungen des Zentralabiturs in NRW genügt.

Es wurden auch erste Konzepte zum Einsatz mobiler Informatiksysteme im Informatikunterricht entwickelt, die später weiterentwickelt und in mehreren Kursen an der Willy-Brandt-Gesamtschule in Bergkamen erprobt wurden. Dabei entstanden auch umfangreiche Unterrichtsmaterialien[17], die aufgrund ihrer Ausrichtung auf das nicht mehr verfügbare Symbian OS leider nur noch begrenzt anwendbar sind.

Die Erfahrungen hiermit waren insgesamt sehr gut. Die Lernziele wurden erfolgreich erreicht und der Unterricht war für die Schülerinnen und Schüler motivierend und spannend.

Kriterien für den Einsatz mobiler Informatiksysteme

Ein wesentlicher Teil meiner Arbeit war die Suche nach Kriterien für den Einsatz mobiler Informatiksysteme im Informatikunterricht. Die grundlegenden Anforderungen erscheinen dabei zunächst offensichtlich: Die Geräte müssen grundsätzlich sinnvoll in den Unterricht eingebunden werden können und – speziell für den Informatikunterricht – programmierbar sein. Prinzipiell sollten dies fast alle heutigen mobilen Informatiksysteme erfüllen[18], allerdings errichten die Hersteller hier unterschiedlich hohe Hürden technischer und rechtlicher Natur. So benötigt man teilweise teure Lizenzen oder spezielle Hard- und Software für die Programmierung. Sie verbieten teilweise auch die Programmierung der Geräte mit den Geräten selbst, sodass zusätzliche Informatiksysteme benötigt werden. Dies verhindert einen Großteil der möglichen Flexibilisierung des Unterrichts, da man weiterhin an Informatikräume gebunden wäre. Außerdem werden wesentliche Aspekte der Betriebssysteme vor dem Nutzer versteckt – etwa die Dateisysteme, sodass ein Verlassen der Anwendungsperspektive unmöglich gemacht wird. Speziell Apple ist hier für derartige Einschränkungen bekannt.

In diesem Sinne ist es wünschenswert, dass die Geräte freie Software verwenden. Denn hier ist es am ehesten möglich, alle Anforderungen zu erfüllen und künstlichen Einschränkungen zu entgehen. Außerdem kann benötigte Software in der Regel ohne relevante Einschränkungen und Kosten an die Schülerinnen und Schüler weitergegeben werden, sodass diese auch zuhause mit den Geräten arbeiten können.

Eine hohe Verbreitung der Plattform ist aus zwei Gründen unerlässlich: Erstens sollten die Geräte sich im Alltag der Schülerinnen und Schüler wiederfinden lassen, zweitens ist nur so eine breite Unterstützung und die Verfügbarkeit entsprechender Werkzeuge und Dokumentationen wahrscheinlich.

Der Motivation zuträglich ist es, wenn auf die Geräte der Schülerinnen und Schüler zurückgegriffen werden kann. Nichtsdestotrotz ist es erforderlich, dass eine gewisse Menge an schulischen Geräten zur Verfügung steht, damit Schülerinnen und Schüler ohne eigene Geräte mitarbeiten können und nicht etwa auf Emulatoren angewiesen sind. Außerdem muss darauf geachtet werden, dass Schülerinnen und Schüler, die über teurere

und besser ausgestattete Systeme verfügen, keine übermäßigen Vorteile erlangen.

Spezielle Anforderungen gelten auch in Bezug auf die Haltbarkeit der Geräte. Aus finanziellen wie aus Umeltschutzgründen sollte hierauf viel Wert gelegt werden. So kann bereits ein fest verbauter Akku einer dauerhaften, langfristigen Nutzung in der Schule entgegenstehen.

Unabhängig davon sollte die Schule sich ihrer Vorbildfunktion bewusst sein und generell soziale wie auch Umweltschutzaspekte berücksichtigen, sofern dies möglich ist.

Folgerungen und Forderungen

Die gesetzten Kriterien zu erfüllen, ist aktuell nicht ganz einfach. Am ehesten sind sie mit Android-Geräten zu erfüllen, die glücklicherweise momentan die höchste Verbreitung bei Schülerinnen und Schülern aufweisen.

Windows-Systeme sind zwar (je nach Version unterschiedlich stark) eingeschränkt, könnten jedoch mutmaßlich sinnstiftend genutzt werden. Die (noch) sehr geringe Verbreitung macht allerdings entsprechende Überlegungen derzeit weitgehend überflüssig.

Es besteht zudem die Hoffnung, dass weitere offene Systeme einen relevanten Verbreitungsgrad erreichen können. Hier sind etwa Sailfish OS, Tizen oder Firefox OS zu nennen. Diese haben durchaus das Potential, die Kriterien besser zu erfüllen als Android.

Völlig ungeeignet sind hingegen rein auf den Konsum gerichtete Plattformen wie Amazons Kindle oder Apples iOS. Hier sollten Informatiklehrkräfte dringend Widerstand leisten, sollte die Einführung derartiger Systeme an ihren Schulen zur Debatte stehen.

Die Erfahrung mit Symbian OS zeigt, dass nach Möglichkeit ein plattformübergreifender Wrapper als Schnittstelle entwickelt werden sollte, sodass bestehende Unterrichtsmaterialien in Zukunft weiterverwendet werden können. Diesen Weg habe ich im Rahmen meiner Arbeit eingeschlagen und gehe ihn jetzt in meinem Referendariat weiter.

Die gesellschaftsverändernden Systeme sollten auf die eine oder andere Weise in der Schule berücksichtigt werden. Dies kann am ehesten im Rahmen eines verpflichtenden Informatikunterrichts geleistet werden, der diesem Namen gerecht wird (auch und insbesondere in den unteren Jahrgängen).

Dabei ist darauf zu achten, dass nicht nur die reine Anwendungsperspektive, sondern auch die Analyse und die Veränderung von Wirklichkeit[19] berücksichtigt werden. So kann nicht nur der allgemeinbildende Anspruch und das Ziel der mündigen Gesellschaftsangehörigen erreicht werden, sondern auch ein Beitrag zu einem aktuellen, motivierenden und zielgerichteten Informatikunterricht geleistet werden.

Anmerkungen

1 *Daniel Spittank: Auswahl und Gestaltung mobiler Informatiksysteme für den Einsatz im Informatikunterricht. Masterarbeit – Master of Education. Wuppertal: Bergische Universiät – Fachbereich Mathematik und Naturwissenschaften, August 2012. https://edu.spittank.net/downloads/mobile/examensarbeit.pdf.*

2 *National Security Agency, Auslandsgeheimdienst der USA*

3 *Government Communications Headquarters, britischer Nachrichtendienst*

4 *vgl. Spiegel u. a.: Method and system for anticipatory package shipping. US 8,615,473. 24. Dezember 2013. http://pdfpiw.uspto.gov/.piw?Docid=08615473.*

5 *BBC. Russia: Hidden chips ‚launch spam attacks from irons'. en. BBC. Oktober 2013. http://www.bbc.co.uk/news/24707337.*

6 *vgl. DGB. Arbeitshetze, Arbeitsintensivierung, Entgrenzung – So beurteilen die Beschäftigten die Lage. März 2012.*

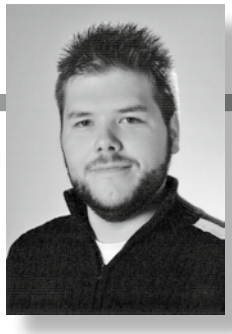
7 *Sebastian Deterding u. a. Gamication: Toward a Definition. Mai 2011. http://hci.usask.ca/uploads/219-02-Deterding,-Khaled,-Nacke,-Dixon.pdf.*

8 *vgl. MPFS. JIM 2013. Jugend, Information, (Multi-)Media. Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger in Deutschland. Forschungsbericht. MPFS – Medienpädagogischer Forschungsverbund Südwest. Stuttgart: mpfs, November 2013. http://www.mpfs.de/fileadmin/JIM-pdf13/JIMStudie2013.pdf.*

9 *vgl. Christian F. Görlich und Ludger Humbert: Open Source – die Rückkehr der Utopie? In: Open Source Jahrbuch 2005. Zwischen Softwareentwicklung und Gesellschaftsmodell. 2005, S. 311-327. http://www.opensourcejahrbuch.de/download/jb2005/OpenSourceJahrbuch2005_online.pdf, S. 311.*

10 *vgl. Ludger Humbert: Schüler brauchen keine Entwicklungsumgebung – ein Editor reicht aus. In: If Fase 2.13 (November 2006), S. 2. http://humbert.in.hagen.de/iffase/Artikel/programmieren-2006-11-01.html.*

11 *vgl. TMS-Infratest u. a.: Our Mobile Planet Survey. Hrsg. von Inc. Google. geprüft: 7. Juli 2012. Mountain View, CA, USA, 2012. http://www.thinkwithgoogle.com/mobileplanet/de.*



Daniel Spittank

Daniel Spittank studierte bis 2013 an der Bergischen Universität Wuppertal Informatik und Sozialwissenschaften für das Lehramt an Gymnasien und Gesamtschulen. Im Rahmen des ersten Staatsexamens schrieb er seine Abschlussarbeit zum Einsatz von mobilen Informatiksystemen im Informatikunterricht. Derzeit absolviert er sein Referendariat und setzt die begonnene Arbeit fort.

12 *Tarik Ahmia. Apple wird zum Bildungsmoloch. Januar 2012. http://werkstatt.bpb.de/2012/01/apple-wird-zum-bildungs-moloch/.*

13 *In der Regel sind dies bestimmte Apps oder Webseiten, die genau einer Unterrichtseinheit oder -reihe dienen, dabei aber häufig einen recht gezwungenen Eindruck vermitteln. Medieneinsatz um der Medien willen.*

14 *Ralph Carrie: Einsatz mobiler Informatiksysteme im Informatikunterricht der gymnasialen Oberstufe. Hausarbeit gem a OVP. Hamm: Studienseminar für Lehrämter an Schulen – Seminar für das Lehramt für Gymnasien Gesamtschulen, Juli 2006. http://www.ham.nw.schule.de/pub/bscw.cgi/315319.*

15 *Matthias Heming: Einsatzszenarien von Mobiltelefonen im Informatikunterricht. Masterarbeit – Master of Education. Wuppertal: Bergische Universität – Fachbereich Mathematik und Naturwissenschaften, November 2009. http://blog.familie-heming.de/?p=111.*

16 *Ludger Humbert: Mit Python auf dem Mobiltelefon bis ins Zentralabitur. April 2007. http://humbert.in.hagen .de/iffase/Artikel/programmieren-2007-04-01.html.*

17 *vgl. Heming, a. a. O.*

18 *ebd.*

19 *vgl. Spittank, a. a. O., S. 32 f.*

Agata Królikowski

FIfF-Studienpreis 2013
2. Preis

‚Due To Legal Issues' – Packet Inspection

Packet Inspection (PI) ist die Vereinigung verschiedener Technologien, um über ein Netz versendete Informationen zu analysieren und zu verwalten. Zum einen gibt es die Deep Packet Inspection *(DPI), bei der Pakete über Steuerdaten hinaus bitweise analysiert werden, zum anderen gibt es die* Statistical Packet Inspection *(SPI), die auch bei verschlüsselten Daten erfolgreiche Analysen durchführen kann. PI wird auf vielfältige Weise von Staaten, Internet Service Providern oder Netzwerkadministratoren eingesetzt.*

Doch wie funktionieren Paketanalysemethoden und wie effizient sind sie? Und gibt es aus Sicht eines Nutzers des Netzes einen technischen oder rechtlichen Schutz gegen diese Analysen?

Diese beiden Fragen wurden in der Diplomarbeit aufgegriffen und ausgehend von den Begriffen der Schutzziele untersucht. Da Schutzziele sowohl in der Datensicherheit als auch im Datenschutz verwendet werden, eignen sie sich, eine Brücke zwischen der Technik und den juristischen Aspekten zu schlagen. Im Wesentlichen wurden Integrität, Vertraulichkeit, Verfügbarkeit und Unverkettbarkeit als Metrik bei der Bewertung von Paketanalysesystemen herangezogen, um auch den Umfang dieser Arbeit etwas einzugrenzen [1].

Packet Inspection: The Medium is the Message

DPI ist zunächst ein Oberbegriff für verschiedene Technologien, die über ein Netzwerk verschickte Pakete bitgenau untersuchen können. Pakete sind Informationseinheiten, die aus Steuerdaten (engl. header) und Nutz- bzw. Inhaltsdaten (engl. payload) bestehen. „Deep" bezieht sich auf das TCP/IP[1]-Referenzmodell, welches die einzelnen Funktionen einer Kommunikation und damit auch die Paketinformationen logisch in sieben Schichten unterteilt.

Das Ziel einer DPI-Analyse ist, die Pakete anhand der vorgefundenen Muster (Signaturen) möglichst genau und ohne Fehler zu klassifizieren und dann anhand der zu der Signatur gespeicherten Regeln entweder weiterzuleiten, zu verlangsamen oder zu verwerfen.

Da es sich bei DPI um die Analyse von Zeichenketten handelt, erschweren alle Mechanismen DPI, die diese Zeichenketten verändern. Auf den ersten Blick scheinen Verschlüsselung oder das Verwenden von Verschleierungsmechanismen (z. B. Ändern des Ports oder Tunnelprotokolle) als gute Instrumente, um DPI zu erschweren bzw. sogar unmöglich zu machen und damit die Vertraulichkeit und Unverkettbarkeit von Daten zu schützen.

Allerdings kommt es für den Schutz auch auf die Ebene der Verschlüsselung oder der Verschleierung an. Verschlüsselt man die eigentlich übertragenen Protokolle auf der Anwendungsebene, sind die vom Nutzer übertragenen Daten nicht mehr sichtbar. Im unverschlüsselten Text bleiben jedoch genug Informationen übrig, aus denen Signaturen und damit Klassifikatoren erstellt werden können. Verschlüsselung schützt also nicht automatisch vor Paketanalysen. Bei der Analyse verschlüsselter Daten geht es auch nicht darum, die darunter liegenden kryptografischen Verfahren zu brechen, sondern darum, die Informationen gerade trotz verwendeter Verschlüsselungs- und Verschleierungsmechanismen auswerten zu können. Die Form der Nachricht verrät häufig schon den Inhalt der Nachricht.

Diese Art der Analysen erfolgt mit Hilfe der sogenannten Statistical Packet Inspection (SPI). SPI bezeichnet Analysemethoden, die statistische Eigenschaften sowie Wahrscheinlichkeitsverteilungen der Pakete und Paketströme berechnen und so auf bestimmte Eigenschaften hin untersuchen. Die Eigenschaften können sich auch auf alle Daten eines Pakets – also auch Nutzdaten – beziehen.

Um die prinzipiellen Möglichkeiten von SPI zu beleuchten, wurden exemplarisch Verfahren untersucht, die Paketklassifikation vornehmen können, obwohl auf den unterschiedlichen Schichten Verschlüsselung oder Verschleierung eingesetzt werden. Entlang des Schichtenmodells wurde systematisch gezeigt, welche Paketinformationen bei Analysen sichtbar werden. Die in der Arbeit vorgestellten Untersuchungen zeigen dabei nur einen kleinen Ausschnitt der vorhandenen Forschung. Auch wenn die Forschungsergebnisse nur mit Vorsicht auf kommerzielle Systeme übertragbar sind, lassen sich prinzipielle Lösungen und Tendenzen aufzeigen. Die Analysemöglichkeiten reichten dabei von der Rekonstruktion verschlüsselter Sprachpakete bei variablen Bitra-

ten [2] oder verschlüsselten MPEG4 -Videodaten [3], Analysemethoden der Secure Shell (SSH) [4] hin zu Website Fingerprinting [5]. Aber auch Kommunikation über SSL/TLS sowie IPSec bieten genügend Anhaltspunkte für erfolgreiche Analysen [6].

So wird beispielsweise zur Identifizierung einer bestimmten Anwendung, die über SSL übertragen wird, die Tatsache ausgenutzt, dass verschiedene Verschlüsselungsmechanismen verschiedene Paketgrößen verursachen. Zwar sind bei SSL über 50 verschiedene Verschlüsselungsarten möglich, allerdings gibt es besonders häufig implementierte Algorithmen wie AES, RC4, so dass sich die Herstellung eines Zusammenhangs zwischen Paketgröße und ursprünglicher Paketgröße auf diese Algorithmen konzentrieren kann [7].

Um aus den über das Netz verschickten Paketen Strukturen abzuleiten, werden Algorithmen aus dem Bereich des maschinellen Lernens angewendet. Im Gegensatz zu DPI, bei der Signaturen aus Zeichenfolgen oder Hashwerten der Zeichenfolgen bestehen, werden Muster unabhängig von konkreten Zeichenfolgen gewonnen. Durch die genaue Analyse bestimmter Protokolle und verwendeter Verschlüsselungs- bzw. Verschleierungsmechanismen gibt es inzwischen umfassende Kataloge mit Parametern, die analysiert werden müssen, um wiederum Rückschlüsse auf Protokolle und Inhalte zu schließen. Analysiert werden z. B. Paketlängen, Reihenfolge der Pakete, Entropie, Abstand zwischen den Paketen, bestimmte gesetzte Bits usw. [8]. Es werden dann alle möglichen Varianten, wie ein Protokoll aussehen müsste, wenn es durch eine bestimmte Art und Weise verschlüsselt oder verschleiert wird, in einer Bibliothek gespeichert. Hinweise darauf, wie wirkungsvoll ein solcher Brute-Force-Ansatz ist, liefert beispielsweise das Datenblatt von PACE der Firma Ipoque [9]. Dort sind mehrere Hundert Protokolle ausgewiesen, die nach eigener Aussage erkannt werden können.

Um Übertragungsverzögerungen zu vermeiden, werden Packet-Inspection-Lösungen immer auch mit dem Ziel entwickelt, die Analyse und Klassifikation in Echtzeit durchzuführen [10]. Dies ist allerdings bei bei Datenübertragungsraten von beispielsweise 10 Gbit/s in Rechnernetzen mit einem hohen Rechen-, Speicher- und Strombedarf verbunden. Um dies zu erreichen, und auch Fehlerraten, die bei der Klassifikation entstehen niedrig zu halten, werden Pakete und Paketströme DPI und SPI sowie weitere verschiedene Arten von port-, inhalts-, verhaltens- und statistikbasierter Methoden ergänzend mit eingesetzt. Pakete werden in hybriden Mehrkernarchitekturen vorgefiltert, indem sie in einzelne Bestandteile zerlegt und mit jeweils spezialisierten Architekturen getrennt nach den verschiedenen Paketschichten analysiert werden. PI-Systeme wie beispielsweise *Procera PakketLogic PL20000 Series* können auf diese Weise Durchsatzraten bis zu 320 Gbit/s erzielen [11]. Zum Vergleich: Der größte Internetknoten der Welt – Deutscher Commercial Internet Exchange Frankfurt (DE-CIX) – hatte 2011 einen durchschnittlichen Durchsatz von etwa 1,5 Tbit/s [12].

Welchen technischen Schutz gibt es noch?

Um sich also vor dieser Art von Analysen zu schützen, muss das Aussehen schon verschlüsselter Nachrichten derart verändert werden, dass daraus keine Informationen gezogen werden können. Ebenfalls sollte im Idealfall verborgen werden, dass Nutzer überhaupt Schutzmechanismen verwenden, da auch dies verdächtig sein könnte [13].

Die Idee, Nachrichten derart zu verschleiern, ist schon relativ alt und wurde bereits 1964 von *Paul Baran* vorgeschlagen. Sogenannte „Dummy"-Paketströme sollten Parameter von Paketen und Paketströmen direkt manipulieren. 1981 hat *David Chaum* das Konzept der Mixnetzwerke eingeführt, um E-Mails unverfolgbar zu machen. Eine Weiterentwicklung dieses Konzepts ist das Projekt *The Onion Routing* (TOR), welches Mixing, Rerouting und Verschlüsselung kombiniert. Doch gibt es prinzipielle Grenzen, wenn der Angreifer beispielsweise den Eingangs- und Ausgangsrouter kontrolliert. Auch ist die Verkettung von Inhalten und Umständen der Nachrichten durch den Einsatz statistischer Verfahren in Verbindung mit Wasserzeichen möglich [14].

In weiteren Projekten wie z. B. *Traffic Morphing* [15], werden verschiedene Ansätze zur Verschleierung erprobt und weiterentwickelt. Ein Problem dieser (und doch recht exotischen) Ansätze ist allerdings, dass ein großer Overhead entsteht und die Kommunikation merklich verlangsamt wird. Zudem werden in den Forschungsprojekten häufig nur einzelne Protokolle mit einzelnen Webseiten untersucht, so dass noch keine generellen Ergebnisse zur Verfügung stehen. Das größte Problem dieser Lösungsansätze ist allerdings, dass sie sich immer an technisch versierte Nutzer richten.

Daneben wurden in der Arbeit Maßnahmen untersucht, die streng genommen nicht unter Schutzmaßnahmen fallen, jedoch in der Lage sind, Paketdiskriminierung auf Seite von ISPs sichtbar zu machen. Die Aufdeckung von Paketdiskriminierung ist aber dennoch interessant und ein erster Schritt, die dahinter liegenden Überwachungsmechanismen zu identifizieren. Zu den untersuchten Projekten gehören *Network Neutrality Bot* [16],

Agata Królikowski

Agata Królikowski hat an der Humboldt-Universität zu Berlin zunächst Jura und dann Informatik studiert. Bis 2012 war sie wissenschaftliche Mitarbeiterin am Lehrstuhl Informatik in Bildung und Gesellschaft von Prof. Dr. Wolfgang Coy, wo sie ihre beiden Fachrichtungen miteinander verbinden konnte. Zur Zeit ist sie wissenschaftliche Mitarbeiterin am Innovations-Inkubator der Leuphana Universität Lüneburg und arbeitet dort in den Projekten Hybrid Publishing und Grundversorgung 2.0. Sie ist Präsidiumsmitglied sowie Mitglied des erweiterten Vorstands der GI und außerdem Sprecherin der Fachgruppe *Internet und Gesellschaft*.

Agata Królikowski und Stefan Hügel bei der Preisverleihung
Foto: Benhamin Kees

DiffProbe [17] und *Glasnost* [18]. Die Diskriminierung wird aufgedeckt, indem die Verzögerungszeiten zweier Paketströme miteinander verglichen werden.

Auch wenn diese Forschungsansätze ein klein wenig Anlass zur Hoffnung geben, verbergen sich dahinter im Moment noch einige Probleme. Da Schutzmechanismen nicht standardmäßig zur Verfügung stehen, müssen Nutzer sich selbst auf ihren Endgeräten darum kümmern. Gleichzeitig können Analysen großflächig an wenigen Knoten implementiert werden. Des Weiteren bieten über das Netz versendete Pakete eine Fülle von Parametern, die untersucht und ausgewertet werden können. Es ist kaum möglich, alle Parameter von vornherein zu verschleiern, so dass eine kleine Änderung in einem Analysealgorithmus einen Schutzmechanismus gänzlich aushebeln kann. Die entwickelten Werkzeuge sind von einem Standard weit entfernt.

Es gibt zur Zeit keinen wirklich wirksamen technischen Schutz gegen die eingesetzten Systeme und man muss bei der Kommunikation über das Internet mit der ständigen Verletzung von Vertraulichkeit, Integrität, Verfügbarkeit und Unverkettbarkeit rechnen. Aus technischer Sicht bleibt höchstens, dass man möglichst viele seiner Daten verschlüsselt und ab und zu testet, wie weit die ISPs in eine Kommunikation beispielsweise durch QoS[2]-Maßnahmen eingreifen. Letztendlich sind Schutzziele auf technischer Ebene aber nicht durchsetzbar.

Rechtliche Probleme

Betrachtet man Kommunikation mittels Post, Funk oder Telefon, die sehr leicht überwindbare oder keine technischen Schutzmaßnahmen aufweisen, stellt sich aber zunächst die Frage, weshalb Analysen von Internetverkehr überhaupt in der rechtlichen Grauzone liegen und damit problematisch sein könnten. Privater Funkverkehr ist in Deutschland von jedem mithörbar, Briefe können unbemerkt geöffnet und Telefonate zumindest von technisch Versierten abgehört werden. Aus diesem Gedanken heraus hat der Gesetzgeber das Brief-, Post- und Fernmeldegeheimnis in Art. 10 GG[3] geschaffen.

Grundgedanke bei diesem Grundrecht ist, dass der Austausch von Information so geschützt sein muss, als ob er von Angesicht zu Angesicht stattfinden würde, d. h. die Nachrichten dürfen von Unbefugten nicht zur Kenntnis genommen werden. Da Grundrechte im Allgemeinen zunächst nur den Staat binden, das TK-Geheimnis jedoch einen hohen Stellenwert genießt, wurde im Zuge der Privatisierung der Post und TK-Anbieter der Wesensgehalt des Art. 10 GG auf §88 TKG[4] übertragen, der nun auch private Stellen bindet. Telekommunikation (TK) ist der „technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels TK-Anlagen“ [19]. Die Vertraulichkeit der Kommunikation wird durch das TK-Geheimnis in Art. 10 GG geschützt und umfasst deren Inhalt und Umstände, unabhängig davon, welche Technik verwendet wird. Inhaltliche Daten sind E-Mails, Chatnachrichten, Bilder usw. – Umstände umfassen Verkehrsdaten und Daten, die es ermöglichen, die Kommunikation von anderen zu unterscheiden. Darunter fallen Identifizierungsmerkmale und Kennungen.

Der Schutz über das Grundrecht des Art. 10 GG bzw. §88 TKG bietet jedoch nur auf den ersten Blick Sicherheit. Denn es kann durchaus auch erforderlich werden, das TK-Grundrecht einzuschränken.

So sind gem. §109 Abs. 2 S. 1 TKG TK-Anlagebetreiber verpflichtet, technischen Maßnahmen zum Schutz ihrer Anlagen zu ergreifen. Ein weiterer Anwendungsfall von PI ist die effektive Nutzung der Bandbreite. So dürfen z. B. Verkehrsdaten zweckgebunden erhoben und verarbeitet werden (§96 Abs. 1 TKG), um TK-Dienste zu erbringen. TK-Dienste sind dabei Transportdienstleistungen, die zur Übertragung von Signalen dienen. Nun wird z. B. die Übertragung von VoIP[5]-Paketen in Anschluss an die Tradition des Telefons als TK-Dienst betrachtet, die Übertragung von Daten (z. B. FTP)[6] hingegen nicht:

> *„Während die Bereitstellung eines Internet-Zugangs [...] eine besondere Dienstleistung darstellt, weist das bloße Telefonieren über das Internet keinen äußerlich erkennbaren Unterschied zur herkömmlichen leitungsgebundenen Telefonie auf. Insoweit handelt es sich um einen einheitlichen Lebensvorgang, der keiner anderen rechtlichen Bewertung als die herkömmliche Sprachtelefonie unterliegt und damit als eine reine TK-Dienstleistung anzusehen ist, die ganz in der Übertragung von Signalen über Kommunikationsnetze besteht und daher ausschließlich dem TKG zuzuordnen ist“.*[7]

Diese Unterscheidung zwischen Datenübertragung und VoIP ist willkürlich, die Kenntnis des Anwendungsprotokolls ist für die Übermittlung der richtigen Signale und damit für die Erbringung eines TK-Dienstes nicht notwendig. An dieser Stelle wird den ISPs Tür und Tor geöffnet, Analysemethoden anzuwenden.

Ein weiteres berechtigtes Interesse liegt in der sogenannten *Lawful Interception*. Die TK-Unternehmen sind gesetzlich verpflichtet, dem Staat eine Überwachungsinfrastruktur zur Verfügung zu stellen. In Deutschland besteht eine Mitwirkungspflicht gem. §110 TKG in Verbindung mit der Telekommunikations-Überwachungsverordnung. TKG-Überwachungen können beispielsweise im Rahmen der Verfolgung von Straftaten gem. §100 a StPO,[8] zur Überwachung durch den Nachrichtendienst (vgl. G10-Gesetz) oder aufgrund anderer Polizeigesetze erfolgen. Diese Mitwirkungspflicht hat zur Folge, dass eine Infrastruktur vorhanden ist, sich in den Händen dieser Firmen befindet und gleichzeitig aber

auch dieselbe Technologie umfasst, die man zur Bandbreitenmanagement, Traffic Shaping oder Netzwerksicherheit verwendet.

Neue Dimension: Statistische Analysen

Das Problem ergibt sich jedoch nicht nur aus der Überwachung als solcher, sondern vor allem aus dem Ausmaß. PI-Systeme sind leistungsfähig genug, um an zentralen Internetknoten wie dem DE-CIX Echtzeitanalysen des gesamten Internetverkehrs in Deutschland durchzuführen. Das TK-Verhalten jedes einzelnen Nutzers kann detailliert aufgenommen, analysiert und gespeichert sowie mit anderen Daten verknüpft und rückwirkend auch in anderen Zusammenhängen betrachtet werden. Da das Internet aber nicht nur der Kommunikation, sondern darüber hinaus auch als Plattform für virtuelle Versammlungen, Beschaffen künstlerischer Werke jeglicher Art, Presse, Rundfunk usw. dient, werden dadurch viel mehr Facetten eines Nutzers erfasst als nur die Tatsache, wer mit wem wann worüber kommuniziert hat. Es ist möglich, ein „Meinungsbild der Nation" aufzunehmen und dieses auch zu steuern. Bereits statistische Analysen wären dazu in der Lage. Zu bedenken ist jedoch, dass nur wenige Nutzer Schutzmaßnahmen ergreifen und somit sogar Klartextanalysen in großem Ausmaß möglich sind. Es zeigt sich, dass mit dem Internet nicht nur Grenzen der Kommunikation verschoben, sondern mit der Digitalisierung auch die Hemmschwelle zur Überwachung deutlich gesenkt wurde.

Diese großflächige Überwachungsmöglichkeit führt die Unschuldsvermutung ad absurdum, wenn ohne einen konkreten Anfangsverdacht nach Mustern gesucht wird, um daraus auf ein bestimmtes Verhalten der Nutzer zu schließen.

Neben diesen Betrachtungen gibt es noch zahlreiche weitere rechtliche Problemkreise. Problematisch sind auch Fragen der Netzneutralität, Meinungs- und Informationsfreiheit, Beweislast bei Online-Diensten wie z. B. De-Mail oder das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme. Auch ergeben sich durch mögliche Analysen allgemeine datenschutzrechtliche Probleme wie z. B. die Frage, ob man QoS widersprechen darf, da personenbezogene Daten erhoben und verarbeitet werden. Doch auch wenn, wäre es technisch nicht realisierbar, die einen Pakete zu analysieren und die anderen nicht, so dass im Endergebnis dem Nutzer nur übrig bliebe, den Provider zu wechseln oder das Internet gar nicht mehr zu nutzen, wenn er einer Überwachung entgehen will.

Diese Schlussfolgerung ist jedoch bedenklich. Die Vielfalt der Nutzung führt über die Möglichkeit reiner Kommunikation hinaus. Und daher ist nicht nur ein einzelnes, sondern eine Vielzahl von Grundrechten betroffen: Angefangen bei dem TK-Recht und Recht auf Selbstbestimmung kommt das Recht eines jeden gem. Art. 5 Abs. 1 GG hinzu, „*seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten*", Vereinigungen zu bilden (Art. 9 Abs. 2 GG) oder seinen Beruf auszuüben (Art. 12 GG). Ein Verzicht auf das Nutzen des Internets kann keine Freiheitsausübung sein, wenn damit so viele Freiheitsverzichte einhergehen. Auf der anderen Seite ist die Aufgabe der Privatsphäre und die Kontrolle des Nutzerverhaltens ebenfalls kein Ausweg.

Was noch bleibt

Wenn grundrechtlich geschützte Kommunikation nur noch unter bestimmten Umständen und wenn überhaupt nur technischen Experten offen steht, bietet dies keine Grundlage für eine freie Informations- und Kommunikationsgesellschaft [20].

Es ist daher die Aufgabe des Gesetzgebers, klarzustellen, welche Rechte und Pflichten die einzelnen Akteure haben, welche rechtliche Grenzen bei der Verwendung von PI zu beachten sind und auch Sanktionen zu definieren. Es ist Aufgabe der TK-Anbieter ihre Systeme offenzulegen und jeden Nutzer darüber aufzuklären, was eigentlich mit seinen Daten passiert. Denn Freiheit kann nur derjenige ausüben, der die Folgen seines Handeln abschätzen kann.

Aus technischer Sicht gilt es, Verfahren zu finden, technische Prozesse wie Paketdiskriminierung in einer Form sichtbar zu machen, dass es nicht mehr Expertenkreisen vorbehalten ist, diese Techniken zu benutzen und zu verstehen, was im Netz passiert. Der nächste Schritt ist die Entwicklung von weiteren Schutzmaßnahmen, die nicht nur theoretisch oder im Labor erfolgreich sind, sondern ebenfalls auf breiter Basis angelegt auch für den Laien verständlich konzipiert sind. Die vorgestellten Verfahren sind ein Anfang, jedoch ist es bis zu einer Standardimplementation solcher Werkzeuge noch ein weiter Weg.

Schließlich ist nicht nur beim Nutzer, sondern in der Politik, den Juristen und verschiedenen Entscheidungsträgern Aufklärungsarbeit notwendig, um die Problematik der Manipulation im Netz deutlich zu machen.

Referenzen

[1] Pfitzmann, Andreas/Rost, Martin: Datenschutz-Schutzziele – revisited, in: Datenschutz und Datensicherheit (DuD), (2009), S. 353 – 358.

[2] Wright, Charles V./Ballard, Lucas/Coull, Scott E./Monrose, Fabian/ Masson Gerald M.: Spot me if you can: Uncovering spoken phrases in encrypted VoIP conversations, in: Proceedings of the 2008 IEEE Symposium on Security and Privacy, May 2008.

[3] Liu, Yali/Sadeghi, Ahmad-Reza/Ghosal, Dipak/Mukherjee, Biswanath: Video Streaming Forensic – Content Identification with Traffic Snooping, in: M. Burmester et al. (Hrsg): Information Security, 13th International Conference, ISC 2010, LNCS 6531, Berlin, Heidelberg, Springer-Verlag, 2011, S. 129–135.

[4] Dusi, Maurizio/Crotti, Manuel/Gringoli, Francesco/Salgarelli, Luca: Tunnel hunter: Detecting application-layer tunnels with statistical fingerprinting, in: Elsevier Computer Networks, Volume 53, Nr. 1, S. 81–97, 2009.

[5] Panchenko, Andriy/Niessen, Lukas/Zinnen, Andreas/Engel, Thomas: Website Fingerprinting in Onion Routing- based Anonymization Networks, in: Proceedings of the Workshop on Privacy in the Electronic Society, 2011, S.103– 114.

[6] Herrmann, Dominik/Wendolsky, Rolf/Federrath, Hannes: Website fingerprinting: attacking popular privacy enhancing technologies with the multinomial naïve-bayes classifier, in CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security. New York, NY: ACM, 2009, S. 31 – 42.

[7] Bernaille, Laurent/Teixeira, Renata: Early recognition of encrypted applications, in: Proceedings of the Eighth Passive and Active Measurement Conference, 2007.

[8] Hjelmvik, Erik: The SPID Algorithm – Statistical Protocol IDentification, URL: http://sourceforge.net/apps/mediawiki/spid/index.php?title=Main_Page [8.2.2014].
[9] Ipoque: Supported Protocols and Applications, URL: http://www.ipoque.com/sites/default/files/mediafiles/documents/data-sheet-supported-protocols.pdf [8.2.2014].
[10] Bar-Yanai, Roni/Langberg, Michael/Peleg, David/Roditty, Liam: Realtime Classification for Encrypted Traffic, in: Festa, Paola (Hrsg.): Proceedings of the 9th International Symposium on Experimental Algorithms, (SEA 2010), LNCS 6049, 2010, Berlin, Heidelberg, Springer-Verlag, 2010, S. 373–385.
[11] Procera: PacketLogic Real-Time Enforcement platforms (PRE), http://www.proceranetworks.com/pre-packetlogic-real-time-enforcement.html [8.2.2014]
[12] DE-CIX: Statistiken, http://www.de-cix.net/about/statistics/ [8.2.2014].
[13] Sokolov, Daniel/Ungerer, Bert: Berichte: Iran kappt sichere Internet-Verbindungen, Artikel auf Heise vom 11.2.2012, URL: http://www.heise.de/newsticker/meldung/Berichte-Iran-kappt-sichere-Internet-Verbindungen-1432960.html [8.2.2014].
[14] Houmansadr, Amir/Borisov, Nikita: SWIRL: A scalable watermark to detect correlated network flows, in: Proc. NDSS, 2011.
[15] Wright, Charles V./Coull, Scott E./ Monrose, Fabian: Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis, in: Proceedings of the 16th Network and Distributed Security Symposium, S. 237 – 250. IEEE, 2009.
[16] Basso, Simone/Servetti, Antonio/De Martin, Juan Carlos: The network neutrality bot architecture: a preliminary approach for self-monitoring of Internet access QoS, in: Proceedings of the 16th IEEE Symposium on Computers and Communications (ISCC), 2011, S. 1131–1136.
[17] Kanuparthy, Partha/Dovrolis, Constantine: Diffprobe: detecting ISP service discrimination, in: INFOCOM, 2010 Proceedings IEEE, 2010, pp. 1–9.
[18] Dischinger, Marcel/Marcon, Massimiliano/Guha, Saikat/ Gummadi, Krishna P./Mahajan, Ratul/Saroiu, Stefan: Glasnost: Enabling End Users to Detect Traffic Differentiation, in: Proceedings of the 7th USENIX conference on Networked systems design and implementation, 2010.
[19] Durner zu Art. 10 GG in: Epping, Volker/Hillgruber, Christian (Hrsg.): Beck'scher Online-Kommentar GG, München: Springer Verlag, Edition 13, 2012.
[20] Gusy, Christoph: Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, in: Datenschutz und Datensicherheit (DuD), 2009, S. 33-41.

Anmerkungen

1 *Transmission Control Protocol/Internet Protocol.*
2 *Quality-of-Service.*
3 *Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 11. Juli 2012 (BGBl. I S. 1478) geändert worden ist.*
4 *Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 2 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 2958) geändert worden ist.*
5 *Voice over IP.*
6 *File Transfer Protocol.*
7 *BT-Drs. 16/3078.*
8 *Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 Absatz 30 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 3044) geändert worden ist.*

Julia Hofmann

FIfF-Studienpreis 2013 3. Preis

Zweckgebundener Datenbrief

für das Identitätsmanagementsystem mittels Web-basiertem Benutzerinterface

Mit der fortgeschrittenen Durchdringung des Alltags mit Web-basierten Computeranwendungen ist beinahe kein Verwaltungsprozess mehr denkbar, ohne dass personenbezogene Daten verarbeitet werden. Mit dem zweckgebundenen Datenbrief können sich Angehörige der TU Darmstadt über ein Web-basiertes Benutzerinterface selbstständig informieren, welche ihrer personenbezogenen Daten für welchen Zweck am Hochschulrechenzentrum verarbeitet werden. Ohne weiteren Schriftverkehr, transparent und tagesaktuell ist so die im Bundesdatenschutzgesetz §34 geforderte Auskunftspflicht umgesetzt. Der technische Datenschutz orientiert sich an den Schutzzielen als Richtschnur für gutes Design (Privacy by Design). Die Schutzziele dienen daher als eine Anleitung, wie die Interessen der TU-Angehörigen zu wahren sind und verbinden damit Gesetz und Technik. Der zweckgebundene Datenbrief wurde an der TU Darmstadt umgesetzt und ist das Ergebnis einer Abschlussarbeit zur Fachinformatikerin Fachrichtung Anwendungsentwicklung an der IHK Darmstadt. Dieser Beitrag erklärt, wie der Datenbrief für die Selbstauskunft technisch realisiert ist.

Die durch das Hochschulrechenzentrum bereitgestellten Dienste nutzen personenbezogene Daten der Menschen an der Technischen Universität Darmstadt. Ziel des zweckgebundenen Datenbriefs ist es, alle Personen darüber zu informieren, welche Daten wozu genutzt werden. Sie sollen nachvollziehen können, zu welchem Zweck ihre Daten verarbeitet werden, und sollen letztlich die Möglichkeit haben, anhand dieser Information zu intervenieren, wenn sie nicht einverstanden sind. Die TU-Angehörigen können den Datenbrief als Web-Anwendung zu jeder Zeit und an jedem Ort mit einem üblichen Web-Browser aufrufen. Das erfüllt auch die Anforderungen an die Systemverantwortlichen, die nach Telemediengesetz §5 und §13 verpflichtet sind, „Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten" [BMJustizTMG2010].

Identitätsmanagement (IDM) bedeutet die Verwaltung von personenbezogenen Daten für alle Angehörigen der TU Darmstadt. Das Hochschulrechenzentrum (HRZ) übernimmt diese Verwaltung in Vertretung, um geregelte und geschützte verwaltungstechnische Prozesse in IT-Dienstleistungen abzubilden [BT2011]. Die digitale Identität repräsentiert die Summe aller Merkmale, die elektronisch verarbeitet werden. Diese Merkmale sind in der

Dienstvereinbarung zum IDM der TU Darmstadt am Hochschulrechenzentrum festgelegt [TUDAIdM2009, TUDAIdM2010]. Die öffentlich zugänglichen Verfahrensverzeichnisse erfüllen die Meldepflicht nach Bundesdatenschutzgesetz §4e und dokumentieren die verwaltungstechnischen Prozesse von Quell- zu Zielsystemen [BMJustizBDSG2009]. Eine Teilidentität entspricht einer Auswahl von personenbezogenen Daten, die für einen oder mehrere gleichartige Dienste benötigt und an die angeschlossenen Zielsysteme übertragen werden. Sie umfasst Daten, die vom entsprechenden IT-System zur Ausführung des Dienstes benötigt werden. Andere personenbezogene Daten werden nicht im Identitätsmanagementsystem (IDM-System) gespeichert. Das IDM-System besteht aus drei Funktionselementen: der Datenhaltung im Kern, einer Familie von Prozesssteuerungs- bzw. Controlling-Mechanismen zur Datenübermittlung aus Quell- und zu Zielsystemen und einem Web-basierten Benutzerinterface, dessen Bestandteil der zweckgebundene Datenbrief ist.

Für die Selbstauskunft muss weder auf Quellsysteme noch auf Zielsysteme einzeln zugegriffen werden, denn das IDM-System ist das zentrale System zur gesicherten Datenhaltung. Die Weitergabe an angeschlossene Dienste erfolgt über definierte Schnittstellen, die in ihrem Modell den Teilidentitäten entsprechen.

Privacy By Design für die Selbstauskunft

Die Schutzziele *Datenintegrität, Vertraulichkeit* und *Verfügbarkeit* sind im IT-Grundschutzkatalog des BSI festgelegt [BSIWeb2013]. Sie konzentrieren sich auf die Verarbeitung der Daten innerhalb technischer Systeme. Ergänzend dazu werden mit den weiteren Schutzzielen *Transparenz, Zweckgebundenheit* und *Intervenierbarkeit* Verfahren aus einer prozessorientierten Sicht betrachtet [RB2011]. *Transparenz* erklärt, welche Verfahren personenbezogene Daten verarbeiten. *Zweckgebundenheit* soll den TU-Angehörigen die Sicherheit geben, dass ihre Daten nur für die Zwecke eingesetzt werden, die ihnen bekannt sind. *Intervenierbarkeit* setzt voraus, dass Nutzer Zugriff auf ihre eigenen personenbezogenen Daten haben, so dass sie ggf. Einspruch erheben können. Der Datenbrief mit Selbstauskunft steht TU-Angehörigen unter geregeltem und geschütztem Zugriff bereit.

Das IDM-System verwaltet vier Personengruppen: Beschäftigte, Studierende, Gäste und Partner und den Sonderfall, dass eine Person gleichzeitig Beschäftigter und Studierender ist. Diese vier Personengruppen bekommen teilweise unterschiedliche Web-Seiten und verschiedene Informationen im Datenbrief angezeigt. Offengelegt werden die Identifikations-, Tätigkeits-, Mail- und Notfallangaben. Je nachdem, welche Personengruppe sich angemeldet hat, bekommen diese bei den Tätigkeiten die Dienst-, Studien- oder Unternehmerangaben geliefert. Die Notfallangaben werden ausschließlich für die Passwort-Wiederherstellung benötigt. TU-Angehörige können auch beim Service intervenieren, indem sie eine Mail an den HRZ-Service senden.

Zusätzlich kann jede Person eine tagesaktuelle PDF-Datei mit der eigenen digitalen Identität erzeugen und erhält dann einen Hinweis, mit dieser PDF-Datei entsprechend sorgsam umzuge-

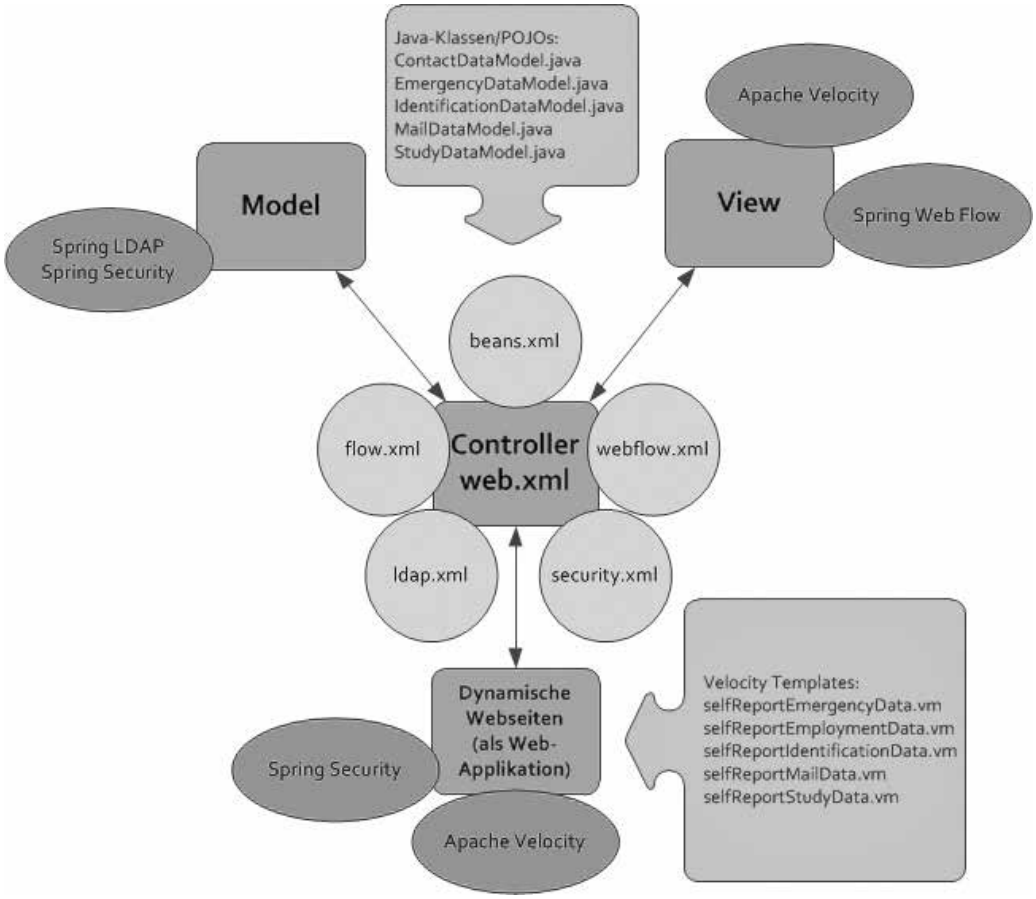


Abbildung 1: MVC-Konzept mit Konfigurationsdateien (Quelle: Eigene Darstellung)

hen, weil ab dieser Stelle das HRZ nicht mehr verantwortlich ist. Wer möchte, kann diese PDF-Datei wie einen persönlich versandten Brief auffassen. Die Anwendung steht nicht nur in deutscher sondern auch in englischer Sprache zur Verfügung. Genutzt wurden die Strukturen eines Grundgerüstes für dynamische Web-Seiten zur Umsetzung des Corporate Designs der TU Darmstadt.

Angewendete Techniken im Web-basierten Benutzerinterface

Die Implementierung nutzt das Java-basierte *Spring Framework* [SpringWeb2013]. Es dient der Gestaltung dynamischer und konfigurierbarer Web-Seiten, die in jedem Web-Browser aufrufbar sind. Die Konstruktion von Benutzeroberflächen wird durch das Entwurfsmuster des *Model-View-Controller-Konzepts* (MVC-Konzept) unterstützt und im Spring Framework verwendet (Abbildung 1).

Dem *Model* ist die Datenhaltung im IDM-System zugeordnet, in dem die personenbezogenen Daten der TU-Angehörigen gespeichert sind. Die Datenhaltung ist durch einen Verzeichnisdienst realisiert und lässt sich über eine LDAP-Schnittstelle *(Lightweight Directory Access Protocol)* ansprechen. Für jedes Daten-Objekt aus der Datenhaltung gibt es eine entsprechende Java-Klasse. Die Abbildung von Inhalten des Verzeichnisdiensts auf die Java-Klassen wird durch ein so genanntes *Object Directory Mapping* (ODM) realisiert, die Implementierung ist der ODM-Manager. Mit dem Spring Framework ist es möglich, mehrere *Controlling-Mechanismen* zu konfigurieren: Spring Web Flow, das eine Darstellung dynamischer Web-Seiten ermöglicht, sowie Spring Security und Spring LDAP, die für eine sichere Anbindung der Datenhaltung des IDM-Systems an das Benutzerinterface sorgen.

Die Konfiguration der Controlling-Mechanismen wird in XML-Dateien vorgenommen. Die Datei *flow.xml* legt die Reihenfolge der Seiten für die jeweiligen Nutzer fest. Die View entspricht dynamisch generierten Web-Seiten, die die Daten aus den übermittelten Java-Klassen in Form von Beans enthalten. Diese Web-Seiten bekommen die Nutzer im Browser zusehen.

Programmcode-Beispiel

Der Programmcode (Abbildung 2) zeigt die Übergabe der Verzeichnisdienstvariablen an die Variablen in der Java-Klasse durch die ODM-Manager Klasse (@Attribute). Damit der ODM-Manager die Verzeichnisdienstvariablen in die Klassenvariablen schreibt, müssen @Entry und @Attribute in die Klasse eingebaut werden. Die unter @Entry aufgelisteten Objekte enthalten alle Attribute, die auf den Web-Seiten angezeigt werden. Die erforderliche Zuordnung von einzelnen Attributen im Verzeichnisdienst zu Attributen in Java-Klassen wird durch @Attribute garantiert. Die *getter* wurden angelegt, um auf die Variablen zuzugreifen.

```
package de.tudarmstadt.hrz.ui.datamodel;
import org.springframework.ldap.odm.core.
OdmManager;
import java.io.Serializable;
import org.springframework.ldap.odm.
annotations.*;
[…,J.H.]
@Entry(objectClasses = {"dfnEduPerson",
"homeInfo", "idmPerson",
"idmSap", "idmTucan", "inet-
OrgPerson", "ndsLoginProperties",
"organizationalPerson", "Person",
"sapUser", "Top", "tudUser"})
public final class EmploymentDataModel
implements Serializable{
private static final long serialVersionUID =
-184745070218370696L;
@Transient
private transient final Logger LOG = Logger.
getLogger(this.getClass());
@Id private Name dn;
@Attribute (name="facsimileTelephoneNum
ber")
private String businessFaxnumber = "";
@Attribute (name="telephoneNumber")
private String businessPhonenumber = "";
@Attribute (name="personalTitle")
private String job = "";
[…,J.H.]
public EmploymentDataModel() { }
public String getBusinessFaxnumber()
{return businessFaxnumber;}
public String getBusinessPhonenumber()
{return businessPhonenumber;}
public String getJob() {return job;}
}
```

Abbildung 2: Java-Klasse(EmploymentDataModel.java; Quelle: Eigene Darstellung)

Julia Hofmann

Julia Hofmann hat im Juni 2013 erfolgreich ihre Ausbildung zur Fachinformatikerin/Fachrichtung Anwendungsentwicklung am Hochschulrechenzentrum der TU Darmstadt abgeschlossen. Sie interessiert sich für Fragen aus den Bereichen des Technischen Datenschutzes und ihre programmiertechnische Umsetzung. Heute arbeitet sie als Software-Entwicklerin in der Abteilung Basisdienste am Hochschulrechenzentrum.

Fazit

Die Auskunftspflicht wird oft als zu aufwändig kritisiert, da angenommen wird, dass sie nur über einen Schriftwechsel möglich ist. Das Hochschulrechenzentrum verwaltet im IDM-System 45.000 Benutzer-Accounts für die TU-Darmstadt. Tatsächlich ist daher praktisch kein postalischer Schriftwechsel möglich.

Durch die Implementierung des Datenbriefs und unter Berücksichtigung der Designprinzipien aus dem technischen Datenschutz ist kein Schriftwechsel mehr nötig. Gleichzeitig ist der Datenbrief geschützt, da er erst nach dem Login mit TU-ID (Benutzerkennung) und Passwort eingesehen werden kann. Hiermit ist zusätzlich ein gewisses Maß an Vertraulichkeit garantiert. TU-Angehörige können sich durch den neuen zweckgebundenen Datenbrief selbstständig mit einem üblichen Web-Browser informieren.

Referenzen

[BT2011] Elisa Bertino, Kenji Takahashi: Identity Management- Concepts, Technologies and Systems. Norwood 2011.

[BSIWeb2013] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Standards. https://www.bsi.bund.de/DE/Themen/IT-Grundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html (letzter Aufruf: 5.6.2013)

[BMJustizBDSG2009] Bundesministerium der Justiz: Bundesdatenschutzgesetz (BDSG). http://www.gesetze-im-internet.de/bdsg_1990_index.html (letzter Aufruf: 30.04.2013)

[BMJustizTMG2010] Bundesministerium der Justiz: Telemediengesetz (TMG). http://www.gesetze-im-internet.de/tmg/index.html (letzter Aufruf: 06.11.2012)

[RB2011] Martin Rost, Kerstin Bock: Privacy by Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen. In: Datenschutz und Datensicherheit. Nr. 1, 2011, S.30-35.

[SpringWeb2013] Spring Source Community: Spring Framework – Einstiegsseite unter: http://www.springsource.org/ (letzter Aufruf: 11.01.2013)

[TUDAIdM2009] Technische Universität Darmstadt: Dienstvereinbarung über die Einführung und Anwendung eines Identity Management Systems. Darmstadt, September 2009. http://www.personalrat.tu-darmstadt.de/media/personalrat/personalrat_pdf/dv_idm.pdf (letzter Aufruf: 31.01.2014)

[TUDAIdM2010] Technische Universität Darmstadt: Änderung der Dienstvereinbarung über die Einführung und Anwendung eines Identity Management Systems, Darmstadt April 2010. http://www.personalrat.tu-darmstadt.de/media/personalrat/personalrat_pdf/aenderung_dv_idm.pdf (letzter Aufruf: 31.01.2014)

Ingo Ruhmann

Retrospektive

Politik der Chiffren

Die Verschlüsselung von Nachrichten, die Kryptographie, ist die einzige Möglichkeit vertraulicher elektronischer Kommunikation. Ihre Nutzung wird durch Militärs und Geheimdienste behindert. Dies ist Kern der derzeitigen Debatte um Kryptographie. Doch während der Nutzen kryptographischer Verfahren deutlich wird, bleibt die Rolle staatlicher Stellen vage, schießen wilde Vermutungen über Aktivitäten des Gesetzgebers und der Exekutive ins Kraut. Wenig konkret bleiben die Rolle der Militärs und ihre Interessen, die der folgende Beitrag beleuchtet.

Kryptographie, Informatik und Militär war eine Kombination zu wechselseitigem Vorteil. Einer der ersten Computer entstand für die Entschlüsselung des ENIGMA-Codes der Wehrmacht in der britischen Chiffriereinrichtung Government Communications Headquarters (GCHQ). Nach dem Zweiten Weltkrieg gab der US-Chiffriergeheimdienst *National Security Agency* (NSA) allein in den 50er Jahren über eine Milliarde Dollar für die Entwicklung von Hochleistungsrechnern aus und blieb seither größter Anwender von Supercomputern. Erste Supercomputer in der Bundesrepublik nutzten Chiffrierexperten des heute zum *Bundesamt für Sicherheit in der Informationstechnik* (BSI) mutierten früheren Gegenstücks zur NSA, der *Zentralstelle für das Chiffrierwesen* (ZfCh), die derzeit einen neuen Supercomputer für die Kryptoanalyse beschaffen[1].

Worum es geht: Betriebsgeheimnisse und CyberCash

Alle diese Dienste sind entweder eine militärische Organisation oder kooperierten innig mit Militärs. Doch die Kryptographie ist nicht länger alleinige militärische Domäne, das zivile Interesse an Kryptographie führt zu Konflikten. Dieser moderat als Kryptographie-Debatte umschriebene Konflikt ist einer zwischen kommerziellen und staatlichen Interessen. Worum geht es dabei?

Der Schutz der Privatsphäre durch Kryptierung wird gern angeführt, hat aber bei der Bewertung kaum Einfluß. Es ist die kommerziell genutzte elektronische Kommunikation, die Kryptierverfahren zur Verschlüsselung als Schutz von Betriebsgeheimnissen und zur Abwicklung von Geschäften, die elektronische Signatur zur Authentisierung von Geschäftsvorgängen und digital signierte elektronische Geldäquivalente zur Abwicklung elektronischer Zahlungen benötigt. Ohne diese Kryptierverfahren ist der Rationalisierungsgewinn elektronischer Kommunikation nicht zu erzielen: Allein die digitale Signatur elektronischer Kommunikation macht 250.000 Arbeitsplätze jener überflüssig, die bislang eingehende Papierdokumente gesichtet und bearbeitet haben[2]. Die Absicht der Banken, Zweigstellen durch Tele-Banking zu ersetzen und damit hier 100.000 Arbeitsplätze abzubauen, läßt sich nur durch den Einsatz von Kryptierverfahren bei Transaktionen erreichen[3]. Das Internet zum Warenhaus zu

machen, setzt schließlich kryptographisch realisiertes elektronisches Geld voraus.

Von ENIGMA bis Information Warfare

Dem entgegen stehen auf staatlicher Seite Aufklärungswünsche der Strafverfolgungsbehörden, vor allem aber der Geheimdienste und Militärs. Das gern genutzte Bild des verschlüsselnden Mafioso verzerrt die Bedeutung, die Kryptographie für staatliche Stellen hat. Dort schützt sie Kommunikation gegen Kenntnisnahme durch Dienste anderer Staaten. Dabei geht es um weltweite diplomatische oder militärische Kommunikation mit Inhalten von hoher politischer Bedeutung, wodurch Kryptographie als Mittel zur Wahrung staatlicher Autonomie wirkt. Das drückt sich gleichermaßen darin aus, die Kommunikation anderer auszuspionieren, um daraus für eigene Zwecke einen Nutzen zu ziehen: Geheimdienste werten die elektronische Kommunikation anderer Länder aus, Militärs versuchen, Daten ihrer potentiellen Gegner zu nutzen. Doch es sind die Erfahrungen der Militärs, die die Furcht der Geheimdienste und Strafverfolger vor Kryptierung schüren.

Im Ersten Weltkrieg fand die letzte Schlacht zwischen hochtechnisierten Armeen statt, die durch fehlende Verschlüsselung entschieden wurde. Im Zweiten Weltkrieg bestimmte nicht zuletzt die Entschlüsselung der ENIGMA über den Kriegsausgang. Die Entwicklung der Chiffriersysteme während des Kalten Krieges schließlich gefährdete die Bedeutung der Entschlüsselung, da die erreichte Qualität der Kryptiersysteme direkte Entschlüsselungserfolge trotz Supercomputern begrenzte. Das Speichern abgefangener Nachrichten und das Warten auf ausspionierte Schlüssel, bessere Computer oder besseres Wissen um gegnerische Codes wurde zum Schauplatz des einzigen seit 1945 konstant geführten Kampfes, der elektronischen Kriegsführung. Sie wird gegenwärtig zum *Information Warfare* weiterentwickelt.

Information Warfare ist besonders für die USA ein neues Kampfmittel. Informationen über einen Gegner und die Manipulation seiner Daten erlangen kriegsentscheidende Bedeutung. Zum eigenen Schutz werden bis zum Jahr 2000 über 2 Millionen Kryptiersysteme in die Computer des sensitiven zivilen und militärischen Behördenverkehrs der USA eingebaut[4]. Gleichzeitig sollen Gegner umfassend ausgespäht werden[5]. Kryptierung ist dabei der größte Hemmschuh.

Seit sich aus militärischen Nachrichteninhalten kaum noch Informationen gewinnen lassen, gewannen Strukturdaten darüber an Bedeutung, auf welcher Frequenz von welchem Ort aus in welchem Code gesendet wurde. Als *Signals Intelligence* hat diese Klasse von Spionagedaten eigene Bedeutung erlangt. Nächster Schritt war das Verbergen von Nachrichten und Sender durch Frequenzsprungverfahren oder Frequenzspreizung. Zivile Variante dieser Techniken zum Verbergen der bloßen Existenz einer Nachricht ist die *Steganographie*, bei der Nachrichten in großen Datenmengen versteckt werden.

Bei der militärischen Kryptographie kam es also zu der semiotischen Abwärtsspirale, statt der Information aus Inhalten lediglich Struktur und Form der Signale zu erlauschen. Nun lassen sich auch diese immer weniger detektieren und damit immer weniger Informationen erhalten. Für die Chiffrier-Geheimdienste ist dies Warnung genug, um eine ähnliche Entwicklung in nichtmilitärischen Sektoren so lange wie möglich zu verhindern. Der Eifer, Kryptiersysteme vom zivilen Markt zurückzuhalten oder dort so weit wie möglich zu behindern, liegt in der hohen Bedeutung, die ein gut lesbarer internationaler Datenverkehr für sie hat.

Hinzu kommt die Ausweitung geheimdienstlicher Aufgaben. Das Organisierte Verbrechen hat den Warschauer Pakt als Hort des Bösen abgelöst, weiteres neues Einsatzgebiet ist die Wirtschafts- und Industriespionage. Der US-Geheimdienst CIA arbeitet ebenso auf diesem Gebiet wie der *Bundesnachrichtendienst* (BND). Wie nützlich dabei Schwächen in Kryptosystemen sind, zeigte sich kürzlich auf dem europäischen Rüstungsmarkt. US-Botschaften unterstützen ihre Rüstungsindustrie durch die Weitergabe von Spionagedaten über die europäische Konkurrenz durch US-Dienste an die Unternehmen. In der Schweiz ging es um den Verkauf von Flugzeugen, in Griechenland um *Phantom*-Jets und Radaranlagen[6]. Nach dem Bombenanschlag auf das World Trade Center ermittelte die NSA, daß Geld für die Attentäter per Banküberweisung aus Frankfurt gekommen war, wo es wiederum Mittelsmänner nahöstlicher Geheimdienste eingezahlt haben sollen. Wichtige Teile der zivilen Wirtschaft bleiben nicht unbeobachtet.

Nichtmilitärische Objekte von Geheimdiensten sind nicht ernsthaft auf ein Ausspähen von Daten vorbereitet und weisen erhebliche Mängel in ihren Schutzvorkehrungen auf. Erfolge der Geheimdienste sind hier noch leicht zu erzielen. Das ändert sich mit einer weitverbreiteten Nutzung von Kryptosystemen.

Wissen um Kryptographie wurde in den zurückliegenden Jahrzehnten staatlicherseits monopolisiert. Es gab nur wenige Experten, die in meist nur einer nationalen staatlichen Einrichtungen zusammengezogen wurden und dort unter Ausschluß der Öffentlichkeit arbeiteten. Die genutzten Kryptoverfahren ließen sich so gut unter Kontrolle halten. Es ist deshalb interessant, den Fragen nachzugehen, welche Situation im Kryptierbereich erstens heute vorzufinden ist und zweitens, wie es überhaupt dazu kommen konnte, daß das Wissen um Kryptographie heute so weit verbreitet ist, daß es nur noch schwer zu kontrollieren ist.

Strategische Kontrolle des Krypto-Marktes

Staaten wie die USA, Großbritannien, Frankreich, China, die ehemalige Sowjetunion, aber auch die Bundesrepublik haben Verschlüsselungs-Verfahren entwickelt, die als sicher gelten. Kleinere Staaten haben nicht die Kapazitäten zu Eigenentwicklungen und sind vom Import von Kryptiersystemen abhängig. Deren Export ist eng geregelt und kommt dem von Massenvernichtungsmitteln gleich. Die Regeln entstammen dem Kalten Krieg und wurden im Exportkontroll-Gremium COCOM (für: *Coordination Commitee)* verbindlich festgelegt. Die USA haben das Exportverbot in der *International Traffic in Arms Regulation* (ITAR) festgelegt, die Bundesrepublik in der Ausfuhrliste Teil I C Abschnitt 5 Teil 2 gemäß Außenwirtschaftsverordnung. Ausfuhren begutachten – und damit genehmigen – Chiffrierdienste wie NSA oder BSI[7].

Weltweit gibt es nur fünf Anbieter für kryptographisches Gerät[8]. Diese übersichtliche Zahl sorgt für die Anbieterländer zu einer „strategischen Kontrolle“ über die geschützte Kommunikation ihrer Kunden[9]. Trotzdem sind Kryptosysteme aus Europa in kleineren Ländern gefragt. Siemens entwickelte zusammen mit dem BSI verschiedene Geräte zur Verschlüsselung, ohne daß dies dem Absatz geschadet hätte. Schließlich arbeiten BSI und zuvor ZfCh „grundsätzlich mit allen deutschen Kryptoherstellern zusammen“[10]. Wenn Systeme, die das BSI von der Industrie entwickeln ließ und für die es Exportlizenzen vergibt[11], von anderen Staaten genutzt werden, ist dem BSI der Aufbau der verkauften Systeme bekannt, was die Entschlüsselung erleichert.

Eine Besonderheit ist die seit 1959 in der Schweiz ansässige *Crypto AG*. Sie galt als unabhängiger Lieferant, obwohl die NSA seit 1957 offenbar über technologische Entwicklungen der Firma informiert wurde[12]. Auch die undurchsichtigen Besitzverhältnisse haben ihrem Ruf nicht geschadet – den Kunden fehlen die Alternativen. Ein freier Markt für Kryptiersysteme wäre ein erheblicher Rückschritt für die Chiffrierdienste der jeweiligen Länder.

Kryptographie als Wissenschaft – wie konnte es dazu kommen?

Heute besteht für die Chiffriergeheimdienste die Hauptgefahr nicht in den arbeitslos gewordenen Krypto-Experten der ehemaligen Ostblockstaaten, die im Gegensatz zu den Nuklearphysikern offenbar geräuschlos in andere Beschäftigungsverhältnisse gewechselt sind, sondern in der Verbreitung von Krypto-Know-How durch Wissenschaftler und neue Firmen. Dabei haben sie ihr bestes gegeben, um diese Verbreitung zu behindern.

Die heutige Kontroverse verweist auf eine vor über zehn Jahren in den USA ausgetragene Debatte. Seit Mitte der 70er Jahre wurden kryptographische Verfahren mit Zunahme des elektronischen Verkehrs auch von zivilen Nutzern eingesetzt. 1977 wurde der *Data Encryption Standard* (DES) publiziert[13], der Kryptierleistung auf einem Chip preiswert verfügbar machen sollte. Ende der 70er Jahre hatte die Kryptographie als Fachgebiet in den USA den Schwellwert für eine eigendynamische Entwicklung erreicht[14].

Dies hielt die NSA für eine Gefährdung der nationalen Sicherheit. Ab 1978 versuchte die NSA, ausländische Teilnehmer von Konferenzen fernzuhalten, die Publikation von Forschungsergebnissen zu verhindern und die zivile Förderung für die Forschung an Kryptosystemen zu unterbinden, und ließ Patente für geheim erklären[15]. Höhepunkt war die Idee, die Kryptographie-Forschung als *born secret* zu klassifizieren. Diese nur für Atomwaffen-relevante Forschung existierende Klassifikation hätte bedeutet, alle zivilen und nichtzivilen Forschungsarbeiten für geheim zu erklären und vor einer Veröffentlichung einer Kontrolle durch die NSA zu unterwerfen. Da viele Universitäten in den USA keine Geheimforschung dulden, hätte dies die Kryptographie-Forschung effektiv behindert[16].

Die eingesetzte *Public Cryptography Study Group* schlug ein System der Selbstzensur vor, da eine andere Regelung kaum verfassungsmäßig gewesen wäre[17]. Dennoch sollte sogar die Informatik allgemein kontrolliert werden. Erst der Druck der *National Academy of Science*[18] und der Boykott der Wissenschaftler, Forschungsaufträge des Pentagon unter derartigen Bedingungen anzunehmen, führte zu einem ersten Umdenken[19]. Auch weiterhin gab es Probleme vor allem bei Exporten. Erst das Ende des Kalten Krieges und der Wechsel der US-Administration brachte einen Wandel.

Daß wir über widerstandsfähige zivile Kryptiersysteme verfügen, geschah nicht mit Zustimmung der Militärs und Geheimdienste. Sie waren bereit, das System wissenschaftlicher Öffentlichkeit aufs Spiel zu setzen, um zivile Kryptographie zu behindern. Erst die Drohung der US-Wissenschaftsgemeinde, keine Aufträge des Militärs anzunehmen und die zusätzliche Drohung mit einer Verfassungsklage[20] brachten Pentagon und NSA schließlich dazu, die Kontrolle der zivilen Forschung zurückzuschrauben. Diesem Konflikt um die Freiheit der Forschung in der Kryptographie entspringt der heutige Entwicklungsstand in diesem Fachgebiet.

Wie wenig Krypto ist noch möglich?

Die heutige politische Haltung ist vorläufig. Noch vor der Amtseinführung berieten NSA und FBI die Clinton-Administration[21]. Seither koppelt sie – entgegen ihrer sonst unternehmensnahen Wirtschaftspolitik – Kryptierung mit einer bedarfsweisen Überwachung durch staatliche Stellen, wie die sogenannte *Clipper*-Initiative zeigte[22]. Dennoch gab der Nationale Forschungsrat im Juni einen Bericht mit dem Resultat heraus, auf lange Sicht würden die Vorteile einer Freigabe von Kryptoverfahren deren Nachteile überwiegen[23].

Auch die OECD wurde aktiv. Auf Konferenzen Ende Dezember 1995 und im Juni 1996 vertraten die USA die Position, Kryptosysteme müßten die Entschlüsselung des eingehenden wie ausgehenden Verkehrs ermöglichen. Kennern asymmetrischer Kryptierverfahren wird dies deswegen verdächtig sein, da die Kenntnis des privaten Schlüssels einer Zielperson nur den ein-

Ingo Ruhmann

Ingo Ruhmann ist Informatiker, wissenschaftlicher Referent und Lehrbeauftragter an der FH Brandenburg und arbeitet zu Datenschutz, IT-Sicherheit sowie Informatik und Militär. 1996 war er wissenschaftlicher Mitarbeiter des forschungs- und postpolitischen Sprechers von Bündnis90/Die Grünen, Dr. *Manuel Kiper*, sowie Mitglied des FIfF-Vorstands.

gehenden Verkehr lesbar macht. Erst die Kenntnis der privaten Schlüssel aller Adressaten jedoch ermöglicht das Mitlesen des ausgegehenden Verkehrs. Eine Überwachung hieße damit entweder eine Freigabe privater Schlüssel in großer Zahl oder die generelle Einigung auf Kryptosysteme, die schwach genug sind, um auch ohne Kenntnis der privaten Schüssel leicht brechbar zu sein.

Die Bundesregierung hält sich zurück; seit etwa 1993 läßt sie sich beraten. 1995 wurde ein Entwurf zur Regelung einer digitalen Signatur bekannt – ein auf asymmetrischer Kryptierung basierendes Verfahren, bei dem staatliches Entschlüsseln durch die Schlüsselverwaltung durch „vertrauenswürdige Dritte" ermöglicht wird. Dies findet sich nun im Informations- und Kommunikationstechnik-Dienstegesetz wieder. Gleichzeitig hält sich das Gerücht, im Bundes-Innenministerium liege ein fertiger Entwurf des Verbots anderer Kryptierverfahren in der Schublade, bis sich die geeignete Situation ergebe.

Fazit

Die verbreitete Nutzung von Kryptiersystemen steht den militärischen Zielen und den Aufgaben der Geheimdienste entgegen. Der bisher übersichtliche Markt für Kryptiersysteme gerät ins Wanken durch Entwicklungen auf wissenschaftlichem Gebiet. Trotzdem ist es Chiffrier-Geheimdiensten bei aller Anstrengung nicht gelungen, die Publikation des Erkenntniszuwachses zu verhindern. Erfolge wurden von ihnen durch ein Verlangsamen der Verbreitung von Kryptiersystemen erzielt.

Die Regierungen der OECD-Staaten und vor allem ihre Geheimdienste sehen sich nun vor einer Zäsur. Die von ihnen forcierte Entwicklung der Informationsgesellschaft benötigt dringend die verbreitete Nutzung von Chiffriersystemen. Bisher hat sich jeder Versuch, sichere, aber brechbare Chiffriersysteme zu verbreiten, als undurchführbar erwiesen. Die nächsten Monate werden zeigen, ob die Einführung neuer Chiffriersysteme mit dem Verbot anderer Systeme gekoppelt wird und wie Öffentlichkeit und Unternehmen darauf reagieren. Damit wird sich auch entscheiden, ob sich die Informationsgesellschaft als eine Zivilgesellschaft entwickelt oder nicht.

Dieser Artikel ist die überarbeitete Fassung eines Beitrags in der *FIfF-Kommunikation* 3/1996, S. 45-49. Wir danken dem Autor herzlich für die Genehmigung zum Abdruck.

Anmerkungen

1 *Antwort der Bundesregierung auf die Kleine Anfrage von Dr. Manuel Kiper „Sicherheit der Informationstechnik und Kryptierung", Drs. 13/4105, auf Frage 5*

2 *Dirk Fox: Automatische Autogramme; in: c't 10/95, S. 278-284, S. 278*

3 *Für die USA basiert dies auf einer Studie von Deloitte & Touche LLP: 450000 Banken-Jobs verschwinden in den USA; in: Süddeutsche Zeitung, 16.8.95, S. 20 und Eine Welt ohne Bankfilialen; in: ebd., 30.8.95. Die Entwicklung in der Bundesrepublik wurde analysiert von Arthur D. Little: Heißer Draht; in: Der Spiegel, 17/95, S. 121-125*

4 *David Lawrence: Many Options for Implementing Fortezza is in the MISSI Framework; in: Defense Electronics, 11/95, S. S. 8-10*

5 *Dieser braucht weder Nationalstaat zu sein noch muß es sich bei militärischen Aktionen um einen bewaffneten Konflikt handeln, vgl.: Ingo Ruhmann: Netwar und Cyberwar – Kriegsführung in der Zukunft; in: FIFF-Kommunikation, Nr. 4, 1994, S. 39-42*

6 *Craig Covault: U.S. Export Push Challenges Europeans; in: Aviation Week & Space Technology, May 27, 1996, S. 20-22*

7 *vgl. Antwort der Bundesregierung auf die Kleine Anfrage von Dr. Manuel Kiper „Sicherheit der Informationstechnik und Kryptierung", Drs. 13/4105, auf Frage 6*

8 *Erich Schmidt-Eenboom: Der BND. Schnüffler ohne Nase, Düsseldorf, 1993, S. 221*

9 *Mike Witt: Tactical Communications; in: Military Technolgy, Nr 5, 1991, S. 19-25, S. 22*

10 *Antwort der Bundesregierung auf die Kleine Anfrage von Dr. Manuel Kiper „Sicherheit der Informationstechnik und Kryptierung", Drs. 13/4105, auf Frage 3*

11 *Antwort der Bundesregierung auf die Kleine Anfrage von Dr. Manuel Kiper und Manfred Such „Das Bundesamt für Sicherheit in der Informationstechnik", Drs. 13/3408, auf Frage 44*

12 *James Bamford: The Puzzle Palace, New York, 1983, S. 407ff*

13 *obwohl dessen Schlüssellänge als zu kurz galt: Whitfield Diffie, Martin Hellman: A Critique of the Proposed Data Encryption Standard; in: Communications of the ACM, March 1976, S. 164-165*

14 *So waren aus zwei Patenten für Kryptosysteme pro Jahr ein halbes Dutzend pro Monat geworden vgl.: David Kahn: The Public's Secrets; in: Cryptologia, Jan. 1981, S. 20-26*

15 *Kahn, S. 23f*

16 *vgl dazu: Ingo Ruhmann: Beeinträchtigung der wissenschaftlichen Freiheit durch die neue Wissenschaftspolitik der USA; in: J. Bickenbach, H. Genrich, R. Keil, W. Langenheder, M. Reisin: Informatik und Militär, Berlin, 1984, S. 61-66*

17 *David Dickson: More secrecy on cryptography research; in: Nature, 19.2.1981, S. 621*

18 *Mitchel B. Wallerstein: Scientific Communication and National Security in 1984; in: Science, May 4, 1984, S. 460-466*

19 *John Walsh: DOD Springs Surprise on Secrecy Rules; in: Science, June 8, 1984, S. 1081*

20 *James R. Ferguson: Scientific Freedom, National Security and the First Amendment; in: Science, Vol 221, S. 620*

21 *Steven Levy: Scared Bitless; in: Newsweek, June 10, 1996, S. 38-40, S. 38*

22 *Als Clipper-Initiative wird der Versuch der Clinton-Administration bezeichnet, einen sog. Clipper-Chip zu entwickeln und zu verbreiten, mit dem Daten in einer Art verschlüsselt werden, durch die eine Identifikation des Urhebers und über die Clipper ausgebende Stelle dessen geheimer Schlüssel für Geheimdienste und Strafverfolger verfügbar wird.*

23 *NRC: Cryptography's Role in Securing the Information Society, Washington, June 1996*

Klaus Haller

„Computer Chess“: Ein Film von skurrilen InformatikerInnen und der Angst vor dem 3. Weltkrieg in den 1980ern

Wie langweilig wird wohl ein Kinofilm über eine Informatikkonferenz sein? Gar nicht, das zeigt Andrew Bujalski mit Computer Chess*. Der Film versetzt die Kinobesucher zurück in die Atmosphäre der 1980er. Dreißig, vierzig Informatiker von Universitäten und der Industrie treffen sich. Sie haben Schachprogramme entwickelt. Die Programme treten in einem Turnier gegeneinander an, um das beste Schachprogramm Nordamerikas zu küren. Im sonnigen Westen der USA ziehen sich die Teilnehmer für ein Wochenende in das Innere eines kleinen Hotels zurück. Doch das Turnier ist nur der Rahmen. Die Gespräche am Rande und an den Abenden lassen ein Sittenbild der Informatik und der Informatiker der 1980er Jahre entstehen.*

Drei Themen ziehen sich durch den Film. Erstens behandelt der Film das Verhältnis von Doktorand und Betreuer. Zweitens stellt der Film die Frage, ob Computerprogramme intelligent handeln. Ist ein System intelligent, wenn wir einen Sinn in seinem Handeln erkennen? Oder erliegen wir einer Illusion von Intelligenz, wenn Programmkomponenten so interagieren, dass wir es nicht mehr verstehen, aber das resultierende Handeln des Programms sinnhaft wirkt?

Das dritte Thema ist das Verhältnis von Informatikforschung und Militär. Es ist die Zeit von Ronald Reagans „Krieg der Sterne“-Adaption *Strategic Defense Initiative* (SDI). Einige Beobachter des Turniers stehen dem Pentagon nahe. Schnell werden das Wettrüsten im Kalten Krieg und der drohende dritte Weltkrieg zum Gesprächsthema, inklusive, wie die Informatik dabei „hilft“. Algorithmisch ist es (fast) kein Unterschied, ob Schachfiguren auf einem Schachbrett oder Truppen, Panzer und Flugzeuge auf einem Schlachtfeld verschoben werden. Das wirft zwei Fragen auf: Sollen InformatikerInnen für das Militär arbeiten? Und auch: Sollen InformatikerInnen Themen bearbeiten, die auch für das Militär interessant sind?

Da der Film Schachprogramme und Künstliche Intelligenz anspricht, sieht es nach einer Frage der 1980er Jahre aus. Eine solche hätte sich mit dem Ende des Kalten Kriegs erledigt. Doch das ist eine Illusion. Die Frage ist zeitlos. Heute geht es um den NSA-Skandal oder den Einsatz von Überwachungstechnologien, die repressiven Regimes helfen, Proteste effizient niederzuschlagen. Das betrifft die Forschung zu *Information Retrieval*, *Big Data* und IT-Security oder die *DARPA-Challenges* für autonome Systeme. Die Qualität des Films ist es, Fragen aufzuwerfen, ohne zu urteilen. Es gibt keinen Diskurs, keine moralische Wertung. Gespräche zu kritischen Themen folgen im Film einem typischen Ablauf. Ein Protagonist macht eine Aussage. Es folgen zwei, drei Repliken. Darauf wechselt das Thema wieder.

Die Hauptakteure des Films sind InformatikerInnen, Hardcore-Nerds der 1980er. Sie sind begeistert von ihrer Arbeit. Sie wetteifern, das beste Schachprogramm zu entwickeln. Interagieren sie mit anderen Menschen, führt das oft zu Missverständnissen. Doch Andrew Bujalski zeigt keine Freak-Parade sonderbarer Menschen. Es sind facettenreiche Charaktere, deren Interaktion die Dynamik des Films auslöst. Dazu einige Beispiele: Pat Henderson ist Organisator und Hauptmoderator der Veranstaltung. Er inszeniert sich als Koryphäe, doch die Kamera porträtiert ihn eher ironisch-unvorteilhaft. Peter Bishton ist der tragische Held des Films. Der schüchterne Doktorand ruiniert seinen Betreuern die Titelverteidigung, da sein Programm fehlerhaft ist. Interaktionen mit Frauen und seinen Betreuern verlaufen eher bizarr. Tom Schoesser ist mehrfach gefordert. Er hat Ehefrau und Baby mit zur Konferenz gebracht. Seine Frau kümmert sich um das Baby, wobei er sie – bei Bedarf – wegschickt. Seine eigentliche Herausforderung ist nämlich Peter Bishton, der ihn des Öfteren verzweifeln lässt. Les Carbray ist Informatiker in der Industrie. Er träumt von Computerschachprogrammen, mit denen Kinder spielen können. Er genießt, dass ihm Geld und Ressourcen zur Verfügung stehen. Woher das Geld kommt oder ob seine Resultate militärisch verwendet werden, das ist für ihn nachrangig. Und schließlich Michael Papageorge – er ist der Papagei und Querdenker des Turniers, Freelancer, elegant gekleidet und eloquent, doch nicht unbedingt gut bei Kasse und eher chaotisch.

Die Turnierteilnehmer mögen skurril sein, doch ist eine Seminargruppe im gleichen Hotel noch viel schräger und lässt das skurrile Verhalten der InformatikerInnen fast normal wirken. Die Seminargruppe ist auf einem „Suche-nach-sich-selbst-Trip“ inklusive Wiedergeburtsritus. Treffen Sinnsucher und Informatiker aufeinander, sind Verwicklungen und Situationskomik garantiert.

Eine große Stärke des Films ist seine atmosphärische Dichte, zu der der Dreh in Schwarz-Weiß, die entlarvende Verwendung von Floskeln aus der Welt der Informatik und Forschung, sowie der Quasi-Reportagestil beitragen. Der Film hat einen sehr subtilen Humor. Das ist der Unterschied zu massentauglichen Serien wie *The IT Crowd* oder *The Big Bang Theory*, mit denen Nerd-Themen in den letzten Jahren die Unterhaltungsindustrie erobert haben. In *Computer Chess* thematisiert Andrew Bujalski en-passant die Wechselwirkungen gesellschaftlicher Fragen und der Arbeit der InformatikerInnen, wobei die Zuschauer selbst nachdenken und sich ihre eigene Meinung bilden müssen. Kurz gesagt, ein Film für einen ruhig-nachdenklichen Kino- oder Filmabend mit einigen absurd-amüsanten Szenen und ein Muss für die I*nformatik&Gesellschaft*-Community.

Computer Chess, *ein Film von Andrew Bujalski, 92 min, Schwarz-Weiß und Farbe, Englisch, erhältlich als DVD/BlueRay oder als Download von www.computerchessmovie.com und iTunes.*

Klaus Haller arbeitet im Consulting mit den Schwerpunkten IT Risiko/Data Loss Prevention und Organisation von Test Centern. Mehr auf seiner Homepage *www.klaushaller.net*.

Dietrich Meyer-Ebrecht

„Inside Wikileaks“

Ein ‚must see‘ trotz Kritik

Der Film lässt es noch offen – *wikileaks.org* ist wieder online. Die Geschichte der Whistleblower-Plattform Wikileaks ist noch nicht zu Ende gespielt. Und die Zukunft ihres ‚Schöpfers' Julian Assange ist ungewiss. Kam der Film zu früh? Oder zu spät? Als der Film über Wikileaks und seine Protagonisten in die Kinos kam, war er in einem Punkt bereits von der Realität überholt: Edward Snowden hatte in jenen Wochen die Notwendigkeit einer Whistleblower-Plattform in den Hintergrund treten lassen. Mit einer beispiellosen Zivilcourage bewies er – unter Inkaufnahme hoher persönlicher Risiken –, wie viel wirksamer und überzeugender ein offenes persönliches Eintreten für den Akt des zivilen Ungehorsams, die Aufdeckung gesellschaftlicher Missstände sein kann. Die kritische, verantwortungsvolle, überlegt argumentierende und handelnde Person gibt sich uneitel zu erkennen – nicht zuletzt im NDR-Interview mit Hubert Seipel am 22. Januar 2014 (straft es nicht jene Medien Lügen, die Snowden mit den Attributen „geltungssüchtiger, linkischer junger Mann“ demontieren möchten?). Nur, es gibt so viele gesellschaftliche Missstände, die aufzudecken sind – und darf die Gesellschaft erwarten, dass es für jeden einen Menschen gibt, der für die Aufdeckung seine Existenz riskiert? Solange die Gesellschaft Wistleblowern ambivalent gegenüber steht, solange die Rechtsprechung sie nicht unter einen vorbehaltlosen Schutz stellt, sind Anonymität bietende Whistleblower-Plattformen nicht weniger dringend nötig als vor den Snowden-Enthüllungen. Wobei wir uns allerdings fragen müssen, ob ein Informantenschutz angesichts der Übermacht der staatlichen Spionage-Instrumentarien überhaupt noch garantiert werden kann …

Doch die Gefahren und Probleme eines solchen Unternehmens – und damit kommen wir zu *Inside Wikileaks* – liegen (noch) auf einer ganz anderen Ebene, der menschlichen. Ein solches Unternehmen ist kein kühl kalkuliertes Geschäft, kein ‚professionally managed business'. Das liegt in der Natur der Sache. Hier bedarf es eines Teams von Menschen mit nahezu unvereinbaren Eigenschaften: draufgängerisch und verantwortungsvoll, spontan und planvoll, technisch hoch spezialisiert und dabei zu unkonventionellen Experimenten bereit, motiviert und zusammengehalten von einer Idee, einer Mission. Reicht sie aus, um das gemeinsame Unternehmen auch in schwerem Wetter trotz aller divergierender Energien über Wasser zu halten? Daniel Domscheit-Berg, mit überzeugender Zurückhaltung gespielt von Daniel Brühl, lässt sich in den Sog der großen Idee ziehen, als er mit Julian Assange zusammen kommt. Assange, bis in Gestik und Mimik meisterlich verkörpert von Benedict Cumberbatch, personifiziert für Domscheit-Berg das ‚Unternehmen', hinter dem dieses verwegene Team zu stecken scheint. Bis seine Aura sich nach und nach auflöst, bis Assange als Einzelkämpfer entzaubert wird, der überall zugleich sein will, der egomanische Facetten nicht mehr verbergen kann. Wenn es am Ende auch Sachfragen zu sein scheinen, an denen die Zusammenarbeit zerbricht – Domscheit-Berg fordert redaktionelle Eingriffe in das Material zum Schutz der Informanten, Assange will rigoros die *unzensierte* Veröffentlichung –, vermittelt der Film das Scheitern einer nachhaltigen Arbeitspartnerschaft an der Unvereinbarkeit der Charaktere.

Die Originale: Julian Assange and Daniel Domscheit-Berg at the 26C3 in Berlin, 2009, Foto: andymcgee, CC BY 2.0

Vermutlich ist die Geschichte der Zusammenarbeit gefärbt gesehen aus der Perspektive Domscheit-Bergs, denn Josh Singers Drehbuch liegt wohl vor allem Domscheit-Bergs autobiographisches Buch *Inside WikiLeaks: Meine Zeit bei der gefährlichsten Website der Welt* zugrunde. Von dem sich Assange vehement distanziert – wie auch von dem Film. Einäugigkeit ist nicht die einzige Kritik, die dem Film zuteil wird. Mit dem Untertitel „Geradezu sträflich obskur und phantasielos“ kanzelt beispielsweise eine Filmkritik in der Frankfurter Rundschau den Film ab, aus cineastischer Sicht vielleicht nachvollziehbar. Nur, das Sujet ist schwierig. Und doch gelingt es dem Regisseur Bill Condon, die Netzwelt in ihrer Abstraktheit sichtbar zu machen, das Grenzenlose des virtuellen Raums zu vermitteln, die Gleichzeitigkeit bei aufgelöster Ortsgebundenheit. Über die Metaphern, die er verwendet, kann man geteilter Meinung sein, aber sie funktionieren. Wir erleben die Hektik der Akteure, der Nerds, die sich noch faszinieren lassen von den irrealen Mechanismen der Netzwelt. Auch die realen Handlungsorte ordnen sich dem ratlosen Takt der digitalen ‚messages' unter – ein ad hoc angesagtes konspiratives Treffen in Liège in Calatravas Stahl-Glas-Ambiente des neuen Fernbahnhofs, eine Stippvisite zu versteckten Internetservern im Viehstall eines abgelegenen schwedischen Bauernhofs, und immer wieder Berlin mit seiner virulenten Hackerszene. Eingebettet in das Stakkato dieser Welt ist das geradezu klassische Drama, der Protagonist Assange, der Antagonist Domscheit-Berg. Dessen Weg vom ‚follower' eines fast kultisch emporgehobenen Assange zum emanzipierten Gegenspieler. Die nie einhaltenden schnellen Schnitte fordern das Publikum, lassen die Spannung nicht abreißen.

Ein Stück gute Unterhaltung. Um die Wikileaks-Geschichte nachzuvollziehen, muss dieser Film nicht gesehen werden. Um einen Schlüssellochblick hinter die Kulissen zu werfen auf das menschliche Miteinander, das die Geschichte von Wikileaks wohl entscheidend beeinflusst hat – und das symptomatisch für Unternehmen mit vergleichbaren Ambitionen zu sein scheint –, ist er ganz gewiss interessant. Eine Szene jedoch ist es, derentwegen der Film gesehen werden *muss*, im Kino, auf Groß-

leinwand: das eingespielte (und in seiner optischen und akustischen Qualität aufbereitete) Video *Collateral Murder*, mit dem Wikileaks 2010 Geschichte machte, die Bildszene des kaltblütigen Mordanschlags auf Zivilisten aus der Perspektive des Schützen, dazu der klar verständliche O-Ton der Anweisungen an den Schützen aus dem Off der Kanzel des US-Hubschraubers. Mit den Bildern dieser kurzen Szene im Kopf gehe ich aus dem Kino, die Stimme noch im Ohr – wir haben das Video noch in Erinnerung, aber dieses Mal, in diesem Kontext, in dieser Aufmachung trifft es mich tief: diese Arroganz, diese Menschenverachtung! Die Macht ist enttarnt.

Inside Wikileaks *(englischer Titel* The Fifth Estate*), USA 2013, Regie: Bill Condon. 124 Min.*

Dietrich Meyer-Ebrecht ist Stellvertretender Vorsitzender des FIfF. Er war bis 2004 Inhaber des Lehrstuhls für Bildverarbeitung der RWTH Aachen.

Dagmar Boedicker

Mark Mazzetti: „Killing Business. Der geheime Krieg der CIA“

Nach den fragwürdigen Aktivitäten der CIA *zu Beginn des Kalten Kriegs bewirkt in den 1970er Jahren der* Church-Ausschuss *ein Verbot gezielter Tötungsaktionen. Seitdem bewegt der Geheimdienst sich in einem Auf und Ab von Aggression und Risikoscheu, abhängig von der öffentlichen Meinung und politischer Einflussnahme. Heute ist die CIA das Instrument – das Skalpell*[1] *– des Präsidenten für gezielte Aktionen, die das Militär aus rechtlichen Gründen nicht ausführen darf bzw. durfte. Sie beauftragt eine Vielzahl von Agenten, die von privaten Unternehmen beschäftigt werden, in einer Parallele zum Pentagon, das seit dem Irak-Krieg ebenfalls zahlreiche Aufgaben privatisiert hat.*

Private Unternehmen kämpfen nicht nur für die USA, sie spionieren auch für sie. Das führt zu höchst eigenartigen, unkoordinierten Kooperationen zwischen Militär, Geheimdiensten verschiedener Länder und Firmen auf mehreren Kontinenten. Während die USA früher vorwiegend in ihrem *Hinterhof* Lateinamerika, den Philippinen und anderen Einflussgebieten geheime Strippen zogen und gegen die Menschenrechte verstießen, tun sie es jetzt hauptsächlich in Afrika und Asien. Folter oder Tötungsaktionen durch Drohnen mit unbeteiligten Opfern rechtfertigen sie mit einem *Krieg gegen den Terrorismus,* den sie inzwischen auf die ganze Welt ausgedehnt haben. Protagonist ist dabei das *CTC,* das *Counterterrorism Center.*

Mazzetti, Mark:
Killing Business.
Der geheime Krieg der CIA.
Berlin, Berlin Verlag 2013
ISBN 978-3827011749
Hardcover, 416 Seiten
22,99 €

Psychologische Kriegführung – telekommunikativ

Während des Kalten Kriegs gab die CIA viel Geld für Propaganda und psychologische Kriegführung aus. Das änderte sich nach dem Fall des Eisernen Vorhangs, und die Mittel wurden in den 1990er Jahren gekürzt. An sich ist es dem Geheimdienst verboten, die US-Bürger durch Propaganda zu beeinflussen. Das war kein juristisches Problem, solange die CIA „erfundene Geschichten in ausländischen Zeitungen“ platzieren konnte, ohne dass „diese Lügengeschichten auch von amerikanischen Medien aufgegriffen“ wurden, also vor der Zeit des Internet. Inzwischen hat das Militär sich dieser Aufgaben angenommen, obwohl es das eigentlich auch nicht darf, „doch der Kongress lässt dem Verteidigungsministerium in der Regel mehr Spielraum für psychologische Kriegführung, wenn es beweisen kann, dass sie der Unterstützung kämpfender amerikanischer Soldaten dient.“

Das *US Special Operations Command (SOCOM)* hat eine Abteilung für psychologische Kriegführung. Die suchte nach Wegen, „im Nahen Osten Propagandakampagnen durchzuführen und Nachrichten zu beschaffen“. Als Teil einer breiten Kampagne mit dem Codenamen *Native Echo* ließ sie 2006 von einem tschechischen Unternehmen, *U-Turn Media,* Videospiele entwickeln, die man im Nahen Osten auf Handys laden konnte. Ziel war es, mehr über Muslime zu erfahren, indem man die Spielerdaten sammelte. Gleichzeitig sollten die Spiele ein positives Bild der USA vermitteln: „Das Spiel *Iraqi Hero* war so aufgebaut, dass es leicht für alle möglichen Länder in der muslimischen Welt modifiziert werden konnte.“ Die Grafik war vielseitig einsetzbar, mit Anpassungen der Dialoge sollte das Spiel für 13 Länder geeignet sein. Der Titel der libanesischen Fassung lautete *Maghaweer,* „nach einer libanesischen Kommandoeinheit“.

„U-Turn entwickelte noch zwei weitere Spiele für Operation Native Echo: In *Oil Tycoon* baute der Spieler Ölpipelines und musste die Ölanlagen des Staats gegen ständige Angriffe von Terroristen verteidigen, und in *City Mayor* musste er beim Wiederaufbau einer von Terroristen zerstörten Großstadt über die Verwendung begrenzter Mittel entscheiden.“ Die Spiele wurden auf Websites und Blogs gepostet und über Tausende von Speicherkarten auf Märkten und Basaren verkauft und verschenkt. Auf den Websites „konnte das SOCOM außerdem überwachen, wie viele Personen sie herunterluden und, wichtiger noch, wer sie herunterlud.“

Ende 2007 erweiterte das Pentagon seine Propaganda weltweit. U-Turn sollte ein SOCOM-Projekt unterstützen, „das darin be-

stand, Websites für Zentralasien, Nordafrika, China und andere Regionen zu betreiben. Die sogenannte Trans-Regional Web Initiative engagierte freie Journalisten, …" Sie sollten gute Nachrichten über die USA und ihre Verbündeten (kaum lupenreine Demokratien) verbreiten, zunächst ohne den Urheber Pentagon zu enthüllen. Als Nachrichten von dem Projekt durchsickerten und Unruhe entstand, brachte man „unten auf jeder Seite ein kleines Etikett an, das sie als Produkt des US-Verteidigungsministeriums kennzeichnete."

Als die CIA-Station in Prag das Projekt hinterfragte und darauf hinwies, „dass es russischen Geheimagenten womöglich leichtfallen könnte, U-Turn zu infiltrieren", kam ein weiteres Problem ans Licht. SOCOM hatte 2007 „in aller Stille die Computerserver mit den Daten, die es über [US-]amerikanische Staatsbürger gesammelt hatte, nach Prag ausgelagert." Die tschechische Regierung war darüber nicht informiert. Diplomatische Verwicklungen waren programmiert, weil Russland die US-Pläne nicht gefielen, in Prag ein Radarsystem für das Raketenabwehrprogramm zu installieren. Wohl auch deshalb wussten nicht einmal die US-Botschaft und die CIA-Niederlassung in Prag Bescheid.

Der einseitige *Krieg gegen den Terror* hat die nachrichtendienstlichen Fähigkeiten der CIA entscheidend geschwächt, weil ausländische Nachrichtendienste ihre Zusammenarbeit einschränkten und das Personal für Kontakte in den Ländern fehlte, über die Informationen gesammelt werden sollten. Die parallelen Aktivitäten von CIA und Militär bei gleichzeitiger Rivalität verursachen grobe Schnitzer, weil beide ohne Abstimmung operieren und sich dabei in die Quere kommen. „Und es ist ein militärisch-geheimdienstlicher Komplex entstanden, mit dem eine neue amerikanische Art des Kriegs geführt wird."

Mazzetti ist investigativer Journalist und Pulitzer-Preisträger. Er schreibt ausgezeichnet und seine Art, die beteiligten Personen zu schildern, ist manchmal sogar erheiternd. Die geschilderten Fakten sind es nicht. Mazzetti benennt seine zahlreichen Quellen (auch Wikileaks) im Detail, außerdem enthält das Buch ein Orts- und ein Personenregister, es ist also gut als Nachschlagwerk geeignet. Kleiner Wermutstropfen: Es wurde von zwei Personen übersetzt, vermutlich getrennt für die erste und zweite Hälfte. Die zweite hätte ein Lektorat gebraucht. Killing Business ist trotzdem eine spannende und informative Lektüre.

Anmerkung

1 *John Brennan, CIA-Chef seit März 2013: „Statt mit dem ‚Hammer' zuzuschlagen, setzt Amerika jetzt das ‚Skalpell' an." (S. 22)*

Dagmar Boedicker ist Journalistin und technische Redakteurin. Sie hat Politikwissenschaft studiert.

Stefan Hügel

Christian Fuchs und John Goetz: „Geheimer Krieg – wie von Deutschland aus der Kampf gegen den Terror gesteuert wird"

Der internationale Ausspähskandal wird in der Regel als *NSA-Skandal* diskutiert. Allenfalls wird das britische GCHQ erwähnt. Das erweckt den Eindruck, dass wir lediglich das Opfer der Spionage ausländischer – freilich befreundeter – Mächte sind. Hatte nicht bereits der damalige Bundeskanzler Gerhard Schröder 2002 die Beteiligung am Irak-Krieg abgelehnt? „We were not convinced" – wir waren nicht überzeugt, und deswegen hielten wir uns heraus, aus einem Krieg, den wir nicht für gerechtfertigt angesehen hatten.

Gar nicht dazu passen wollten Nachrichten, nach denen die Zurückhaltung weniger konsequent war, als es Schröder – und Fischer – im Wahlkampf suggerierten. Offenbar wurde doch auch von deutschem Boden aus operiert, zumindest Überflug- und Landerechte gewährt, und damit zumindest im Verborgenen der Krieg unterstützt, wegen dessen vorgeblicher Ablehnung die damalige Regierung vermutlich wieder gewählt wurde.

Während nun die Ausspähung der NSA und des GCHQ in der Öffentlichkeit diskutiert wird und immer neue Enthüllungen ans Licht kommen, haben die Reporter des *Norddeutschen Rundfunks*, *Christian Fuchs* und *John Goetz* – mit Unterstützung aus der *Süddeutschen Zeitung* – analysiert, welchen Beitrag Deutschland leistet – zu mutmaßlichen Drohnenmorden, zur

Christian Fuchs, John Goetz (2013)
Geheimer Krieg. Wie von Deutschland aus der Kampf gegen den Terror gesteuert wird
Reinbek bei Hamburg: Rowohlt
ISBN 978-3-498-02138-2
Hardcover, 256 Seiten
19,95 €

Überwachung, zum *Krieg gegen den Terror*. In gewisser Weise kann der Band auch als Fortsetzung zu *Josef Foschepoths* Studie *Überwachtes Deutschland* gelesen werden (vgl. unsere Rezension in *FIfF-Kommunikation* 4/2013) – freilich nicht mit historisch-wissenschaftlichem, sondern *nur* mit journalistischem Anspruch.

Dem journalistischen Anspruch ist sicherlich das erste Kapitel geschuldet, das mit einem Schockeffekt in die Thematik einführt.

Drastisch wird dort beschrieben, wie die in der Öffentlichkeit gerne als *präzise*, *chirurgische* Schläge dargestellten Drohnenangriffe in der Praxis aussehen: Menschen werden zerrissen, es herrschen Tod und Zerstörung (S. 11-15). Häufig warten die Drohnen offenbar, ob es Überlebende gibt, um sie mit einem zweiten Schlag ebenfalls zu töten. Da dies mitunter auch geschieht, während Überlebende von Sanitätern gerettet werden, handelt es sich möglicherweise um Kriegsverbrechen, wie *Amnesty International* in der Studie *Will I be next?* feststellt.

Im Kontext dieses Buches ist aber auch ein anderer Aspekt von Bedeutung: Bei einem der Opfer des Drohnenangriffs handelte es sich um einen deutschen Staatsbürger – unklar scheint, ob der entscheidende Hinweis vom deutschen Bundesnachrichtendienst (BND) kam. Liefert Deutschland seine eigenen Staatsbürger tödlichen Angriffen aus? Die Bundesregierung bestreitet das (S. 11-15).

Abgeschlossen wird dieser einleitende Teil mit der Frage, ob Deutschland – auf der Seite der USA – zum *tiefen Staat* geworden ist, zu einem Staat, in dem aufgeblähte Sicherheitsbehörden mittlerweile zu einem *Staat im Staate* geworden sind (S. 23-24). Wir kennen das aus dem Geschichtsunterricht zur Rolle des Militärs zu Beginn des 20. Jahrhunderts – wohin das damals letztendlich geführt hat, sollte uns allen noch deutlich vor Augen stehen.

Die folgenden fünf Kapitel bilden den zweiten Teil des Bandes, der sich mit dem *US-amerikanischen Afrikakommando* in Stuttgart auseinandersetzt. Der Grundstein für die Koordination der Kriege in Afrika wurde 2007 gelegt – offenbar wurden zuvor eine Reihe von Anfragen an afrikanische und andere Staaten, das US-Kommando AFRICOM in diesen Ländern anzusiedeln, von deren Regierungen abgelehnt. *Abu-Ghuraib* und *Waterboarding* waren in aller Munde, das moralische Kapital der USA aufgebraucht. Anscheinend kein Problem für die damalige deutsche Bundesregierung: Man wurde sich einig. Offenbar werden nun militärische Operationen aller Art in Afrika von Stuttgart aus koordiniert – was dem Band zufolge die Verschleppung und Folterung Verdächtiger und die gezielte Tötung einschließt (S. 27-37). Der britische Staatsbürger *Bilal al-Berjawi* gilt als der erste Mensch, der bestätigtermaßen durch einen gezielten Drohnenangriff am 21. Januar 2012 getötet wurde – kurz nach einem Telefonat mit seiner Frau, durch das er wohl seinen Aufenthaltsort offengelegt hat. Dem Band zufolge wurde diese Hinrichtung von Stuttgart aus befehligt (S. 71-72). „*AFRICOM ist verantwortlich für alle Operationen, Übungen und Sicherheitskooperationen des US-Verteidigungsministeriums auf dem afrikanischen Kontinent, seinen Inseln und den umgebenden Gewässern*“ (S. 76). Was bedeutet, dass alle diese Operationen von deutschem Boden aus koordiniert werden.

Deutschland und der amerikanische Drohnenkrieg ist Teil III überschrieben. Zentrum des von Deutschland aus gesteuerten Drohnenkriegs ist der Stützpunkt in Ramstein, der in den 80er Jahren durch einen verheerenden Unfall bei einer militärischen Flugschau traurige Berühmtheit erlangt hat. „*In Ramstein sitzen Leute, die minutiös und in Echtzeit überwachen, wer gerade wo fliegt und wer wo schießt und welche Bilder kommen. Ramstein ist die Operationszentrale*“ (S. 88), zitieren die Autoren einen ehemaligen Offizier der Luftwaffe der Bundeswehr. Dazu der Richter am Bundesverwaltungsgericht, *Dieter Deiseroth*: „*Jede deutsche Regierung steht vor dem Abgrund des Verfassungsbruchs, wenn sie bewusst das Hoheitsgebiet in die Führung eines völkerrechtswidrigen Krieges verwickeln und einbeziehen lässt*“ (S. 114), und „*Jede Entscheidung einer deutschen Regierung, die USA heute bei ihren Kriegen zu unterstützen, ist immer politisch gewollt und muss rechtlich verantwortet werden*“ (S. 113-114). Die Antwort der Bundesregierung auf Nachfrage der Autoren im Rahmen der Recherchen zu dem Buch folgte offenbar dem bekannten Muster: „*... es lägen keine Anhaltspunkte vor, dass Drohnenangriffe über Deutschland geplant oder durchgeführt werden*“ (S. 115).

Teil IV setzt sich mit den *Aktivitäten der NSA in Deutschland* auseinander. Öffentlich diskutiert wurde dazu bereits der *Dagger-Complex* bei Darmstadt, wo offenbar Teile des *United States Army Intelligence and Security Command* (INSCOM) ihren Stützpunkt haben. Deren Hauptsitz in Deutschland ist eine Kaserne bei Wiesbaden. Offenbar erfolgt die Überwachung des Fernmeldeverkehrs in Deutschland von diesen Standorten aus – durch INSCOM und durch die NSA. Dass die NSA auch den Internetverkehr direkt vom Knoten *DE-CIX* in Frankfurt am Main abgreift, wird von den Verantwortlichen bestritten, aber: „*... die NSA kann natürlich irgendwo anders ein Kabel hier in Frankfurt außerhalb des Firmengeländes angezapft haben*“ (S. 177).

Der letzte Teil des Bandes – Teil V – thematisiert die *guten Geschäfte*, die auf deutschem Boden bei den nachrichtendienstlichen Operationen gemacht werden. Deren Zentrum ist offenbar eine CIA-Logistikzentrale, die sich im Osten Frankfurts, in der Nähe der *Friedberger Warte* befindet (S. 181ff.) und von der aus offenbar auch geheime Gefängnisse aufgebaut wurden, um Terrorverdächtige außerhalb der USA gefangen zu halten und zu verhören (S. 186ff.). In diesem Zusammenhang gehen die Autoren auch auf die Verschleppung des deutschen Staatsbürgers *Khaled al-Masri* 2003-2004 ein, bei der ein US-amerikanisches IT-Unternehmen mit deutschem Hauptsitz in Wiesbaden eine nicht unerhebliche Rolle gespielt hat (S. 193-194).

Der Band stellt die vielfältigen Aktivitäten vor allem US-amerikanischer Militärs und Geheimdienste dar, deren Legalität zumindest zweifelhaft erscheint. In Summe macht er damit deutlich, dass es nicht ausreicht, sich wohlig vor den Presseberichten über die NSA-Überwachung zu gruseln. Es ist eben nicht nur folgenlose Überwachung, und es sind eben nicht nur Amerikaner und Briten, auf die wir die Verantwortung abwälzen können. Es spricht einiges dafür, dass auch deutsche Behörden in den Überwachungsskandal verstrickt sind – und es spricht auch einiges dafür, dass die Überwachung massive Folgen hat: Zumindest die grausame Tötung vermeintlicher *Terroristen* und in der Nähe befindlicher Unbeteiligter, gerne zynisch als *Kollateralschäden* bezeichnet.

Die Empfehlung zu dem Band dürfte nicht mehr überraschen: Unbedingt lesen! Empfehlenswert ist dazu auch die Web-Seite mit weiteren Informationen: *http://geheimerkrieg.de.*

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

Britta Schinzel

Karin Harrasser: „Körper 2.0. Über die technische Erweiterbarkeit des Menschen“

Dieses vergleichsweise schmale Buch zu lesen macht mit jeder Zeile Vergnügen. Es ist vor allem erhellend, aber zugleich auch unterhaltsam und kurzweilig geschrieben. Es handelt von Prothesen in verschiedenen Funktionen, als Ersatzglieder, als Mittel zur Selbstverbesserung, als Instrument zur Markierung von Unterschieden, bis hin zur ununterscheidbaren Verschmelzung von Körper und Technik. Harrasser stellt ihre Untersuchungen in einen historischen Rahmen, um die Kontingenz der Entwicklungen zu verdeutlichen. Sie bezieht sich auf Foucault, Deleuze, Stiegler, Kracauer, Latour, Haraway, Sloterdijk u. a., und setzt sich doch stets von ihnen ab. Als Literatur- und Medienwissenschaftlerin zieht sie jedoch auch Elfriede Jelinek, Oswald Wiener, Alfred Jarry, oder Werner Herzogs Film F*itzgeraldo. Wo die grünen Ameisen träumen* heran, um ihren Argumente zu erklären oder ihnen Nachdruck zu verleihen. Wenn sie sich dabei, jeweils anhand verschiedener historischer oder literarischer Beispiele, oft wiederholt, so rechne ich das ihrer Absicht zu, uns ihre sehr nachvollziehbaren Thesen nachhaltig einzubläuen.

In neun unterschiedlich fokussierten Kapiteln entwickelt sie ihre kulturkritische Haltung zu Vorstellungen von kontinuierlich verbesserbaren Körpern, von technischen Körpermodifikationen und -enhancement, und weiter von einer stetigen technischen Evolution im Sinne von Steigerung und Optimierung, indem sie diese Entwicklungen in eine höchst voraussetzungsvolle historische, epistemologische und politische Konstellation positioniert, ohne dabei persönlich oder situativ sinnvolle Verbesserungen für Einzelne oder Gruppen zu leugnen. Womit der konstruktive Vorschlag schon anklingt, anstelle des schneller, weiter, höher, das Enhancement in den Möglichkeitssinn zu legen, in einer *slow science* die Alternativen auszuloten und die kontingente Situierung zu betonen.

Der Text beginnt mit dem paralympischen Sport und der Geschichte von Oskar Pistorius, dem ohnbeinigen Läufer, der bei den olympischen Spielen konkurrieren durfte, weil ein Gutachten bezeugte, dass seine Prothesenbeine ihm beim Laufen keine Vorteile verschafft hätten. Hingegen zeigt Harrasser auf, dass diese natürliche Beine keinesfalls ersetzen, da sie gerade auch nur für diese Distanz des Laufens gut geeignet sind, nicht jedoch für Stehen oder andere Bewegungen. Dann stellt sie den Biomechatroniker am MIT *Media lab* Hugh Herr und die Leichtathletin Aimee Mullins vor, die sich beim Symposium 2007 *humans 2.0* als Vorreiter einer technischen Erweiterung gegenüber Normalkörpern dadurch privilegiert sehen, dass sie „eine Evolution der technischen Zukunft vorantreiben“. Die Prothesen sind zwar zunächst Serienfertigungen, dann jedoch individualisiert und singulär auf den Träger angepasst. Es fällt auf, dass die in *humans 2.0* gezeigten Behinderungen fast immer nur die Beine betreffen, sodass die Behinderung Schönheit und Normalität in einem Produktivitätssinn nicht behindert. Dies geht einher mit einer die Behinderung umdeutenden Sprache und Episteme der Selbstverbesserung, die nur im Wettbewerb erreichbar ist, und die teure Technologien und Eigenschaften wie Leistungsbereitschaft, Intelligenz oder Risikobereitschaft voraussetzt. Solche sind untrennbar mit einer neokapitalistischen Kultur der wertschöpfenden Selbstoptimierung verknüpft, charakterisiert durch Training und ein funktionales Verständnis des Körpers. An ihnen zeigt sie, wie die Architektur der eigenen Identität auch mittels symbolisch-ästhetischer Mittel für das Selbstdesign des eigenen Körpers als Besitz letztlich der Vermarktung und Produktionssteigerung dient.

Karin Harrasser (2013):
Körper 2.0.
Über die technische Erweiterbarkeit des Menschen.
Reihe X-Texte,
Bielefeld: Transcript-Verlag
ISBN 978-3-8376-2351-2
Broschiert, 144 Seiten
17,99 €

Die Umwertung der technisch Erweiterten in Superhumans birgt etliche Gefahren, wie die Disability Studies deutlich machen: Nietzsches Übermensch klingt an, ebenso wie die Gefahr kategorialer Auf- und Abwertungen als nicht-menschlich im posthumanistischen Diskurs. Abwertung vor allem, wenn die Behinderung nicht nur die Beine betrifft, sondern auch Gesicht, Kopf, oder das Gehirn. Die Aufwertung wiederum setzt die sehr menschliche Fähigkeit der Selbstbemeisterung voraus, Hindernisse zu überwinden, Schwächen auszumerzen, und das individuell wie gesellschaftlich mit hohem Preis: der Betonung von Konkurrenz als Triebkraft des Sozialen, der Ideologie der permanenten Selbstoptimierung, der Ausdehnung der Wertschöpfungskette auf die gesamte Persönlichkeit, der Ununterscheidbarkeit zwischen individueller und technischer Leistung, und der Auflösung des Mythos von der Gleichheit aller Körper und der Universalität von Leistungs- und Trainingsbedingungen im olympischen Gedanken durch die Verlagerung des Sports in die Hände von Ingenieuren.

Konsequent stellt Harrasser auch die enge Verknüpfung von Medizintechnik, IT- und Robotik-Branche mit dem militärisch industriellen Komplex heraus: enormer Bedarf an Prothesen entstand durch die Kriege, sowohl was ihre historische Behandlung und Wiedereingliederung von Kriegsversehrten in Gesellschaft und Arbeitsprozesse betrifft, als auch um die ins Wanken geratene Geschlechterordnung wieder herzustellen. Hier schon beginnt die Auseinandersetzung zwischen Prothesen als Ersatz und als Mittel zur Selbstregulierung. Letztere mündet in die Vorstellung von einem Kontinuum der (Selbst-)Verbesserung des grundsätzlich mangelhaften Körpers, und dem Ziel der Prothetik statt von Ersatzgliedern zum Gliederersatz. Der

Normale erscheint nun als potentieller Krüppel und der Krüppel als normal, solange er produktiv ist. Das Kapitel über Brillen und *Google Glass* erhellt, was die unterschiedlichen Funktionen von Prothesen sein können, nicht nur ein Ausgleich von Mängeln, ein Mittel, unauffällig zu werden, Fetisch, Waffe oder nur eine Markierung von Differenz. Solche Kapitalisierung von Differenz bringt eine Ethik der Selbstsorge mit Interkonnektivität, Selbstverwirklichung und Gesundheitsvorsorge hervor. Und so erscheint ein neuer Menschentypus, der *designable human*. Doch auch die Frage der Besitzverhältnisse des eigenen Körpers, in den investiert werden kann, damit er Profit abwirft, einer Utopie der beliebigen Verbesserung und Vernetzung und das Recht auf Enhancement sind nicht von einer neokapitalistischen Logik der Selbstoptimierung zu trennen. Die Bezeichnung *H 2.0* hybridisierter Körper suggeriert eine Verbesserung mit Bezug auf die Vorgängerversionen, eine offene Stufenleiter zur Perfektion. Im Kapitel zur Geschichte des verbesserbaren Menschen kritisiert Harrasser solches Enhancement des Körpers als Narration evolutionärer Notwenigkeit und stellt die kontingenten Bedingungen einer solch vermeintlichen Determinierung dar. Mit Sloterdijk entstammt solche „Anthropotechnik" dem Humanismus als Form der Bemeisterung des Menschen durch sich selbst und sie hat die historisch spezifische Selbstwahrnehmung des Menschen als souverän, individuell, autonom hervorgebracht. In solcher Selbstsorge von Prothesenversorgung einer Behinderung übergehend zu einem Konzept des unverletzten gesunden Körpers als Mangelwesen und seiner Disziplinierung mithilfe flexibler Methoden der Selbststeuerung sieht Harrasser den pardigmatischen Wechsel von der Sicht eines unverletzt perfekten Körpers zu einem kontinuierlich verbesserungsfähigen prothetisch mit seiner Umwelt verschalteten Körper, oder mit Elfriede Jelinek (Sportstück): „Heute ist vom unvollkommenen Körper zu sagen, dass jeder selbst schuld ist, wenn er ihn hat." Sie erinnert an Oswald Wiener, der in *Die Verbesserung von Mitteleuropa* mittels eines *Bio-Adapters* über Sprache eine kybernetisch-regulatorische Optimierung des Körpers imaginierte, und als Effekt der kybernetischen Rückkopplung bereits ein sozialtechnisches biopolitisches Government vorausahnte, das wie Harrasser bemerkt, Bernard Stieglers Thesen zur Psychomacht vorwegnahm und sich teilweise wie Gilles Deleuze's *Postscriptum über die Kontrollgesellschaft* liest. Der Bio-Adapter bedient alle menschlichen Begehrlichkeiten bis zur Selbstauflösung in einer technischen Selbststeigerung.

Eine Möglichkeit, Behinderung anstelle des Asyls gesellschaftlich zu inkludieren, ist die Normalisierung. Die Angebote reichen von unterschiedlichen Leistungsschemata über eine Ästhetik des Ungefügen grotesker Körper bis hin zu einer Tradition perverser karnevalesker Rituale, die zwar temporäre Überschreitungen ermöglichen, jedoch alle in einer Logik des zumindest symbolischen kognitiven und affektiven Kapitalismus verbleiben. Sie schließt, dass die Körperbearbeitungen im Kontext einer Neubewertung dessen was Leben ist, analysiert werden müssen.

Harrasser schlägt statt dessen ausgehend von einem inklusiven Humanismus ein Narrativ vor, die Parahumanität, die sich den Menschen als teilsouverän im Konzert unterschiedlicher, auch nichtmenschlicher Akteure, mit offenem Horizont, der einen Möglichkeitsraum offen hält. Sie erinnert an Haraways Cyborg als einen Technokörper, einen instabilen wandelbaren Körper als Träger und Generator eines selbstreflexiven Individuums, mit der Freiheit zur Selbstverbesserung, der nicht weiß, was oder wer er ist, bereit zu überraschenden neuen Verbindungen, Verkörperungen vergangener und kultureller Beziehungen und weltgenerierender Milieus. Der Mensch wäre weder ein zu kompensierendes Mängelwesen noch auf dem Wege zur Gottgleichheit, sondern in einem Milieu mit Maschinen, Tieren, usw., in dem alle zusammen wahrnehmen und kooperieren. Die Cyborg von Donna Haraway ist eine Figur, die abbremsen will, indem sie die Optionen verbreitern, ein Mehr an möglichen Zukünften implantieren soll.

Harrasser entwickelt ihre bereits dargestellten Thesen dann wiederholt anhand weiterer Literaturbeispiele. Sie zieht insbesondere Alfred Jarry's *Pataphysik* als Instrumentarium zur Befragung von Generalisierungen und Reduktionismen von Naturwissenschaften und seine Mensch-Maschine Hybride heran. Die *Pataphysik* sollte, so rationalisiert Harrasser Jarry's abseitige Erzählungen, zwischen Kunst, Wissenschaft und Philosophie einen Raum öffnen, indem mit Mimikry wissenschaftliche Stile und Sprache so lange imitiert werden, bis sie sich demaskieren und implodieren. In seiner Erzählung 1902 *Der Supermann* verliebt sich eine Liebesmaschine, die seiner Liebesfähigkeit gewachsen ist, so, dass sie ihn in der elektrischen Verschmelzung tötet und sich dabei selbst auflöst. Jarrys Maschinen sind aus dem Funktionalen gerutscht. Die Kurzgeschichte *Der Hummer des Hauptmanns* 1901 beschreibt die eigenmächtige Aktion der Handprothese des Hauptmanns aus einem lebendigen greiffreudigen Hummer, die macht was sie will. Damit verdichtet er die Frage der Zurechenbarkeit von Handlungen innerhalb unübersichtlicher sozial-technischer Systeme mit dem Natur-Technik-Verhältnis in nicht funktionalen Maschinen-Diskursen. Technik ist hier nicht Kontrolle und Beherrschung der Natur, sondern selbst Welt erzeugend, ohne Auftrag zur Selbstverbesserung, durch einen Kommunikationsimperativ mit Individuen verschaltet, und die Geschichte in ihrer Funktionalität verkapselnd. Es gibt keinen *Körper 2.0*, keine Versionierung, keine Vorhersehbarkeit technischen Fortschritts, aber Teilsouveränität des Handelns. Vorgeschlagen wird dazu eine spekulative Wissensethik, die sich auf Praxisformen statt auf Wissensformen, auf Ökologien von Interessen bezieht und nicht auf die Fiktion eines vom souveränen Subjekt ausgehenden Willens. Ungegangene Wege insistieren dabei mit Wirkung einer *slow science*, die Möglichkeiten anreichert und die Situierung betont.

Lesen Sie dieses schöne Buch!

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.

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-Büro

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

Die aktuellen Bürozeiten entnehmen Sie bitte unseren Webseiten.

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

FIfF im Netz

Das ganze FIfF:
www.fiff.de
Twitter-Accounts: *@FIfF_de* und *@FaireComputer*

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-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, Sylvia Johnigk, Kai Nothdurft, Jens Rinne
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-Logo von Sanne Grabisch *ideal.istik.de*, CC BY-SA 3.0
Druck	Meiners Druck, Bremen

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

Aktuelle Ankündigungen

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

BigBrotherAwards-Verleihung
11. April 2014 in Bielefeld

GPN14 – GulaschProgrammierNacht 14
19. bis 22. Juni 2014 in Karlsruhe
Zentrum für Kunst und Medientechnologie (ZKM) und Hochschule für Gestaltung (HfG), Karlsruhe

FrOSCon 2014 – Free and Open Source Software Conference
23. und 24. August 2014 in St. Augustin

MRMCD14 – MetaRheinMainConstructionDays
5. bis 7. September 2014, Hochschule Darmstadt

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

FIfF-Kommunikation
2/2014 »Datenausspähung und Videoüberwachung«
Stefan Hügel, Peter Bittner
Redaktionsschluss 1.5.2014
3/2014 »Gender«
Britta Schinzel, Sara Stadler
Redaktionsschluss 1.8.2014

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

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

DANA – Datenschutz-Nachrichten
1/14 - Konzerndatenschutz
2/14 - Internet der Dinge

Das FIfF-Büro

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

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

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

Schluss FIfF

„Verdächtig sicher“ – Donald Duck und die NSA

Phantomias – das *Alter ego* von Donald Duck – ist frustriert. Er, dessen Hauptaufgabe die Verbrechensbekämpfung in Entenhausen ist, wird nicht mehr gebraucht. Verantwortlich dafür ist die flächendeckende Überwachung der Stadt durch Kameras, die jedes Verbrechen bereits im Keim erstickt.

Die Vermutung liegt nahe, dass die Leserinnen und Leser der *FIfF-Kommunikation* nicht zu den regelmäßigen Rezipienten der *Lustigen Taschenbücher* von Walt Disney gehören. Doch in dem Ende 2013 erschienenen Band *Winterzeit* steckt eine Geschichte, die überrascht. Walt Disney nimmt sich der Ausspähung und Überwachung an.

Zunächst scheint Phantomias – neben den Gaunern der Stadt – der einzige zu sein, der unter den durch die Firma ***N****asweiser,* ***S****picker und* ***A****usspecht* in der gesamten Stadt installierten Überwachungskameras zu leiden hat. Doch die Geschichte nimmt eine überraschende Wendung: Die Kameras sollen die Einwohner Entenhausens in Sicherheit wiegen. Irgendwann übernimmt die Firma *NSA* auch die Überwachung selbst, die zuvor von der Polizei geleistet wurde. Durch einen Stromausfall sollen in einem geplanten Coup die Kameras deaktiviert und alle Gauner der Umgebung vorher davon informiert werden. Für diese Information soll der Hauptteil der dann erbeuteten Gegenstände in den Taschen der NSA-Bosse landen.

Doch natürlich ist Phantomias rechtzeitig zur Stelle, um das Komplott zu verhindern. Und so erkennen die Einwohner Entenhausens, dass man sich auf ihn, und nicht auf die Technik verlassen sollte. Wie immer bei Walt Disney: Das Gute siegt.

Am Ende werden die Kameras wieder abgebaut, mit der Erkenntnis: „Bewacht werden wollen die Menschen wohl, aber überwacht werden nicht.“

Nun steht Walt Disney eher im Ruf eines konservativen Konzerns. Aus deutscher Sicht würde man also erwarten, dass er die Überwachung als Schutz der Menschen befürworten würde, wie es konservative Innenpolitiker in Deutschland immer wieder betonen. Doch in den USA scheint dies anders zu sein: Hat sich nicht gerade der als ultrakonservativ geltende Senator *Rand Paul* an die Spitze einer Bewegung gestellt, die sich mit einer Sammelklage gegen die Ausspähung durch die NSA und deren Protagonisten wendet – gemeint ist freilich nur die Ausspähung amerikanischer Staatsbürger.

Amerika, Du hast es besser? Wohl eher nicht. Doch eines bleibt: Die Geschichte der NSA bei Donald Duck könnte helfen, Kinder für die Gefahren der Überwachung zu sensibilisieren. Und das ist schon etwas wert. Egal, aus welchem politischen Lager.

Stefan Hügel

Referenzen

Walt Disney Enterprises, Inc. (2013): Verdächtig sicher, in dies.: Winterzeit. Lustiges Taschenbuch Nr. 449. Berlin: Egmont Ehapa Verlag, Seite 91-124

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