H 7625

FIfF-Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

32. Jahrgang 2015 Einzelpreis: 7 EUR

4/2015 – Dezember 2015

Cybercrime

Kunstprojekt *11 TAGE*

ISSN 0938-3476

• Studienpreisverleihung • FIfFKon 2015 • Flüchtlinge und das Netz •

FIfF Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V.

Titelbild: Valid street photography, Foto: Isengardt, CC BY 2.0, https://www.flickr.com/photos/isengardt/21593846012 (links) Aufnahme aus Ego-Shooter-Perspektive auf die Ratte: Kunstprojekt 11 TAGE von Florian Mehnert (rechts)

Inhalt

Ausgabe 4/2015

inhaltt

Aktuelles

FIfF intern

„Cybercrime“

„Kunstprojekt 11 TAGE“

Lesen & Sehen

Rubriken

Editorial

„Zweieinhalb" Schwerpunkte enthält diese Ausgabe der *FIfF-Kommunikation*:

Cybercrime ist – wie mittlerweile viele Begriffe, die die Vorsilben „*Cyber-*" tragen – zum *Buzzword* geworden, das jeder so verwenden kann, wie es seinen eigenen Partikularinteressen nutzt. Wir verstehen unter *Cybercrime* im gleichnamigen Schwerpunkt dieser Ausgabe massive Internetkriminalität: Gewaltige finanzielle Interessen, die beispielsweise mit Identitätsdiebstahl oder Erpressung arbeiten, Regierungen und Geheimdienste als Auftraggeber krimineller Akte im Internet oder fremdenfeindliche Organisationen, die Hasskampagnen über das Netz orchestrieren. An Letzterem wird auch die Hilflosigkeit der Politik sichtbar: „*... einem bundesdeutschen Justizminister fällt dazu nicht mehr ein, als Facebook um freundliche Mithilfe zu bitten, eine ganz neue Auffassung von Public Private Partnership, wie es scheint*", kommentiert *Eberhard Zehendner*, der den Schwerpunkt betreut hat, in seinem einleitenden Schwerpunkteditorial auf Seite 21.

Auch anlässlich unseres zweiten Schwerpunkts trat die Polizei auf den Plan. Doch bei dem Kunstprojekt *11 TAGE* von *Florian Mehnert* handelt es sich keinesfalls um *Cybercrime*, wie vielleicht einige uns glauben machen wollten – eher schon bei der massiven Bedrohung des Künstlers, die auch vor Morddrohungen nicht zurückschreckte. Über sein Projekt hat Florian Mehnert bereits in der vorangegangenen Ausgabe berichtet. In Freiburg im Breisgau fand dazu am 6. Oktober 2015 ein Symposium statt, in dem die Ereignisse um das Projekt aus unterschiedlichen Blickwinkeln reflektiert wurden. *Britta Schinzel* hat diesen Schwerpunkt zusammengestellt und leitet ihn in ihrem Schwerpunkteditorial auf Seite 40 ein.

Vom 6. bis 8. November 2015 fand in Erlangen die diesjährige FIfF-Konferenz statt. *Kommerzialisierung des Sozialen – Markt und Macht im Zeitalter digitaler Kompletterfassung* war das Motto der Konferenz, über die in dieser Ausgabe kurz berichtet wird. Einer der Höhepunkte war auch in diesem Jahr die Verleihung des *FIfF-Studienpreises*, dessen Laudationes in dieser Ausgabe enthalten sind. Wir gratulieren dem Preisträger *Christian Kühne* und den Preisträgerinnen *Laura Fichtner* und *Angela Meindl* zu ihren Auszeichnungen. Für die nächste Ausgabe sind ausführliche Beiträge der Preisträger.innen und der Vortragenden der Konferenz geplant.

Bei der Mitgliederversammlung im Rahmen der Konferenz wurde auch ein neuer FIfF-Vorstand gewählt – ich freue mich, *Anne Schnerrer*, *Michael Ahlmann* und *Benjamin Kees* als neue Vorstandsmitglieder willkommen zu heißen.

Ergänzt werden die Schwerpunkte durch mehrere Beiträge im aktuellen Teil: *Silke Holtmanns* und *Ian Oliver* stellen in ihrem Beitrag *Sicherheit und Privacy innerhalb des Mobilfunknetzwerks* die praktischen Schwierigkeiten und Herausforderungen dar, die bei der Umsetzung von vielen verschiedenen Anforderungen, Richtlinien und Grundsätzen für die Handhabung persönlicher Daten im Mobilfunknetz entstehen. *Max Maaß* setzt sich mit *Fairen Algorithmen* auseinander: „*In der öffentlichen Diskussion werden Algorithmen oft als objektiv oder gar unfehlbar dargestellt. Ein Algorithmus habe schließlich keine versteckten Vorurteile, er behandle alle gleich, und sei damit per definitionem objektiv. … In diesem Artikel soll die Frage untersucht werden, ob Algorithmen tatsächlich objektiv sind, und welche Probleme sich ergeben können, wenn Algorithmen die Arbeit von Menschen übernehmen.*"

Menschen, die aus unterschiedlichen Gründen ihre Heimat verlassen müssen und bei uns Schutz suchen, beherrschen seit Monaten die politische Debatte und die Schlagzeilen. Die öffentliche Diskussion, die sich insbesondere nach den Ereignissen von Köln gegen Flüchtlinge richtet, ist besorgniserregend. Für das FIfF ist klar: diese Menschen sind bei uns willkommen. Die Organisation der Unterbringung und Betreuung Geflüchteter wird auch technisch unterstützt – damit setzen sich zwei Beiträge im aktuellen Teil auseinander. Die Notwendigkeit eines angemessenen *Datenschutzes* betont *Dagmar Boedicker* in ihrem Beitrag – dies ist angesichts der Gefährdung politisch Verfolgter besonders wichtig. Leider ist das Bewusstsein dafür in einigen Bereichen erst noch zu schaffen. Das mag bei der Vielzahl der Aufgaben verständlich sein – dennoch ist ein angemessener Schutz der Daten unverzichtbar.

Auf die Bedeutung des *Internet für Flüchtlinge* weisen *Fritjof Bornebusch*, *Helmar Hutschenreuter*, *Daniel Koch* und *Aaron Lye* hin und sie berichten von Initiativen, ihnen Zugang zu verschaffen. Ihr Bericht über die praktischen Erfahrungen beim Aufbau eines WLAN in einer Flüchtlingsunterkunft zeigt die Schwierigkeiten auf, die sich dabei ergeben. „*Für die Zukunft wünschen wir uns, dass in mehr Unterkünften ein WLAN bereitgestellt wird*", so die Autoren, denn: „*für viele Flüchtlinge ist dies die einzige Möglichkeit, den Kontakt zu zurückgelassenen Familienmitgliedern und der Heimat aufrechtzuerhalten.*"

Ergänzt werden die aktuellen Beiträge durch unsere Berichte und Kolumnen. *Dietrich Meyer-Ebrecht*, *Ingo Ruhmann* und *Thomas Reinhold* berichten vom Internationalen *Pugwash-Workshop* am 23. und 24. Oktober 2015 in Berlin: *Cyberwar & Cyberpeace: Sind neue Regeln im Cyberspace möglich?* Sie betonen die Wichtigkeit, dass das Thema *Cyberwar* zunehmend von wissenschaftlichen Veranstaltungen aufgegriffen wird und bedauern gleichzeitig eine zögerliche Haltung der Informatik – hier speziell im Fachgebiet *Cybersecurity* –, sich mit diesem „heißen" Themenkomplex zu befassen.

Ein Team von neun Autorinnen und Autoren haben ein *Digitales Manifest* veröffentlicht, in dem sie ihre Sorge um eine neue Bedrohung der Demokratie artikulieren. *Dietrich Meyer-Ebrecht* kommentiert das Manifest und fragt nach den Konsequenzen für die inhaltliche Arbeit des FIfF.

Die Reden von *Sylvia Johnigk* (in München) und *Dietrich Meyer-Ebrecht* (in Köln) auf der Deutschland-Tour 2015 der *Freiheit-statt-Angst*-Demonstrationen sind ebenfalls in diesem Heft enthalten. Weitere Kurzberichte und Rezensionen ergänzen die Ausgabe.

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

Stefan Hügel
für die Redaktion

Terror – und unser Umgang damit

#VDS lehne ich entschieden ab – verstößt gg Recht auf Privatheit u Datenschutz. Kein deutsches Gesetz u keine EU-RL! […]
Bundesjustizminister Heiko Maas (@HeikoMaas) auf Twitter, 15. Dezember 2014

Liebe Leserinnen und Leser, liebe Mitglieder des FIfF,

was am 13. November 2015 in Paris geschehen ist, ist furchtbar. Erneut sind dem internationalen Terrorismus viele Menschen zum Opfer gefallen. Wir trauern mit den Angehörigen und Freunden der Opfer.

Terror (lat. *terror* – „Schrecken") wird in Wikipedia definiert als die systematische und oftmals willkürlich erscheinende Verbreitung von Angst und Schrecken durch ausgeübte oder angedrohte Gewalt, um Menschen gefügig zu machen. Dass es sich bei den Anschlägen von Paris um Terror handelt, bestreitet niemand ernsthaft. Täter.innen und ihre Unterstützer.innen müssen verfolgt und zur Rechenschaft gezogen werden. Doch die Wirkung des Terrors wird auch unbeabsichtigt gefördert – beispielsweise durch die stakkatoartigen Medienberichte und -kommentare nach den Pariser Anschlägen, die tagelang den Menschen eine Terrorangst einredeten. Fast schon zynisch ist es, wenn dieselben Medien nach den tagelangen Berichten scheinheilig die Frage nach den Ursachen der selbst geförderten Terrorangst stellen. *„Kann es sein, dass überhaupt erst diese Hysterie, unsere überdrehte Berichterstattung, dem Terror einen Sinn gibt?"*, fragte der Kabarettist Dieter Nuhr in seinem Jahresrückblick 2015.

Dazu kommen Terroralarme der Geheimdienst- und Polizeibehörden. An Silvester wurde in München ein Großalarm ausgerufen, im November in Hannover gar ein Fußball-Länderspiel abgesagt, offenbar auf Grund von Hinweisen auf terroristische Anschläge. Welche Hinweise das sind, erfährt die Öffentlichkeit nicht oder nur bruchstückhaft; ihre Stichhaltigkeit kann sie kaum beurteilen. Die Behörden tragen hier eine große Verantwortung – dafür, Anschläge zu verhindern, aber auch dafür, besonnen zu reagieren und Panikreaktionen zu vermeiden. Dazu benötigen sie das Vertrauen der Bevölkerung: ein Vertrauen, das durch die Geheimdienstskandale, die in der jüngeren Vergangenheit bekannt wurden – Stichworte NSA-/BND-Skandal und NSU-Affäre –, schweren Schaden erlitten hat.

Weder in Hannover noch in München ist nach dem Terroralarm etwas passiert – zum Glück! War es also ein Fehlalarm oder haben die Sicherheitsmaßnahmen gegriffen? Egal – es werden sofort neue Befugnisse für Sicherheitsbehörden gefordert. Jedes Ereignis ist recht, um neuen freiheitseinschränkenden Befugnissen – und damit dem Rechtsstaatabbau – den Boden zu bereiten. Vertrauensbildung sieht anders aus.

Aber wie reagiert man angemessen auf einen Anschlag wie in Paris? Als Anders Breivik in Norwegen seine Anschläge verübte, reagierte die damalige norwegische Regierung unter Ministerpräsident Jens Stoltenberg besonnen. Der französische Präsident François Hollande dagegen spricht von Krieg und reagiert mit militärischer Gewalt. Leider haben sich Bundesregierung und Bundestag ebenfalls dafür entschieden, durch ihren Kriegseinsatz in Syrien diese Gewaltspirale weiterzudrehen. Es spricht einiges dafür, dass erst das militärische Engagement der westlichen Staaten den jihadistischen Terror auf das heutige Maß ausgeweitet hat. Dieser Terror trifft meist die Menschen in den arabischen Staaten selbst – die dort stattfindenden Anschläge mit ihren Opfern erreichen freilich nur selten die Schlagzeilen unserer Tageszeitungen.

Warum werden diese Anschläge verübt? Zweifellos ist der „Islamische Staat" eine Terrororganisation, die unter dem Deckmantel des Islams für schreckliche Anschläge verantwortlich ist. Doch was ist die Ursache für das Entstehen solcher Organisationen? „Sie hassen uns für unseren freiheitlichen Lebensstil", so heißt es häufig. Doch damit macht man es sich sehr einfach. Vielleicht hassen sie uns ja auch dafür, dass wir ihre Städte bombardieren und durch Drohnenangriffe ihre Menschen töten – auch hier fallen den Angriffen Kinder, Frauen und Männer zum Opfer, ob jung oder alt, ob schuldig oder unschuldig. Sind wir bei anderer Gelegenheit nicht stolz auf unseren Rechtsstaat, der jedem Menschen ein faires Verfahren garantieren soll?

Auch sonst nähren die Maßnahmen gegen den Terror Sorgen um den Fortbestand des Rechtsstaates, nicht nur in Frankreich. Ein monatelanger Ausnahmezustand wurde dort ausgerufen, der den Behörden weitgehende Befugnisse verleiht; dieser Ausnahmezustand soll nun verlängert und in der französischen Verfassung verankert werden. Gleichzeitig beschneidet die neu gewählte polnische Regierung die Rechte des Verfassungsgerichts und der Medien. In Deutschland wurde erneut die Vorratsdatenspeicherung beschlossen, nachdem das Bundesverfassungsgericht die vorherige Umsetzung für verfassungswidrig und der Europäische Gerichtshof die entsprechende EU-Richtlinie für unvereinbar mit der europäischen Charta der Menschenrechte befunden hatten. Die nun neu beschlossene Vorratsdatenspeicherung sei grundrechtskonform, so wird uns versichert. Doch die Praxis, das Grundgesetz so zu überdehnen, dass sich Maßnahmen der inneren „Sicherheit" stets am gerade noch verfassungsrechtlich erlaubten orientieren, gefährdet den Rechtsstaat. Und der Versuch, die Bevölkerung durch verschleiernde Begriffe wie „Höchstspeicherfrist" und den ständig wiederholten Hinweis, es würden ja keine Inhalte gespeichert, zu täuschen, beschädigt das Vertrauen in die Sicherheitspolitiker zusätzlich. „We kill people based on Metadata" – diese Aussage von Michael V. Hayden, dem ehemaligen Direktor von CIA und NSA, lässt dazu keine Zweifel mehr offen.

Auch dieses Mal wird es Verfassungsbeschwerden gegen die Vorratsdatenspeicherung geben – wir können nur hoffen, dass sie erfolgreich sind.

Das gilt um so mehr, als alle neuen Überwachungsmaßnahmen im Kontext des Geheimdienstskandals gesehen werden müssen, der, nachdem er durch die Enthüllungen von Edward Snowden bekannt wurde, weiter andauert, und sich mit jeder Ausweitung der Überwachung vergrößert. Mit bemerkenswerter Chuzpe werden die Rechte von Geheimdiensten ausgeweitet, als ob es die Skandale und Debatten der letzten Jahre nicht gegeben hätte. Zur Erinnerung:

- Die Telekommunikation und der Internetverkehr werden weltweit umfassend überwacht, und die Überwachungskapazitäten und -aktivitäten werden weiter ausgebaut – das wissen wir durch die Enthüllungen von Edward Snowden.

- Die Daten werden dafür genutzt, Menschen ohne Gerichtsurteil durch Drohnenangriffe zu töten – dabei wird in Kauf genommen, dass Unschuldige den Angriffen zum Opfer fallen. Erste Hinweise deuten darauf hin, dass dies sogar bewusst geschieht. Eine entscheidende Rolle dafür spielt der US-Stützpunkt in Ramstein – das wissen wir vom Whistleblower und ehemaligen Drohnenpiloten Brandon Bryant.

- Rechtsstaatliche Mechanismen werden reduziert oder außer Kraft gesetzt, siehe als Beispiele die aktuellen Entwicklungen in Frankreich und Polen – nebenbei: die Einschränkung der Befugnisse des Bundesverfassungsgerichts wurde in Deutschland von konservativer Seite ebenfalls bereits gefordert.

- Gleichzeitig werden Befugnisse und Ausstattung der Geheimdienste und Sicherheitsbehörden weiter gestärkt – die Vorratsdatenspeicherung ist nur ein Beispiel dafür.

Wir müssen wohl davon ausgehen, dass auch die durch die Vorratsdatenspeicherung gesammelten Daten – entgegen vorheriger Beteuerungen – schnell den Weg zu den Geheimdiensten finden. Einen ersten Schritt in diese Richtung hat die bayerische Landesregierung bereits gemacht, entsprechende Beschlüsse gibt es auch bei der CDU. Das Bundesverfassungsgericht urteilte in seinem Urteil gegen die Vorratsdatenspeicherung 2010, dass die „Überwachungsgesamtrechnung", die gesamtheitliche Betrachtung aller staatlichen Überwachungsmaßnahmen, im Blick behalten werden muss. Legen wir dieses Prinzip zugrunde, ist das akzeptable Maß auch ohne die Vorratsdatenspeicherung bereits weit überschritten. Gleichzeitig ist ihr Nutzen fraglich, das haben Studien gezeigt. Gegen die Pariser Anschläge hat die in Frankreich längst in Kraft gesetzte Vorratsdatenspeicherung nicht geholfen. Dennoch wird sie seit Jahren von Innen- und Sicherheitspolitikern gebetsmühlenartig gefordert. Nicht zuletzt der Sinneswandel von Bundesjustizminister Maas hat dazu beigetragen, dass die Befürworter.innen einen Etappensieg errungen haben.

Weniger öffentliche Aufmerksamkeit erfährt eine Form des Terrors in Deutschland, der nicht die Deutschen trifft, sondern die Menschen, die bei uns Schutz suchen. Unterkünfte für Geflüchtete werden von „besorgten Bürger.innen" angezündet – 2015 gab es mehr als 800 Fälle, zumeist mit rechtsradikalem Hintergrund.

Es geht gerade um nicht weniger als unsere freiheitliche Gesellschaft. Sie ist bedroht durch Terrorismus, aber sie ist auch bedroht durch eine Sicherheitsdoktrin, die Überwachung und Rechtsstaatabbau im Inneren und militärische Gewalt nach außen zum Mittel der Wahl erklärt. Noch ist es möglich, dass die Verantwortlichen besonnen auf Bedrohungen reagieren und rechtsstaatliche Prinzipien (wieder) in den Vordergrund rücken – sie sollten diese Möglichkeit nutzen. Und: Wenn wir vom Terrorismus reden, dürfen wir vom alltäglichen Rassismus und Rechtsradikalismus nicht schweigen. Unser freiheitlicher Rechtsstaat und damit die Zukunft unserer Gesellschaft hängt davon ab.

Mit FIfFigen Grüßen

Stefan Hügel

Thomas Reinhold

Wie werden Kriege gemacht

Veranstaltung mit den beiden ehemaligen CIA-Analysten Ray McGovern und Elisabeth Murray, am 14. September 2015 an der Universität Hamburg im Rahmen der Kampagne *Cyberpeace*

Am 14. September 2015 waren die beiden ehemaligen CIA-Analysten Ray McGovern und Elisabeth Murray im Rahmen ihrer Deutschland-Rundreise auf Einladung des FIfF e.V. an der Universität Hamburg zu Gast. Die Veranstaltung, die mit Unterstützung des Instituts für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH) umgesetzt werden konnte, war mit etwa 80 Personen gut besucht. Leider waren außer Mitgliedern der Piratenpartei keine Vertreter anderer Parteien anwesend, was angesicht der Brisanz der Informationen wünschenswert gewesen wäre.

Die beiden Referenten, die unter anderem als Quell-Analysten für den Nahen Osten und zeitweise für die täglichen nachrichtendienstlichen Berichte an den US-Präsidenten zuständig waren, haben über ihre Erfahrungen im Rahmen ihrer jahrzehntelangen Arbeit bei der CIA berichtet. Dabei ging es zum einen darum, wie aus einer Organisation, die ursprünglich als reine *Intelligence*-Institution aufgebaut wurde, der weltweite Geheimdienst werden konnte, der – oft fernab jeglicher Kontrolle oder Transparenz – Exekutivbefugnisse für sich beansprucht und sich dabei das eine und andere mal in außenpolitische Konflikte verstrickt hat. Dabei haben die beiden Referenten unter anderem anhand der Enthüllungen von Edward Snowden aufgezeigt, in welchem Umfang die USA und Großbritannien gezielt Informationen und Erkenntnisse aus öffentlichen und geheimen Quel-

len einsetzen, um ihre Außenpolitik zu gestalten. Elisabeth Murray, zu deren Aufgabenbereich die Analyse arabischer Quellen gehörte, konnte dabei unter anderen an den Beispielen des ersten Irak-Krieges (1990/91) erläutern, wie sich die Informationspolitik der US-Regierung oft den außenpolitischen Zielen beugen muss. Wenn notwendig, wurden und werden dabei gelegentlich auch die medial vermittelten Realitäten angepasst und „Fakten" geschaffen. So konnte sie berichten, wie angesichts der seinerzeit als Interventionsgrund genannten fahrenden Biowaffenlabore, für deren Existenz keine verlässlichen Quellen gefunden wurden, immer wieder durch Vorgesetzte nach Beweisen gefragt wurden – mit dem Verweis dass es „da doch irgendwas geben muss". Anhand ähnlicher Beispiele konnte auch Ray McGovern zeigen, wie in der Vergangenheit immer wieder Kriege und kriegsähnliche Situationen „gemacht" wurden. Über solche Situationen konnten die beiden anhand der vergangenen und gegenwärtigen Verhandlungen über das iranische Nuklearprogramm und die Rolle der israelischen Regierung berichten sowie die aktuellen Konflikte in der Ukraine beleuchten.

Beide Referenten, die zu den ersten US-Amerikanern gehörten die Edward Snowden in seinem Moskauer Asyl besucht haben, haben darüber berichtet, wie die Informationsbeschaffung von der US-Regierung als zentraler Bestandteil ihrer außenpolitischen und innenpolitischen Tätigkeit angesehen wird. Dabei wurde die Rolle der NSA mit ihrer „alles was technisch möglich ist, wird auch umgesetzt"-Attitüde in diesem Kontext beleuchtet. In den Betrachtungen ging es auch um die Frage, ob der Cyberspace als weitere Domäne des staatlichen und insbesondere des militärischen Handelns ein *game changer* sein wird, der aufgrund seiner relativ unaufwendigen Teilhabe die internationalen Kräfteverhältnisse zwischen Staaten verändern kann. Die Referenten waren sich dabei einig, dass es angesichts der weltweiten Abhängigkeit von IT-Infrastrukturen und Diensten dringend geboten ist, für diese neue Domäne verbindliche Abkommen zu entwickeln, mit deren Hilfe die militärische Aufrüstung eingedämmt und die zukunftige friedliche Entwicklung sichergestellt werden kann.

Mit Blick das zivilgesellschaftliche Engagement haben sowohl Ray McGovern als auch Elisabeth Murray auf die Initiativen der vergangenen Jahrzehnte verwiesen, die sich in mühevoller Arbeit gegen atomare Aufrüstung, Atomtests oder die Stationierung von Raketen eingesetzt haben und das Auditorium ermuntert, den Kampf gegen neuerliche militärische Rüstungs- und Aggressionsspiralen im Bereich des Cyberspace fortzusetzen. Die Veranstaltung war mit etwa 80 Personen, darunter Professoren, Studenten, Aktivisten netzpolitischer Vereine und Pressevertreter gut besucht. Es wurde rege debattiert und im Anschluss an den offiziellen Teil noch ausgiebig in Einzelgesprächen mit den Referenten diskutiert. Im Anschluss fand auch ein Interview mit der Online-Zeitung *Schattenblick* statt. Die beiden Referenten waren eine große Inspiration und ein Beispiel, wie sich moralische Integrität und ethisches Bewusstsein in der täglichen Arbeiten darstellen kann.

Da die Veranstaltung, die auch an weiteren Orten in Deutschland durchgeführt wurde, im Netz als Video verfügbar ist, sei sie jeder und jedem dringend ans Herz gelegt.

Siehe auch Artikel auf der Webseite: *http://cyberpeace.fiff.de/Kampagne/VeranstaltungCIAnalystenBericht*

Dietrich Meyer-Ebrecht

Das *Digital Manifest*

Neun Wissenschaftler.innen artikulieren ihre Sorge um eine Aushöhlung der Demokratie – ein Kommentar

Nudging – engl. *to nudge so.*: jmdn. anstupsen, jmdn. sanft anstoßen. Ein harmlos klingendes Wort. In unserer digitalen Gesellschaft allerdings benennt es ein Phänomen von weitreichender gesellschaftlicher Bedeutung. Die Myriaden digitaler Spuren, die wir – *always online* – hinterlassen, Informationen über uns, die wir wissentlich, leichtfertig und sehr oft auch unwissentlich preisgeben, werden bereits heute weidlich für ein personalisiertes Feedback ausgenutzt. Wir erhalten Suchergebnisse, Nachrichtenextrakte, Kaufempfehlungen, Reiseangebote, Wegbeschreibungen, medizinische Ratschläge, Verhaltenstipps, die so subtil auf unsere persönliche Situation abgestimmt sind, so plausibel zu unserer persönlichen Lebenswelt passen, dass wir die Entscheidungen, zu denen sie uns unterschwellig lenken, für unsere eigenen halten.

Es wird weiter daran gearbeitet werden, immer mehr Daten über unsere Lebensweise, unsere Umgebung, unsere Vorlieben und Ansichten zu sammeln und diese zu immer schärferen Profilen zu verdichten. Mit *persuasive computing* werden Techniken entstehen, mit denen nicht nur unsere Ansichten und Entscheidungen manipuliert werden können, sondern sogar unser Verhalten. Unmerklich wird unsere Selbstbestimmtheit in Frage gestellt werden. Wirtschaftliche und politische Interessen, die hinter dieser modernen Form eines Paternalismus stehen, werden verschmelzen – ein Prozess, der unvermeidlich zu einer Aushöhlung der Demokratie führen wird. Diese Sorge treibt eine Gruppe von neun renommierten Wissenschaftler.innen um: Dirk Helbing, Bruno S. Frey, Gerd Gigerenzer, Ernst Hafen, Michael

Hagner, Yvonne Hofstetter, Jeroen van den Hoven, Roberto V. Zicari und Andrej Zwitter fordern in ihrem *Digital Manifest* eine digitale Demokratie statt einer Datendiktatur. Sie prognostizieren darin, dass eine auf Big-Data-Technologien und Nudging-Techniken gestützte Verhaltenssteuerung zu einer „Automatisierung der Gesellschaft durch Algorithmen und künstliche Intelligenz" führen wird. Das *Digital Manifest* ist ihr gemeinsamer Appell, unsere digitale Gesellschaft vor dem Abgleiten in eine autoritäre Gesellschaft zu bewahren. Sie machen ein wirksames Gegensteuern zur Prämisse für die Sicherung von Freiheit und Demokratie.

Das *Digital Manifest* setzt sich auseinander mit der derzeitigen technischen Entwicklung, in der digitale Steuerungs- und Regelungsverfahren unaufhaltsam in die Geräte und Systeme unseres Alltags vordringen und sie zu Metasystemen von zunehmender Komplexität vernetzen – ‚smart homes', ‚smart factories', ‚smart cities' ... – und zum potenzierten Sammeln von Daten einladen. Sie werfen einen Blick auf die Entwicklung in China und den ‚citizen score'. Mit behördlichen oder privatwirtschaftlichen Profildatenbanken wie etwa unserem Schufa-Punktkonto oder dem britischen *Karma Police Programme* seien wir jedoch nicht mehr zu weit entfernt von dieser Zukunft. Von dort wird es nur ein kleiner Schritt sein, mit dem aggregierten Wissen unser Verhalten zu beeinflussen, uns zu manipulieren – *big nudging*. Das ist für die Politik in gleicher Weise verlockend wie für die Wirtschaft – der Wirtschaft dient es für die Maximierung der Gewinne, die Politik kann ‚durchregieren', ohne die Bürger mehr als nur scheinbar in demokratische Verfahren eizubeziehen. Die Frage ist, welche ungewollten negativen Effekte löst eine solche ‚Optimierung' unseres gesellschaftlichen Systems aus? Wie ein Ökosystem, in dem etwa die Bekämpfung eines Schädlings neue, schwieriger zu beherrschende Schädlinge hervorbringt, wird auch unser hochkomplexes sozio-psychisches System unvorhersehbar reagieren.

Die Autor.innen beschäftigen sich mit der Geschichte des digitalen Wachstums. Über viele Jahre haben wir geglaubt, dass einfach die Datenmenge nicht dazu ausreicht, damit Entscheidungsalgorithmen nicht-technische Entscheidungen sinnvoll fällen könnten. Das gleichzeitige Wachsen der verfügbaren Datenmengen und der Rechnerleistung hat jedoch einen multiplikativen Effekt auf die systemische Komplexität: *Big-Data* erlaubt evidenzbasierte Entscheidungen. Rechtliche und ethische Fragen stellen sich: Dürfen wir ungefragt zu *guinea pigs* für Nudging-Experimente gemacht werden? Und das in einem gesamtgesellschaftlichen Maßstab? Wer trägt die Verantwortung für Schäden, die unser gesellschaftliches System nimmt? Wer definiert überhaupt, was ein Schaden ist, was von Nutzen ist? Woher nehmen wir die Sicherheit, dass der Prozess einer ‚gesellschaftlichen Automatisierung', der derzeit unaufhaltsam fortzuschreiten scheint, nicht in Sackgassen läuft, aus denen wir nur schwer oder gar nicht herausfinden? Die Evolutionsgeschichte führt uns vor, wie die Optimierung einer Spezies zu ihrem Aussterben führt, wenn sie sich an Veränderungen ihrer Umgebung nicht schnell genug anpassen kann.

Wir stehen an einem Scheideweg, konstatieren die Autor.innen des *Digital Manifests*. Wollen wir uns nicht in eine ‚Datendiktatur' fallen lassen, in ein zunehmend autoritäres, ja totalitäres System, müssen wir beginnen gegenzusteuern. Noch ist es nicht zu spät, die Richtung der sozio-technischen Entwicklung so zu korrigieren, dass alle gleichermaßen von der digitalen Revolution profitieren – Wirtschaft, Staat und Bürger. Mit einer 10-Punkte-Agenda, die sie am Ende aufstellen, möchten sie den Weg weisen.

Das *Digital Manifest* macht auf eine kritische Entwicklung unserer digitalen Gesellschaft aufmerksam. Viele Fakten werden zusammengestellt und Folgerungen entwickelt. Ein Kasten, der detailliert über die diesbezügliche Entwicklung in China informiert, eine Zusammenstellung weiterführender Schriften und eine Liste von Literaturzitaten ergänzen die Schrift. In seiner gedanklichen Fülle allerdings erscheint mir der Text beim ersten Lesen heterogen und zu wenig stringent, um auch Leser.innen zu erreichen, die bisher noch nicht für darin aufgeworfenen Fragestellungen sensibilisiert sind. Und er ist mir zu wenig pointiert und nicht bissig genug. Dennoch ist das *Digital Manifest* ein wertvoller und wichtiger Beitrag von berufener Seite, um den Diskurs in die Öffentlichkeit zu tragen – und in die Politik!

Gestattet sei mir die Nachfrage, warum nicht längst auch das FIfF im Diskurs dieser Thematik präsent ist. Sind wir zu sehr unserer technischen Welt verhaftet? Mit dem „... und gesellschaftliche Verantwortung" in unserem Namen bekennen wir uns dazu, uns mit den Wechselwirkungen zwischen Informatik/Informationstechnik und Gesellschaft verantwortlich auseinandersetzen zu wollen. Das hieße wohl auch, dass wir uns mit den komplexen soziologischen und psychologischen Facetten dieser Wechselwirkungen befassen müssen. Das in dem *Manifest* angestoßene Thema erfordert ein solches disziplinübergreifendes Herangehen. Und es betrifft ein Feld, in dem eine umwälzende Entwicklung schon eine ziemliche Geschwindigkeit aufgenommen hat. Es wird Zeit, dass sich das FIfF auch auf diesem Feld bemerkbar macht.

Dirk Helbing, Bruno S. Frey, Gerd Gigerenzer, Ernst Hafen, Michael Hagner, Yvonne Hofstetter, Jeroen van den Hoven, Roberto V. Zicari und Andrej Zwitter: Digitale Demokratie statt Datendiktatur. Spektrum der Wissenschaft, Januar 2016; spektrum.de/news/wie-algorithmen-und-big-data-unsere-zukunft-bestimmen/1375933

Silke Holtmanns und Ian Oliver

Sicherheit und Privacy innerhalb des Mobilfunknetzwerks

Wie schützt man Nutzer im Mobilfunknetz?

Ziel dieses Artikels ist es, auf verständliche Weise die praktischen Schwierigkeiten und Herausforderungen darzustellen, die bei der Umsetzung von vielen verschiedenen Anforderungen, Richtlinien und Grundsätzen für die Handhabung persönlicher Daten im Mobilfunknetz entstehen.

Stellen Sie sich vor, Sie sind ein Programmierer und sollen ein Programm für einen Mobilfunk-Netzwerkknoten entwickeln, welches das Netz selbst und seine Benutzer vor Angriffen schützt. Durch Ihren Knoten gehen u. a. Informationen und Kommandos, die für Benutzermobilität gebraucht werden, zum Beispiel Logs für Handover zwischen Funkzellen, Anrufaufbau, Daten, Änderung von Benutzerprofilen etc. Sie haben sich eine Liste der ganzen Daten angelegt, die durch Ihren Knoten gehen oder dort gespeichert werden. Was machen Sie jetzt? Sie wollen Nutzer schützen und dafür sorgen, dass das Netz verfügbar bleibt, aber Sie haben keine genaue technische Beschreibung und wenden sich deshalb in Ihrer Ratlosigkeit an verschiedene interne Stellen.

Sie gehen erst einmal in die Kaffeeecke und denken darüber nach, was Sicherheit für das Netz, die Benutzer und Privacy eigentlich bedeutet. Ihre erste Idee ist, dass die Benutzer nicht abgehört werden möchten, und dass der ganze Service funktionieren sollte. Der Kollege am Nachbartisch von der *Radio Network Konfiguration* sagt, dass die Luftschnittstelle recht gut verschlüsselt ist mit A5/3, zumindest in den neueren Knoten, und dass die alten Knoten eh Auslaufmodelle bei den fortschrittlichen Netzwerkbetreibern seien. Er erklärt auch, wie schwierig die ordentliche Konfiguration des Netzes sei, um zu vermeiden, dass Gespräche und *Data Sessions* abbrechen, der Benutzer keine Verbindung mehr hat, dem Telefon die Batterie leer gesaugt wird oder manche Telefone nicht mehr funktionieren. Um das zu konfigurieren, schauen sich er und seine Kollegen die Logs, Fehlernachrichten und die ganzen Metadaten genauer an, um dann entsprechend die Fehler zu entdecken und zu beseitigen. Er rät Ihnen, alle Metadaten zu speichern, zumindest für eine Weile.

Sie gehen zurück zu Ihrem Arbeitsplatz und schauen in den Security Newsticker, wo Sie sehen, dass eine große Webseite gehackt worden ist und Tausende von Kundendaten nun im Internet liegen. Da ein Telefonnetzwerk ja eigentlich auch nur ein Netzwerk mit vielen Kundendaten ist, entschließen Sie sich mit der IT-Sicherheitsabteilung zu reden, die sollten doch wissen, wie man Benutzer schützt. Die IT-Abteilung ist gerade dabei, eine *Denial-of-Service*-Attacke von einem Botnet abzublocken, welche schon einen Hauptknoten überlastet hat und gerade dabei ist, auch die Backup-Knoten anzugreifen, und wenn der runtergeht, wäre das Netz vollständig lahmgelegt. Sie kriegen nur brüsk an den Kopf geworfen, dass Benutzer erwarten, dass der Netzwerkbetreiber sich um die Sicherheit kümmert, anstatt selbst was dafür zu tun. Dafür würde man alle Daten brauchen, die man kriegen kann. Sie schleichen leise aus dem Raum. In dem Moment ruft Ihr Vater an, er hätte da so eine merkwürdige Meldung beim Browsen gekriegt und wisse nicht, was er machen soll. Sie hatten schon im Newsticker gelesen, dass das neuste Security Update mit dem falschen Schlüssel unterschrieben war und der Browser eine Zertifikatswarnung rauswirft. Sie beruhigen also Ihren Vater und sagen, dass es in dem Fall in Ordnung ist und er *Erlauben* klicken kann.

Sie gehen zurück zu Ihrem Büro und grübeln. Auch wenn Sie die IT-Kollegen verstehen, scheint Ihnen das alles doch etwas viel der Datensammlung. Andererseits, dem Benutzer das Sicherheitsmanagement aufzubürden, nein, das scheint auch nicht richtig zu sein und funktioniert sicherlich auch nicht. Da es um Privacy und persönliche Daten geht, wenden Sie sich nun an die Abteilung *Ethics & Compliance*. Die schickt Ihnen eine 10 Seiten lange *Privacy Guidance* von ihrer Webseite, welche generisch und allumfassend beschreibt, wie gut und verantwortlich Ihr Arbeitgeber mit den Daten seiner Kunden umgeht, und dass er der *EU Privacy Regulation* streng folgt. Die Idee und der Tenor des Dokumentes sind gut, aber was sollen Sie jetzt mit den Log-Files und den Metadaten in Ihrem Knoten machen? Sollen Sie sie einfach löschen? Die Abteilung *Ethics & Compliance* setzt auch den Kollegen von *Legal Compliance* ins *cc*-Feld. Der meldet sich bei Ihnen und erklärt, dass wenn eine richterliche Anordnung vorliegt, ein Netzwerkbetreiber verpflichtet ist, die Kommunikationsdaten eines Kunden als Kopie an die entsprechende Behörde über eine spezifizierte Schnittstelle weiterzureichen. Diese Kommunikation muss natürlich lesbar sein für die Behörde, zumindest darf der Netzwerkbetreiber nicht die Kommunikation eines potenziellen Kriminellen oder Terroristen verstecken[1]. Diese gesetzliche Anforderung muss vom Netzwerkbetreiber erfüllt werden, sonst darf das Netz nicht betrieben werden. Da Sie an die Rechtstaatlichkeit Ihrer Regierung glauben und auch ganz gerne einen Job haben, haben Sie soweit kein Problem mit der Idee, dass nach einem richterlichen Beschluss Nutzerdaten an die Behörden gegeben werden.

Aber da war doch letztens noch was in den Nachrichten über NSA, Merkel und Benutzerortung. Sie werden neugierig und lesen nach, was da eigentlich los war. Mobilfunkbetreiber haben vor ungefähr 30 Jahren angefangen, die Netzwerke zu verbinden, um Benutzern *Roaming* zu ermöglichen. Damals waren es wohl nur eine Handvoll staatlicher Netzwerkbetreiber, welche sich gut kannten und vertrauten. Mittlerweile gehören Hunderte Netzwerkbetreiber zu dem Roaming-Netzwerk und obendrein diverse Service Provider. Da die EU den globalen Wettbewerb fördert und Netzwerkbetreiber ihre Zugänge auch vermieten, ist die Zahl sicher noch steigend. Diese Netze sind entweder direkt per Kabel miteinander verbunden, wenn es viele Benutzer gibt, die ständig zwischen zwei Netzen *roamen*, oder über *Roaming Hubs* für Netzwerk-Kombinationen, die etwas seltener sind. Roaming funktioniert weltweit, egal ob Deutschland, Malediven, Bangladesch, Russland oder China. Das Roaming läuft über ein Netzwerk, welches hauptsächlich die Protokoll-Suite SS7/

SIGTRAN verwendet, die aber keine Absenderauthentifizierung hat, da man sich vor 30 Jahren ja gut kannte und vertraut hat. Sie werden hellhörig und graben weiter. Die NSA hat zum Beispiel diese fehlende Authentifizierung benutzt, um Informationen aus den Netzen abzufragen. Und zwar über eben die Verbindung, welche eigentlich für das Roaming gedacht ist. Snowden-Dokumente behaupten, dass die NSA 701 der 985 Mobilfunknetzwerke weltweit mittels *Auroragold* gehackt habe[2]. Der prominenteste Privacy-Hack über das Roaming-Netzwerk ist die Benutzerortung[3], wobei das ursprüngliche Kommando (MAP_ATI) eigentlich für Mobilitätsmanagement netzwerkintern gebraucht wird. Solche Daten-Akquise in Wild-West-Manier verträgt sich nicht mit Ihrem Verständnis von Rechtsstaatlichkeit und Unschuldsvermutung. Sollen Sie die Metadaten einfach alle hashen? Sollen Sie einen Filter für solche externen Roaming-Anfragen entwickeln, um die Benutzer vor diesen Anfragen zu schützen? Sollen Sie Roaming unterbinden und das Interface schließen und alle externen Kommandos einfach blocken?

Sie sind verzweifelt und reden mit Ihrem Chef. Der fragt Sie, wie teuer so ein Filter sein wird, was ist das Return-on-Investment? Bald sind wieder Quartalsergebnisse und Shareholder-Meeting, jede Investition für die Softwareentwicklung wird von den Shareholdern auf ihren Wert hin geprüft. Werden die Benutzer mehr für ihren Mobilfunkvertrag zahlen, wenn wir die Filter installieren? Was ist der *Business Case*? Der Chef weist darauf hin, dass Shareholder-Meetings nicht für ihren Altruismus bekannt sind und Benutzer auch nicht mehr zahlen, bloß weil es sicher ist und die Privatsphäre schützt, die benutzen doch eh' alle Google und Facebook, kriegen Sie zu hören. Als Sie das Schließen des Roaming-Interfaces erwähnen, wird Ihr Chef blass und meint, dann sollten wir uns alle nach einer neuen Arbeit umsehen. Aber der Chef versteht auch Ihr Problem und hat einen guten Hinweis: Sie sollen mal mit der Forschungsabteilung reden, die machen „Privacy, Security und so 'n Gedöns". Sie wenden sich also mit wenig Hoffnung der Forschungsabteilung zu.

Die Forschungsabteilung hat mehrere Experten. Ein Experte erklärt Ihnen, dass das Sicherheitsproblem im Roaming-Netzwerk nicht nur ein Privacy-Problem ist, sondern auch zu großem finanziellen Schaden für den Netzwerkbetreiber führen kann. Über das Roaming-Netzwerk können nicht nur Kommandos für die Benutzerortung geschickt werden, sondern auch Kommandos, welche das Benutzerprofil im Hauptknoten ändern. Das Benutzerprofil enthält wichtige Daten, die festlegen, dass den Kunden ihre Netznutzung korrekt berechnet wird oder welche Premiumservices eine Benutzerin in ihrem Vertrag hat etc. Ändert man dort geschickt einige Felder, dann können Benutzer Services erhalten, ohne dafür zu zahlen, oder *Roaming Fraud* begehen, was zu großen finanziellen Einbußen führen kann. Sie gehen zusammen in die Kaffeeecke und setzen einen Business Case für einen Filter auf dem Roaming-Interface auf. Ein Mitarbeiter aus der Standardisierungsabteilung erwähnt, dass die Vereinigung der Netzwerkbetreiber GSMA an einer Spezifikation für SS7-Filter arbeitet. Sie präsentieren den Business Case Ihrem Manager, der damit zufrieden ist und die Ressourcen genehmigt, um einen Roaming-Filter für die eingehenden Kommandos zu entwickeln. Aber was ist mit den IT-Security-Problemen, polizeilichen Anfragen und den Log-Dateien?

Sie gehen zurück zu Research. Ein anderer Forscher erzählt etwas wirr von *non-Euklidean spaces, weighted distances* und *data distortion*. Sie wollen sich gerade höflich aus der Diskussion entfernen, als er Ihnen die Demo-Implementierung zeigt. Mit dieser Implementierung lassen sich stufenweise Network Traces und Logs anonymisieren. Die Daten werden entsprechend ihres Informationsinhalts mittels verschiedener Methoden anonymisiert, z. B. mit *k-anonymity, l-diversity* etc. Die Anonymisierung ist so angelegt, dass die Daten zwar *verzerrt* werden, aber *Malware* und *Radio Network Bug Tools* immer noch reagieren. Wenn so ein Fall eintritt, dann kann die Anonymisierung für diesen Traffic-Stream schrittweise heruntergefahren werden. Sie schleppen den Forscher zur IT-Abteilung und diese bestätigt, dass sie mit diesem Tool sicher noch die meisten Botnets und Malware finden werden. Die IT-Abteilung hat es geschafft, das Netz am Laufen zu halten und gibt zu, dass sie eigentlich ganz froh ist, nicht die heißen Rohdaten direkt zu haben. Deshalb schickt sie eine Mail an Ihren Manager, dass sie so ein Tool benötigen und wohl bei der Integration mit Ihnen und der Forschungsabteilung zusammenarbeiten würden. Da die Forschungsabteilung die Hauptarbeit der Entwicklung schon erledigt hat, steht Ihr Manager der Integration der stufenweisen Anonymisierungssoftware positiv gegenüber. Danach schauen Sie bei den Radio-Kollegen vorbei, die auch bestätigen, dass sie hauptsächlich bei Auffälligkeiten gewisse Details benötigen. Die Daten, die die Demo rausgibt, würden wahrscheinlich reichen. Nur bei dem *l-diversity* oder *k-anonymity,* da war der Kollege nicht sicher, welches Verfahren wohl besser wäre. Auf die Anfrage bei Ethics, ob sie für das Feld *Protokoll* im Header im Zusammenhang mit der Anonymisierung der Länge der Nachricht lieber *l-diversity* oder *k-anonymity* nehmen, erhalten Sie nur eine *Out-of-Office*-Antwort und beschließen, es einfach im Testnetzwerk mit ein paar alten Datensätzen auszutesten.

Silke Holtmanns und Ian Oliver

Dr. **Silke Holtmanns** arbeitet seit mehr als 15 Jahren im Bereich der Mobile Security und ist zurzeit als *Security Specialist* in der Thematik SS7/*Diameter Roaming Security* bei *Nokia Networks* tätig.

Dr. **Ian Oliver** ist seit 16 Jahren im Mobilfunkbereich tätig. Er ist Autor des Buches *Privacy Engineering* und als *Security Specialist* für *Privacy/Malware Data Analysis* bei *Nokia Networks* beschäftigt.

Nachdem Sie endlich die Ressourcen für Ihre Arbeit erhalten haben, Ihre Arbeit getan ist, die Filter hoffentlich vernünftig funktionieren, Malware erkannt wird, die Radio-Experten das Netzwerk am Laufen halten können und den Gesetzen genüge getan ist, trinken Sie erst mal einen großen Kaffee und grübeln darüber nach, ob die Sicherheit und Privacy der Benutzer jetzt wohl wirklich zu 100 % geschützt sind und ob wohl alles der *Privacy Policy* entspricht? Als Ihr Kaffeebecher leer ist, sieht es so aus, als hätte eine Pille auf dem Grund gelegen, manchmal scheint sie rot, manchmal blau …

Nachtrag

Die Autoren haben diese Geschichte natürlich komplett erfunden. Die Geschichte und die hier repräsentierten Meinungen sind die der Autoren und nicht notwendigerweise die von *Nokia Networks*. Und unser Manager hat ein gutes Sicherheitsverständnis. Wir haben einige technische Details verallgemeinert, um die Leser nicht mit 3-5-Buchstaben-Abkürzungen zu bombardieren. Falls aber Interesse an selbigen besteht, werden wir diese selbstverständlich auf direkte Anfragen genau erläutern. Das Thema Sicherheit der Luftschnittstellen haben wir bewusst nicht genauer erläutert, da es recht heterogen ist. In diesem Bereich gibt es viele Varianten die den Rahmen des vorliegenden Textes sprengen würden und einen eigenen Artikel verdienen.

Anmerkungen

1 *Wenn Benutzer HTTPS Ende-zu-Ende benutzen, ist das keine Maßnahme, die vom Netzwerkbetreiber angewandt wird*

2 *Status 2012, es geht nicht daraus hervor, ob diese Zahlen auch die Virtual Operator enthalten*

3 *Chaos Computer Club, Dez. 2014, Tobias Engel*

Max Maaß

Faire Algorithmen

In der öffentlichen Diskussion werden Algorithmen oft als objektiv oder gar unfehlbar dargestellt. Ein Algorithmus habe schließlich keine versteckten Vorurteile, er behandle alle gleich, und sei damit per definitionem *objektiv. Diese Einschätzung nutzen einige als Argument, um immer mehr Aufgaben von Menschen auf Algorithmen zu übertragen – von der Verkehrsplanung über die Auswahl von Bewerber.innen bis hin zur Strafverfolgung mittels* Predictive Policing.[1] *In diesem Artikel soll die Frage untersucht werden, ob Algorithmen tatsächlich objektiv sind, und welche Probleme sich ergeben können, wenn Algorithmen die Arbeit von Menschen übernehmen.*

Eine Geschichte unfairer Algorithmen

Die Untersuchung von Algorithmen auf Verfälschungen und Befangenheit[2] geht bereits mehr als 30 Jahre zurück. Schon in den 1980ern wurde dem Buchungssystem *Sabre* (betrieben von *American Airlines*) vorgeworfen, bestimmte Flüge bevorzugt anzuzeigen. Tatsächlich stellte sich heraus, dass das System von American Airlines gezielt dazu verwendet wurde, konkurrierende Fluglinien systematisch zu benachteiligen.[3] Dadurch erhielt American Airlines einen Vorteil gegenüber der Konkurrenz, der sich auch in den Bilanzen niederschlug.

In diesem Fall wurde der Algorithmus gezielt so entworfen, dass er bestimmte Ergebnisse bevorzugt. Schwieriger wird es beim anderen Extrem: Ein Algorithmus, der möglichst neutral sein soll, aber *trotzdem* befangen ist. Ein Beispiel dafür war ein Algorithmus, der in den 1970ern von einer englischen *Medical School* entwickelt wurde, um den Bewerbungsprozess um die limitierten Studienplätze zu beschleunigen. Das Programm sollte eine erste Auswahl der Kandidat.innen vornehmen, die für ein Bewerbungsgespräch eingeladen werden sollten. Es wurde über mehrere Jahre weiterentwickelt, bis es eine Übereinstimmung von bis zu 95 % mit den Ergebnissen der (menschlichen) Bewerbungskommission ergab.

Der Algorithmus war über fünf Jahre im Einsatz, bis sich herausstellte, dass er gegen Frauen und ethnische Minderheiten diskriminierte. Dieses Verhalten wurde ihm nicht explizit beigebracht, er hatte es aus den Entscheidungen der Kommission gelernt, die (bewusst oder unbewusst) eine solche Diskriminierung an den Tag gelegt hatte.[4]

Der Stand der Forschung

Diese Beispiele zeigen, dass Algorithmen sowohl gezielt als auch unbeabsichtigt verzerrend wirken können. Während *analoge* Diskriminierung schon seit längerer Zeit wissenschaftlich untersucht wird, ist das Feld der Erforschung digitaler Diskriminierung vergleichsweise wenig erschlossen. Die erste Arbeit zu diesem Thema wurde 1987 von Huff *et al.* geschrieben und weist auf die Gefahr von Gender-Stereotypen in der Softwareentwicklung hin.[5] Diese Arbeit stammt allerdings aus der Psychologie, nicht der Informatik.

Die ersten Informatikerinnen, die sich mit diesem Themenkomplex beschäftigten, waren Batya Friedman und Helen Nissenbaum, die 1996 einen Artikel über die verschiedenen Formen von Verfälschungen in Computersystemen schrieben. Sie identifizierten drei Formen von Verfälschung: *preexisting bias* (Tendenzen, die aus der realen Welt übernommen werden), *technical bias* (Verfälschungen durch technische Limitationen), und *emergent bias* (Verfälschungen, die erst im Verlauf der Zeit entstehen, weil sich die Software nicht an neue Begebenheiten anpasst).[6] Der bereits diskutierte Fall des Bewerbungs-Algorithmus' wäre in diesem Modell ein Fall von *preexisting bias*. Ein Beispiel

für *technical bias* wäre, gleichwertige Ergebnisse alphabetisch zu ordnen, wodurch einige Ergebnisse durch prominentere Positionen in der Ergebnisliste systematisch bevorzugt werden. Ein häufiger Fall von *emergent bias* sind binäre Auswahlfelder für Geschlechter, die keine abweichenden Geschlechtsidentitäten zulassen.

Über die nächsten Jahre beschäftigen sich auch andere Wissenschaftler.innen mit dem Thema. 2005 studiert Phoebe Sengers, wie unterbewusste kulturelle Annahmen das Softwaredesign beeinflussen können.[7] Einige Arbeiten beschäftigten sich mit den Algorithmen von Werbenetzwerken, die teilweise gegen Frauen und ethnische Minderheiten diskriminierten.[8] Im Jahr 2014 schrieb Nicolas Diakopoulos einen Report über *algorithmic accountability reporting,*[9] also das Untersuchen und kritische Hinterfragen von Algorithmen (auch) durch Journalisten. Im selben Jahr schreibt Tal Z. Zarski einen Artikel über *discrimination in the scored society*,[10] in dem er Formen der Diskriminierung in *Scoring*-Verfahren (wie der Berechnung der Kreditwürdigkeit) analysiert.

Algorithmische Kollateralschäden

Der Schaden, den unfaire Algorithmen anrichten, bleibt für Nicht-Betroffene meist unsichtbar. Er trifft häufig die, die bereits benachteiligt sind, etwa durch die Verfestigung von Geschlechter-Stereotypen (wie ein Zugangskontrollsystem, das annimmt, dass alle Menschen mit Doktor-Titel männlich sind[11]).

Auch neue Polizei-Technologien könnten einen solchen Effekt haben: Die Polizei in Chicago setzt maschinelles Lernen ein, um aus Listen registrierter StraftäterInnen neue Listen von bisher nicht auffällig gewordenen Menschen zu generieren, die ein (angeblich) erhöhtes Risiko haben, straffällig zu werden. Dazu werden Faktoren wie die Kriminalitätsrate der Nachbarschaft, aber auch die sozialen Netzwerke der Personen verwendet. Die derart identifizierten Menschen werden von der Polizei darüber informiert, dass man ein Auge auf sie hat.[12] Doch was passiert, wenn bestimmte Minderheiten wie Afro-Amerikaner in diesen Strafregistern überrepräsentiert sind, weil die Polizei durch *racial profiling* überdurchschnittlich viele von ihnen wegen Drogendelikten festnimmt? Das scheint wie ein Einfallstor für *preexisting bias* in diese angeblich neutralen Algorithmen.

Bisher laufen solche Programme noch nicht lange genug, um diese Befürchtungen zu bestätigen oder zerstreuen. Doch die Erfahrung zeigt: Wenn eine Technologie erst einmal im Einsatz ist, ist es ungleich schwerer, sie fundamental zu ändern oder gar wieder abzuschaffen, falls sich herausstellt, dass sie schädlich ist. Wäre es nicht besser, solche Fragen zu klären, *bevor* ein System in den Produktiveinsatz geht?

Bei vielen Algorithmen liegt die Fehler- und Verfälschungsfreiheit sogar im Interesse der Hersteller – wenige Firmen bauen absichtlich rassistische Algorithmen, und noch weniger möchten öffentlich des Rassismus' bezichtigt werden. Insofern fehlen meist nicht die Gesetze, sondern die Methoden, um festzustellen, ob ein Algorithmus verzerrend wirkt oder nicht – und das Bewusstsein, dass dieses Problem überhaupt existiert.

Das Thema der Fairness von Algorithmen findet sich in kaum einem Lehrplan. Viele Informatiker.innen gehen ins Berufsleben, ohne auch nur von diesem Problem gehört zu haben. Dadurch fehlt ihnen der kritische Blick, um ihre Algorithmen und Systeme auf diese Probleme zu prüfen. Und während sexistische Zugangskontrollsysteme leicht erkennbar sind, ist in Zeiten von Big Data ein *preexisting bias* in der Datenbasis nicht leicht aufzudecken.

Perspektive

Schon heute entscheiden Algorithmen über die Kredite, die wir erhalten (oder auch nicht), die Suchergebnisse, die wir sehen (oder auch nicht), und die Status-Updates unserer Freunde, die uns unser *social network* anzeigt (oder auch nicht). Deswegen ist es wichtig, die Frage nach der Fairness dieser Algorithmen zu stellen und zu beantworten.

Die Instrumente existieren: Friedman *et al.* vertreten den Ansatz des *value-sensitive design,*[13] bei dem schon während des Design-Prozesses über die möglichen sozialen Folgen und Nachteile der Design-Entscheidungen nachgedacht werden soll. Shneiderman *et al.* formalisieren dieses Verfahren mit so genannten *social impact statements*, die Entwickler dazu bringen, strukturiert schon während der Entwicklung über mögliche negative Auswirkungen von Algorithmen nachzudenken und diese zu beheben.[14] Auch Ansätze wie *Reflective Design*[15] von Phoebe Sengers *et al.* enthalten Ideen, die für das Erkennen und Entfernen von Vorurteilen und Verfälschungen in Algorithmen hilfreich sein können. Wir sollten uns mit dieser Problematik vertraut machen, wenn wir möchten, dass unsere Arbeit ein Teil der Lösung anstatt ein Teil des Problems wird.

Lawrence Lessig schreibt *„Code is Law"*.[16] Angesichts der zunehmenden Macht von Algorithmen liegt es auch an uns Informatiker.innen, sicherzustellen, dass diese Gesetze nicht diskriminierend sondern *fair* sind.

Max Maaß

Max Maaß studiert IT-Sicherheit in Darmstadt und forscht im Bereich der *Privacy-Enhancing Technologies.*

Anmerkungen

1 *Predictive Policing wird hier als Oberbegriff für eine Reihe verschiedener Verfahren genutzt, von der automatischen Planung von Polizeistreifen basierend auf Kriminalstatistiken bis hin zur Risikobewertung, welche BürgerInnen eventuell straffällig werden könnten.*

2 *Im Englischen wird der Begriff bias verwendet, der alles von unabsichtlicher Verfälschung bis zu bewusstem Rassismus bezeichnen kann. Im Deutschen gibt es kein äquivalentes Wort.*

3 *L. G. Locke, "Flying the Unfriendly Skies: The Legal Fallout Over the Use of Computerized Reservation Systems as a Competitive Weapon in the Airline Industry", Harv. J. Law Technol. Vol. 1449, pp. 219-237, 1990*

4 *S. Lowery, "A Blot on the Profession", Br. Med. J., vol 296, no. 6623, pp. 657-658, 1988.*

5 *C. Huff and J. Cooper, "Sex Bias in Educational Software: The Effects of Designers' Stereotypes on the Software They Design", J. Appl. Soc. Psychol., vol. 17, no. 6, pp. 519-532, 1987.*

6 *B. Friedman, E. Brok, S. K. Roth, and J. Thomas, "Minimizing Bias in Computer Systems", ACM SIGCHI Bull., vol. 28, no. 1, pp. 48-51, 1996.*

7 *P. Sengers, K. Boehner, S. David, and J. "Joyfish" Kaye, "Reflective Design", Proc. 4th Decenn. Conf. Crit. Comput. Between Sensib., pp. 49-58, 2005.*

8 *Siehe zum Beispiel M. Datta, M. C. Tschantz, and A. Datta, "Automated Experiments on Ad Privacy Settings", Proc. Priv. Enhancing Technol., vol. 2015, no. 1, pp. 92-112, 2015 and L. Sweeney, "Discrimination in Online Ad Delivery", Commun. ACM, vol. 56, pp. 44-54, 2013.*

9 *N. Diakopoulos, "Algorithmic Accountability Reporting: On the Investigation of Black Boxes", Tow Cent. Digit. Journal., 2014.*

10 *T. Z. Zarsky, "Understanding Discrimination in the Scored Society", Washingt. Law Rev., vol. 89, no. 4, pp. 1375-1412, 2014.*

11 *http://www.dailymail.co.uk/news/article-3000705/Female-paediatrician-locked-gym-changing-room-computer-assumed-Doctor-title-MAN.html*

12 *https://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist*

13 *B. Friedman, P. H. Kahn Jr., and A. Borning, "Value Sensitive Design and Information Systems," Human-Computer Interact. Manag. Inf. Syst. Found., pp. 348–372, 2006.*

14 *B. Shneiderman and A. Rose, "Social impact statements," Proceedings of the Symposium on Computers and the Quality of Life, pp. 90–96, 1996.*

15 *P. Sengers, K. Boehner, S. David, and J. "Joyfish" Kaye, "Reflective Design", Proc. 4th Decenn. Conf. Crit. Comput. Between Sensib., pp. 49-58, 2005.*

16 *http://harvardmagazine.com/2000/01/code-is-law-html*

Dagmar Boedicker

Refugees Welcome – at Your Secret Service

Zur Zeit helfen viele Ehrenamtliche den Flüchtlingen. Ohne ihr freiwilliges Engagement würde vielerorts kaum etwas laufen. Sie betreuen unbegleitete Minderjährige oder Familien, geben Deutschunterricht, machen Stadtführungen, übernehmen Patenschaften, ... Nur haben sie leider kaum eine oder gar keine Sensibilität für die Notwendigkeit, die Daten der Flüchtlinge zu schützen. Datenschutz für Flüchtlinge? – Fehlanzeige!

Deutschland hat sich viele Jahre lang weggeduckt. Wir liegen in der Mitte der EU, umgeben von anderen Mitgliedstaaten, die sich nach dem Dublin-Abkommen um Aufnahme von und Asyl für geflohene Menschen kümmern mussten. Seit das UNHCR eigentlich gar kein Geld mehr für den Anteil der 60 Millionen[1] gewaltsam Vertriebener hat, um die es sich kümmern soll und will, findet eine kleine Völkerwanderung in die EU statt. Dafür sind wir und andere Industriestaaten verantwortlich, auch, aber nicht nur, weil wir versprochene Zahlungen an die UN nicht geleistet haben.[2]

Migranten am Wiener Westbahnhof am 5. September 2015, die zu Tausenden Richtung Deutschland weiterreisen
Foto: Bwag, CC BY-SA 4.0

Jetzt ist es kompliziert, eine menschenwürdige Unterbringung und Betreuung so vieler Menschen möglichst schnell zu organisieren. Ehrlicherweise müssen wir aber auch zugeben, dass es keine Regierung geschafft hätte, ausreichend Unterkünfte, medizinische und psychologische Hilfe, Bildungsangebote usw. auf Vorrat zu halten. Der Protest gegen eine solche *Mittelverschwendung* wäre Pegida-ähnlich gewesen. Dasselbe gilt für den Versuch, Fluchtursachen zu bekämpfen: Prävention ist nicht vermittelbar, nur mit Krisenbewältigung kann Politik Anerkennung ernten.

Information und Kommunikation

Für ein Land mit 80 Mio. Einwohnern ist eine Million Flüchtlinge sicher keine Katastrophe. In München aber ließ sich beobachten, dass Information und Kommunikation große Schwierigkeiten bereiten. Selbst die Profis in der Verwaltung oder den caritativen Einrichtungen sind überlastet und schaffen es nicht immer, Koordination und Informationsvermittlung aktuell zu halten.

Wie lassen sich die Ehrenamtlichen vernetzen? Wie können sie ihre Termine abstimmen? Natürlich über Twitter, Google oder Facebook! Anfang September führte ein Tweet von Helfer.innen am Hauptbahnhof *(Wir haben keine Milch mehr!)* dazu, dass

Menschen noch Tage nach dem Absenden des Tweets Milch zum Bahnhof brachten, obwohl es dort weder Lager- noch Kühlmöglichkeiten gab.

Awareness dringend geboten

Ehrenamtliche Helfer.innen kommen aus allen möglichen Bereichen, ihre Kompetenzen liegen meist auf anderen Gebieten als der IT. Ein Beispiel, erzählt von einer Helferin: Sie erhielt neulich eine Liste mit mehr als 200 Flüchtlingsnamen, *natürlich unverschlüsselt.* Die versendende Koordinatorin hatte übersehen, dass die Excel-Datei diese Namen in Tabelle 2 enthielt. Noch weniger war ihr klar, dass diese Namen bei mehr als einem Nachrichtendienst landen, der sie mit den Diensten der Herkunftsländer tauschen und damit die Angehörigen der Flüchtlinge in Lebensgefahr bringen kann. Schließlich ist es sehr wahrscheinlich, dass das Herkunftsland keine Demokratie ist und die Angehörigen Oppositionelle sind, dass sie möglicherweise verhaftet oder sogar getötet werden. Ich weiß nicht, wie weit die Hacker-Fähigkeiten rechter Ausländerfeinde reichen. Wahrscheinlich besteht auch da ein Risiko für Flüchtlinge und Unterstützer.

Trotzdem nutzen nicht einmal alle */bcc* für ihre Mails. Es wäre zu wünschen, dass alle Beteiligten Datenschutz praktizieren, das *Dudle* beispielsweise der TU-Dresden[3] nutzen würden und verschlüsseln, zumindest personenbezogene Daten in verschlüsselten *Zip*-Dateien verschicken würden.

Wie sich das verbreiten lässt, ohne die vielen gutwillig Ahnungslosen zu verprellen? Ich weiß es nicht. Wenn Sie/Ihr eine Idee habt, wie sich das Bewusstsein und die Fähigkeiten schärfen lassen, bitte nutzt alle medialen und anderen Möglichkeiten dafür.

Anmerkungen

1 *Die Mittel des UNHCR reichen weiterhin nicht aus, voraussichtlich wird es nur halb so viel Geld erhalten wie es braucht. http://news.yahoo.com/un-refugee-chief-funding-shortage-triggered-europe-arrivals-220840004.html (abgerufen 17.12.15)*

2 *Ende Mai 2015 hatte das UNHCR lediglich 23 % der zugesagten Mittel erhalten. http://www.unhcr.org/558acbbc6.html (abgerufen 17.12.15)*

3 *https://dudle.inf.tu-dresden.de/privacy/Allgemeine_Infos_/*

Fritjof Bornebusch, Helmar Hutschenreuter, Daniel Koch, Aaron Lye

Internet für Flüchtlinge

Flüchtlinge befinden sich in einer äußerst prekären Situation. Sie sich oft isoliert und zahlreichen Repressionen durch Behörden ausgesetzt. Des Weiteren wird diese Isolation von Behörden nicht als Problem erkannt und beseitigt. Deswegen engagieren sich bundesweit Menschen, um dieses Problem selbst zu lösen. Allerdings birgt es auf unterschiedlichsten Ebenen viele Hindernisse. Mit diesem Text wollen wir das Problem näher betrachten und Möglichkeiten und Schwierigkeiten aufzeigen.

Warum brauchen Flüchtlinge Internet?

Selbstverständlich brauchen Geflüchtete Nahrungsmittel, medizinische Versorgung und menschenwürdige Unterbringung. Doch selbst wenn sie diese Grundversorgung erhalten – was leider oft nicht der Fall ist – befinden sich Asylbewerbende in einer prekären Lage. In Deutschland sind sie oft isoliert und haben keine Möglichkeit zur gesellschaftlichen Teilhabe. Sie erleiden in vielerlei Form massive Repression und sind in den Unterkünften zahlreichen Sanktionen und Restriktionen ausgesetzt. Hinzu kommen das, für Laien kaum verständliche, komplizierte Asylrecht und massive bürokratische Hürden, die selbst für Menschen mit Deutschkenntnissen nur schwer zu bewältigen sind.

Mit einem Internetzugang können die Menschen einige dieser Probleme angehen. Zentral ist nicht nur die Kommunikation mit ihren Verwandten und Bekannten, sondern auch am gesellschaftlichen Diskurs teilzunehmen und so ihren Anliegen in der Öffentlichkeit Gehör zu verschaffen und mit der Öffentlichkeit zu kommunizieren, in der meistens nur *über* sie gesprochen wird. Wichtig ist es auch, Zugang zu Informationen, zu Gesetzen, ihren Rechten, Übersetzungen in die jeweiligen Sprache und Lernmaterialien zu erhalten sowie Informationen zu den Heimatländern und den dortigen Entwicklungen zu bekommen. Natürlich dient der Internetzugang auch dem Austausch über Routen, Repressionen und Schlepper.

Allerdings ist ein Internetzugang, der für viele selbstverständlich ist, ein Privileg. Solange Asylbewerber auf ihren Bescheid warten, bekommen sie kein Konto. Ohne Bankverbindung können sie keinen Telefonanschluss anmelden und damit keinen Vertrag für schnelles und preisgünstiges Internet abschließen. Stattdessen sind sie auf Prepaid-Anbieter, wie Lebara, Ortel oder Lyca angewiesen.

Aktuell läuft eine Kampagne[1] zur Unterstützung des Projekts *Refugees Emancipation*[2]. Es wird unterstützt durch den Chaos Computer Club, Freifunk Berlin, das Förderverein Freie Netzwerke e.V., das LinuxHotel, die Digitale Gesellschaft, Idealo, die Open Knowledge Foundation Deutschland, Systemli und das Forum Informatiker.innen für Frieden und Gesellschaftliche Verantwortung (FIfF). Das Projekt Refugees Emancipation errichtet und unterhält bundesweit Internet-Cafés in Unterkünften für Geflüchtete. Dabei will es nicht paternalistisch agieren, sondern Selbstorganisation vorantreiben, d. h. von Geflüchteten für Geflüchtete. Die von Geflüchteten gegründete und unterhaltene Initiative errichtet bundesweit selbstorganisierte und -verwaltete Internet-Cafés. Ziel des Projekts ist es, Menschen aus der Isolation zu holen und miteinander sowie mit der Gesellschaft ins Gespräch zu bringen. Des Weiteren können Geflüchtete Übersetzungsdienste benutzen, um sich über die neue Umgebung und die eigenen Rechte und Möglichkeiten zu informieren.

Internetcafés & Computerkurse für Geflüchtete
Ein Hilfsprojekt von Refugees Emancipation *(Stand: 14.1.16)*
Quelle: www.betterplace.org/de/projects/

Bundesweit engagieren sich Freifunk-Communities, um Flüchtlingen freies WLAN bereitzustellen. So engagieren sich Menschen in fast allen Großstädten in solch einer Initiative. Insgesamt hat die Freifunk-Community bis jetzt ca. 100 Flüchtlingsunterkünfte mit freiem WLAN ausgestattet. In Bremen ist die Situation wie folgt: Die Übergangswohnheime werden von unterschiedlichen Trägern betrieben. Einige haben sich in Trägerverbünden zusammengeschlossen. Bisher hat die Bremer Freifunk Initiative mit einigen Trägern erfolgreich zusammengearbeitet. Dazu zählen unter anderem der Trägerverbund Borfelder Warft (Caritas, Alten Eichen, JUS, Kriz) und ION Berckstraße (Caritas, Alten Eichen, JUS, DRK). Allerdings ist die Arbeit aufwendig und nicht leicht. Deshalb haben aktuell (Stand 18. Dezember 2015) 11 Übergangswohnheime in Bremen Internet; wohingegen noch 23 ohne Internet sind.

Freifunk

Freifunk steht für freie Kommunikation in digitalen Datennetzen. Es agiert nach dem Prinzip, dass Zugang zu Informationen und Wissen frei sein sollte („*free as in freedom*"). So dass ein freies Kommunikationsmedien öffentlich zugänglich, nicht kommerziell, im Besitz der Gemeinschaft und unzensiert ist. Das Netzwerk ist, wie das Internet, unverschlüsselt und offen, wodurch teilnehmende Personen auch hier selbst für die Sicherheit ihrer Verbindungen und ihrer Endgeräte verantwortlich sind.

Freifunk ist kein Internetprovider. Stattdessen ist es ein dezentral organisierter Zusammenschluss lokaler Initiativen und Communities, die mit Hilfe der Freifunk-Technik Menschen ihren Internetzugang anbieten. Individuell werden WLAN-Router für den Datentransfer der anderen zur Verfügung gestellt um so eine freie Infrastruktur aufzubauen[3]. So werden freie Netze von immer mehr Menschen in Eigenregie aufgebaut und gewartet. Die Vision ist die Demokratisierung der Kommunikationsmedien durch freie Netzwerke[4].

In Deutschland ist das rechtliche Problem bei der Bereitstellung eines Netzwerkzuganges für andere Teilnehmer die sogenannte Störerhaftung – § 1004 Bürgerliches Gesetzbuch (BGB)[5]. Danach kann jeder – ohne Täter oder Teilnehmer zu sein –, der in irgendeiner Weise an der Verletzung eines geschütztes Gutes beteiligt ist, als Störer belangt werden. Der Störer kann dabei auf Unterlassung in Anspruch genommen werden. Im Internet bedeutet dies, dass jeder Anschlussinhaber für Rechtsverletzungen belangt werden kann, die über seinen Anschluss begangen wurden, auch wenn er oder sie nicht selbst beteiligt war. Es genügt, dass er ein Werkzeug (Router) zur Verfügung stellt, mit dem eine Rechtsverletzung begangen wird. Diese Sichtweise hat sich zwar in den letzten Jahre bei den Gerichten etwas gelockert, allerdings besteht das Grundproblem immer noch und es ist auch abhängig davon, vor welchem Gericht die Verhandlung stattfindet. Ist man allerdings als Provider bei der Bundesnetzagentur registriert, kann man sich auf das Telemediengesetz berufen, durch welches ein Provider nicht für die Rechtsverletzungen seiner Kunden haftbar gemacht werden kann. Das gilt allerdings nicht automatisch für Inhaber eines Internetanschlusses, auch wenn sie diesen teilen, z. B. in einer Wohngemeinschaft (WG).

Die Freifunk-Initiative umgeht dieses Problem, indem jeder einzelne Freifunk-Knoten (WLAN-Router) eine VPN-Verbindung zu den Servern der örtlichen Freifunk-Community aufbaut. Diese Community gibt es in jeder größeren Stadt, es können sich auch mehrere Umgebungen zu einer Community zusammenschließen. Die VPN-Server dieser Communities leiten alle Verbindungen an verschiedene Internet-Service-Provider (ISP), z. B. an den Förderverein Freie Netzwerke e.V.[6] Diese ISPs sind bei der Bundesnetzagentur als Provider registriert und unterliegen daher nicht der Störerhaftung. Dadurch ist es möglich, dass trotzdem jede.r zu Hause einen Freifunk-Knoten betreiben kann, ohne sich vor Rechtsverletzungen fürchten zu müssen. Durch die Verwendung einer VPN-Verbindung und die Weiterleitung an einen Internet-Service-Provider ist die Verbindung zum Internet langsamer als die direkte Verbindung über den heimischen Internet Zugang. Andererseits kann dadurch die Störerhaftung für die einzelnen Knotenbetreiber eliminiert werden, sodass diese keine rechtliche Verfolgung, z. B. wegen Urheberrechtsverletzung, befürchten müssen.

Erfahrungsbericht Flüchtlingsunterkunft in Oberneuland

Zu Hause ist die Einrichtung eines WLAN oft eine einfache Sache. Der eigene WLAN-Router wird mit dem Internetanschluss verbunden und nach einigen wenigen Konfigurationsschritten kann man mit seinen Geräten drahtlos im Internet surfen. Dass die Einrichtung eines WLAN auch deutlich komplexer sein kann, merkten wir – Helmar Hutschenreuter und Daniel Koch – als wir Ende 2015 ein WLAN in einer Flüchtlingsunterkunft einrichteten.

Diese Unterkunft befindet sich im Büropark Oberneuland in Bremen und wurde dort im August 2015 errichtet, um weitere Plätze für ankommende Flüchtlinge zu schaffen. Wie bei vielen provisorisch errichteten Unterkünften handelt es sich um eine Zeltunterkunft, die von der AWO, der Arbeiterwohlfahrt in Bremen, betrieben wird. Zwei große Zelte schaffen Platz für ca. 420 Flüchtlinge und werden durch einen Bürocontainer für die Mitarbeiter der AWO, mehrere Waschcontainer und ein Verpflegungszelt ergänzt. Letzteres enthält einen großen Essensbereich, ein Spielzimmer für Kinder und eine Kleiderausgabe. Um auf den

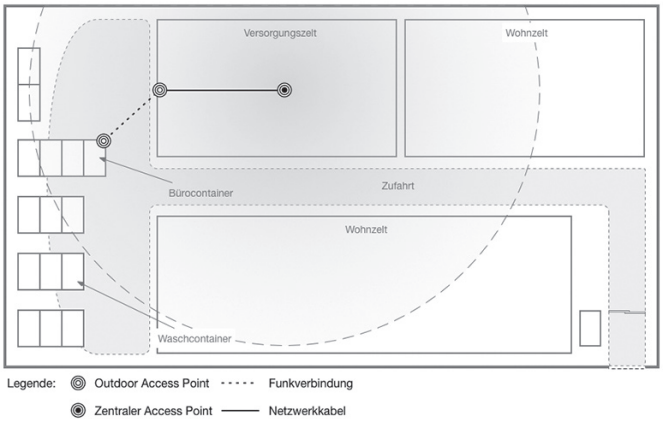
Winter vorbereitet zu sein, werden alle Zelte von großen Heizaggregaten laufend mit warmer Luft versorgt. Die Unterkunft dient vor allem als Erstaufnahmeeinrichtung für Familien aus Syrien und dem Balkan und alleinreisenden Männern aus Syrien.

Kurz nach Eröffnung der Unterkunft erfuhren wir bei einem Besuch, dass die Computer der AWO über mobiles Internet angebunden waren, welches im Bürocontainer aber sehr schlecht zu empfangen war. Die Internetverbindung fiel deshalb oft aus, was der AWO die Arbeit erschwerte. Glücklicherweise hatte Helmar Hutschenreuter Kontakt zu *Bremen Briteline*, einem Internet-Service-Provider, der sich auf breitbandige Internetanbindungen für Geschäftskunden spezialisiert hat. Nach einer kurzen Prüfung erklärte sich Bremen Briteline bereit, kostenlos einen Internetanschluss per Richtfunk bereitzustellen. Mit einer Bandbreite von 100 Mbit/s (Up- und Download) verfügte die Unterkunft damit über einen besonders leistungsfähigen Anschluss. Deshalb war es für uns ein naheliegender Gedanke, diesen Anschluss ebenfalls zu nutzen, um den dort Wohnenden einen kostenfreien Internetzugang per WLAN anzubieten.

Bei einem ersten Planungstreffen in der Unterkunft legten wir gemeinsam mit der AWO den Aufbau des WLAN fest. Aufgrund der Größe der Unterkunft schlug die AWO vor, nicht die gesamte Einrichtung mit WLAN zu versorgen, sondern nur den Essensbereich im Versorgungszelt. Dieser bietet Platz für ca. 150 Bewohnende, die sich dort auch außerhalb der Essenszeiten aufhalten können. Wegen der Größe des Essensbereichs und der Anzahl der Menschen mussten wir davon ausgehen, dass mehrere hundert Geräte später zeitgleich mit dem WLAN verbunden sein würden. Die meisten Access-Points für Heimnetzwerke erlauben aber nur 30 bis 50 simultane Verbindungen. Um dennoch ein stabiles WLAN gewährleisten zu können, mussten wir leistungsfähigere und somit teurere Hardware einsetzen. Eine weitere Herausforderung war die Anbindung des Versorgungszelts an das Internet, denn der Übergabepunkt von Bremen Briteline befand sich im Bürocontainer und zwischen diesem und dem Versorgungszelt waren bisher keine Kabel verlegt worden. Daher war es nicht möglich, einfach ein Netzwerkkabel in einen vorhandenen Kabelkanal zu legen. Ebenso wäre ein einzelnes Kabel keine langfristige Lösung gewesen. Daher entschieden wir uns für eine Funkverbindung zwischen Bürocontainer und Versorgungszelt. Hierfür benötigten wir einen speziellen Outdoor-Access-Point, denn das Signal eines Access-Points innerhalb des Containers wäre außerhalb des Containers nicht empfangbar gewesen. Ein weiterer Outdoor-Access-Point am Zelt sollte dann das Signal vom Container empfangen. Um das Netzwerk gegen unberechtigte Zugriffe aus dem Internet abzusichern und den Nutzenden des WLANs via DHCP IP-Adressen zuteilen zu können, sollte im Bürocontainer ein Router mit Firewall- und DHCP-Funktionalität zwischen Übergabepunkt und Outdoor-Access-Point geschaltet werden.

Solche Hardware war für uns nicht mehr durch eine kleinere Spendensammlung im Bekanntenkreis zu finanzieren. Glücklicherweise fanden wir mit dem Unternehmen *Harren & Partner* einen Sponsor. Die Bremer Reederei hat ihren Unternehmenssitz in direkter Nachbarschaft und beteiligte sich bereits in der Vergangenheit an Spendenaktionen für die Unterkunft. Das Unternehmen bestellte die Hardware über seine IT-Abteilung und spendete sie anschließend der Unterkunft.

Nach der Lieferung der Hardware konfigurierten wir die einzelnen Access-Points und den Router, um sie dann bei einem erneuten Besuch der Unterkunft vor Ort nur noch montieren zu müssen. Die Konfiguration ähnelte dabei stark der Konfiguration, die von einem normalen Heim-WLAN bekannt ist. Wir konfigurierten den Router mit den Zugangsdaten, die wir von Bremen Briteline erhalten hatten und richteten einen DHCP-Server ein. Um mehr als 254 IP-Adressen an Endgeräte vergeben zu können, wählten wir einen lokalen IPv4-Adressbereich der Klasse B. Dabei stehen maximal 65.534 Adressen zur Verfügung, wovon der DHCP-Server die ersten 1.000 Adressen automatisch an Endgeräte vergibt. Jedem Access-Point und dem Router selbst ordneten wir eine statische IP-Adresse außerhalb des DHCP-Adressbereichs zu, um die Konfigurationsinterfaces der Geräte einfach über das Netzwerk ansprechen zu können. Das WLAN selbst konfigurierten wir als offenes WLAN ohne Verschlüsselung, obwohl dieses ein gewisses Sicherheitsrisiko mit sich bringt. Dadurch sollen Probleme der Bewohnenden beim Verbinden mit dem WLAN ausgeschlossen werden, da die AWO nicht zusätzlich zu ihren Aufgaben WLAN-Unterstützung anbieten kann.



Der WLAN-Empfang nach der Montage

Bei der Montage in der Unterkunft half uns ein Mitarbeiter einer IT-Abteilung der Bundeswehr, der im Rahmen der Flüchtlingshilfe der Bundeswehr in der Unterkunft freiwillig arbeitete. Ihn hatten wir bei unserem ersten Planungstreffen kennengelernt. Seine Mithilfe ermöglichte uns eine schnellere Installation, denn er konnte uns zeigen, wo sich die Access-Points am besten montieren ließen und wo Stromanschlüsse zu finden waren. Gerade der Stromanschluss im Versorgungszelt stellte eine Herausforderung bei der Montage dar. Denn dort wurde der Strom über einen Verteiler bereitgestellt, zu dem bis zu 30 Meter lange Kabel über verschiedene provisorische Wände gelegt werden mussten. Für die Anbindung unseres Access-Points, den wir an zentraler Stelle unter der Zeltdecke montierten, verlegten wir ein ca. 20 Meter langes Kabel für den Stromanschluss. Die beiden Outdoor-Access-Points versorgten wir per *Power over Ethernet* (PoE) mit Strom, dabei wird der Strom über das Netzwerkkabel bereitgestellt. Nach der Montage der Geräte prüften wir mit unseren Smartphones den WLAN-Empfang auf dem Gelände der Unterkunft. Dabei deckte das WLAN nicht nur das gesamte Versorgungszelt ab, sondern konnte auch in den beiden angrenzenden Wohnzelten empfangen werden.

Fazit

Insgesamt war das Projekt eine lohnende und spannende Erfahrung für uns. Wir hatten den Aufwand anfangs unterschätzt, konnten aber alle notwendigen Herausforderungen dank unserer Unterstützer meistern. Aus unserer Perspektive von zwei Studenten der Informatik war dieses praktische Projekt eine willkommene Abwechslung zu den vielen theoretischen Inhalten des Studiums. Für die Zukunft wünschen wir uns, dass in mehr Unterkünften ein WLAN bereitgestellt wird.

Bei dem von uns installierten WLAN haben wir sehr leistungsfähige Hardware eingesetzt, die im Gesamtpreis aber nur etwa 500 € kostete. Die vom Provider installierte Internetanbindung kostet im Normalfall für Unternehmen ca. 500 € monatlich. Bei einer Messung des Traffics einige Tage nach der Installation des WLAN wurde im Durchschnitt allerdings nur eine Bandbreite von 3 Mbits/s genutzt. Die Höchstbandbreite lag bei 19,7 Mbits/s. Demnach ließe sich eine Unterkunft wahrscheinlich auch mit einer geringeren Bandbreite von 30 bis 50 Mbits/s ausreichend versorgen und somit die Kosten reduzieren. Dennoch sind die Kosten, verglichen mit den Gesamtkosten, die eine solche Unterkunft verursacht, eher gering. Demnach wäre es wünschenswert, wenn das Land Bremen als Betreiber solcher Unterkünfte ein kostenfreies WLAN in der Grundausstattung seiner Unterkünfte vorsehen würde. Einige Bundesländer, wie z. B. Baden-Württemberg[7], haben das bereits beschlossen, denn für viele Flüchtlinge ist es die einzige Möglichkeit, den Kontakt zu zurückgelassenen Familienmitgliedern und der Heimat aufrechtzuerhalten.

Wir finden es toll, wie viele Menschen sich für Flüchtlinge engagieren. Wir sehen aber auch die Notwendigkeit, rassistische Praktiken von Behörden abzuschaffen und die kontinuierlichen Verschärfungen der Asylgesetze seit den 90er Jahren rückgängig zu machen.

Die Flüchtlingshilfe der Bundeswehr in Unterkünften ist zudem eine Problematik, die umfangreicher diskutiert werden muss. Zwar wird die Hilfe wirklich benötigt, da zivile Einrichtungen und Behörden, wie das Technische Hilfswerk, auch am Rand ihrer Kapazitäten arbeiten. Allerdings wird durch den Bundeswehreinsatz im Inneren ein Normativ etabliert, was stark zu kritisieren ist.

Montage und Konfiguration der Hardware

Anmerkungen

1 *http://support.refugeesemancipation.com/*
2 *https://www.betterplace.org/en/projects/20601-internet-cafes-computer-workshops-for-refugees*
3 *http://freifunk.net/*
4 *http://freifunk.net/worum-geht-es/*
5 *http://www.gesetze-im-internet.de/bgb/__1004.html*
6 *http://foerderverein.freie-netzwerke.de/*
7 *http://www.sueddeutsche.de/digital/baden-wuerttemberg-kostenfreies-wlan-fuer-fluechtlinge-1.2610850*

Fritjof Bornebusch, Helmar Hutschenreuter, Daniel Koch, Aaron Lye

Fritjof Bornebusch ist Informatiker und arbeitet als Softwaretester. Er ist engagiert in den Bereichen Anonymität, freie Netzwerke und der Förderung von verschlüsselter Kommunikation.

Helmar Hutschenreuter ist Student im Masterstudiengang Informatik der Universität Bremen. Seine Interessen liegen in der IT-Sicherheit sowie im Themengebiet *Programmiersprachen und Compilerbau*. Darüber hinaus interessiert sich er sich für Datenschutz und *Privacy by Design*.

Daniel Koch ist wissenschaftlicher Mitarbeiter der Arbeitsgruppe *Soziotechnische Systemgestaltung und Gender* an der Universität Bremen. Er arbeitet im Projekt *ParTec*, welches Verfahren zur partizipativen und nutzerorientierten Entwicklung von Software für und mit älteren Menschen erforscht und erprobt.

Aaron Lye ist wissenschaftlicher Mitarbeiter der Arbeitsgruppe *Technische Informatik/IT-Sicherheit* mit dem Forschungsschwerpunkt *Kryptographie und Komplexitätstheorie* an der Universität Bremen. Im FIfF engagiert er sich im Bereich Überwachung, computergestützte Kriegsführung und Cyberpeace.

Dietrich Meyer-Ebrecht, Ingo Ruhmann, Thomas Reinhold

Cyberwar & Cyberpeace: Sind neue Regeln im Cyberspace möglich?

Internationaler Pugwash-Workshop, Berlin, 23.–24. Oktober 2015

Militärische Aktivitäten können heute wohl nirgendwo mehr auf dieser Welt unbeobachtet ablaufen – außer im Cyberspace. Das klingt paradox, dient doch der Cyberspace als übermächtiges Instrument für eine Ausspähung bis in den letzten Winkel der Erde. Dennoch, mit den nötigen Kenntnissen und Mitteln ausgestattet, können zumindest Inseln im Informationsraum weitgehend vor Beobachtung geschützt werden. Hier können Waffen entwickelt, produziert und ‚stationiert' werden, ohne physikalischen Raum zu benötigen, hier können Waffen getestet und zum Einsatz vorbereitet werden, ohne physikalische Spuren zu hinterlassen, und ihre digitalen Spuren können verschleiert oder sogar ausgelöscht werden. Mit seinem überlegenen Potenzial zur Geheimhaltung ist der Cyberspace bereits seit Langem als fünfter Operationsraum – neben Land, Luft, See und Weltraum – in die militärischen Strategien fest eingebunden. In der Zivilgesellschaft sind Kenntnisse über militärische Aktivitäten im Cyberspace jedoch eher vage, auch nach den Snowdenschen Enthüllungen. Das ist nicht nur der Geheimhaltung zuzurechnen. Die abstrakte Natur der Materie bringt es mit sich, dass ein öffentliches Interesse wenig ausgeprägt ist. Entsprechend schwierig ist es auch, die Auswirkungen militärischer Cyberoperationen abzuschätzen. Unklar ist zudem die völkerrechtliche Einschätzung. Über reale Risiken hinaus ist es die Summe dieser Unsicherheiten, die bedrohlich wirkt.

Vor dieser Situation ist es umso wichtiger, dass das Thema *Cyberwar* zunehmend von wissenschaftlichen Veranstaltungen aufgegriffen wird, so auch vom diesjährigen Treffen der Deutschen *Pugwash*-Gruppe in Berlin. Die deutsche Pugwash-Gruppe wurde im Zusammenhang mit der Gründung der *Vereinigung Deutscher Wissenschaftler* (VDW) bereits im Jahre 1959 ins Leben gerufen, zwei Jahre nach der ersten *Pugwash Conference on Science and World Affairs*. Mit dem diesjährigen Workshop *Cyberwar & Cyberpeace: Sind neue Regeln im Cyberspace möglich?* setzt die Gruppe eine Veranstaltungsreihe zu Cyberthemen fort, die im Rahmen der europäischen Pugwash-Gruppen im Sommer 2013 in den Niederlanden initiiert wurde. Ziel des Workshops war es, die mit der Thematik befassten nationalen und internationalen Gemeinschaften von Wissenschaft, Politik und Zivilgesellschaft miteinander ins Gespräch zu bringen und einen Beitrag dazu zu leisten, dass sowohl in Fachkreisen als auch in der Öffentlichkeit ein Bewusstsein für die Komplexität der Sachzusammenhänge entsteht.

Das Programm spiegelt die Vielfalt der Thematik wider. Eröffnet wurde es mit Vorträgen über die technischen Aspekten gegenwärtiger Cyberangriffe, über Konsequenzen für die globale digitale Infrastruktur und über Möglichkeiten für Gegenmaßnahmen und Verteidigung. Hier wurde auch speziell nach den Aufgaben der Regierungen und der Rolle der EU gefragt. Dass der Cyberspace als neuer politischer Raum verstanden werden muss, dessen Gestaltung neue juristische und friedenspolitische Fragen aufwirft, machten Vorträge zur juristischen Situation deutlich, die sich mit der Anwendbarkeit internationalen Rechts im Cyberspace, mit der Bedeutung des Tallinn-Manuals in dieser Hinsicht und mit der Herausforderung der NSA-Affäre an nationales und internationales Recht befassten. In zwei Vorträgen wurde analysiert, wie effektiv internationale Bemühungen zur Gewährleistung der Sicherheit in den globalen digitalen Netzen sein können. Eine Panelsitzung befasste sich mit den Forderungen an Verwaltung, Politik und Wirtschaft, speziell bezüglich der Sicherheitsbelange, und dies auch im Hinblick auf humanitäre Fragen.

Einen der für Cyberangriffe spezifischen Aspekte waren die Folgen der Schwierigkeiten einer Attribution. Dass die Herkunft von Angriffen und die Identifikation eines Angreifers ein Problem ist, hat auf politischer und strategischer Ebene die Folge, dass es ohne klare Attribution auch keinen eindeutigen Gegner gibt und damit auch keine politische Möglichkeit der Abschreckung oder Begrenzung. Aus Sicht der Diplomatie gibt es damit keine Möglichkeit zwischenstaatlicher Abkommen, sondern allein die Option auf eine weitere Aufrüstung.

In der Plenarsession *Military Options and Arms Control für the Cybersphere* wurden systematisch die für bisherige Rüstungskontroll-Vereinbarungen entwickelten Denkweisen, Ziele und Umsetzungsmaßnahmen betrachtet und versucht, diese auf den Cyberspace zu übertragen. Diese Sichtweise erlaubt neue Schlussfolgerungen für die Arbeit zur Begrenzung der Rüstung im Cyberspace. So ist die bei Atomwaffen – etwa durch den Verzicht auf Abwehrraketen – mögliche Option auf Nicht-Verteidigungsfähigkeit in der Informatik keine Option, da IT-Sicherheit (die vielfach ohnehin lückenhaft ist) gegen vielerlei Gefährdungen erreicht werden muss. Dagegen kann eine Strategie der gegenseitigen Zerstörung (*mutually assured destruction*, MAD, bei Atomwaffen von Bedeutung) bei Cyberangriffen durchaus eine Option sein, wenn demonstriert werden kann, dass ein Gegenschlag auch bei und nach einem Angriff erfolgen kann. Allerdings liegt auch hierin eher eine Tendenz zur Aufrüstung. Ein beachtenswerter Sonderfall war der einer unilateralen reziproken Abrüstung wie beim Zerfall der UdSSR: USA und UdSSR haben ihre Atomwaffen einseitig ohne Vereinbarung zurückgezogen, um zu einer schnellen Lösung zu kommen. Als universeller Weg zur Rüstungskontrolle wurde der Aufbau vertrauensbildender Maßnahmen beschrieben, die in der IT-Welt etwa die verstärkte Kooperation von CERTs bedeuten würde. Etablierte Strategien zur Abrüstung sind in jedem Fall wichtige und viel zu wenig untersuchte Ansatzpunkte auch für die Abrüstung im Cyberspace.

In dieser Session ging es auch darum, für die Rüstungskontrolle aus den Erkenntnissen zu lernen, die aus den Snowden-Dokumenten zu ziehen sind. Dies fängt damit an, dass Cyberwaffen bisher gar nicht als solche erkannt werden. Die XKeyscore-Software der NSA ist eine klassische Angriffswaffe, über die lediglich als Spionagewerkzeug berichtet wird. Auch die Infrastrukturen der Cyberkrieger sind heute noch nicht ausreichend erhoben und systematisiert. Wie das *Transgression*-Programm der NSA zeigt, haben die Cyber-Einheiten genügend Kenntnisse voneinander, um sich gegenseitig – sogar auf dritter und vierter Ebene – durch Cyberattacken die Ergebnisse der jeweils gegnerischen

Arbeit zu stehlen. Diese Erkenntnisse ließen sich ebenfalls für die Rüstungskontrolle nutzen. Mindestens ebenso wichtig sind die personellen und finanziellen Ressourcen der Cyber-Einheiten, die – der Darstellung verfügbarer Daten zufolge – das sechs- bis zehnfache der Ressourcen zur Verfügung haben wie ihre Gegenüber in der zivilen Strafverfolgung und der zivilen staatlich organisierten IT-Sicherheit. Auch diese Kräfteverhältnisse sollten für die Rüstungskontrolle bewertet und genutzt werden. Als Fazit wurde gezeigt, dass die zahlreichen neuen, aber auch die bereits bekannten Daten und Fakten zu Cyberwar-Akteuren bei weitem nicht angemessen für Rüstungskontrollansätze genutzt werden und damit zahlreiche Lösungsansätze ungenutzt bleiben.

Ein wichtiges Element der Pugwash-Workshops ist die Diskussion spezieller Themen in Arbeitsgruppensitzungen, die der persönlichen, thematischen und wissenschaftlichen Vernetzung dienen sollen. In parallelen Sitzungen waren drei Arbeitsgruppen angesetzt. Es ging darin um die Kontrolle des Internet (*Internet Governance*) und den Datenschutz, um die Verwundbarkeit der zivilen kritischen Infrastrukturen wie der Energieversorgung oder des Finanzsystems (*Humanitarian Issues*) und um die Frage, ob der Cyberspace zur Arena einer neuen Kriegsführung werden könnte oder dies bereits ist (*Cyberspace and Warfare*).

Diese letztgenannte Arbeitsgruppe fokussierte sich in ihrer Diskussion auf das friedenspolitisch zentrale Problem der Rüstungskontrolle: Lassen sich Methoden der Rüstungskontrolle, die in den vergangenen Jahrzehnten für andere Waffentechnologien entwickelt wurden, auf den Cyberspace übertragen? Eine entscheidende Voraussetzung dafür wurde in einer präziseren Fassung des Begriffs ‚Cyberwaffe' gesehen, insbesondere um eine Abgrenzung zu legitimen zivilen sowie defensiven militärischen Anwendungen wie Penetrationstests zu gewährleisten. Eine Klassifikation über das Schadenspotential erscheint notwendig, aber schwierig. Es fehlen verlässliche Klassifikationsmethoden. Vor allem lassen sich Kettenreaktionen beim Angriff auf IT-Systeme nicht abschätzen. Weitere wissenschaftliche Arbeit ist dringend geboten, insbesondere um eine Grundlage für internationale Vereinbarungen zu legen.

An dieser Arbeitsgruppe nahm ein einziger Informatiker teil. Überhaupt waren Informatiker.innen deutlich unterrepräsentiert, nimmt man den Ruf nach wirkungsvollerer technisch-wissenschaftlicher Unterstützung friedenssichernder Ansätze angesichts des Potenzials militärischer Operationen im Cyberspace ernst. In Gesprächen am Rande wurde eine zögerliche Haltung der Informatik – hier speziell im Fachgebiet Cybersecurity – deutlich, sich mit diesem ‚heißen' Themenkomplex zu befassen. Dabei ist eine aktive Teilhabe der Disziplin auch deshalb so wichtig, als der Cyberspace im Gegensatz zu allen anderen militärischen Operationsräumen ausschließlich von Menschen gemacht ist und seine Funktionsweise von Fachleuten definiert und kontrolliert wird. Beeindruckend war andererseits, welche Vielfalt an wissenschaftlichen Disziplinen an diesem Workshop beteiligt war. Die Komplexität des Themas fordert dies. Allerdings, und das ist eine andere Beobachtung, müssen die Verständigungsbrücken zwischen den Wissenschaften noch erheblich ausgebaut werden.

Die Präsentationen zu einzelnen Vorträgen sowie Berichte aus den Arbeitsgruppen sind aus dem Internet abrufbar: *http://neu.vdw-ev.de/veranstaltungen/international-pugwash-workshop/*

Übernommen mit freundlicher Genehmigung aus *Wissenschaft und Frieden* 1/2016.

FIfF e.V. – Pressemitteilung

FIfF fordert endlich Aufklärung zum Cyberangriff auf den deutschen Bundestag

25. August 2015 – Im Mai wurde bekannt, dass zahlreiche Computer im *Parlakom*-Netzwerk des Deutschen Bundestages Schadsoftware enthalten. Diese ermöglicht es unbekannten Angreifern, Daten von Abgeordneten und ihren Mitarbeiter.innen zu entwenden. Nach wie vor gibt es bisher keine öffentlichen Informationen und es existieren lediglich Hinweise, dass mehrere Gigabyte E-Mail-Schriftverkehr von Parlamentariern und ihren Mitarbeitern kopiert wurden. Das Ausmaß der Affäre lässt sich dabei nur erahnen. Einzelne Abgeordnete wurden bereits im Juni 2014 über mögliche Manipulationen ihrer Computer informiert; dennoch wurde das Parlakom-System erst jetzt für Reparaturen abgeschaltet. Angesichts der Bedeutung des Systems als primäre Kommunikations- und Arbeitsplattform des deutschen Bundestages kritisiert das FIfF, dass zuständige Stellen den Angriff offenbar nur zögerlich und mangelhaft untersucht haben. Die Öffentlichkeit wurde bis jetzt nur unzureichend über den Schaden und die Konsequenzen für die Arbeit der Volksvertreter informiert.

Fatal ist, dass nicht nur die Parlamentarier hilflos erscheinen, sondern auch die Behörden, deren Aufgabe es ist, den Angriff zu untersuchen. Vom Bundesamt für Sicherheit in der Informationstechnik (BSI), das für den Schutz von Bundeseinrichtungen vor Internetangriffen verantwortlich ist, gibt es nach wie vor keine offizielle Stellungnahme. Dabei muss die Rolle des BSI, das direkt dem Innenministerium unterstellt ist, selbst kritisch hinterfragt werden. Als Teil der Regierung, deren Handeln eigentlich von den Parlamentariern kontrolliert werden soll, könnte das Ministerium durch die Untersuchung der Rechner aller Parlamentsmitglieder mittelbar an Informationen über deren Pläne und Standpunkte gelangen. Eine Institution hingegen, die klar dem Schutz unserer Demokratie und ihrer Werte auf dem Gebiet der Informationstechnik dient, muss unabhängig sein. Im Fall des BSI sind Zweifel daran berechtigt, zumal die Behörde immer wieder auch im Verdacht der Kooperation mit dem US-amerikanischen Geheimdienst NSA stand.

„Insider" und Medien spekulieren währenddessen über den Ursprung des Angriffs. „Ein sinnvoller Rückschluss auf einen bestimmten Angreifer ist jedoch kaum gesichert möglich. Im Bereich mutmaßlich zwischenstaatlicher Spionage sind derartige Fragen ohnehin vielmehr Gegenstand außenpolitischer Interessen als echter Fakten", stellt Thomas Reinhold klar, Campaigner

der Cyberpeace-Kampagne des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF). „Es ist ebenso vorstellbar, dass die scheinbaren Quellen des Angriffs durch Dritte benutzt wurden, um absichtlich Spuren in eine falsche Richtung zu legen." Dies gilt umso mehr, da die Rechner, von denen der vermeintliche Angriff erfolgte, zum Zeitpunkt der Angriffe selbst fehlerhafte Software in Form der *Heartbleed*-Schwachstelle enthielten. Dies ergab die Analyse eines unabhängigen IT-Experten im Auftrag der Bundestagsfraktion der Partei *Die Linke*. Nicht russische – wie zwischenzeitlich gemutmaßt wurde – sondern beliebige Geheimdienste könnten am Ende hinter diesem Angriff stecken.

Immer wieder gelingt es Angreifern, sich Zugang zu sensiblen oder kritischen IT-Strukturen zu verschaffen.

„Computer sind grundsätzlich angreifbar, wir müssen unsere Systeme daher besser schützen und die Sicherung von IT angesichts deren zentraler gesellschaftlichen Bedeutung als Kernaufgabe verstehen", mahnt Stefan Hügel, Sprecher der Cyberpeace-Kampagne und Vorsitzender des FIfF e.V. Dazu bedarf es vor allem auch seitens der Bundesregierung ein klares Bekenntnis zur Förderung sicherer Informationstechnik, des Schutzes von IT-Strukturen durch öffentliche und unabhängige Institutionen und die Abkehr von nebulösen Geheimdienstkooperationen. Vor allem aber brauchen wir einen transparenten und einer Demokratie würdigen Umgang mit derart massiven Vorfällen wie dem Bundestagshack – einem Cyberangriff auf die Infrastruktur der Vertretung der gesamten deutschen Bevölkerung.

Sylvia Johnigk – Rede bei der Demonstration

Freiheit statt Angst – Kundgebung 10. Oktober 2015, München

Ich werde einen Aspekt in den Fokus rücken, der in der Diskussion zu wenig beachtet wird – die militärische Motivation für Überwachung.

Was treibt unsere Regierungen an, sich seit Jahrzehnten beim Versuch, die Voratsdatenspeicherung zu etablieren, ständig bei unseren Verfassungsgerichten blutige Nasen zu holen?

Parallel terrorisieren uns Regierung und Sicherheitsbehörden seit Jahren mit abstrakten Gefahren und vermeintlichen Terrordrohungen, um uns weichzukochen. Damit wir endlich folgsam werden – sie wollen, dass wir zukünftige Überwachungsmaßnahmen klaglos akzeptieren: an Flughäfen, Bahnhöfen, Autobahnen, in Bahnen, Bussen, Stadien, auf öffentlichen, nicht-öffentlichen Plätzen und inzwischen, weil es so schön einfach geht, im digitalen Raum.

Dabei geht es ihnen um uns alle zusammen – die Gesellschaft als Ganzes, die, wenn sie allumfassend überwacht wird, leichter manipulierbar und beherrschbar ist.

Je mehr die Regierung über die Stimmung in der Gesellschaft weiß und mit welchen Faktoren sie sich verändert, desto leichter fällt es, die Stimmung durch gezielte Manipulation zu beeinflussen.

Es geht in erster Linie darum, hegemonale wirtschaftliche Strukturen zu festigen, uns gefügig für TTIP, Ceta, Hartz IV, private Vorsorge zu machen und um Kriege zu führen – jetzt auch im digitalen Raum.

Das Strategiepapier der Verteidigungsministerin von der Leyen sieht vor, im digitalen Raum, beim Cyberkrieg, aktiv mitzuwirken – deshalb muss die Bundeswehr digitale Waffen für einen Angriffskrieg bauen.

Interessanterweise spielt bei Kriegen Überwachung und Spionage – und damit die Vorratsdatenspeicherung – eine tragende Rolle.

Überwachung im eigenen Land bedeutet die eigene Gesellschaft, Spionage bedeutet den Gegner zu kennen. Dabei geht es nicht nur um technische sondern insbesondere auch um organisatorische und gesellschaftliche Informationen, die genutzt werden – um Kriege mit möglichst großer Zustimmung in der eigenen Bevölkerung führen zu können.

Das eigentlich kriegsmüde, pazifistische Deutschland soll wenigstens den digitalen Krieg mittragen. Aber digitale Kriege bleiben nicht digital, sie haben wie herkömmliche Kriege Auswirkungen auf Menschen.

Im digitalen Krieg werden Stromnetz und Telekommunikationseinrichtungen angegriffen. Um digitale Waffen bauen zu können, muss man Schwachstellen in Computern geheimhalten und kann die Computer der eigenen Bevölkerung nicht mehr dagegen absichern.

Wir haben als FIfF deshalb eine Kampagne für Cyberpeace gestartet, die sich insbesondere gegen Cyberwaffen richtet. Unterschriftenlisten liegen an unserem Stand aus.

Ich will grundsätzlich nicht überwacht werden, und schon gar nicht um mich manipulieren zu lassen, ich bin keine Marionette sondern ein freier Mensch, ich bin Informatikerin und ich warne vor einem digitalen Krieg, der erst durch Überwachung möglich wird.

Münchner FIfF-Aktivisten im Einsatz

Foto: Sylvia Johnigk

Dietrich Meyer-Ebrecht – Rede bei der Demonstration

Freiheit statt Angst – Kundgebung 29. August 2015, Köln, Neumarkt

Freiheit statt Angst – dieses Motto muss jede Gesellschaft mit an die vorderste Stelle setzen! Ein großer Dank an die Organisatoren dieser Kundgebung und euch allen für euer Engagement, dass ihr nach einer langen Demo hier wieder zusammengekommen seid, um Solidarität zu zeigen, um der politischen Forderung Nachdruck zu geben.

Angst kann man nur durch Wissen begegnen. Hier ist es das Wissen über die Akteure und ihre Ziele. Dort, wo die Akteure nationale Behörden oder Unternehmen sind, ist noch mit Einschränkungen transparent, was ihre Ziele sind. Dunkel wird es, sobald die Geheimdienste ins Spiel kommen. Sie unterliegen keinerlei parlamentarischer Kontrolle, und die Politik tut alles, ihr Tun zu vernebeln. Noch undurchsichtiger wird es durch die internationale Zusammenarbeit der Geheimdienste – NSA, GCHQ, BND. Gemeinsam mauscheln sie sich an nationalen Richtlinien und Gesetzen vorbei. Von den Geheimdiensten geht jedoch die stärkste Triebkraft zur flächendeckenden Ausspähung aus. Über die Kriterien, mit denen sie die Netze durchkämmen, wissen wir nichts. Und wir erfahren nicht, wenn wir selber ins Fadenkreuz geraten – nicht wann, nicht wie, nicht warum. Regelmäßig werden Fälle bekannt, dass Unbescholtene ins Netz geraten – Kollateralschaden …

Hinter den Geheimdiensten stehen militärische Interessen. Für die Militärs ist der Cyberspace ein Spionageinstrument von einer bisher unerreichten Mächtigkeit. Aber dies ist erst die Grundstufe des Informationskrieges. Die Militärs wollen mehr. Sie nutzen das Internet, um in unsere Computer, in unsere Intranets, in unsere Infrastrukturen einzudringen und geheime Zugänge anzulegen. Einige sind entdeckt worden, z. B. bei der Telekom. Wir wissen nicht, wie viele und welche bis heute unentdeckt geblieben sind.

Über diese geheimen Zugänge zu den Netzen von Behörden, Institutionen und Unternehmen kann das volle Programm des Informationskrieges abgespielt werden: Durch Einspeisen von Missinformation und Desinformation kann eine nationale Zivilgesellschaft destabilisiert werden. Beispiele gab es in Osteuropa. Mit dem Einschleusen von Schadsoftware kann Sabotage bis zu physischen Zerstörungen bewirkt werden. Prominentes Beispiel ist die Zerstörung einer Reihe von Urananreicherungszentrifugen im Iran durch den Trojaner *Stuxnet*. Solche hochkomplexen Software-Entwicklungen sind Cyberwaffen. Kaspersky hat kürzlich über die Identifizierung und Analyse von allein 36 im Netz gefundener Schadprogramme dieser Art berichtet. Unvorstellbare Folgen kann die Übernahme der Kontrolle über kritische Infrastruktursysteme wie Energieversorgung, Verkehrssteuerung, Mobilfunknetze haben. Die Bundesregierung hat vor einigen Jahren eine Studie anfertigen lassen über die Folgewirkungen eines länger andauernden, großflächigen Stromausfalls. Die Ergebnisse lesen sich wie ein Albtraum. An dieser Flanke kann eine Nation niedergezwungen werden, ohne dass konventionelle Waffen zum Einsatz kommen müssen.

Cyberwarfare ist inzwischen fester Bestandteil der militärischen Szenarien. Darin ist der Cyberspace fünfter Operationsraum neben Land, Luft, See und Weltraum. Auch die Bundeswehr mischt jetzt mit. Ministerin von der Leyen arbeitet gerade daran, den Etat des BND und der Bundeswehr auf diesem Sektor um 750 Stellen aufzustocken. Unter anderem dient dieses Personalbudget zum Aufbau staatlicher Hackertrupps, die nach Sicherheitslücken fahnden und passende Exploits als digitale Einbruchswerkzeuge entwickeln. Kenntnisse und Exploits, auf einem prosperierenden Schwarzmarkt aufgekauft, ebenfalls mit unseren Steuergeldern. Natürlich werden diese Erkenntnisse und Entwicklungen geheim gehalten. Anderenfalls wären sie für Geheimdienste und Militärs wertlos. Absichtsvoll werden sie der Zivilgesellschaft vorenthalten: In zivilen Systemen bleiben diese Sicherheitslücken offen!

Es gibt weitere Risiken für die Zivilgesellschaft: Operationen mit Cyberwaffen sind unkontrollierbar, wie das Beispiel Stuxnet zeigt. Der Trojaner hat weltweit eine große Anzahl baugleicher Prozesssteuerungsanlagen befallen – Kollateralschaden. …

Cyberoperationen hinterlassen keine physischen Spuren. Der Urheber kann seine Identität verschleiern und die Spuren eines Angriffs verwischen. Ein Gegenschlag des Angegriffenen kann den Falschen treffen und zur Eskalation führen.

Dies sind nur einige der Risiken für die Zivilgesellschaft, die bereits heute sichtbar sind. Es wird höchste Zeit, dem militärischen Missbrauch unserer zivilen Netze entgegenzusteuern. Das will das FIfF mit seiner Kampagne *Cyberpeace* bewirken. Wir wollen über diese viel zu wenig beachtete Entwicklung aufklären. Wir wollen die Öffentlichkeit mobilisieren, Druck auf die Politik zu machen, um Maßnahmen für eine ausschließlich friedliche Nutzung der Informations- und Kommunikationsnetze einzufordern. Wir appellieren an unsere Regierung und an das Parlament:

- Frau von der Leyen, verzichten Sie auf Cyberwaffen für die Bundeswehr!
- Frau Merkel, Herr Steinmeier, setzen Sie sich für einen weltweiten Bann dieser Waffengattung ein!

Freiheit statt Angst – wer das will, muss auch diese Forderungen unterstützen!

Eberhard Zehendner

Cybercrime – Editorial zum Schwerpunkt

Der Schwerpunkt *Cybercrime* handelt von massiver Internetkriminalität: *Cybercrime* (deutsch *Internetkriminalität*, manchmal fälschlich mit *Computerkriminalität* gleichgesetzt) ist ein schillernder Begriff, unter dem mancher zu verstehen vorgibt, was seinen Partikularinteressen nutzt. Denn nicht jedes Vergehen, bei dem ein Computer benutzt wird, ist *Cybercrime*. Und *Skriptkiddies* sind sicher anders zu be- (und ver-)urteilen als hochprofessionelle Vermieter von *Botnetzen*. Denn hinter *Cybercrime* können – obschon Beute und Schaden selten genau und nachprüfbar bezifferbar sind – gewaltige finanzielle Interessen stehen, die z. B. mit Identitätsdiebstahl oder Erpressung arbeiten. Aber – das haben diverse Enthüllungen der letzten Jahre wieder einmal deutlich gezeigt – auch Regierungen und Geheimdienste fungieren mitunter als Auftraggeber systematischer und umfassender krimineller Akte im Internet. Ganz aktuell nutzen fremdenfeindliche Organisationen das Netz, um ihre Hasskampagnen zu orchestrieren – und einem bundesdeutschen Justizminister fällt dazu nicht mehr ein, als *Facebook* um freundliche Mithilfe zu bitten, eine ganz neue Auffassung von *Public Private Partnership,* wie es scheint.

Dominik Brodowski und *Felix Freiling* sehen in ihrem Beitrag *Cyberkriminalität – Erscheinungsformen, Entwicklungslinien, Herausforderungen* Begriff und Thematik im Schnittfeld von rechtlichen und technischen Fragen. Aus zentralen Besonderheiten des *Cyberspace* leiten sie ein – im Vergleich zur klassischen Kriminalität – anderes oder erhöhtes Bedrohungspotential (insbesondere für ökonomisch motivierte Kriminalität) ab. Die Autoren beschreiben die historische Entwicklung von Cyberkriminalität und deren strafrechtlicher Erfassung, und thematisieren daraus entstandene Herausforderungen, bis hin zu noch wenig verstandenen und strafrechtlich noch kaum thematisierten Deliktsformen.

Carlo Schäfer beleuchtet in seinem Beitrag *Die Rolle von Spam im Cybercrime* die Zusammenhänge zwischen Spam, Phishing und Botnetzen als Grundlage vieler kleiner täglicher Akte von Internetkriminalität, die sich – mögen sie auch als Einzelne genommen eher unbedeutend erscheinen – bereits zu weltweit dramatischen volkswirtschaftlichen Schäden summiert und nicht selten auch Fälle spektakulärer *Cyberspionage* vorbereitet haben. Er kritisiert die bisher übliche Vorgehensweise der Spam-Bekämpfung, die nicht an der Quelle des Problems ansetzt und daher Service-Einschränkungen und *Blacklisting* von E-Mail-Providern nicht verhindern kann, und verweist auf tatsächlich wirksame Alternativen – deren Wirkungsweise zwar veröffentlicht, aber vielen Verantwortlichen anscheinend noch nicht bekannt ist.

In seinem Beitrag *Wardriving – die unterschätzte Gefahr* erläutert Stefan Jäger eine Technik, die Schüler der *Thüringer Junior-Akademie* 2013 ebenso benutzt haben wie zuvor schon der berüchtigte *Albert Gonzalez*. Während jedoch die Schüler sich (und die Bevölkerung) damit nur – und lobenswerterweise – über die (Un-)Sicherheit zahlreicher WLAN-Router am Akademieort informierten, stahl Gonzalez, u. a. mit Hilfe von *Wardriving,* in den Jahren 2005 bis 2007 die Daten von mehr als 180 Millionen Kredit- und Bankkarten. Der *SchlussFIfF* streift in einer satirischen Kurzbiografie von Gonzalez auch das Thema der Verflechtungen zwischen Internetkriminellen, Sicherheitsbehörden und Geheimdiensten.

In ihrem weiteren Beitrag *Transnationale Cyberkriminalität vs. nationale Strafverfolgung: Mögliche Auswege aus einem grundsätzlichen Dilemma* widmen sich *Dominik Brodowski* und *Felix Freiling* vertiefend der – häufigen – Situation, dass Akte von Cyberkriminalität über Staatsgrenzen hinweg verübt werden bzw. Täter sich und/oder ihre Daten in einen anderen Staat in Sicherheit bringen. Die Autoren diskutieren dabei drei Wege, wie dieser Problemlage grundsätzlich begegnet werden könnte.

Alle Beiträge des Schwerpunkts zitieren aus zahlreichen Quellen, die schon für sich genommen interessant sind und tiefer in die Thematik eintauchen. Besonders hingewiesen sei dabei auf das Werk (Brodowski & Freiling, 2011), zu dem es in diesem Heft auch eine Rezension gibt. Die von der Schwerpunktredaktion auf den Seiten 25–28 sowie 38 eingeschobenen Erläuterungsblöcke basieren auf dem Vortrag *Verbrechen im Netz: Cyberkriminelle und ihre Tricks*, den *Felix Freiling* am 15. Juni 2015 im Rahmen der Reihe *Wissenschaft auf AEG* auf dem *Energie Campus Nürnberg* gehalten hat.

Hacking is no Cybercrime!

*„Es geht hierbei **nicht** darum, irgendwelche Passwörter zu knacken, sondern lediglich darum, Systeme und Methoden zu analysieren und zu verstehen, die uns alle alltäglich umgeben. Wenn Firmen Hardware und Software verkaufen, die den Eindruck von Sicherheit vermitteln, dann soll man sich darauf auch verlassen können. Wenn allerdings schon Laien ohne besondere Vorkenntnisse diese Sicherheitssysteme aushebeln und Verschlüsselungsmethoden erkennen können, dann stellt das für Profis erst recht keine Hürde mehr dar. Diese Seite dient dazu, solche Sicherheitsrisiken aufzudecken und Thesen für schwache Verschlüsselungsmuster aufzustellen."*

Wardriving-Forum.de Enzyklopädie, Standardpasswörter http://bit.ly/1nagMvR, Stand: 07.01.2016, CC BY-NC-SA 3.0

Dominik Brodowski und Felix Freiling

Cyberkriminalität – Erscheinungsformen, Entwicklungslinien, Herausforderungen

Als Cyberkriminalität wird aus juristischer Sicht in einem weiten Sinne jede strafbare Verhaltensweise bezeichnet, bei der Informations- und Kommunikationstechnologie entweder als Werkzeug zur oder bei der Deliktsbegehung verwendet wird, oder bei der diese selbst Objekt strafbaren Verhaltens ist (Brodowski & Freiling, 2011, 28 f.; Chawki, Darwish, Khan & Tyagi, 2015, 3). Aus Sicht der Informatik wird hingegen die Rolle der eingesetzten Technik hervorgehoben und dabei technikorientierte Cyberkriminalität – bei der typischerweise Schadsoftware zum Einsatz gelangt – und menschenorientierte Cyberkriminalität – bei der die Kommunikation zwischen Menschen unter Einsatz von technischen Hilfsmitteln im Vordergrund steht – unterschieden (Brodowski & Freiling, 2011, 29). Beiden Sichtweisen ist gemein, dass sie nicht nur Angriffe auf Informationstechnologie thematisieren (so aber die europastrafrechtliche Definition, vgl. Brodowski & Freiling, 2011, 180), sondern auch den Menschen als von kriminellem Verhalten im Netz Geschädigten in den Vordergrund rücken. Aus dieser Perspektive heraus beschreiben wir schlaglichtartig Erscheinungsformen, Entwicklungslinien und die aktuellen wissenschaftlichen und gesellschaftlichen Herausforderungen des Gebietes.

Erscheinungsformen

Cyberkriminalität ist heute ein nahezu ubiquitäres Phänomen: Mit der Verlagerung vieler Aktivitäten in den Cyberspace verlagert man auch alle mit diesen Aktivitäten einhergehenden, klassischen Delikte dorthin. Alles, was es ohne das Internet gab – etwa Betrug, Beleidigung oder Erpressung –, gibt es daher nun auch im Internet. Aus fünf zentralen Besonderheiten des Cyberspace (s. hierzu auch Gercke, 2008, 291 ff.; Sieber, 2012, 132 ff.; Wall, 2007, 34 ff.) resultiert jedoch ein anderes und teils erhöhtes Bedrohungspotential, insbesondere für ökonomisch motivierte Kriminalität:

- **Automatisierbarkeit:** Im Cyberspace kann man Aktivitäten programmieren und durch Computer ausführen lassen. Ein konstanter Aufwand kann durch massenhafte Ausführung ein Vielfaches an Wirkung erzielen (sogenannte Multiplikatoreffekte).

- **Flüchtigkeit:** Im Gegensatz zu greifbaren und beständigen körperlichen Sachen sind Computerdaten häufig flüchtig. Spuren verwischen so schneller als in der realen Welt.

- **Räumliche Entgrenzung:** Virtualisierung und Vernetzung führen dazu, dass programmierte Handlungen unabhängig von einem physischen Ort durchgeführt werden können. In einem *grenzenlosen* Cyberspace sind nur der Ein- und Ausstiegspunkt einer Aktivität lokalisierbar, die Verlaufswege nicht oder nur mit hohem Ermittlungsaufwand. (Siehe zu diesem Problemkreis ergänzend Brodowski & Freiling, in diesem Heft, S. 36)

- **Kopierbarkeit:** Beliebige Artefakte können im Cyberspace perfekt kopiert werden, also auch Authentifizierungsinformationen. Wird also eine Aktivität in den Cyberspace verlagert, kann man sie innerhalb des Cyberspace nicht mehr zweifelsfrei einer realen Identität zuordnen.

- **Angreifbarkeit:** IT-Systeme enthalten Schwachstellen, die von Angreifern ausgenutzt werden können, um schädliches Verhalten des IT-Systems zu erzeugen.

Entwicklungslinien

Mit diesen Herausforderungen gehen auch folgende Entwicklungslinien der Cyberkriminalität und deren strafrechtlicher Erfassung einher, die historisch aufeinander aufbauen und dabei ineinander übergehen. Sie reichen von bisher gut verstandenen und erfassten Delikten aus dem Umfeld einer örtlich begrenzten Datenverarbeitung, über Delikte, die aus der massenhaften Vernetzung entstehen, bis hin zu noch wenig verstandenen und strafrechtlich noch kaum thematisierten Deliktsformen, die aus der räumlichen Entgrenzung entstehen.

Verwendung elektronischer Datenverarbeitung

Zunächst ergab sich aus der isolierten *Verwendung* informationstechnischer Systeme und *elektronischer Datenverarbeitung* das Erfordernis, Schutzlücken zu schließen, die sich aus der Ersetzung menschlicher Entscheidungsprozesse durch automatisierte Verfahren ergab. Paradigmatisches Beispiel hierfür ist die Einfügung des Delikts des Computerbetrugs (§ 263a StGB) durch das 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität im Jahre 1986. Im gleichen Zuge wurde die Geheimhaltung, der Bestand und die Verwendung von Daten strafrechtlich geschützt (§§ 202a, 303a, 303b StGB).

Internationale Vernetzung der Computertechnologie

Die zunehmende, *internationale Vernetzung der Computertechnologie,* insbesondere durch das Internet, führt zu einer zweiten Entwicklungsstufe und begleitet die Transformation von Industrie- zu Informationsgesellschaften. Rechtliche Schwierigkeiten ergeben sich hierbei etwa aus der neuen Nutzungsmöglichkeit als Kommunikationsmedium (E-Mail und Chat als Individualkommunikation, Webseiten als Massenkommunikation) und daher zur menschenorientierten Cyberkriminalität, aus räumlichen Diskrepanzen zwischen Dateneingabe, -speicher und -ausgabeort und den hieraus entstehenden Problemen einer Strafdurchsetzung, aus der wahrgenommenen Anonymität und leichteren Zugriffsmöglichkeiten auf inkriminierte Informationen (etwa kinderpornografische Bilder und Videos) oder auch aus räumlich verteilten, koordinierten und nur in ihrer Summe erheblichen Angriffen (Distributed Denial-of-Service-Attacken), die erst durch die Neufassung des § 303b Abs. 1 Nr. 2 StGB durch das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität im Jahre 2007 effektiv strafrechtlich erfasst werden können.

Daneben resultiert aus der Ubiquität – und zunehmenden Abhängigkeit – von Informations- und Kommunikationstechnologie, dass auch bei nahezu jeder *klassischen* Straftat digitale Spuren auszuwerten sind: Sei es, um den mutmaßlichen Aufenthaltsort eines Verdächtigen anhand der Standort- oder Verbindungsdaten seines Mobiltelefons herauszufinden; sei es, um anhand vorangegangener Kommunikation die Motivlage des Täters herauszufinden; sei es, um anhand von Kommunikationsstrukturen potenzielle Hintermänner und Gehilfen, aber auch potenzielle weitere Geschädigte ausfindig zu machen.

Vollständige räumliche Entgrenzung

Erst in ihren Kinderschuhen steckt die rechtliche Erfassung der zunehmenden *Virtualisierung*, die zusammen mit der Vernetzung zur vollständigen Abkopplung von Berechnungsvorgängen vom Ort ihrer Ausführung führt. Konsequenz dessen ist etwa, dass der Speicherort der Daten eines virtualisierten E-Mail-Servers nicht ohne Weiteres feststellbar ist, auf mehrere Rechner auf mehreren Kontinenten verteilt sein könnte und auch eine Verlagerung des Speicherorts in Sekundenschnelle – etwa von den USA nach Japan – möglich ist.

Auf sozialer Ebene sind zudem virtuelle (Parallel-)Welten entstanden, etwa in Massen-Mehrspieler-Online-Rollenspielen, in denen Beteiligte („Bewohner", Spieler) die Steuerung virtueller Charaktere übernehmen und sich teilweise mit diesen eher identifizieren als mit ihrem eigenen Körper. Diese virtuellen Charaktere können auch Handel treiben mit rein virtuellen Gütern oder virtuellen Währungen, welche aber regelmäßig mit *echter*, *harter* Währung bezahlt („getauscht") werden können; zudem können sie Opfer oder Täter virtuell dargestellter Straftaten – bis hin zu Vergewaltigung und Mord – sein.

Ökonomisierung und zunehmende Organisierung

Die Motivationslage für Cyberkriminalität ist phänomenologisch betrachtet mannigfaltig: Bei der Verbreitung und dem Zugriff auf Kinderpornografie dominieren Pädokriminelle das Bild; rassistische Hetze im Netz beruht auf menschenverachtenden Motiven; manche Denial-of-Service-Attacken oder Datenveröffentlichungen beruhen auf politischen Überzeugungen. Dennoch lässt sich für die große Mehrzahl an Cyberstraftaten eine ökonomische Motivation herleiten (Brodowski & Freiling, 2011, 188), auch wenn sich die Schäden der Cyberkriminalität – und spiegelbildlich der von Cyberkriminellen erzielte Gewinn – nur unzureichend bestimmen lassen (Kshetri, 2010, 7). Das Potential für ökonomisch motivierte Kriminalität steigt dabei mit der Verlagerung des Handels in das Internet immer weiter an.

Teil dieser Ökonomisierung der Cyberkriminalität ist auch, dass sich hier eine höchst arbeitsteilige Vorgehensweise herausdifferenziert hat: Spezialisten für jeden Arbeitsschritt vernetzen sich über spezielle Plattformen untereinander, um ihre jeweiligen Fertigkeiten gegen Bezahlung auszutauschen (Brenner, 2002; Krebs, 2014, 113 ff.; Spoenle, 2010). Damit verbunden ist eine Diffusion von Wissen, aber auch von strafrechtlicher Verantwortlichkeit, und es handelt sich mitnichten um organisierte Kriminalität klassisch-hierarchischen Musters, sondern um ein „flat e-commerce business model" (Wall, 2010, 54). Allerdings zeigt sich in den letzten Jahren auch die klassische organisierte Kriminalität vermehrt interessiert am ökonomischen Potential der Cyberkriminalität, wird aber ihrerseits durch die Arbeitsweise von Cyberkriminalität transformiert (Brodowski, 2016).

Herausforderungen

Der Cyberspace ist ein großer und komplexer digitaler Raum, der in unsere reale Welt eingebettet ist. Die im Cyberspace agierenden Personen stehen am Rand dieses Raums und interagieren durch diesen Raum hindurch miteinander. Die sozialschädigenden Effekte der Kriminalität entstehen notwendigerweise in der realen Welt, sodass der Beziehung zwischen den handelnden Personen (Tätern, Opfern, Ermittlern) eine zentrale Bedeutung zukommt. Abbildung 1 stellt die Zusammenhänge schematisch dar. Sie soll im Folgenden auch dazu dienen, die Herausforderungen aufzuzeigen, denen sich die IT-Sicherheit und das Computerstrafrecht gegenübersehen.

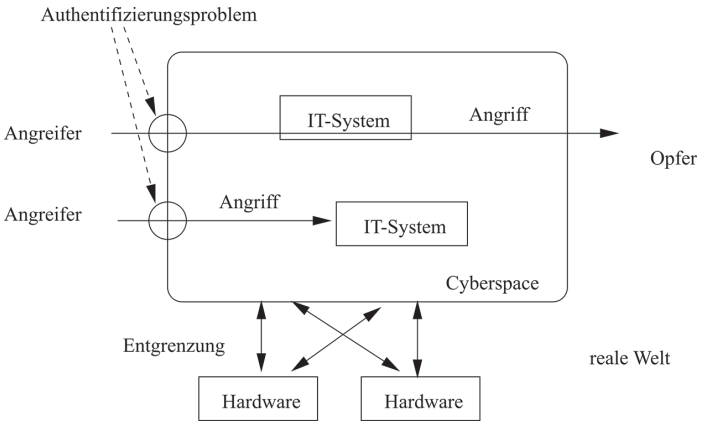


Abbildung 1: Auswirkungen der Informationstechnologie auf die Kriminalität im Cyberspace (aus Brodowski & Freiling, 2011, 54)

Probleme bei der Identifizierung handelnder Personen

Egal ob ein IT-System als Ziel oder Werkzeug einer Straftat verwendet wird, ist es unter den gegebenen Rahmenbedingungen des Cyberspace deutlich schwieriger als in der realen Welt, die Ursache einer Systemaktivität zurückzuverfolgen. Dies beruht auf den vielen „Indirektionen", die im Cyberspace auf einfache Art und Weise aufgebaut werden können, um Aktivitäten zu verschleiern.

Die erste Indirektion existiert an der Grenze zwischen Cyberspace und der realen Welt (siehe Abbildung 1) und wird vielfach als *Anonymität* wahrgenommen (zur juristischen Diskussion siehe etwa Brunst, 2009; Gercke & Brunst, 2009, Rdn. 22 f.; Hilgendorf & Valerius, 2012, Rdn. 460). Die im Cyberspace verwendeten Identitäten, wie etwa E-Mail-Adressen oder Namen in Diskussionsforen, müssen in keinem Zusammenhang stehen mit der realen Identität eines Benutzers. Zwar besteht bei der Vergabe von Zugangskennungen in Organisationen wie Unternehmen, Behörden oder Hochschulen oft eine erkennbare Verbindung, wenn etwa die E-Mail-Adresse aus dem Vornamen und dem Nachnamen der Person zusammengesetzt wird. Im

privaten Bereich, wenn man etwa eine E-Mail-Adresse bei einem Diensteanbieter registriert, ist dies regelmäßig ohne Nachweis der Legitimation möglich. Ähnlich gestaltet es sich bei der Verwendung von frei zugänglichen Netzzugangspunkten wie Internetcafés oder fremden, ungesicherten WLAN-Zugängen.

Problematisch wirken hier zusätzlich die Probleme, die durch die Kopierbarkeit im Cyberspace entstehen. Anders als eine handschriftliche Unterschrift, die per Definition nur die betreffende Person selbst leisten kann, ist die Zuordnung einer Aktivität zu einer konkreten Person in der Regel sehr schwierig, da die Authentifizierungsinformationen wie Passwort oder PIN leicht weitergegeben werden können. Im Cyberspace ist es folglich viel einfacher, die Identität einer anderen Person anzunehmen, als in der realen Welt, was sich im Phänomen des massenhaften Identitätsdiebstahls manifestiert. Begünstigt wird dies durch die Unachtsamkeit vieler Nutzer und die Möglichkeit, durch automatisierte Verfahren deren Zugangsdaten auszuspähen, etwa beim Phishing.

Zunehmend versucht man, das Phänomen des Identitätsdiebstahls durch die Bindung der Authentifikationsinformationen an Hardware wie eine Chipkarte einzudämmen. Dabei ist es allerdings wichtig, dass diese Informationen durch die Hardware *geschützt* gespeichert werden, also nicht ohne weiteres auslesbar sind. Diese Bindung ist etwa bislang bei Kredit- oder EC-Karten nicht gegeben, was sich im Phänomen des *Skimming* äußert.[1] Sind die Authentifikationsinformationen innerhalb der Hardware verborgen, so kann man eine Zugangskennung mit derjenigen Person in Verbindung bringen, die sich im Besitz der Hardware befindet. Dies ist ein erster wichtiger Schritt bei der Zuordenbarkeit einer digitalen Handlung zu einer realen Person. Beispiele für entsprechende Technologien sind viele Chipkarten im Bereich des Online-Banking (das so genannte Chip-TAN-Verfahren) und der neue elektronische Personalausweis.

Ähnlich zu bewerten ist die Identifizierung eines Anschlussinhabers, etwa bei der Auflösung einer IP-Adresse. Allerdings erschweren auch bei der Auflösung von IP-Adressen wieder andere Effekte die Identifizierung. Im Cyberspace können beliebige Systemaktivitäten programmiert werden. Statt einer Person kann also auch eine Maschine als Aktivitätsträger auftreten. Dies geschieht etwa bei der Verwendung von Re-Mailern, Web-Proxies oder Anonymisierungsdiensten wie AnON oder TOR (Dingledine, Mathewson & Syverson, 2004; Köpsell, Federrath & Hansen, 2003). Bei unzureichend gesicherten Kommunikationsverbindungen besteht dadurch auch die Gefahr von Angriffen durch zwischengeschaltete Mittelsmänner, so genannte *Man-in-the-middle*-Angriffe. Hierbei gibt eine dazwischen geschaltete Maschine beiden Kommunikationspartnern wechselseitig vor, dass sie sich mit dem jeweils anderen unterhalten. Tatsächlich sitzt die Maschine zwischen den Kommunikationspartnern und leitet die Nachrichten weiter. Dabei kann sie die Inhalte mitlesen und unter Umständen auch verändern. Dies passiert etwa bei Schadprogrammen, die Transaktionen beim Online-Banking auf dem Rechner des Benutzers manipulieren, bevor diese an die Bank weitergeleitet werden (Holz, Engelberth & Freiling, 2009). Ähnlich funktioniert auch die so genannte *Quellen-Telekommunikationsüberwachung*, bei der sich ein Überwachungsprogramm zwischen das Mikrophon und die Software schaltet, die die Sprachsignale verschlüsselt. Diese Angriffe sind besonders tückisch, da es für sie in der realen Welt kaum Analogien gibt.

Die Verwendung von biometrischen Technologien löst die Probleme nur bedingt. Einerseits müssen die Erkennungsalgorithmen hinreichend robust sein, um eine eindeutige Identifizierung von Personen zu gewährleisten. Andererseits muss sichergestellt werden, dass die verwendete Technologie es nicht erlaubt, über Mittelsmänner oder durch die digitale Einspielung von biometrischen Informationen angegriffen zu werden. So kursierte im Internet der digitale Fingerabdruck des ehemaligen deutschen Innenministers (Chaos Computer Club, 2008).

Inhärente Transnationalität

Die Probleme an den Systemgrenzen setzen sich innerhalb des Systems fort. Dabei spielt die räumliche Entgrenzung des Cyberspace eine wesentliche Rolle, also die Abkopplung des Cyberspace vom geographischen Ausführungsort (siehe Abbildung 1). Die nationalen Grenzen spielen bei der Übertragung von Daten dabei nicht notwendigerweise dieselbe Rolle wie beim Transfer physischer Waren oder beim Grenzübertritt durch Personen. Eine solche räumliche Entgrenzung der Computertechnologie stellt seit jeher ein handfestes Problem für die transnationale Strafdurchsetzung dar. Einerseits betrifft dies Diskrepanzen der jeweils geltenden Strafgesetze, Grundrechte und Grundwertungen am Handlungs- und Erfolgsort, am Ergreifungs- und Verfolgungsort. Andererseits aber sind auch die rechtlichen Schwierigkeiten der Beweissicherung, -erhebung und des Beweistransfers aus Sicht der Ermittlungsbehörden (Gercke & Brunst, 2009, Rdn. 31) und die Gefahren von Parallelermittlungen (*shadow proceedings, forum shopping*) zu diskutieren (Gercke & Brunst, 2009, Rdn. 40 ff.). Dieser Frage widmen wir uns in einem gesonderten Beitrag in diesem Heft (S. 36).

Größe, Geschwindigkeit, Entwicklungsdynamik

Die dynamische, weltweite Entwicklung und Verbreitung der Computertechnologie erzeugt zusätzliche Herausforderungen. Zum einen sind dies technische Herausforderungen, die aus der Geschwindigkeit und Flüchtigkeit der Technologie herrühren. Zum anderen sind die Herausforderungen gesellschaftlicher Natur.

Im Gegensatz zu körperlichen Sachen sind Computerdaten regelmäßig flüchtig. So hinterlässt etwa ein Chat regelmäßig keine Daten auf Festspeichern und auch der Versand einer E-Mail hinterlässt nicht notwendigerweise Spuren auf einem Rechner. Verschlüsselt auf einem Festspeicher abgelegte Daten sind regelmäßig nur vorübergehend im Arbeitsspeicher eines informationstechnischen Systems entschlüsselt verfügbar, der nach Unterbrechung der Stromzufuhr oder jedenfalls nach dem Überschreiben nicht oder nur selten wiederhergestellt werden kann. Dies führt regelmäßig zu Problemen bei der Spurensicherung durch die Ermittlungsbehörden.

Als gegenläufige Strömung ist aus technischer Sicht auch ein umgekehrtes Phänomen zu beobachten, nämlich die massenhafte Ansammlung von Daten auf Datenspeichern. Im privaten Bereich ist es beispielsweise kaum mehr nötig, Dateien, Bilder oder E-Mails zu löschen, weil die Kapazität von Festplatten stetig zunimmt. Außerdem werden bei der individuellen Anpassung von Software, etwa bei der Wahl der persönlichen Benutzungs-

präferenzen, zahlreiche Einstellungen vorgenommen, die persistent gespeichert werden. Aus vielfältigen Gründen wird heute auch vielfach das Verhalten von Benutzern protokolliert, beispielsweise bei der Benutzung von Firmenrechnern, beim Surfen im Internet (durch das Verfolgen von Cookies; s. Steidle & Pordesch, 2008) oder im Rahmen der Beteiligung an sozialen Netzwerken. Schließlich benötigen Suchmaschinen wie Google oder Bing riesige Datenspeicher, um einen einfachen Zugang zu den Informationsressourcen im Netz zu bieten. Die gespeicherten Datenmengen übersteigen mittlerweile mutmaßlich alles, was jemals in nicht-digitaler Form gespeichert wurde. Eine neue Qualität erreicht diese Datenmenge aber aus der Möglichkeit, die gespeicherten Daten automatisiert zu verarbeiten. So können große Textmengen in Sekundenbruchteilen nach Schlüsselwörtern durchsucht werden, und es ist bekannt, dass Nachrichtendienste einen Großteil des Netzwerkverkehrs im Internet automatisiert hinsichtlich bestimmter IP-Adressen, Begriffe oder Zahlenkombinationen wie Telefonnummern analysieren (Bamford, 2002).

Die Verarbeitungsgeschwindigkeit der Computertechnologie birgt insbesondere in Verbindung mit der Kopierbarkeit digitaler Information auch noch andere Herausforderungen. Manipulationen von Finanztransaktionen können bereits binnen weniger Millisekunden zu erheblichen Schäden führen. Datenmengen sind innerhalb weniger Sekunden über Ländergrenzen hinwegzuschaffen und können so schnell dem Zugriff von Strafverfolgungsbehörden entzogen werden. Umgekehrt bieten diese Umstände auch den Nährboden für Plattformen wie WikiLeaks, die darauf basieren, dass man in einfacher Weise und in großen Mengen Daten dem Herrschaftsbereich seiner rechtmäßigen Besitzer entziehen kann. Rechtswidrige Inhalte und urheberrechtlich geschützte Werke können ebenfalls in kürzester Zeit an ein großes Publikum verbreitet werden (Gercke & Brunst, 2009, Rdn. 18). Hinzu treten auch die Schnelligkeit der Weiterentwicklung der Computertechnologie und die damit verbundenen technischen wie rechtlichen Schwierigkeiten für Ermittlungsbehörden, hiermit Schritt zu halten.

Die Automatisierbarkeit und die weltweite Vernetzung führen zu Massenphänomenen und Multiplikatoreffekten, die durch das Internet erst ermöglicht werden oder eine gänzlich neue Bedeutung gewinnen. Eines der bekanntesten Beispiele ist der massenhafte Versand von unerwünschten E-Mails (Spam). Aber auch der massenhafte parallele Zugriff auf eine Website ist problematisch. Dabei ist unerheblich, ob dies durch unabhängige Benutzer geschieht, wie etwa bei der Online-Vergabe der Eintrittskarten zur Fußballweltmeisterschaft 2006, oder durch eine koordinierte Aktivität eines einzigen Cyberkriminellen, etwa durch Nutzung von Tausenden von kompromittierten Rechnern in Form eines *Botnetzes*. Analog sind die Betrugsmaschen, die pro Transaktion einen unscheinbaren Geldbetrag bewegen (beispielsweise den Bruchteil eines Cents) und erst in der millionenfachen Ausführung einen bemerkbaren Schaden erzeugen.

Durch einen einzelnen Eintrag auf einem viel gelesenen Blog kann eine Person aus der Anonymität geholt und zum *Star*, aber auch zum Opfer der öffentlichen Aufmerksamkeit werden. Andererseits aber verschafft das Internet vielen die Möglichkeit, sich selbst zum Urheber, Multiplikator oder Meinungsmacher zu erheben und dabei selbständig gestaltend tätig zu werden.

Ubiquität und Expansion

Das Internet wird inzwischen von etwa drei Milliarden Menschen genutzt, weitere Formen der Computer- und Informationstechnologie dürften die Reichweite des Cyberspace und auch der Cyberkriminalität noch erhöhen. Ein Internetzugang genügt, um – z. T. auch ohne vertieftes technisches Wissen – eine Computerstraftat zu begehen, und um an weitere Tatwerkzeuge wie Spezialsoftware zu gelangen (Gercke & Brunst, 2009, Rdn. 16). Auch angesichts der Abhängigkeit der Informationsgesellschaft von der IT-Infrastruktur ist daher von einer ubiquitären Bedrohungslage auszugehen. Hinzu tritt eine Expansion der im Internet verfügbaren Daten und der über das Internet vorgenommenen Datenübertragungen, welche die effektive Verfolgung von Cyberkriminalität erschweren (Gercke & Brunst, 2009, Rdn. 38 f.). Die Automatisierung der Erkennung rechtswidriger Inhalte und auch die personelle Ausstattung der Strafverfolgungsbehörden und deren Ausbildung haben mit dieser Entwicklung bislang nicht Schritt halten können.

Fragile Technologien

Schließlich muss man immer wieder feststellen, dass moderne informationstechnische Systeme zum überwiegenden Teil noch recht fragil sind. Dies äußert sich nicht nur in der (Un-)Zuverlässigkeit der Hardware, sondern auch in ihrer mangelnden Benutzbarkeit. In der Informationstechnik entscheidet man sich im Zweifel eher für eine größere Systemkomplexität (mehr *Features*) als für kleine und einfache Systeme. In der IT-Branche wird dies häufig als eine „stürmische Entwicklung" bezeichnet. Der Computerpionier Roger Needham hat jedoch dazu treffend festgestellt: "People have said that computing is a fast moving subject and what they mean is that the wheel of re-incarnation goes faster" (Omitola, 2001).

Aus Systemkomplexität folgen neue Systemschwachstellen. Fragestellungen von Nachhaltigkeit, Benutzbarkeit und den gesellschaftlichen Auswirkungen der Informationstechnologie werden durch die Informatik als Disziplin noch nicht mit dem notwendigen Stellenwert behandelt. Durch Technologie verursachte gesellschaftliche Effekte sind meist erst nach Jahren beobachtbar.

Cyberkriminalität – Bedeutung und Relevanz

- Mit der Kommerzialisierung des Internets hat sich eine hochkomplexe digitale Schattenwirtschaft entwickelt
  - mit professioneller, arbeitsteiliger Vorgehensweise
  - geschützt durch legale Unternehmen
  - eigene „Community" (Foren, IRC, DarkNet etc.)
- Hohes Dunkelfeld, unklare Umsätze
  - schätzungsweise Umsätze in der Größenordnung des Drogenhandels
  - ständig neue Maschen, um fast gefahrlos (teilweise legal) Geld zu verdienen
- Daher ökonomische Betrachtung sinnvoll

Felix Freiling, 2015

In diesem Sinne wird der Gewöhnungsprozess der Gesellschaft an die Informationstechnik noch Generationen andauern.

Zusammenfassung

Cyberkriminalität ist ubiquitär geworden. Es gibt kaum eine *klassische* Straftat, die nicht (auch) über das Internet begangen werden kann und auch wird; es gibt kaum eine Straftat, bei der digitale Spuren nicht wertvolles Material für die Strafverfolgungsbehörden sind. Dennoch muss nicht nur die Strafverfolgung auf die Cyberkriminalität reagieren und ihre Ermittlungsmethoden darauf anpassen, sondern auch das materielle Strafrecht: Die veränderten Rahmenbedingungen des Cyberspace schaffen vor allem in Verbindung mit ökonomisch motivierter krimineller Energie neuartige Probleme, auf die sich mit herkömmlichen Straftatbeständen nur unzureichend reagieren ließ.

Danksagung

Dieser Beitrag ist eine überarbeitete Fassung des Abschnitts 5 *Von klassischer Kriminalität zur Cyberkriminalität* aus (Brodowski & Freiling, 2011). Die Überarbeitung ist im Rahmen des BMBF-geförderten Projekts *Open Competence Center for Cyber Security – OpenC3S* entstanden.

Referenzen

Bamford, J. (2002). *Body of secrets: anatomy of the ultra-secret National Security Agency*. New York: Anchor Books.

Brenner, S. W. (2002). Organized cybercrime? How cyberspace may affect the structure of criminal relationships. *North Carolina Journal of Law & Technology, 4* (1), 1–41.

Brodowski, D. (2016). Transnational organised crime and cybercrime. In P. Hauck & S. Peterke (Hrsg.), *International law and transnational organised crime*. Oxford: OUP.

Brodowski, D. & Freiling, F. C. (2011). *Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft*. Berlin: Forschungsforum Öffentliche Sicherheit.

Brunst, P. W. (2009). *Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen: zum Spannungsfeld zwischen einem Recht auf Anonymität bei der elektronischen Kommunikation und den Möglichkeiten zur Identifzierung und Strafverfolgung*. Berlin: Duncker & Humblot.

Chaos Computer Club (2008). Attrappe des Fingerabdrucks von Wolfgang Schäuble. *Die Datenschleuder* (92).

Chawki, M., Darwish, A., Khan, M. A. & Tyagi, S. (2015). *Cybercrime, digital forensics and jurisdiction*. Cham: Springer.

Dingledine, R., Mathewson, N. & Syverson, P. F. (2004). Tor: The second-generation onion router. In *13th USENIX security symposium* (S. 303–320). Berkeley: USENIX.

Gercke, M. (2008). Die Bekämpfung der Internetkriminalität als Herausforderung für die Strafverfolgungsbehörden. *MMR*, 291–298.

Gercke, M. & Brunst, P. W. (2009). *Praxishandbuch Internetstrafrecht*. Stuttgart: Kohlhammer.

Hilgendorf, E. & Valerius, B. (2012). *Computer- und Internetstrafrecht*. 2. Aufl. Berlin: Springer.

Holz, T., Engelberth, M. & Freiling, F. (2009). Learning more about the underground economy: A case-study of keyloggers and dropzones. In M. Backes & P. Ning (Hrsg.), *Computer security – ESORICS 2009: 14th european symposium on research in computer security*. Berlin: Springer.

Köpsell, S., Federrath, H. & Hansen, M. (2003). Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes. *DuD, 27* (3), 139–142.

Krebs, B. (2014). *Spam nation*. Naperville: Sourcebooks.

Kshetri, N. (2010). *The global cybercrime industry: economic, institutional and strategic perspectives*. Berlin: Springer.

Omitola, T. (2001). ACM fellow profile: Roger Needham. *Software Engineering Notes, 26* (1).

Sieber, U. (2012). *Straftaten und Strafverfolgung im Internet. Gutachten C zum 69. Deutschen Juristentag*. München: Beck.

Spoenle, J. (2010). Underground economy. In M. Bellini, P. Brunst & J. Jähnke (Hrsg.), *Current issues in IT security* (S. 67–79). Berlin: Duncker & Humblot.

Steidle, R. & Pordesch, U. (2008). Im Netz von Google. Web-Tracking und Datenschutz. *DuD, 35* (5), 324–329.

Wall, D. (2007). *Cybercrime*. Cambridge: Polity Press.

Wall, D. (2010). The organization of cybercrime and organized cybercrime. In M. Bellini, P. Brunst & J. Jähnke (Hrsg.), *Current issues in IT security* (S. 51–66). Berlin: Duncker & Humblot.

Anmerkung

1 Bei deutschen EC-Karten gibt es zwar ein Merkmal, das die Karteninformationen an die Karte selbst bindet (moduliertes Merkmal). Um auch im Ausland Geld abheben zu können, enthalten die Karten allerdings zudem einen leicht auslesbaren Magnetstreifen.

Dominik Brodowski und Felix Freiling

Dr. **Dominik Brodowski**, LL.M. (UPenn) ist wissenschaftlicher Mitarbeiter im strafrechtlichen Teilvorhaben des *Open Competence Center for Cyber Security* (OpenC3S) an der Johann Wolfgang Goethe-Universität Frankfurt am Main und Lehrbeauftragter im Masterstudiengang *Digitale Forensik* an der Hochschule Albstadt-Sigmaringen.

Prof. Dr. **Felix Freiling** ist Inhaber des Lehrstuhls für IT-Sicherheitsinfrastrukturen an der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU). Schwerpunkte seiner Arbeitsgruppe in Forschung und Lehre sind offensive Methoden der IT-Sicherheit, technische Aspekte der Cyberkriminalität sowie digitale Forensik (IT-Beweismittelsicherung und -analyse).

Carlo Schäfer

Die Rolle von Spam im Cybercrime

Weltweit werden jeden Tag durchschnittlich mehr als 28 Milliarden Spam- und Phishing-Nachrichten (Wood et al., 2015, S. 12) versandt, das entsprach im September 2015 einem Anteil von 52,2 Prozent aller E-Mail-Nachrichten (Nahorney, 2015, S. 17). Davon wiederum haben etwa 76 Prozent ihren Ursprung in Botnetzen (Wood et al., 2014, S. 14). Vieles im Cybercrime beginnt mit einer einfachen E-Mail: Spam- und Phishing-Nachrichten sind ein zentrales Einfallstor für Computerkriminalität – und Botnetze die geeigneten Werkzeuge zu ihrer Verbreitung. Was also kann, was muss getan werden?

Die Versender von Spam- und Phishing-Nachrichten verwenden unter anderem kompromittierte E-Mail-Accounts (also E-Mail-Konten, deren Zugangsdaten Unberechtigten bekannt geworden sind), um ihre unerwünschten Nachrichten massenhaft über fremde *Simple Mail Transfer Protocol* (SMTP)-Server (Klensin, 2008) zu ihren Bestimmungsorten zu verteilen. Erst dadurch wird es möglich, einen niedrigen Schwarzmarktpreis für die Versendung zu realisieren. Dieser liegt zwischen 70 und 150 (US-) Dollar (Wood et al., 2015, S. 17) für eine Spamkampagne, die an eine Million verifizierter, also auf Existenz und Erreichbarkeit geprüfter, E-Mail-Adressen gerichtet ist.

Die „Service-Leistung" besteht dabei nur in der Auslieferung von Spam an die gebuchten E-Mail-Adressen. Möchte der Auftraggeber die E-Mail-Adressen selbst kennen, um sie erneut oder für andere Zwecke zu benutzen, ist dies teurer; dennoch bezahlt man für 1.000 (zum Beispiel durch das Auslesen von kompromittierten E-Mail-Konten) gestohlene E-Mail-Adressen auch nur bis zu 10 Dollar (Wood et al., 2015, S. 17). Diese Preise zeigen, dass der eigentliche Versandvorgang fast keine Kosten verursacht. Und ein derart geringer Preis wiederum erhöht natürlich für die Auftraggeber den Anreiz zur massiven Verbreitung unerwünschter Nachrichten.

Es wird geschätzt, dass Computerkriminalität im Jahre 2014 weltweit einen volkswirtschaftlichen Gesamtschaden von circa 400 Milliarden Dollar verursacht hat (die Angaben schwanken zwischen 375 Milliarden und 575 Milliarden Dollar) – dies übersteigt die gesamte Wirtschaftsleistung mancher Staaten. Auf die USA, China und Deutschland – drei der vier größten Wirtschaftsnationen – entfielen davon zusammengerechnet etwa 200 Milliarden Dollar. Dabei sind 160 Milliarden Dollar Schaden allein durch den Diebstahl von weltweit 800 Millionen persönlicher Datensätze, wie zum Beispiel gestohlener Kreditkarteninformationen, entstanden (CSIS, 2014, S. 2 f.).

Botnetze

Wegen der hohen Verbreitung sind Botnetze eines der größten Risiken für die Internetsicherheit. Die Gefahr von Botnetzen geht von ihrer großen Anzahl an kontrollierten Bots aus. Erst damit wird es möglich, Computer mit einer *Distributed Denial of Service* (DDoS)-Attacke anzugreifen oder eben eine große Anzahl an unerwünschten E-Mails zu versenden (Ianelli & Hackworth, 2005, S. 7). Die Anzahl bekannter Bots ist im Jahr 2014 zwar auf 1,9 Millionen gesunken, im Vergleich zu 2,3 Millionen im Jahr 2013 bzw. 3,4 Millionen im Jahr 2012. In großen Aktionen haben das FBI, das *European Cybercrime Centre* (EC3) von Europol und andere Regierungsbehörden mit Technologie-Unternehmen zusammengearbeitet, um Botnetze ausfindig zu machen und anschließend zu deaktivieren (Wood et al., 2015, S. 97). Dadurch sollte der entstandenen Gefahr Einhalt geboten werden.

Spam und Botnetze in Symbiose

- Spam führt zur Verteilung von Bots
- Bots werden zum Versand von Spam verwendet
- Wie kann man mittels Spam Bots verteilen?
  - Ausführbare Datei im Anhang
  - Drive-by-Download bei verwundbarem Browser
  - Client-side Exploit bei verwundbarer Anwendung (z. B. Adobe Reader)
- Heute Stand der Technik: Template-based Spamming
- Neue Verbreitungswege: Twitter

Felix Freiling, 2015

Im August 2015 stellte dennoch fast jede zweitausendste E-Mail einen Phishing-Versuch dar, und durchschnittlich eine von 250 Nachrichten war mit Malware (Viren, Würmer, Trojaner) versehen. Täglich kamen 1,5 Millionen neue Malware-Varianten hinzu (Nahorney, 2015, S. 8–11). Die Urheber derart verseuchter Nachrichten bezwecken damit, die eigene Malware weiter zu verbreiten, um das Botnetz zu vergrößern, sowie Daten auszuspionieren. Einmal auf einem Gerät eingeschleust, kann die Malware – etwa über Keylogger, die jede Tastatureingabe protokollieren – Online-Banking-Passworte, Kreditkartennummern, Zugangsdaten für E-Mail-Accounts oder ähnliches auslesen, die dann weitergenutzt oder wiederum auf dem Schwarzmarkt verkauft werden.

Spamming

Massive Spam-Verteilung ist deutlich anspruchsvoller als ein reiner DDoS-Angriff. Für DDoS-Attacken braucht man nur einen Internetzugang, um darüber zum Beispiel *Domain Name System* (DNS)-Abfragen oder Aufrufe von Internetseiten zu tätigen, und kommt somit mit Bordmitteln des Betriebssystems aus.

Um Spam- und Phishing-Nachrichten im großen Stile zu versenden, werden dagegen ein offener *SMTP-Relay-Server* oder eben gültige Zugangsdaten für einen bestehenden SMTP-Server benötigt. Die Verbreitung unerwünschter Nachrichten wird zusätzlich dadurch erschwert, dass aktuelle Anti-Spam-Engines fast keine Nachrichten von dynamischen IP-Adressen annehmen (wie sie Bots vorwiegend besitzen), die mittels *DNS-based*

Blackhole List (DNSBL) – einer Art Schwarzen Liste zur Spam-Bekämpfung – propagiert werden (The Spamhaus Project, 2015).

Offene SMTP-Server sind glücklicherweise eher selten und werden gleichfalls in DNSBL geführt, womit sie an Relevanz verlieren. Im Gegensatz dazu sind Zugriffe mit validen Zugangsdaten zu einem SMTP-Server vor DNSBL geschützt, da E-Mail-Provider ihren Kunden die Möglichkeit geben möchten, E-Mail von jedem Internetzugang aus versenden zu können.

Phishing

Durch Phishing-Nachrichten selbst bzw. auf Internetseiten, die in den E-Mails verlinkt sind, wird versucht, an die verschiedensten Zugangsdaten von Nutzern zu gelangen – und damit Identitätsdiebstahl zu begehen. Ziele sind unter anderem Bankkonten, Konten von Bezahlsystemen wie PayPal, Zugänge zu Versandhäusern sowie Online-Auktionshäusern – oder eben auch E-Mail-Zugänge, die zur weiteren Verbreitung solcher Nachrichten missbraucht werden. Im Jahre 2013 begannen 95 Prozent (Verizon, 2015, S. 12) aller im öffentlichen Sektor erkannten Cyberspionage-Vorfälle mit einer Phishing-Nachricht – und trotz großer Bemühungen war es bisher nur möglich, diesen Anteil auf 66 Prozent im ersten Halbjahr 2015 zu senken. Dabei deuten Daten von *Verizon Enterprise Solutions* darauf hin, dass aktuell immer noch 23 Prozent aller Empfänger von Phishing-Nachrichten diese öffnen und 11 Prozent auf Anhänge klicken (Verizon, 2015, S. 12).

Aus diesen Daten lässt sich ableiten, dass fast alles Unglück mit einer E-Mail beginnt. Spam- und Phishing-Nachrichten bilden ein zentrales Einfallstor für Computerkriminalität. Darum ist ja der Markt der Anti-Spam-Engines so gut vertreten. Dass diese Produkte außerdem recht gute Erkennungsraten besitzen, um die Mailboxen der Anwender vor solchen unerwünschten Nachrichten zu schützen, gibt Anlass zur Hoffnung. Aber durch dieses Vorgehen werden nur die Symptome, leider jedoch nicht die Ursachen bzw. Quellen der Spam- und Phishing-Nachrichten bekämpft.

Die Verursacher sind eher selten und nur mit großem Aufwand ausfindig zu machen und entziehen sich selbst dann häufig einer Bestrafung. Wohingegen die Quellen schnell gefunden sind: es sind vorwiegend die unzähligen Bots. Diese Bots sind aber meist nur der Ort der Erzeugung unerwünschter Nachrichten. Für die eigentliche Versendung missbrauchen die Bots jedoch häufig andere Rechner, insbesondere auch solche, zu deren E-Mail-Systemen sie sich unberechtigt Zugang verschaffen können. Auf diese Weise kann der Spammer auch seine Identität verbergen, da die Empfänger der – gefälschten – Nachrichten nur die IP-Adressen der missbrauchten E-Mail-Systeme sehen, aber nicht die der Bots.

Phishing und Pharming

- Definition nach Arbeitsgruppe *Identitätsschutz im Internet* (a-i3)
- „Verfahren, bei denen ein Täter mit Hilfe gefälschter E-Mails vertrauliche Zugangs- und Identifikationsdaten von arglosen Dritten zu erlangen versucht."
- Pharming: Phishing via DNS-Manipulation
  - Manipulation des lokalen DNS-Resolvers
  - Modifikation der lokalen HOSTS-Datei
  - DNS cache poisoning/pollution bei verwundbaren DNS-Servern
- Besonders tückisch, da üblicherweise DNS vertraut wird

Felix Freiling, 2015

Die übliche Vorgehensweise

Ein Ziel effektiver Spam-Bekämpfung müsste es sein, kompromittierte Accounts zu erkennen, da erst diese es ermöglichen, den SMTP-Server zu missbrauchen. Durch Deaktivierung oder Blockierung dieser Accounts würde der Spam- und Phishing-Versand sofort und unmittelbar an der Quelle reduziert. E-Mail-Provider müssten nicht mehr befürchten, dass ihre eigenen Server auf verschiedenen DNSBL landen; letzteres bedeutet ja regelmäßig, dass sie von der Außenwelt faktisch abgeschnitten sind oder der reguläre ausgehende E-Mail-Verkehr maßgeblich beeinträchtigt ist.

Wenn der Fokus auf eine schnelle Erkennung von kompromittierten Accounts gelegt wird, kann die Integrität weiterer Systeme gewahrt werden, wie zum Beispiel die des Mailboxservers, der das eigentliche Konto mit allen E-Mails vorhält. Auf diesem Server befinden sich valide E-Mail-Adressen – von denen jede einzelne E-Mail mindestens je eine als Absender bzw. Empfänger enthält –, die auf dem Schwarzmarkt sehr begehrt sind. Und unglücklicherweise sind die Zugangsdaten für den Mailboxserver meistens mit denen für den SMTP-Server identisch. Die Folgen eines missbrauchten Kontos haben auch Auswirkungen auf die komplette E-Mail-Infrastruktur des E-Mail-Providers, da alle anderen Kunden in Mitleidenschaft gezogen werden, wenn die Server durch die vom Spammer erzeugten Nachrichten überlastet sind oder andere E-Mail-Provider die Annahme von Nachrichten verzögern oder sogar ablehnen.

Carlo Schäfer

Carlo Schäfer ist Diplom-Informatiker und arbeitet an der Friedrich-Schiller-Universität Jena im Bereich E-Mail und IT-Sicherheit. Zuvor war er mehrjährig Projektleiter für Spam-Abwehr im Thüringer Landesrechenzentrum.

Meistens wird die Erkennung kompromittierter SMTP-Accounts vernachlässigt. In den wenigsten Umgebungen werden ausgehende Nachrichten durch Spamfilter analysiert, da nicht klar ist, was man anschließend mit diesen Nachrichten anfängt. Zustellen möchte man den Spam nicht; aber den Absender kann oder will man gegebenenfalls auch nicht informieren, da die vorgebliche Absenderadresse gefälscht sein könnte. Vom Gesetzgeber her ist es auch nicht gestattet, E-Mails einfach zu löschen (Heckmann, 2014, Kap. 8, Rn. 207). Somit sind der Aufwand und die entstehenden Probleme der Spamkontrolle von ausgehenden Nachrichten nicht wirklich zu rechtfertigen.

Am weitläufigsten ist daher die Limitierung der Anzahl an E-Mails (in einem definierten Zeitintervall) je IP-Adresse oder besser sogar je Konto. Dadurch werden aber wiederum nur die Symptome des Spam-Versands behandelt, die Konten jedoch bleiben dagegen meistens unangetastet oder werden erst durch manuelle Kontrolle von Mitarbeitern des E-Mail-Providers gesperrt. In den wenigsten Umgebungen werden die Server rund um die Uhr von Administratoren überwacht, was zur Folge hat, dass außerhalb der Regelarbeitszeit tagsüber sowie an Wochenenden, Feiertagen oder in der Urlaubszeit diese SMTP-Server ihrem Schicksal überlassen werden. In dieser Zeit werden weitere Spam- und Phishing-Nachrichten zu Tausenden erzeugt – bis ein Mitarbeiter diesem Vorgang schließlich doch Einhalt gebietet.

Wirkungsvolle Abhilfe

Eine schnelle Erkennung und Reaktion ist nötig, um Anomalien von missbrauchten Konten festzustellen. Dadurch wird direkt der Ursprung von Spam- und Phishing-Nachrichten bekämpft, und die Auswirkungen auf die eigene E-Mail-Infrastruktur werden auf ein Minimum reduziert.

Neue Methoden und Ansätze, welche diese Anforderung umsetzten, sind bereits veröffentlicht. Diese erkennen wesentlich schneller und zuverlässiger einen Kontenmissbrauch, als dies aktuell verbreitete Methoden ermöglichen. Dabei wird nicht der E-Mail-Inhalt analysiert; allein das Kontenverhalten verrät, ob verschiedene Bots (Schäfer, 2014) oder andere Personen (Schäfer, 2015) das Konto missbrauchen. In manchen Umgebungen ist es aus datenschutzrechtlichen Gründen nicht gestattet oder technisch auch gar nicht möglich (z. B. bei Anwendung von E-Mail-Verschlüsselung), auf den Inhalt von E-Mails zuzugreifen, sodass eine inhaltsbasierte Spam-Erkennung ohnehin nicht realisierbar wäre. Durch die angesprochene Anomalie-Erkennung ist es nun tatsächlich möglich, innerhalb von Sekunden zu reagieren und die Anzahl der Spam- und Phishing-Nachrichten auf einen Bruchteil zu reduzieren.

Die letzte Herausforderung ist nun, diese Ansätze zur Bekämpfung der lokal erzeugten Spam- und Phishing-Nachrichten so schnell wie möglich in breite Anwendung zu bringen, so dass der Computerkriminalität ein Teil der (finanziellen) Handlungsgrundlage entzogen wird. Vor einer finanziellen Belastung, etwa als Folge von kostenaufwändigen Plausibilisierungen und technischen Anforderungen, sollte man sich nicht scheuen, da diese durch die gewonnene Sicherheit zeitnah refinanziert wird.

Referenzen

CSIS (2014). Net Losses: Estimating the Global Cost of Cybercrime. Center for Strategic and International Studies, June 2014. URL: http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

Heckmann, D. (Hrsg.) (2014). juris PraxisKommentar Internetrecht. Telemediengesetz, E-Commerce, E-Government. 4. Aufl. Saarbrücken: juris.

Ianelli, N. & Hackworth, A. (2005). Botnets as a vehicle for online crime. Bd. 1. CERT Coordination Center. URL: https://resources.sei.cmu.edu/asset_files/WhitePaper/2005_019_001_51249.pdf

Klensin, J. (2008). Simple Mail Transfer Protocol. Network Working Group, October 2008. URL: https://tools.ietf.org/html/rfc5321 (Stand: 05.01.2016)

Nahorney, B. (2015). Symantec Intelligence Report September 2015. Symantec Corporation. URL: http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_09-2015.en-us.pdf

Schäfer, C. (2014). Detection of Compromised E-Mail Accounts used by a Spam Botnet with Country Counting and Theoretical Geographical Travelling Speed Extracted from Metadata. In Proc. 2014 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Nov. 2014, S. 329–334. URL: http://dx.doi.org/10.1109/ISSREW.2014.32

Schäfer, C. (2015). Detection of Compromised E-Mail Accounts used for Spamming in Correlation with Mail User Agent Access Activities Extracted from Metadata. In Proc. 2015 IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), May 2015. URL: http://dx.doi.org/10.1109/CISDA.2015.7208641

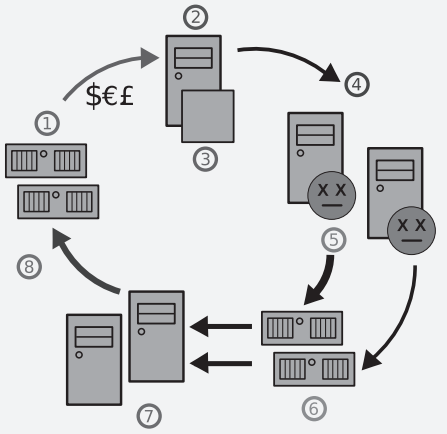
The Spamhaus Project (2015). The Policy Block List. The Spamhaus Project Lt. URL: https://www.spamhaus.org/pbl/ (Stand: 05.01.2016)

Verizon (2015). 2015 Data Breach Investigations Report. Verizon Enterprise Solutions. URL: http://www.verizonenterprise.com/de/DBIR/2015/

Wood, P. et al. (2014). Internet Security Threat Report 2014. Bd. 19. Symantec Corporation. URL: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Wood, P. et al. (2015). Internet Security Threat Report 2015. Bd. 20. Symantec Corporation. URL: https://know.elq.symantec.com/LP=1542

Kreislauf des Spamverkehrs im Internet



(1) Spamwebseite
(2) Spammer
(3) Spam
(4) Infizierte Computer
(5) Virus oder Trojaner
(6) E-Mail-Server
(7) Computernutzer
(8) Internetverkehr

Fubar Obfusco & Admrboltz, CC BY-SA 2.5

Stefan Jäger

Wardriving – die unterschätzte Gefahr

Wardriving ist normalweise nur denjenigen ein Begriff, die sich mit WLAN oder generell Funknetzen beschäftigen. Doch ist oft nicht genau bekannt, um was es sich hierbei handelt. Ist es legal oder illegal, kann es von jedermann oder nur von Fachleuten durchgeführt werden, usw.? Zudem stellt sich die Frage nach dem Zweck dieser Tätigkeit und den daraus resultierenden Einsatzgebieten. Auch ist die Aktualität des Themas zu klären. Gemessen an der Anzahl an Beiträgen in den analogen und digitalen Medien, ist es um das Wardriving seit 2008 sehr ruhig geworden. Generell wird das Thema WLAN-Sicherheit seit der faktischen Umsetzung des WPA2-Standards, etwa im Jahre 2006, kaum noch in der Breite und Tiefe behandelt. Aber ist mit Einführung des WPA2-Standards die Notwendigkeit tatsächlich entfallen, sich mit WLAN-Sicherheitsmechanismen auseinanderzusetzen?

Aber zunächst: was ist eigentlich Wardriving? Nachfolgend zwei unterschiedliche Definitionen:

1. „**Wardriving** ist das systematische Suchen nach *Wireless Local Area Networks* mit Hilfe eines Fahrzeugs. Der Begriff leitet sich von *Wardialing* ab, einer Methode, mittels Durchprobieren vieler Telefonnummern offene *Modem*-Zugänge zu finden. Einige Wardriver sehen die drei Anfangsbuchstaben dabei als *Backronym* für ‚Wireless Access Revolution'."[1]

2. „**War-Driving** Bezeichnet das unbefugte Eindringen in fremde WLANs, das oft vom Auto aus mit dem Laptop durchgeführt wird (daher ‚driving')."[2]

Zwei Definitionen, welche jede für sich einen anderen Schwerpunkt auf die Thematik legen. Die offizielle Definition des *Bundesamtes für Sicherheit in der Informationstechnik* (BSI) ist formal gesehen sogar falsch, da das Wardriving nur das Auffinden von offenen oder schlecht geschützten Funknetzen verfolgt. Das BSI unterstellt dieser Tätigkeit, möglicherweise allein schon wegen der Begriffskomponente *War,* von vornherein eine kriminelle Absicht. Dabei hängt es (wie bei fast jeder Tätigkeit) vom Einzelnen ab, ob Wardriving für gute oder schlechte Zwecke eingesetzt wird.

Der Begriff *Wardialing,* von dem die Bezeichnung Wardriving abgeleitet ist, wurde durch den Film *WarGames* geprägt. Dort wurde mithilfe eines Modems jede Telefonnummer in einem bestimmten Nummernbereich angerufen. Ziel war es, hierdurch einen Computer zu finden, in welchen man anschließend eindringen konnte.

Abbildung 1: Wardriving damals …
Foto: Rudolf Mittelmann

Wardriving in seiner heute üblichen Form wurde erstmals im Vortrag[3] von Peter Shipley auf der Konferenz *DefCon* im Jahre 2001 vorgestellt. Shipley hatte zuvor über einen Zeitraum von 18 Monaten nach Funknetzwerken in Berkeley gesucht.

Ausrüstung

Mittlerweile hat sich weltweit eine große (in einzelne länderbezogene Gruppen aufgeteilte) Wardriving-Community gebildet. Dieses Interesse rührt nicht zuletzt von den folgenden drei Gegebenheiten her:

- Wardriving befriedigt den natürlichen Sammlertrieb des Menschen.
- Wardriving kommt dem Entdeckerdrang des Menschen entgegen.
- Man braucht heutzutage zum Wardriving kaum noch spezielle Hardware.

Benötigte man in der Anfangszeit des Wardriving noch einen Laptop, einen GPS-Empfänger und eine externe WLAN-Antenne (Abbildung 1), kann dies heutzutage alles durch ein normales Smartphone ersetzt werden.

Neben diesen technischen Voraussetzungen bringen Smartphones durch große *App Stores* auch alle notwendigen Applikationen mit. Umfangreiche Softwaresammlungen sind also nicht mehr zwingend notwendig. Für jedes gängige Betriebssystem lassen sich die Tools bzw. Apps leicht aus dem Internet herunterladen (illegal sind sie nicht). Durch die Verwendung nutzerfreundlicher Apps wird auch keinerlei Vorwissen oder tiefgrei-

… und heute
Frame aus WiFi Tracker

fendes technisches Verständnis mehr benötigt. Der Anwender muss lediglich eine Applikation starten und bekommt dann unmittelbar die gefundenen Netzwerke auf einer Karte angezeigt. Hinzu kommt, dass eine nutzerbezogene Entscheidung, welche Netzwerke tendenziell unsicher sind, bereits durch die App gefällt und entsprechend eingefärbt auf der Karte dargestellt wird (Abbildung 2).

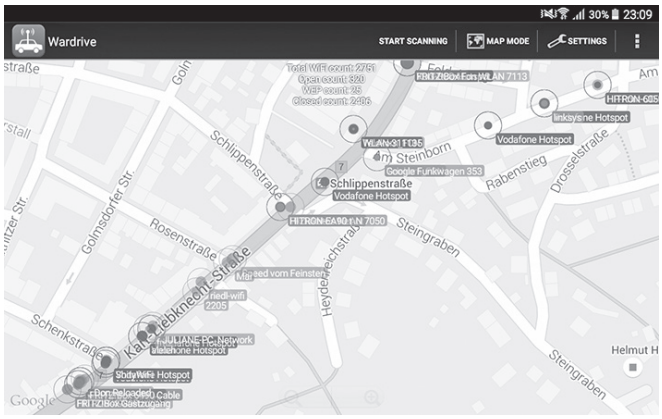


Abbildung 2: Streetmap
eigene Aufnahme vom 21.11.2015

In der Datenbank der Community *wardriving-forum.de* befinden sich fast 18 Millionen *Access Points*[4] (Abbildung 3, Stand 21.11.2015). Auf der Kartendarstellung sind deutlich die Umrisse Deutschlands zu erkennen.

In der Datenbank der Community *wigle.net* befinden sich über 225 Millionen Access Points weltweit, welche von über 28.000 Mitgliedern erfasst wurden (Abbildung 4, Stand 30.11.2015).

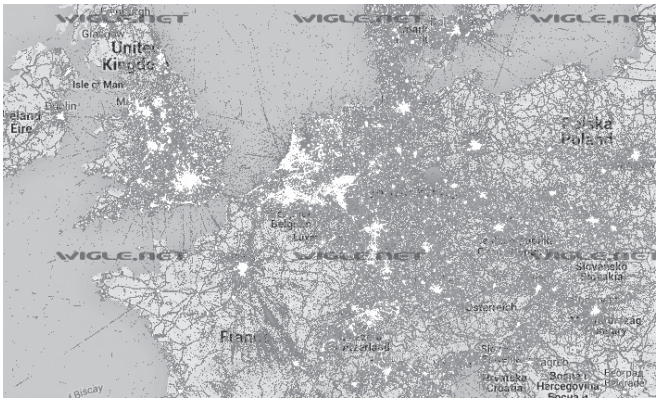


Abbildung 4: Screenshot von Access Points, Quelle: wigle.net
Die Bilddaten stammen von google, Map data ©2015 Google

Gefahren

Es stellt sich die Frage, warum Wardriving überhaupt diskutiert wird und ob von Wardriving eine Gefahr ausgeht. Diese Frage muss leider bejaht werden. Die Scansoftware wertet die erfassten Netzwerke in Echtzeit aus und zeigt offene sowie (z. B. wegen Einsatz von WEP[5]) potenziell schlecht gesicherte Netzwerke sofort an. Diese Netzwerke können von Angreifern missbraucht werden. Ein mehrminütiger Scan innerhalb einer Großstadt reicht (aus eigener Erfahrung) aus, um trotz evtl. vorhandener Sicherungsmechanismen hinreichend viele WLANs zu lokalisieren, auf die aussichtsreiche Angriffe gestartet werden könnten. Alternativ können über die bereits erwähnten Communities potenzielle Opfer auch bequem über die Karte ausgewählt werden. Anschließend kann man mit der benötigten Technik für den Angriff an den Zielort zurückkehren.

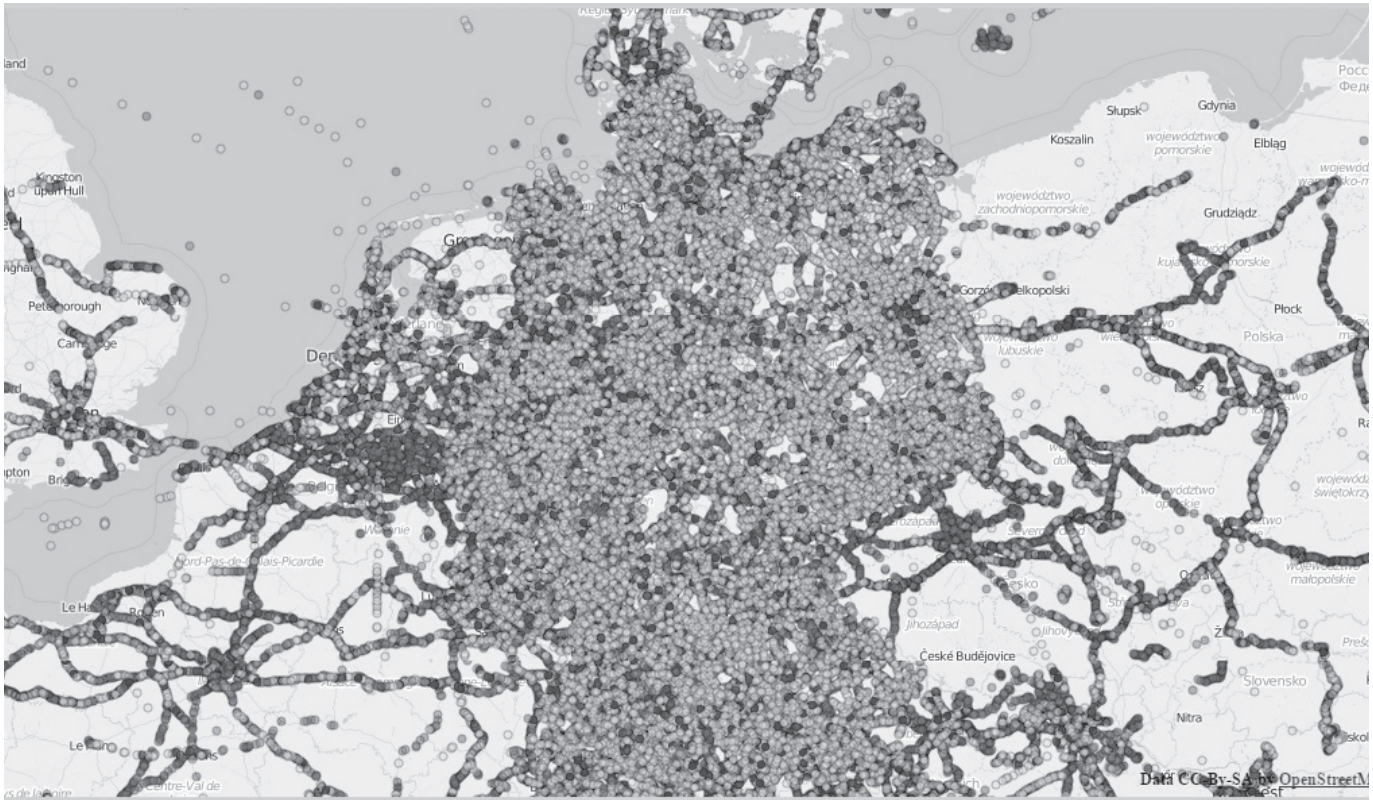


Abbildung 3: Screenshot von Access Points, Quelle: wardriving-forum.de
Diese Karte wird mit Hilfe von OpenLayers und OpenStreetMap erstellt, Stand: 21.11.2015

Sobald die WEP-Verschlüsselung überwunden wurde oder die Einwahl in ein offenes WLAN erfolgt ist, kann das Netzwerk für folgende Aktivitäten missbraucht werden:

- kostenfreies Surfen im Internet
- Auslesen von Dateien im Intranet
- Auslesen des Netzwerkverkehrs, z. B. Zugangsdaten, Kreditkartendaten, …
- Manipulation des Netzwerkverkehrs, z. B. beim Onlinebanking
- Einschleusen von Schadcode, z. B. Botnet-Client, Trojaner, …
- Angriff auf andere Rechner im Internet
- illegales Filesharing, Versand strafbarer Inhalte, Massenversand von E-Mail
- Übernahme von mit dem WLAN verbundenen Alltagsgeräten

Handelt es sich hierbei um eine konstruierte oder eine realistische Bedrohung? Wird dies nur von einigen wenigen Kriminellen oder Scriptkiddies ausgenutzt? Hierzu ein Beispiel aus den Medien: *Im Jahre 2011 konnte die Polizei in Seattle eine Bande festnehmen, welche über fünf Jahre hinweg in schlecht gesicherte Funknetze eingebrochen ist und so wertvolle Informationen stehlen konnte.*[6]

Für den WLAN-Betreiber ist es schwer bis unmöglich, einen solchen Angriff festzustellen. Das größte Problem ist allerdings das mangelnde Sicherheitsbewusstsein in der Bevölkerung. Zum einen wird davon ausgegangen, dass die erworbenen WLAN-Router bereits bei Inbetriebnahme ausreichend geschützt sind. Sowohl dieser Trugschluss als auch die Tatsache, dass von den Herstellern benutzte Standardeinstellungen inkl. Standardpasswort auch (vermeintlich) gut gesicherte WPA2-Netzwerke[7] angreifbar machen, sind sehr beunruhigend. Hinzu kommt ein unbegründetes Sicherheitsgefühl, da kaum jemand davon ausgeht, dass der eigene Internetanschluss für Straftaten missbraucht werden könnte.

Am Vorliegen mindestens eines der folgenden Punkte erkennt ein Angreifer sofort, ob es sich beim gescannten Netzwerk um ein potenzielles Ziel handelt:

- das Netzwerk ist offen
- das Netzwerk ist nur WEP-verschlüsselt
- der verwendete WLAN-Router stammt von einem Hersteller, dessen Geräte für Fehler und schlechte Programmierung bekannt sind
- bei dem sichtbaren Namen des WLAN handelt es sich um einen Standardnamen, welcher vor dem Verkauf automatisch vom Hersteller vergeben wird (hier ist die Chance sehr hoch, mit einem Standardpasswort eindringen zu können)

Um in ein WEP-geschütztes Netz einzubrechen, bedarf es weder starker Rechenleistung noch umfangreichen Vorwissens (vgl. dazu einschlägige YouTube-Videos im Netz). Neben einem Smartphone als Wardriving-Ausrüstung genügt z. B. ein *Raspberry Pi*[8] an einer Powerbank mit angeschlossenem WLAN-USB-Adapter (Abbildung 5), um WEP zu brechen. Über den WLAN-Adapter kommuniziert der *Raspberry Pi* mit dem Smartphone (oder z. B. einem Tablet), von wo aus er über eine SSH-App[9] gesteuert wird.

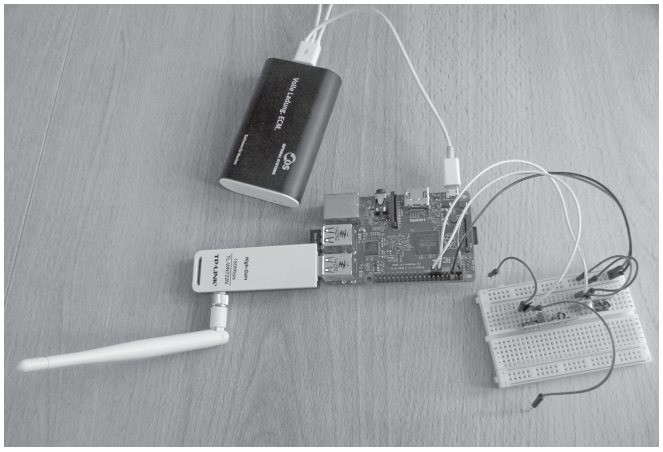


Abbildung 5: Raspberry Pi als modernes Hilfsmittel für Wardriving. Foto: eigene Aufnahme

Aber auch WPA2-geschützte Netzwerke sind mit einer solchen Ausrüstung erfolgreich angreifbar. Das WLAN-Passwort muss ja nicht unbedingt vor Ort entschlüsselt werden. Ist beispielsweise bekannt, dass an einem bestimmten Tag zu einer bestimmten Uhrzeit interessante Informationen über das WLAN übertragen werden sollen, so können alle zu diesem Zeitpunkt übertragenen Datenpakete empfangen und gespeichert werden. Wird im gleichen Zug ein Handshake[10] mit aufgezeichnet, kann zu einem beliebigen späteren Zeitpunkt versucht werden, das Passwort zu entschlüsseln (z. B. in einem leistungsstarken Rechnerverbund). Ist dies gelungen, können die aufgezeichneten Pakete nachträglich lesbar gemacht werden. Es ist zudem möglich, über das WLAN übertragene Druckaufträge zu rekonstruieren und in einer Datei abzuspeichern.

Mittels Wardriving lassen sich aber nicht nur Netzwerke in Gebäuden oder Plätzen erfassen. Auch mobile Hotspots von Notebooks oder mobilen Endgeräten können hierbei erfasst werden. Eine gänzlich neue Gefahr stellt WLAN in Fahrzeugen dar. Sollte das Fahrzeug gehackt und dadurch nicht mehr durch den Fahrer kontrolliert werden können, kann dies lebensbedrohlich enden.[11] Aufsehen erregten die Erfolge von Dr. Charlie Miller (ehemals NSA-Mitarbeiter) und Chris Valasek, welchen es gelang, aus großer Entfernung die Kontrolle über einen Jeep zu übernehmen.[12] Das vom Bund geförderte Sim^{TD}-Projekt soll in Zukunft Verkehrsdaten in Echtzeit erfassen und die vorhandenen Fahrerassistenzsysteme des Fahrzeugs erweitern.[13] Auch bei diesem – auf dem WLAN-Standard basierenden – System besteht die Gefahr der Übernahme durch einen Angreifer und des Verlusts der Fahrzeugkontrolle.

Neben der Vielzahl an Schwächen oder sogar Programmierfehlern in der Steuersoftware/Firmware von WLAN-Routern gibt es auch Schwächen in den Sicherheit suggerierenden werksseitig vergebenen Passwörtern der verkauften WLAN-Router. Auf

legalen wie illegalen Hackerseiten finden sich mittlerweile eine ganze Reihe entdeckter Probleme hinsichtlich der in WLAN-Routern verwendeten Standardpasswörter. In einigen Fällen konnte der Algorithmus zur Generierung der Standardpasswörter bestimmt werden. Auch letzteres ist sehr problematisch, da einige Hersteller von WLAN-Routern das Standardpasswort (oder zumindest Teile davon) mehr oder weniger direkt aus der MAC-Adresse und dem ebenfalls voreingestellten Netzwerknamen (SSID) der WLAN-Schnittstelle berechne(te)n[14] und diese Werte meist vom WLAN-Router bekanntgegeben werden[15].

Der WLAN-Router-Hersteller Arcadyan hat 2008 seinen Algorithmus zur Generierung des Standardpasswortes für seine Geräte in Deutschland sogar zum Patent angemeldet[16] und damit freiwillig öffentlich gemacht. Standardpasswörter für Geräte anderer Anbieter, die Arcadyan-Komponenten verwendeten, wurden gleichfalls nach diesem Algorithmus berechnet, dies betraf in Deutschland z. B. Arcor, EasyBox und Vodafone. Auf Basis der ausführlichen Patentbeschreibung wurden von privater Seite einige Passwortgeneratoren[17] erstellt und zum kostenlosen Download bereitgestellt. Durch Variation der Netzwerknamen blieben für jeden der drei genannten Anbieter nur noch 65536 mögliche Passwörter übrig, die selbst von einem älteren Notebook innerhalb weniger Sekunden getestet werden konnten. Sicherheitsvorkehrungen, wie beispielsweise eine Beschränkung der Anmeldeversuche pro Minute, sind hier wirkungslos, da die Passwörter an aufgezeichneten Datenpaketen getestet werden können. Zudem gibt es eine Vielzahl an Internetseiten, auf welchen gefundene Standardpasswörter und Algorithmen[18] aufgelistet sind; dort kann man auch gut nach bestimmten Gerätetypen und -modellen suchen. Diese Beispiele sollten zum Nachdenken darüber anregen, ob wir uns nicht sicherer fühlen als wir tatsächlich sind.

Neue Ansätze bringt die LINUX-basierte Open-Source-Software *Snoopy-NG* mit sich. Das Tool schneidet alle (über die unterschiedlichsten Funktechnologien) empfangenen Informationen des Gerätes mit, auf dem es (evtl. auch ohne Wissen des Gerätebetreibers) installiert ist, und wertet sie aus. Jedes mobile Gerät sendet bei der Suche nach gespeicherten Netzwerken ununterbrochen *Probe Requests*[19], aus denen sich die weltweit eindeutigen MAC-Adressen der Access Points dieser WLANs ermitteln lassen. Findet man diese MAC-Adressen anschließend in Wardriving-Datenbanken (wie *wigle.net* oder *wardriving-forum.de*), lassen sich in vorhandenen Bewegungsprofilen weitere Aufenthaltsorte ergänzen. Werden die von *Snoopy-NG* erfassten Daten ebenfalls in einer Datenbank abgelegt, könnten über obiges Vorgehen auch Beziehungen zwischen mobilen Geräten hergestellt werden, z. B. welche Geräte im selben WLAN angemeldet waren.[20]

Für Wardriving an sonst unzugänglichen Stellen (z. B. in hohen Gebäuden, abgesperrtem Gelände, Innenhöfen/-räumen) eignet sich der Einsatz von (immer günstiger werdenden) Drohnen, die mit einem Smartphone oder einem Mini-PC à la *Raspberry Pi* bestückt werden.[20] Die ausgespähten Informationen werden auf der Drohne gespeichert oder über Mobilfunk zu einem frei wählbaren Ziel verschickt.[21]

Neben dem Zugang zu geschützten Netzwerken gibt es auch eine Vielzahl an offenen Netzen. Die Zahl von frei zugänglichen Hotspots in Deutschland nimmt weiter zu. Diese könnten natürlich ebenfalls für illegale Tätigkeiten aller Art missbraucht werden.

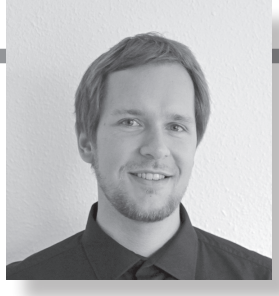
Schutzmaßnahmen

Gegen Wardriving selbst kann man sich nicht direkt schützen. Bedeutend wichtiger ist der Schutz des Zugangs zum eigenen WLAN. Da Wardriving normalerweise nur von außerhalb der Räume der Ausgespähten durchgeführt wird, muss darauf geachtet werden, dass das eigene WLAN-Signal sich nur in erwünschte Bereiche ausbreitet. Erreicht werden kann dies beispielsweise durch Ausrichten der Antennen des WLAN-Routers oder das Anbringen von reflektierender Alufolie.[22]

Für Angreifer wird Wardriving uninteressant, sobald mit angemessenem Zeitaufwand keine offenen oder schlecht gesicherten Funknetze mehr auffindbar sind. Somit besteht ein sinnvoller Schutz darin, das WLAN mit den besten zur Verfügung stehenden Mitteln abzusichern und einen Einbruch in das Netz in akzeptabler Zeit unter Einsatz von angemessenen Mitteln unwahrscheinlich zu machen. Doch kann das notwendige Wissen oder Interesse der Nutzer nicht vorausgesetzt werden. An dieser Stelle ist die Unterstützung der Politik, der Medien und der Industrie gefragt. Nachfolgend zwei positive Beispiele:

- Die indische *Mumbai Police* ist seit 2009 auf Streife, um ungesicherte Funknetzwerke in Mumbai aufzuspüren.[23] Auslöser waren Attentate im Jahre 2008. Dort wurden vermutlich Funknetzwerke für die Koordinierung der Angriffe genutzt.

- Seit März 2012 überprüft die australische Polizei regelmäßig die WLAN-Sicherheit von Brisbane.[24] Ziel ist es, die Straftat WLAN-Einbruch zu verhindern und die daraus resul-



Stefan Jäger

Stefan Jäger ist Diplom-Wirtschaftsmathematiker und arbeitet bei einem Unternehmen im Bereich des Dokumentenmanagements mit dem Schwerpunkt BOS (Behörden und Organisationen mit Sicherheitsaufgaben). Als zertifizierter IT-Sicherheitsbeauftragter in der öffentlichen Verwaltung beschäftigt er sich vor allem mit Funknetzwerken und der Sicherheit mobiler Endgeräte.

tierenden Schäden zu vermeiden. Wird ein solches WLAN entdeckt, weist die *Hi Tech Crime Investigation Unit* den Besitzer mit Bitte um Verbesserung darauf hin.

Eine sinnvolle Ergänzung stellen *Intrusion Detection Systems* (IDS) dar. Diese registrieren jeden Zugangsversuch zum WLAN. Je nach Konfiguration des IDS können so berechtigte von unberechtigten Zugriffen unterschieden werden. Bei einem unberechtigten Zugriff kann anschließend eine Warnmeldung an den Netzwerkbetreiber versandt und/oder das zugreifende Gerät abgewiesen werden.

Rechtliche Lage

In Bezug auf das Gesetz muss deutlich zwischen dem eigentlich Wardriving und dem Eindringen in ein fremdes WLAN unterschieden werden. Für Wardriving im ursprünglichen Sinne ist nur § 30 StVO (Umweltschutz, Sonn- und Feiertagsfahrverbot) einschlägig, in dem unter anderem geregelt ist: „Unnützes Hin- und Herfahren ist innerhalb geschlossener Ortschaften verboten, wenn Andere dadurch belästigt werden." Da es sich beim Begriff „unnütz" um eine Auslegungssache handelt, ist eine Verurteilung relativ unwahrscheinlich.

Folgende Gesetze sind zum Thema WLAN relevant[25]:

- § 202a StGB Ausspähen von Daten
- § 202b StGB Abfangen von Daten
- § 206 StGB Verletzung des Post- oder Fernmeldegeheimnisses
- § 263a StGB Computerbetrug
- § 265a StGB Erschleichen von Leistungen
- § 303a StGB Datenveränderung
- § 303b StGB Computersabotage
- § 89 TKG Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen
- § 148 TKG Strafvorschriften
- § 17 UWG Verrat von Geschäfts- und Betriebsgeheimnissen

Ist das Netzwerk ungesichert, kommen nur Straftaten im Sinne von Diebstahl, Manipulation und Sabotage in Betracht. Sollte das Netzwerk geschützt sein, kommt noch Einbruch hinzu. Handelt es sich dabei lediglich um die Umgehung einer Sicherheitsvorkehrung, spricht man von Hausfriedensbruch, dies kann nach den §§ 123 und 124 StGB verurteilt werden. Dient der Einbruch der Ermöglichung eines Diebstahls, kommen die §§ 243 und 244 StGB in Betracht. Bei einigen der aufgeführten Gesetze liegt das Strafmaß bei 2 bis 5 Jahren Freiheitsstrafe oder Geldstrafe. Sollten aus den oben genannten Straftaten noch Personenschäden resultieren, so steigt das Strafmaß erheblich. Im Netz gibt es gute Literaturzusammenstellungen[25] bzw. Zusammenfassungen[26] zur Thematik.

Frei zugängliche *Hotspots* in deutschen Städten kommen nur langsam voran, da zwar nur wenige gesetzliche Einschränkungen existieren, aber dennoch mehr als in anderen Nationen. So müssen die Betreiber von Hotspots aufgrund der *Störerhaftung* zumindest teilweise für die Handlungen der Nutzer haften, da der WLAN-Betreiber sein Netzwerk für deren (u.U. auch illegale) Handlungen bereitstellt. Zudem unterliegt der Betreiber Prüfungs- und Belehrungspflichten gegenüber allen Netzwerknutzern. Der Bundesgerichtshof hat mit der Entscheidung vom 12. Mai 2010 festgelegt, dass der unbeteiligte Betreiber nur zu max. 100 € Abmahnkosten verurteilt werden kann, falls sein Netzwerk für Urheberrechtsverletzungen im Internet genutzt wurde.[27]

Große Datensammler

Nicht nur Wardriver, sondern auch Institute und Unternehmen sammeln die WLAN-Daten. So überrascht es nicht, dass der größte Datensammler der Welt, *Google,* auch mit dabei ist. 2010 wurde bekannt, dass Google während der Fotoaufnahmen für das Projekt *StreetView* auch WLAN-Daten aufzeichnet. Als Reaktion veröffentlichte Google ein Schreiben[28], aus welchem hervorgehen sollte, dass das Unternehmen nichts Illegales getan hätte. Es würden lediglich WLAN-Name (SSID), MAC-Adresse und Geopositon aufgezeichnet. Ziel sei es, die Lokalisierungs- und Navigationsdienste zu verbessern. Rechtfertigung suchte Google beim Verweis auf analoges Vorgehen bei *Skyhook* und dem *Fraunhofer-Institut*. Die öffentlichen Bedenken, Google würde personenbezogene Daten aufzeichnen wollen, wies das Unternehmen zurück. Der damalige Bundesdatenschutzbeauftragte Peter Schaar sagte zur Namensgebung der Netzwerke: „Bei letzterer verwenden Privatpersonen nicht selten ihre Klarnamen oder andere auf sie hinweisende Informationen. Sowohl mit Blick auf die Benutzung des eigenen Namens als auch auf die Möglichkeit, die WLAN-Netze aufgrund ihrer örtlichen Lage Bewohnern von Häusern zuzuordnen, handelt es sich um die Erfassung und Speicherung personenbezogener Daten und deren Übertragung in die USA."[29]

Neben dem Problem, dass mit den WLAN-Daten auch die StreetView-Bilder der Wohnungen und Häuser verknüpft sind, wurde publik, dass Google auch den Datenverkehr von offenen Funknetzen mitgeschnitten hatte. Nach der Stellungnahme von Google hatte der hamburgische Datenschutzbeauftragte Caspar um Prüfung der Inhalte der durch Google aufgezeichneten Daten gebeten. Bei der internen Überprüfung durch Google wurde festgestellt, dass ohne Absicht der Funkverkehr mitgeschnitten worden war. Dies ist einem der größten und innovativsten Softwareunternehmen der Welt schwer zu glauben. Google ordnete die Löschung dieser Daten und das Stoppen der WLAN-Datensammlung an. Anschließend musste Google an mehrere Einrichtungen Strafen bezahlen, so z. B. an die hamburgische (145.000 €) und an die französische Datenschutzbehörde CNIL (100.000 €).

2011 wurde bekannt, dass das Google-Betriebssystem Android den Netzwerknamen, die MAC-Adresse und die Geoposition aller WLAN-Netze, mit denen das Gerät verbunden ist, an Google überträgt. Hinzu kommen die MAC-Adressen aller Geräte, welche mit dem mobilen Gerät verbunden sind, sobald dieses als Hotspot fungiert. Der Entwickler Samy Kamkar stellte gegen den Willen von Google eine Website zur Verfügung, auf welcher man sich bei Eingabe der MAC-Adresse den zuletzt übermittelten Standort anzeigen lassen konnte.[30] Solch eine Funktion bietet auch die Website *wardriving-forum* an. Während aber die Mitglieder des Forums eher zufällig zu ihren Informationen kommen, werden Scans durch Google automatisch und in regel-

mäßigen Abständen durchgeführt. Dies könnte zur Ortsbestimmung eines bestimmten Mobilfunkgerätes oder einer Person, die dieses mit sich führt, und zur Erstellung von Bewegungsprofilen missbraucht werden.

Fazit

Wardriving ist nicht grundsätzlich kriminell: es kann (und sollte) auch zur präventiven Erkennung schlecht gesicherter Netze eingesetzt werden. Dass Wardriving von Kriminellen im Rahmen von Cyberattacken eingesetzt wird, dürfte sich auch zukünftig nicht prinzipiell verhindern lassen. Versuchen der Industrie (sowie der Behörden und Geheimdienste), mittels Wardriving die Perfektionierung des *gläsernen Bürgers* weiter voranzutreiben, kann und muss jedoch entschieden widersprochen werden.

Aus den aufgeführten Punkten ergibt sich ein größerer Handlungsbedarf für die Politik, die Industrie und vor allem die Medien. Dem Beispiel Indiens und Australiens folgend, sollte ein Team aus entsprechend geschulten Polizisten präventiv die WLAN-Sicherheit der Bevölkerung überprüfen. Die Router-Hersteller sehen derzeit nur Druck aus Wettbewerbssicht. Gesetzlich sind sie lediglich zum Anbieten einer zeitgemäßen Verschlüsselung verpflichtet. Ein Muss sollte es sein, jeden ausgelieferten Router mit voreingestelltem WPA2 und einem zufällig erzeugten langen und sicheren Passwort zu versehen.

Darüber hinaus sollten kundige Anwender ihre WLAN-Router aber auch selbst konfigurieren. Sind Netzwerke gut geschützt und für Unbefugte unsichtbar, und besitzen sie nicht auf die Betreiber zurückführende Namen, werden sie für Angreifer und für den kommerziellen Missbrauch schnell uninteressant. Allerdings führt die Fülle möglicher (und auch noch stark vom konkreten Routermodell abhängiger) Einstellungen schnell zu Überforderung. Für Laien ist es vergleichsweise schwierig, hierzu an brauchbare Informationen zu gelangen. An dieser Stelle soll zumindest auf grundsätzliche Ausführungen für jedermann[31] bzw. detaillierte, auf Unternehmen[32] zugeschnitte Handlungsanleitungen hingewiesen werden.

Für Anwender ist Wissen der beste Schutz. So muss es Aufgabe der Politik sein, Aufklärungskampagnen auf den Weg zu bringen, um vor allem auch über die Medien diese Inhalte aufbereitet an die Allgemeinheit zu bringen. Die deutschen Gesetze decken die Thematik prinzipiell ausreichend ab. Das Problem stellt die Ermittlung der Täter dar. Gehen diese professionell vor und verwischen ihre Spuren, ist es mit angemessenem Aufwand kaum möglich, diese später zu ermitteln.

Anmerkungen

1 *Wikipedia: Wardriving. 20.11.2015. https://de.wikipedia.org/wiki/Wardriving*

2 *Bürger-CERT: Glossar. 20.11.2015. https://www.buerger-cert.de/glossar?index=w*

3 *Peter Shipley: 802.11b War Driving and LAN Jacking. Vortrag auf der DefCon 9, 2001. http://bit.ly/1mFQ8eO*

4 *Die Bezeichnung Access Point wird meist als Synonym für WLAN-Router verwendet. Genau genommen handelt es sich dabei aber um eine Komponente im WLAN-Router, welche für den Datenaustausch zwischen dem WLAN-Router und dem angemeldeten WLAN-Client genutzt wird.*

5 *Bei WEP handelt es sich um das erste in der Praxis verbreitete Verschlüsselungsprotokoll für Datenpakete, welche in drahtlosen Netzwerken übertragen werden. Auf Grund der Schwächen in den Grundprinzipien des Protokolls wird dringend vom Einsatz abgeraten. Erfahrene Hacker können in ein solches Netzwerk in 5–20 Minuten (abhängig vom verwendeten Router und von der Anzahl angemeldeter Clients) eindringen.*

6 *Levi Pulkkinen: Police: Wireless network hacker targeted Seattle-area businesses. seattlepi.com, 19.04.2011. http://bit.ly/1ZcfL2L*

7 *Aufgrund der Schwächen von WEP wurde im Jahre 2003 ein neues Konzept zur verschlüsselten Übertragung von Datenpaketen in drahtlosen Netzwerken unter dem Namen WPA erstellt. Eine überarbeitete und sicherere Variante von WPA wurde 2004 als WPA2-Standard verabschiedet.*

8 *Der Raspberry Pi ist einer der bekanntesten und beliebtesten Minicomputer. Aufgrund seiner sehr geringen Größe und des vergleichsweise niedrigen Preises ist er sehr gut für Eigenbauten und Prozesse jeglicher Art geeignet. Der meist mit Linux betriebene Computer kann durch eine Reihe von Modulen und Adaptern erweitert werden, wodurch die Anzahl seiner Einsatzgebiete sich um ein Vielfaches erhöht.*

9 *SSH (Secure Shell) ist ein Netzwerkprotokoll, über welches Programme, die dieses Protokoll implementiert haben, eine gesicherte Verbindung zu anderen Geräten herstellen können.*

10 *Während des Anmeldeprozesses eines Gerätes am WLAN-Router werden spezielle Datenpakete ausgetauscht. War die Anmeldung erfolgreich, konnten diese als Handshake bezeichneten Datenpakete von einem Angreifer aufgezeichnet werden. Diese stellen die Grundlage fast aller Angriffstechniken gegen WPA2 dar.*

11 *Thomas Harloff: Der Fahrer ist machtlos. Süddeutsche Zeitung, 22.07.2015. http://bit.ly/1IiGS7m*

12 *Charlie Miller & Chris Valasek: Remote Exploitation of an Unaltered Passenger Vehicle. illmatics.com, 10.08.2015. http://bit.ly/1K4CNl4*

13 *sim[TD]: Technologie. 30.11.2015. http://bit.ly/1mKCtTF*

14 *Daniel Bachfeld: Vorkonfigurierte WPA-Schlüssel bei T-Online und Vodafone leicht erratbar. heise online, 20.08.2011. http://bit.ly/1JB3VNz*

15 *Ronald Eikenberg: Router-Schwachstelle für Telefonterror missbraucht. heise Security News, 21.08.2013. http://bit.ly/1ZTqlxQ*

16 *Patent Nr. 096117094. 20.11.2008. http://bit.ly/1OGeDTq*

17 *Google-Code-Project: android-thomson-key-solver. 30.11.2015. http://bit.ly/1cldX2c*

18 *wardriving-forum.de: Standardpasswörter. 30.11.2015. http://bit.ly/14zG4ud*

19 *Bei Probe Requests handelt es sich um spezielle Datenpakete, welche von WLAN-fähigen Geräten ausgesendet werden. Diese dienen dem Zweck, dem Gerät bekannte drahtlose Netzwerke aufzuspüren, um sich anschließend mit ihnen verbinden zu können. Das Gegenstück bilden die Datenpakete, welche als Beacons bezeichnet werden. Diese werden vom WLAN-Router ausgesendet, damit Geräte in Reichweite das dort erzeugte drahtlose Netzwerk finden können.*

20 *Uli Ries: Gratis-Software macht Drohnen zu WLAN-Schnüfflern. heise Security News, 09.08.2014. http://bit.ly/1OXfZoB*

21 *Philipp Schweizer: USB Surfstick am Raspberry Pi verwenden – Mobiles Internet. Raspberry.Tips, 29.04.2015. http://bit.ly/1PUZcYu*

22 *Marco Rinne & Beate Kipphardt: Genialer WLAN-Booster im Eigenbau. Chip, 07.07.2015. http://bit.ly/1Sa0T5J*

23 *Reiko Kaps: Indische Polizei als Wardriver. heise Netze, 19.01.2009. http://bit.ly/1OTxxYT*

24 *Kai Biermann: Polizei in Australien sucht nach offenen WLANs. Zeit Online, 27.03.2012. http://bit.ly/1UEEYRQ*

25 *Herbsttagung „Tatort Internet – eine globale Herausforderung für die Innere Sicherheit" des BKA, 22.11.2007: Strafrecht in der digitalen Welt. COD-Literatur-Reihe, Band 19. http://bit.ly/1Sa140R*
26 *Stefanie Hagemeier: Das Google WLAN-Scanning aus straf- und datenschutzrechlicher Sicht. HRRS, Heft 2/2011. http://bit.ly/1VT6Cfh*
27 *Urteil des Bundesgerichtshofs vom 12.05.2010, 1 ZR 121/08 – Haftung für unzureichend gesicherten WLAN-Anschluss*
28 *Peter Fleischer: Data collected by Google cars. Google Europe Blog, 27.04.2010. http://bit.ly/1Oao0Jp*
29 *Johannes Caspar & Peter Schaar: Presseerklärung „Google-Street-View-Fahrten werden auch zum Scannen von WLAN-Netzen genutzt". datenschutz-hamburg.de, 22.04.2010. http://bit.ly/1OaogrY*
30 *Ernst Ahlers: WLAN-MAC-Adressen: Googles langes Gedächtnis. heise Netze, 16.06.2011. http://bit.ly/1K4DPgW*
31 *Marius Eichfelder: WLAN sichern: Fünf Tipps für mehr Sicherheit. Chip-Praxistipps, 06.08.2014. http://bit.ly/1JhjANY*
32 *Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge. Baustein 4.6 WLAN. September 2011. http://bit.ly/1UEFM9v*

Dominik Brodowski und Felix Freiling

Transnationale Cyberkriminalität vs. nationale Strafverfolgung: Mögliche Auswege aus einem grundsätzlichen Dilemma

Cyberkriminalität wird nicht selten über Landesgrenzen hinweg begangen und stellt daher ein transnationales Phänomen dar. Die Strafverfolgung hingegen wird grundsätzlich von den Nationalstaaten betrieben und ist daher im Ausgangspunkt an nationalstaatliche Regelungen gebunden. Dieser Beitrag möchte durch einen skizzenhaften Problemaufriss zum Nachdenken über dieses grundsätzliche Dilemma anregen.

Das Problem

Das Internet stellt eine Kommunikationsinfrastruktur zur Verfügung, mit deren Hilfe sich Computer und Personen auf sehr einfache Art und Weise weltweit vernetzen können. Interaktive Webseiten wie Blogs und soziale Medien sowie ein transnational ausgerichteter E-Commerce erzeugen bei vielen Menschen den Eindruck eines Raumes grenzenloser Kommunikationsfreiheit. Dass mit dem Internet nationalstaatliche Grenzen jedoch nicht verschwunden sind, merkt man spätestens dann, wenn man selbst Opfer von Cyberkriminalität geworden ist – etwa durch betrügerische Nutzung gestohlener Kreditkarteninformationen oder dadurch, dass man seinen eigenen Rechner nach einer Infektion mit erpresserischer Ransomware freikaufen muss.

Die digitale Schattenwirtschaft agiert professionell, arbeitsteilig und seriösen Schätzungen zufolge (Anderson et al., 2013) mit großem ökonomischen Gewinn. Bei aller Notwendigkeit, die technischen Ursachen von Cyberkriminalität zu verstehen und diesen entgegenzuwirken (Brodowski & Freiling, 2011, S. 81 ff.), erfordert das soziale Problem von Cyberkriminalität auch eine (straf)rechtliche Antwort. Diese wird aber dadurch erschwert, dass Cyberkriminalität nicht vor den Grenzen der Nationalstaaten halt macht.

Auch wenn man das Internet aus technischer wie aus soziologischer Sicht als *virtuellen Cyberspace* verstehen kann, so nimmt jedes Verhalten im Internet seinen Ursprung in einem menschlichen Verhalten und lässt sich daher auf einen physischen Ort zurückführen. Neben diesem *Handlungsort* gibt es noch eine Fülle weiterer Anknüpfungspunkte dafür, dass das materielle Strafrecht eines bestimmten Nationalstaats anwendbar ist. Daher ist ein transnationales, kriminelles Verhalten im Regelfall nach dem Recht mehrerer Staaten strafbar. Das grundlegende Problem, das dieser Artikel beleuchten möchte, entsteht nun in der Vielzahl von Fällen, in denen die Strafverfolgungsbehörden in einem Staat A eine Straftat verfolgen wollen (und dürfen), dabei jedoch auf Ermittlungen in einem anderen Staat B angewiesen sind, um diese Straftat erfolgreich aufzuklären und um den oder die Straftäter wegen dieser Straftat zu verurteilen.

In all diesen Konstellationen sind die Strafverfolgungsbehörden im Staat A nämlich im Ausgangspunkt dadurch eingeschränkt, dass sie nur in diesem Staat – aber nicht im Staat B – tätig werden dürfen, ohne die Souveränität des anderen Staates zu verletzen und möglicherweise eine Straftat nach dem Strafrecht des Staates B zu begehen. Ein Beispiel hierzu aus der analogen Welt: Wenn ein Polizist aus dem Staat A ohne entsprechende Befugnis des Staates B auf dessen Staatsgebiet einen Verdächtigen festnimmt und auf verschlungenen Pfaden nach A verbringt, so wird dies zum einen zu erheblichen diplomatischen Verwicklungen führen. Da Entführungen in wohl allen Staaten strafbar sind, wird sich zum anderen der Polizist im Staat B wegen der nach dortigem Recht rechtswidrigen Entführung des Verdächtigen strafrechtlich verantworten müssen.

Es liegt somit eine Souveränitätskollision vor: Einerseits gehört es zu den Kernaufgaben eines souveränen Staates, seine Staatsgewalt in seinem eigenen Staatsgebiet auszuüben – und damit für den Staat A, sein materielles Strafrecht durchzusetzen und hierdurch auch die Restitution der durch die Straftat Geschädigten zu unterstützen. Andererseits aber bedeutet staatliche Souveränität auch, den Staat und die im Staatsgebiet ansässigen Personen vor einer Machtausübung anderer Staaten zu schützen – und damit für den Staat B, seine Bürger sowohl davor zu schützen, dass sie selbst in den Staat A verschleppt werden, als auch davor, dass ihre Daten in den Staat A transferiert werden.

Welche Wege kann man prinzipiell einschlagen, um dem (jedenfalls in etlichen Fällen legitimen) Schutzbedürfnis der Nutzer Rechnung zu tragen – und damit etwa deutsche Nutzer vor einem zu weitreichenden Datentransfer in die USA zu schützen – und gleichzeitig den Schutzanspruch der Staaten – und damit die transnationale Durchsetzung von Strafnormen – nicht vollständig zu verraten? Wir skizzieren drei mögliche Alternativen.

Alternative 1: Transnationale Kooperation gegen Cyberkriminalität

Die Praxis behilft sich bislang vor allem mit einer Kooperation der nationalen Kriminaljustizsysteme (Brodowski & Freiling, 2011, S. 173 ff.). Stimmt nämlich der Staat B der Durchführung einer Strafverfolgungsmaßnahme in seinem Staatsgebiet zu oder führt der Staat B eine Strafverfolgungsmaßnahme auf Ersuchen des Staates A durch, so liegt keine Souveränitätsverletzung des Staates B vor. Kann das der Strafverfolgung zugrundeliegende Verhalten auch durch den Staat B verfolgt werden, so wird oftmals in beiden Staaten A und B ein Ermittlungsverfahren gegen den oder die Verdächtigen eingeleitet. Beide Staaten nehmen dann in ihrem jeweiligen Staatsgebiet die erforderlichen Ermittlungen vor und tauschen sich regelmäßig über die gewonnenen Erkenntnisse aus. Auch auf diesem Wege sogenannter Spiegelverfahren oder Parallelermittlungen treten somit keine Souveränitätsverletzungen auf.

Solche formellen und informellen Kooperationen sollen durch eine Vielzahl von Instrumenten, die teils spezifisch die Verfolgung von Cyberkriminalität betreffen, beschleunigt und erleichtert werden. So ist exemplarisch zu verweisen auf internationale Übereinkommen wie die sogenannte *Cybercrime Convention* (Übereinkommen über Computerkriminalität, 2001), auf die (noch in nationales Recht umzusetzende) Europäische Ermittlungsanordnung der EU (Richtlinie 2014/41/EU, 2014), auf rund um die Uhr erreichbare Kontaktstellen bei den Polizeien, aber auch auf die Etablierung sehr erfolgreicher informeller wissenschaftlicher und organisatorischer Kooperationen, etwa im Bereich der Internet-Beschwerdestellen und bei der Bekämpfung von Botnetzen.

Dennoch stoßen diese Kooperationsmodelle in vielen Fällen an ihre Grenzen: So dauert insbesondere die förmliche Rechtshilfe in Strafsachen oft recht lange – während sich die gesuchten Daten schnell vom Staat B in einen weiteren Staat C transferieren oder löschen lassen. Faktisch stellt sich nicht selten das Problem, dass es schwierig herauszufinden ist, in welchem Staat die gesuchten Daten tatsächlich gespeichert sind. Schließlich bedeutet die Involvierung mehrerer Kriminaljustizsysteme auch einen erheblichen Ressourcenaufwand. Und nicht immer ist ein Staat – etwa wegen des Ressourcenaufwands oder wegen einer anderen Bewertung, ob das Verhalten tatsächlich verfolgenswert ist – überhaupt bereit, einem anderen Staat Hilfe zur dortigen Strafverfolgung zu leisten.

Auch eine Verlagerung der Verfolgung von Cyberkriminalität auf eine supranationale Instanz – etwa auf einen internationalen Gerichtshof oder ein internationales Tribunal zur Verfolgung von Cybercrime (Schjolberg, 2014) – wäre mit der Schwierigkeit verbunden, dass erst ein Konsens gefunden werden müsste, welches Verhalten überhaupt strafbar sein soll. Zudem wäre eine solche zentrale Institution mit der Quantität an Cyberkriminalität schlicht überfordert und auf die Zusammenarbeit mit den (in ihren Befugnissen unverändert auf ihr Territorium begrenzten) Nationalstaaten angewiesen (Safferling, 2012, S. 262). Ohnehin erscheint eine globale Einigung auf eine zentrale Strafverfolgung – die nicht einmal in Bezug auf schwerste Verbrechen gegen die Menschheit erzielt werden konnte – mit territorial nicht begrenzten Ermittlungskompetenzen politisch schlicht als nicht durchsetzbar.

Alternative 2: Reduktion des Schutzversprechens der Nationalstaaten

Eine zweite Alternative besteht darin, das Schutzversprechen des Staates gegenüber seinen Bürgern einzuschränken. Bezogen auf den Schutz vor Cyberkriminalität beschreibt dies den Zustand, den viele Nutzer derzeit im Internet faktisch erleben. Denn nicht selten merken Nutzer gar nicht, dass sie Opfer von Cyberkriminalität geworden sind; die Strafverfolgungsbehörden sind aus den genannten Gründen nicht selten bei der Verfolgung von Delikten dann ohnmächtig, wenn die Spur der Täter eine Staatsgrenze überquert.

Man kann nun argumentieren, dass man aus der Not – also der Hilflosigkeit von Nutzern und Behörden – dadurch eine Tugend macht, dass man öffentlich feststellt, dass für bestimmte Tätigkeiten und Vorkommnisse keinerlei staatlicher Schutz übernommen wird. In Analogie zu den Reisewarnungen des Auswärtigen Amtes könnte beispielsweise das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) Webseiten oder Netzbereiche als *unsicher* einstufen und Schutzpflichten des Staates gegenüber seinen Bürgern einschränken, sollte man sich trotzdem auf diese Seiten bewegen. Dies hätte sicherlich einen nicht vernachlässigbaren Effekt auf das Verhalten von Nutzern, die bestimmte Online-Dienstleistungen und Websites meiden und sich beim Surfen im Netz anders verhalten würden. Ein solches Vorgehen hätte also durchaus ein präventives Potenzial.

Dennoch sprechen verschiedene, gewichtige Gründe gegen ein solches Vorgehen. Ein erster Grund liegt sicherlich in den ökonomischen Einschränkungen, die die Veränderung des Nutzerverhaltens nach sich ziehen würde, bis hin zu einer generellen *Abkehr vom Netz,* was auch viele Effizienzmaßnahmen in der öffentlichen Verwaltung (E-Government) konterkarieren würde. Viel schlimmer: Durch einen solchen Ansatz würde der Nationalstaat teilweise auf die Durchsetzung des Rechts auf eigenem Boden verzichten; das Internet würde tatsächlich mehr und mehr zu einem *rechtsfreien* Raum werden. Dies käme einer Kapitulation des Strafrechts vor dem Problem transnationaler Cyberkriminalität gleich – ein grundsätzlicher *Dammbruch*, dessen Folgen unabsehbar wären.

In anderer Hinsicht sind jedoch Reduktionen des Schutzversprechens verbreitet – namentlich insoweit, als ein Staat B sein Versprechen zurücknimmt, seine Bürger vor transnationalen Eingriffen des Staates A zu schützen. Das ist beispielsweise faktisch in der Ohnmacht der europäischen Politik gegenüber der Netzüberwachung durch US-amerikanische Geheimdienste zu ver-

zeichnen. Völkervertraglich spiegelt sich dieser Lösungsansatz in einer Erlaubnis wider, die sich die Vertragsstaaten der *Cybercrime Convention* eingeräumt haben: Demzufolge darf ein Vertragsstaat A auch online auf Computerdaten zugreifen, die sich im Vertragsstaat B befinden, wenn A „die rechtmäßige und freiwillige Zustimmung der Person einholt, die rechtmäßig befugt ist, die Daten … [an A] weiterzugeben" (Übereinkommen über Computerkriminalität, 2001).

Nach Auffassung des Schweizerischen Bundesgerichts sind auf dieser Grundlage ausländische E-Mail-Provider befugt, die E-Mails ihrer Kunden an schweizerische Strafverfolgungsbehörden auszuhändigen, soweit diese Provider – wie üblich – in ihren Allgemeinen Geschäftsbedingungen (dem „Kleingedruckten") einen entsprechenden Kooperationsvorbehalt aufgenommen haben (Schweiz. BGer, Urt. v. 14.1.2015, 1B_344/2014, 2015). Das bedeutet eine Privatisierung der Strafrechtspflege, da nicht länger die Nationalstaaten, sondern nunmehr Internetprovider über einen transnationalen Datentransfer zu Strafverfolgungszwecken entscheiden. Noch weiter geht die Auffassung der US-amerikanischen Regierung in einem noch anhängigen Gerichtsverfahren gegenüber Microsoft, die von einer Pflicht zur Kooperation spricht (Microsoft v. USA, 2nd Cir, 14-2985-CV, pending). Und bemerkenswert ist eine vergiftete Klausel in einem aktuellen US-amerikanischen Gesetzesvorhaben, das Ausländern (rudimentären) Rechtsschutz in Datenschutzfragen vor amerikanischen Gerichten einräumt: Sollte nämlich ein ausländischer Staat einem strafverfolgungsbezogenen Datenaustausch eines Internetproviders mit US-amerikanischen Behörden entgegentreten – mit anderen Worten: sollte dieser Staat seinen Souveränitätsanspruch geltend machen –, verlören sämtliche Bürger dieses Staates diese Rechtsschutzmöglichkeiten wieder (Judicial Redress Act, 2015). Doch auch in Deutschland sind Stimmen in der Rechtswissenschaft zu hören, die vertreten, dass man den durch Strafverfolgungsbehörden erzwungenen Zugriff technisch nicht von einem freiwilligen Zugriff des berechtigten Nutzers unterscheiden kann. Solange sich daher der Polizist nicht ins Ausland begebe, sondern auf Daten nur *online* – etwa auf der (insoweit zweifelhaften (Brodowski & Eisenmenger, 2014)) Grundlage des § 110 Abs. 3 StPO – zugreife, werde die Souveränität des ausländischen Staates nicht verletzt (Wicker, 2013; Zerbes & El-Ghazi, 2015).

Zwar hat dieser Lösungsansatz einer Souveränitätsreduktion den Charme, dass er ressourcenschonend eine transnationale Verfolgung von Cyberkriminalität erleichtert. Dennoch sind auch hier etliche Gefahren zu erkennen. So sind die Möglichkeiten, sich effektiv gegen strafrechtliche Vorwürfe zu verteidigen, im transnationalen Kontext noch immer stark eingeschränkt. Besonders bedrohlich ist eine solche Souveränitätsreduktion im Internet jedenfalls dann, wenn sich nicht nur demokratische Rechtsstaaten auf diese berufen und Unrechtsregime global tätige Internetdienstleister in die Pflicht nehmen, sie bei einer illegitimen Strafverfolgung (z. B. gegen Regimekritiker) zu unterstützen.

Alternative 3: Nationale Netze mit Grenzkontrollen

Eine dritte Alternative besteht darin, die Internationalität des Internets einzuschränken, also nationale oder regionale Netze zu schaffen und diese an den Grenzen intensiv zu kontrollieren. Man würde beispielsweise deutsche Netzanbieter dazu verpflichten, ihre Netzinfrastruktur vollständig auf deutschem Territorium zu betreiben und an den Übergangsstellen ins Ausland eine aufwändige Überwachungsinfrastruktur bereitzustellen, die Straftaten einschränken und die Rückverfolgung von Straftätern erleichtern soll. Es gibt durchaus verschiedene Vorbilder für ein solches Vorgehen (Lee & Liu, 2012; Clayton, Murdoch & Watson, 2006; Ensafi et al., 2015) – auch wenn dort die Motivation mitnichten darin besteht, die eigenen Einwohner vor internationaler Cyberkriminalität zu schützen.

Zwar ist bereits viel über nationale Netze diskutiert worden, etwa unter dem Stichwort „Entnetzung" (Gaycken & Karger, 2011) oder im Kontext von *Internetfiltern,* welche den Zugriff auf Kinderpornografie erschweren sollten (Sieber, 2009). Neuen Auftrieb hat diese Diskussion durch ein aktuelles Urteil des EuGH erhalten, das – auch im Kontext der Snowden-Enthüllungen – den Transfer personenbezogener Daten aus der EU in die USA jedenfalls erschwert hat (EuGH, Urt. v. 6.10.2015, C-362/14, 2015).

Drei Gründe sprechen aber zuvörderst gegen eine solche Lösung. Der erste ist ökonomischer Natur, denn nationale Netze sind aus betriebswirtschaftlicher Sicht schwer zu legitimieren. Die großen internationalen Internet-Carrier können sehr viel effizienter die globalen Datenströme abwickeln, wenn sie unabhängig von geographischen Grenzen agieren können. Durch die Medien wird zwar suggeriert, dass ein Großteil des Netzverkehrs in hierarchischer Form über zentrale Internetknoten wie den DE-CIX in Frankfurt abgewickelt wird. Die tatsächliche Vernetzungsstruktur im Internet ist jedoch

Was kann man tun?

Das Internet ist genauso tückisch wie die reale Welt:

- Nepper, Schlepper, Bauernfänger (jetzt weltweit)

Mindeststandard an technischem Schutz

- Virenschutz aktuell halten (auch die kostenlosen Programme sind gut)
- Betriebssystem und Anwendungen aktuell halten (automatische Updates)

Wichtiger noch: Medienkompetenz – drei Regeln

1. Bleiben Sie misstrauisch
   - Es ist naiv zu glauben, im Internet gibt es alles umsonst
   - Woher weiß ich, wer am anderen Ende der Leitung sitzt?
2. Im Zweifel auf Funktionalität verzichten
   - Neue Features bedeuten oft neue Probleme
   - Fremde Software birgt neue Gefahren
3. Erstatten Sie Anzeige oder beschweren Sie sich!
   - Online-Anzeige bei Ihrer Polizei
   - Internet-Beschwerdestelle

Felix Freiling, 2015

durch komplexe und in ihrer Gänze auch nicht öffentlich bekannte Peering-Vereinbarungen zwischen den Netzanbietern gegeben, die gemäß betriebswirtschaftlichen Erwägungen geschlossen werden.

Der zweite Grund ist technischer und rechtlicher Natur, denn es ist nicht einmal in Ansätzen klar, wie man effektive Grenzkontrollen in einem national aufgeteilten Internet realisieren könnte. Das im Zuge der Flüchtlingskrise wieder ins öffentliche Bewusstsein gedrungene realweltliche Analogon, also physische Kontrollen an den Grenzübergängen, erscheint vom Erfolgspotenzial her geradezu traumhaft gut: Zwar mag die Entdeckungsgefahr für Schmuggler oder Schleuser bei physischen Grenzkontrollen gering erscheinen, doch setzen sie sich immer einem nicht vernachlässigbaren Ergreifungsrisiko aus. Im Vergleich hierzu sind digitale Grenzkontrollen durch automatisierte kryptographische Verschleierungstechniken verhältnismäßig einfach zu überwinden. Eine effektive Kontrolle an den Außengrenzen des Netzes wäre vermutlich nur flankiert durch eine umfassende innerstaatliche Netzüberwachung wirksam, welche die Kontrolle von Endgeräten einschließen müsste. Die dadurch notwendigen Grundrechtseingriffe wären um mehrere Größenordnungen gravierender als jene, die im Kontext der Vorratsdatenspeicherung diskutiert wurden und werden.

Drittens würde die Regulierungsmacht der Nationalstaaten über das Internet – beziehungsweise über die dann entstehenden Inter*netze* – gestärkt, was insbesondere in Unrechtsregimes der liberalisierenden Kraft des Netzes Einhalt gebieten würde.

Fazit

Kriminalität überwindet seit jeher räumliche Grenzen: Sei es, dass Waren ü ber Staatsgrenzen hinweg geschmuggelt werden; sei es, dass Täter über Staatsgrenzen fliehen. Die zunehmende Vernetzung und räumliche Entgrenzung der Informationstechnologie führt daher im Ausgangspunkt nur zu einer Intensivierung bekannter Phänomene, namentlich der Frage, wie eine Strafnorm auch über Staatsgrenzen hinaus durchgesetzt werden kann – und wann solch einer transnationalen Strafverfolgung entgegenzutreten ist.

Dieser Beitrag hat drei mögliche Wege aufgezeigt, wie dieser Problemlage grundsätzlich begegnet werden könnte. Alle drei Wege sind jedoch mit erheblichen rechtsstaatlichen und teils auch rechtspraktischen Gefahren verbunden; alle drei Wege sind nicht hinreichend erfolgversprechend; auf allen drei Wegen gerät die nationalstaatliche Souveränität zunehmend an faktische Grenzen. In jedem Falle aber muss ein Mehr an transnationaler Strafverfolgung auch mit einem Mehr an Schutz für den Einzelnen vor illegitimer Strafverfolgung verbunden werden. Denn nur eine legitime, am Schutz von Grund- und Menschenrechten orientierte ausländische Strafverfolgung kann eine hinreichende Rechtfertigung dafür bieten, dass ein Staat seine Bürger – und deren Daten – einer ausländischen Strafverfolgung preisgeben darf.

Danksagung

Wir danken Christoph Safferling und Christian Rückert für deren wertvolle Anmerkungen zu einem Entwurf dieses Beitrags. Dieser Beitrag ist teilweise im Rahmen des BMBF-geförderten Projekts „Open Competence Center for Cyber Security – OpenC3S“ entstanden.

Referenzen

Anderson, R. et al. (2013). Measuring the cost of cybercrime. In R. Böhme (Hrsg.), *The economics of information security and privacy – WEIS 2012: 11th annual workshop on the economics of information security* (S. 265–300). Berlin: Springer.

Brodowski, D. & Eisenmenger, F. (2014). Zugriff auf Cloud-Speicher und Internetdienste durch Ermittlungsbehörden. Sachliche und zeitliche Reichweite der „kleinen Online-Durchsuchung“ nach § 110 Abs. 3 StPO. *ZD,* 119–126.

Brodowski, D. & Freiling, F. C. (2011). *Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft.* Berlin: Forschungsforum Öffentliche Sicherheit.

Clayton, R., Murdoch, S. J. & Watson, R. N. M. (2006). Ignoring the great firewall of China. In G. Danezis & P. Golle (Hrsg.), *Privacy enhancing technologies.* LNCS Bd. 4258 (S. 20–35). Berlin: Springer.

Ensafi, R. et al. (2015, April). Analyzing the great firewall of China over space and time. *Proceedings on Privacy Enhancing Technologies, 2015* (1), 61–76.

EuGH, Urteil v. 6.10.2015, C-362/14.

Gaycken, S. & Karger, M. (2011). Entnetzung statt Vernetzung. Paradigmenwechsel bei der IT-Sicherheit. *MMR,* 3–8.

In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation, United States District Court (SDNY) Memorandum and Order of 25 April 2014, 13-Mag-2814, upheld by Order of the United States District Court (SDNY) of 11 August 2014. Appeal (pending): Microsoft Corporation v. United States of America United States Court of Appeals (2nd Cir) 14-2985-CV.

Judicial Redress Act of 2015. H.R. 1428, 114th Congress; S. 1600, 114th Congress.

Lee, J.-A. & Liu, C.-Y. (2012). Forbidden city enclosed by the great firewall: The law and power of internet filtering in China. *Minnesota Journal of Law, Science & Technology, 13,* 125–152.

Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen. ABlEU 2014 L 130 v. 1.5.2014, S. 1–36.

Safferling, C. (2012). *International Criminal Procedure.* Oxford: OUP.

Schjolberg, S. (2014). *The History of Cybercrime, 1976-2014.* Norderstedt: Books on Demand.

Schweizerisches Bundesgericht, Urteil v. 14.1.2015, 1B_344/2014.

Sieber, U. (2009). Sperrverpflichtungen gegen Kinderpornografie im Internet. *JZ,* 653–662.

Übereinkommen über Computerkriminalität v. 23.11.2001. ETS Nr. 185.

Wicker, M. (2013). Durchsuchung in der Cloud. Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden. *MMR,* 765–769.

Zerbes, I. & El-Ghazi, M. (2015). Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung. *NStZ,* 425–433.

Informationen zu den Autoren Dr. Dominik Brodowski und Prof. Dr. Felix Freiling finden Sie auf Seite 26.

Britta Schinzel

Kunstprojekt *11 TAGE* – Editorial zum Schwerpunkt

Florian Mehnert hat sein Kunstprojekt *11 TAGE* in der *FIfF-Kommunikation* 3/2015 ausführlich dargestellt. Zu diesem Projekt fand am 6. Oktober 2015 im Morat-Institut für Kunst und Kunstwissenschaft in Freiburg i.Br. ein Symposium *11 TAGE* statt, das nicht nur dieses politische Kunstprojekt in einem medienunterstützten Vortrag vorstellte, sondern auch die Ereignisse in diesem Kontext reflektieren sollte. Dazu schien es sinnvoll, das, was Florian Mehnert mit seinem medialen Kunstakt aussagen und bewirken wollte – „Politik kann man mit Kunst erfolgreich beeinflussen" –, und was ihm im Rahmen seines Projektes widerfuhr, aus unterschiedlichen Blickwinkeln zu beleuchten.

Der Livestream zeigte die Ego-Shooter-Perspektive auf die Ratte

- **Aus medientheoretischer Perspektive:** Welche Rolle spielen die Medien hier in vielfältiger Weise – vom Kunstwerk gewollt, aber auch unerwartet, beispielsweise als Reaktion im *shitstorm*?

- **Aus kunsttheoretischer Sicht:** Welcher Art von Kunst ist dieses politische Projekt zuzuschreiben, bzw. was daran ist Kunst, warum ist es nicht einfach nur ein Shooter-Spiel im Internet?

- **Aus Sicht der Polizei und des Rechts:** Warum wurde ein Verfahren gegen Mehnert angestrengt und warum konnte es eingestellt werden?

- **Aus soziologischer, psychologischer und politischer Perspektive:** Wie kann das Projekt zu einer Bewußtseinsschärfung hinsichtlich Überwachung und Drohnenkrieg verhelfen, welche psychosozialen Veränderungen bewirkt die Überwachung, welche der Drohnenkrieg und die automatisierte Kriegführung, wie können die Morddrohungen an Mehnert verstanden werden?

- **Aus Sicht zivilgesellschaftlichen Engagements:** Welche nichtparlamentarischen Aktivitäten können die (cyber-)kriegerische Politik beeinflussen oder gar verhindern?

Der Journalist *Thomas Reintjes* (u. a. *Deutschlandradio Kultur*) trug über das Thema *Roboter im Krieg. Warum Menschen in Zukunft nicht mehr den Abzug, sondern nur noch den Ausschalter betätigen* vor. Der Rechtsanwalt Dr. *Udo Kauß*, auch Vorstandsvorsitzender der *Humanistischen Union Baden-Württemberg* berichtete unter dem Titel *Das Recht schützt den Staat und seine Bürger (vor sich selbst)* von seinen Recherchen bei Polizei und Gericht über die rechtlichen Begründungen für Polizeieinsatz und Verfahren gegen Mehnert, sowie die Begründung für die Einstellung des Verfahrens. *Britta Schinzel*, Mitglied in den Vorständen der NGOs *FIfF* und *Humanistische Union Baden-Württemberg,* zeigte mit *Die NGOs – wir klagen an und fordern auf* die außerparlamentarischen Versuche, gegen Überwachung, Krieg und bewaffneten Drohneneinsatz Einfluß zu nehmen. Die Literaturwissenschaftlerin und Medientheoretikerin Prof. Dr. *Christa Karpenstein-Eßbach* erörterte unter dem Titel *Medien-/Kunst-Konkurrenzen, intermediale Grenzüberschreitungen, Erregungspotentiale und Wirkungsstrategien* medientheoretische bzw. -ästhetische Aspekte des Projekts. Sie alle sollen in diesem Heft zu Gehör kommen.

Den Abschluss des Schwerpunkts bildet der ergänzende Beitrag von *Ulrich Bröckling*: *Drohnen und Helden*, in dem er den Drohnenkrieg und seine Auswirkungen analysiert.

Florian Mehnert

Der Künstler **Florian Mehnert** erlangte mit mehreren Kunstprojekten und Ausstellungen über das Thema Überwachung international Aufmerksamkeit. In seinem Kunstprojekt *Waldprotokolle* verwanzte er Wälder mit Mikrofonen, die vorbeigehende Passanten abhörten. In seiner Videoinstallation *Menschentracks* zeigte er 42 Videosequenzen gehackter Smartphones, deren Kameras und Mikrofone ferngesteuert aktiviert wurden. *(www.florianmehnert.de)*

Florian Mehnert

Kurze Einleitung zum Projekt und Symposium *11 TAGE*

Das Symposium 11 TAGE *im Morat-Institut für Kunst und Kunstwissenschaft in Freiburg i. Br. war der Auftakt zur Aufarbeitung des Kunstexperiments, der Reaktionen darauf und der Fragen, die es auf vielen Ebenen aufwarf.*

Die internationalen Reaktionen auf das Projekt waren extrem kontrovers. Nach ersten Medienberichten folgte ein *Shitstorm* inklusive Morddrohungen. Etliche internationale Petitionen wurden gegen das Projekt gestartet. Die Behörden reagierten nervös. Weil zahlreiche Anzeigen eingingen, musste sich auch die Staatsanwaltschaft mit dem Kunstexperiment *11 TAGE* beschäftigen. Nach sechs Tagen wurde das Projekt aufgrund seiner überwältigenden Rezeption vorzeitig beendet.

11 TAGE konnte nur durch die Partizipation so vieler Rezipienten funktionieren. Dazu war es notwendig, Aufmerksamkeit durch einen besonderen Auslöser zu erregen: die Ratte. Der experimentale Aufbau mit der vermeintlich bedrohten Ratte funktionierte und erzeugte große Resonanz bei Medien und Rezipienten. Kam es durch die Fokussierung mancher Rezipienten auf die Ratte, vor allem die Ratte aus der Installation zu retten, nicht zu einer Überlagerung der künstlerischen Intention? Der Intention, durch den experimentellen Aufbau des Projekts die Folgen der Überwachung, den Einsatz von ferngesteuerten bewaffneten Drohnen zu untersuchen und den Rezipienten über ihre Partizipation die dabei entstehenden Problematiken vor Augen zu führen? Der Installationsaufbau und seine Aussage waren eindeutig formuliert. Vielmehr schien die Fokussierung eine Überforderung der Rezipienten aufzuzeigen, ihre zunehmend komplexe Realität zu bewältigen. Eine Realität, in der es häufig unmöglich ist, eine Verantwortlichkeit zu definieren. Insofern lag es für manche Rezipienten näher, die Ratte vor ihrem möglichen Tod zu retten und den Künstler als Urheber zu bedrohen, als sich mit der komplexen Thematik der bewaffneten Drohneneinsätze auseinanderzusetzen.

Jede Art von Reaktion stellte aber eine Form der Auseinandersetzung dar – ganz unabhängig davon, ob die Reaktion zustimmend oder ablehnend war. Der Shitstorm und die Petitionen gegen das Projekt *11 TAGE* haben auch gezeigt, welche Bereitschaft und Energie Menschen mobilisieren können, um sich gegen gefühltes Unrecht aufzulehnen. Unzählige Diskussionen und Kommentare in Foren zeugen von dieser intensiven Auseinandersetzung.

Das Projekt konnte einen neuen Zugang zu der Problematik der bewaffneten Drohnen schaffen, einen Zugang, der weniger über eine rational geführte Diskussion als über die durch das Projekt aufgeworfenen Emotionen und Selbsterkenntnisse stattfand. Denn die Rezipienten erzeugten jedes Gespräch, jede Diskussion und jedes Gedankenmodell selbst und trugen diesen eigenen Erkenntnis- und Entwicklungsprozess in die Gesellschaft hinein.

Thomas Reintjes

Leben schützen mit Militärrobotern?

Maschinen und Algorithmen beziehen ihre Existenzberechtigung aus der einfachen Tatsache, dass sie Dinge besser können als wir Menschen. Sie haben sich längst von Werkzeugen, die uns helfen, Dinge zu tun, zu eigenständigen Agenten entwickelt. Die Roboter sind uns mit ihren Fähigkeiten überlegen – jedenfalls in ihren spezifischen Talenten: Der Thermomix kocht vermutlich besser als viele seiner Besitzer, der Staubsaugerroboter saugt ausdauernder Staub, und autonome Autos bauen weniger Unfälle, als wenn ein Mensch am Steuer sitzt. Das Auto der Zukunft wird deshalb gar kein Steuer mehr haben. Im Wesentlichen schalten wir die Roboter nur noch an oder aus und die Dinge gehen ihren Gang, gemessen an menschlichen Leistungen überdurchschnittlich gut.

Diese Entwicklung betrifft nicht nur Haushaltsroboter, Industrieroboter oder autonome Maschinen im zivilen Sektor. Sie betrifft auch den militärischen Sektor und wird zum Teil von diesem angetrieben. Siehe Staubsaugerroboter: *iRobot*, der Hersteller der Roomba-Serie, hat auch einen militärischen Zweig. Teilweise sind die Roboter auf derselben Basis aufgebaut. Im Grunde befruchten sich militärische und zivile Entwicklung gegenseitig – und das trägt mit dazu bei, dass hier ein gewaltiges moralisches Dilemma entsteht.

Als ich 2013 und 2014 in den USA über Militärtechnikmessen ging, war an Robotern nicht mehr vorbeizukommen. Es gibt kleine, nicht größer als ein ferngesteuertes Modellauto, und große vom Format eines SUV. An einem Stand fuhren die Roboter auf dem plüschigen Teppich umher, direkt neben einem Banner, auf dem das wichtigste Verkaufsargument kurz und eingängig zu lesen war: *Saving lives*. Diese Roboter retten Leben. Das ist kein leeres Verkaufsversprechen und dahinter steckt keine Zukunftsvision von Roboterarmeen. Roboter haben im Irak und in Afghanistan schon 25 000 Einsätze absolviert. Sie untersuchen vor allem *IEDs, Improvised Explosive Devices,* also potenzielle Bomben, und machen sie unschädlich. Schätzungen zufolge haben sie dabei Hunderte Soldaten vor Verletzungen oder dem Tod bewahrt.

Als nächstes werden die Roboter in die Offensive gehen. Roboter werden als Waffe eingesetzt werden. Zwei bewaffnete Roboter waren schon im Irak stationiert, sollen aber nicht eingesetzt worden sein. Auch zuvor gab es schon Roboter-Waffen. Die Nazis hatten das ferngesteuerte Kettenfahrzeug *Goliath* entwickelt. Es konnte hinter feindliche Linien gelenkt und dort zur Explosion gebracht werden. 5000 Exemplare sind davon gebaut worden.

Bisherige Militärroboter sind quasi bewaffnete Staubsaugerroboter: relativ harmlos und defensiv. Zukünftige Militärroboter werden eher wie bewaffnete Google-Autos sein: autonom und offensiv. Denn wenn wir einmal selbstständig fahrende Autos auf unseren Straßen haben, dann wird das Militär auch autonome Panzer haben. Die Frage ist, wie weit die Autonomie geht und wie viel menschliche Kontrolle noch vorgesehen ist.

Darum ging es auch bei *11 TAGE*: Wer sollte die Macht haben, über Leben oder Tod der Ratte zu entscheiden? Die Ankündigung, die Entscheidungsgewalt auf anonyme Einzelne zu übertragen, hat mit zu den Protesten gegen das Kunstprojekt geführt. Das Töten aus der Ferne per Drohne, agnostisch gegenüber Geographie, physischer Präsenz und Persönlichkeit, ist aus Opferperspektive tatsächlich gut mit dem Aufbau des Kunstprojekts vergleichbar.

Aus der Perspektive des Militärs stellt sich das allerdings anders dar. Eine ehemalige Kampfjetpilotin sagte mir, sie habe damals alleine entscheiden müssen, ob sie Bomben abwirft oder nicht. Heute sitze hinter der Kommandozentrale eines Drohnenpiloten aber ein ganzes Komitee aus Experten, die über einen Angriff entscheiden. Insofern sollte man davon ausgehen können, dass heute völkerrechtswidrige Angriffe seltener sind, weniger Zivilisten getötet werden. Andererseits sind im US-Drohnenkrieg nach Auswertungen der Menschenrechtsorganisation *Reprieve* bis Ende November 2014 bei Angriffen auf 41 Zielpersonen insgesamt 1147 Menschen getötet worden.

Menschen treffen falsche Entscheidungen. Beim Autofahren, beim Kochen, beim Kämpfen. Was, wenn es in Zukunft nicht nur Algorithmen gibt, die die besseren Autofahrer oder Köche sind, sondern auch Systeme, die besser sind als menschliche Soldaten?

Was die reine Waffentechnik angeht, ist die Zukunft schon da. Die Firma *Tracking Point* beispielsweise hat kürzlich ein *Smart Rifle* auf den Markt gebracht: eine Waffe, vollgestopft mit Sensoren. Bei der Abgabe eines Schusses zieht sie Werte wie Temperatur, Luftdruck und Luftfeuchtigkeit, aber auch die Corioliskraft hinzu. Ein Wildtier soll sich damit aus einem Kilometer Entfernung erlegen lassen.

Was die kognitiven Leistungen der Soldaten angeht, ist die Technik noch nicht ganz so weit. Aber es gibt Wissenschaftler, die zumindest laut darüber nachdenken, wie sich Computersysteme schaffen ließen, die etwas von Ethik und Moral verstehen, die das Völkerrecht kennen und die wissen, wer Zivilist und wer Kämpfer ist. Und auch wenn so etwas noch in weiter Ferne ist, lohnt sich das Nachdenken nicht nur über das Wie, sondern auch über das Ob und das Warum.

NGOs protestieren lautstark gegen Maschinen, die sie *Killer-Roboter* nennen. Hunderte Wissenschaftler stehen an ihrer Seite und haben einen offenen Brief unterzeichnet, in dem sie sich gegen Technik aussprechen, die eigenständig über Leben oder Tod von Menschen entscheidet. Ihr Ziel ist es, ein Verbot auf UN-Ebene zu erreichen. Kampfroboter sollen wie zuletzt Landminen geächtet werden. Wie die Chancen dafür stehen, ist schwer abzusehen. Der UN-Sonderberichterstatter für außergerichtliche Tötungen hat einen langen Bericht über Kampfroboter vorgelegt und darin ein Moratorium vorgeschlagen, bis sich ein hohes Gremium mit dem Thema befasst hat. Die Gremien beginnen gerade, das zu tun. In den vergangenen beiden Jahren fanden in Genf mehrtätige Experten-Sitzungen statt und auch die Vertreter der Staaten haben sich dort schon mit Kampfrobotern auseinandergesetzt.

Zuletzt hat das Pentagon Stellung bezogen. Zum ersten Mal seit 1956 hat das US-Verteidigungsministerium im Juni 2015 eine aktualisierte Version des *Law of War Manual* herausgebracht, die Sichtweise der Pentagon-Justiziare auf die Regeln des Krieges, auf 1200 Seiten. Im Kapitel 6.5.9. geht es um autonome Waffensysteme. Darin heißt es, Waffen könnten niemals eine Verpflichtung haben. Und Landminen werden als Vergleich herangezogen: von ihnen sei auch nie gefordert worden, dass sie selbst urteilen, ob die rechtlichen Grundlagen für ihren Einsatz gegeben sind. Unbelebte Objekte sind Werkzeuge; der Mensch ist es, der sicherstellen muss, dass sie ordnungsgemäß eingesetzt werden, heißt es sinngemäß aus dem Pentagon.

Manche Wissenschaftler sind von dieser Darstellung geschockt. Denn sie befassen sich damit, Systeme zu entwickeln, die tatsächlich eigenverantwortlich handeln können sollen. Systeme, die einen moralischen Kompass fest integriert haben. Die Recht und Gesetz besser kennen als ein Mensch es je könnte. Die somit eine bessere Entscheidung fällen können als jeder noch so erfahrene General. Der Schreckensvision der Killer-Roboter setzen diese KI-Forscher die Vision einer Kampfmaschine entgegen, die sich stets einwandfrei verhält – oder die zumindest weniger Fehler macht als Menschen. Wie, fragen die Forscher, wie will man solche Maschinen verbieten, wie will man es rechtfertigen, trotzdem Menschen die Entscheidungsgewalt zu überlassen?

Thomas Reintjes

Thomas Reintjes ist Wissenschafts- und Technikjournalist. Leitmotive seiner Arbeit sind die Mensch-Maschine-Interaktion und die Frage, wie sich Technik und Gesellschaft gegenseitig beeinflussen. Er ist vor allem für die Hörfunk-Sender der Deutschlandradio-Gruppe, aber auch für Print- und Online-Magazine tätig. Reintjes studierte Technikjournalismus an der Hochschule Bonn-Rhein-Sieg. Im Jahr 2004 gründete er zusammen mit ehemaligen Kommilitonen das Redaktionsbüro Viermann, in dessen Team er bis 2013 in Köln arbeitete. Seit 2013 lebt und arbeitet Thomas Reintjes als freier Wissenschaftskorrespondent in New York. Seine Veröffentlichungen zu Kampfrobotern (*http://deutschlandfunk.de/digitalerkrieg*) wurden mit mehreren Journalistenpreisen ausgezeichnet.

Oder: Sollte man das Leben der Ratte aus dem Experiment *11 TAGE* eher Menschen oder eher einer Maschine mit Moral-Chip anvertrauen?

Ob eine solche Maschine jemals Realität werden kann, ist unklar. Man kann beispielsweise bezweifeln, dass sich Gesetze und Abkommen, Menschenrechte und Völkerrecht in Programmcode übersetzen lassen. Diese Texte sind für Menschen gemacht, nicht für Maschinen. Sie lassen sich nicht nach starren Regeln anwenden, vieles ist Auslegungssache. Und um sie angemessen auszulegen, ist Erfahrung unabdingbar – ein weiterer limitierender Faktor. Lässt sich Erfahrungswissen digitalisieren und in einer großen Datenbank sammeln, aus der ein Roboter schöpfen kann, um seine Schlüsse zu ziehen? Oder ist Erfahrung etwas so Persönliches, dass eine künstliche Intelligenz sie niemals nachempfinden kann?

Doch selbst wenn ein intelligenter autonomer Kampfroboter, der korrekter handelt als Soldaten, gebaut werden könnte, gibt es Gründe, es nicht zu tun. Einer der gewichtigsten ist für mich die Tatsache, dass Soldaten Bürger sind. Sie kommen aus der Gesellschaft, kämpfen für diese Gesellschaft und kehren wieder in die Gesellschaft zurück. Sie entscheiden sich aus freiem Willen zu kämpfen. Und wenn dieser Wille nicht da ist, weil sie der Kriegsgrund nicht überzeugt, dann findet der Krieg nicht statt. „Stell dir vor, es ist Krieg und keiner geht hin" ist mehr als eine pazifistische Parole. Der Spruch verdeutlicht, dass Armeen von ihren Gesellschaften getragen und von der Entscheidung jedes Einzelnen abhängig sind. Selbst wenn ein Roboter mit Moral-Modul im Zweifelsfall Befehle verweigern würde – die Armee würde von der Gesellschaft entrückt und stünde viel leichter zur Disposition der Machthabenden.

Und dann ist da noch das dogmatische Argument, dass Entscheidungen über Leben oder Tod nicht von Maschinen getroffen werden sollten. Manche versuchen, dieses Argument zu entkräften, indem sie darauf hinweisen, dass solche Entscheidungen spätestens mit dem Einzug autonomer Autos in den Alltag permanent von Maschinen gefällt werden würden. Bahnt sich ein unausweichlicher Unfall an, muss das Auto vielleicht entscheiden, ob es nach rechts ausschert und mit der jungen Familie kollidiert, oder nach links und mit dem Motorradfahrer zusammenprallt. In meinen Augen ist es allerdings ein Unterschied, ob in einem Unfallszenario das kleinere Übel algorithmisch bestimmt wird, oder im Krieg Menschen getötet oder nicht getötet werden.

Das Thema ist komplex. Und leider verstecken sich manche der Befürworter autonomer Waffensysteme vor der Öffentlichkeit, andere werden von den Gegnern übertönt. Doch es ist wichtig, beide Seiten zu hören, alle Argumente abzuwägen, denn es geht um viel. Einfache Wahrheiten sind fehl am Platz. Eine gesellschaftliche Diskussion über den Krieg der Zukunft ist dringend nötig. „Leben schützen", das Mantra der Militärroboter-Hersteller ist ehrenwert. Nur ist noch offen, wie man die Leben von Soldaten und Zivilisten tatsächlich am besten und moralisch einwandfrei schützt, welcher Einsatz von Technik und welcher Einsatz von Menschen dafür angemessen ist. Wie gut es gelingen kann, solche Diskussionen in der Gesellschaft beispielsweise durch Kunst anzufachen, hat *11 TAGE* erfolgreich bewiesen.

Udo Kauß

Öffentliche Diskussion nicht erwünscht

Reaktionen von Polizei und Justiz zum Kunstexperiment *11 TAGE*

Das Ziel der Aktion von Florian Mehnert, militärische Drohneneinsätze und deren Problematik in das Blickfeld der Öffentlichkeit zu rücken, spielte weder in den Reaktionen aus dem Netz noch in den Reaktionen von Polizei und Justiz irgendeine Rolle. Dieses Ziel ist, salopp gesagt, Meinung pur und als solche von der allgemeinen Meinungsfreiheit gedeckt. Das ist auch gut so. Es ist die von Florian Mehnert eingesetzte Form, die Kunst-Form eines im Internet präsentierten Scenario mit der Möglichkeit zur sogar aktiven Partizipation an der Tötung einer Ratte, die die Reaktionen aus dem Netz verursachte und darüber die Mühlen von Justiz und Polizei in Bewegung setzte. Weil Florian Mehnert die Aktion nach sechs Tagen abgebrochen hatte, kam es nicht zur härteren Konfrontation mit Polizei und Staatsanwaltschaft, sondern zur Einstellung der gegen Florian Mehnert gerichteten Strafverfahren. Gegen die vielen Personen, die Florian Mehnert beleidigt und bedroht hatten, wurde hingegen erst gar nicht ermittelt.

Gliederung

Der Beitrag ist folgendermaßen gegliedert:

1. Rechtliche Bedingungen des Kunstexperiments
2. Bedrohung von Florian Mehnert
3. Drohnen im militärischen Bereich
4. Drohnen im innerstaatlichen Einsatz
   - durch Polizei und Geheimdienste
   - durch Private

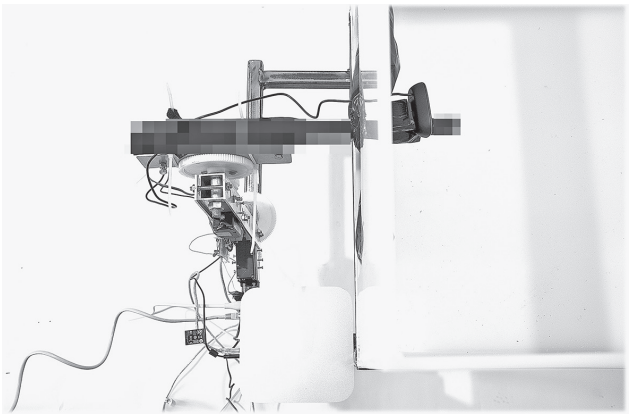
Zu 1. Rechtliche Bedingungen des Kunstexperiments

Vor mir liegen 334 Seiten der staatsanwaltschaftlichen Ermittlungsakte, mit dem Tatvorwurf: Verstoß gegen das Tierschutzgesetz. Diese Akte ist entstanden in dem kurzen Zeitraum vom 15. März 2015, dem Tag des Eingangs der ersten Strafanzeige bei der Polizei, bis zur Einstellung des Verfahrens am 5. Mai 2015.

§17 des Tierschutzgesetzes lautet: „Mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe wird bestraft, wer ein Wirbeltier ohne vernünftigen Grund tötet."

Auslöser für die polizeilichen Ermittlungen gegen Florian Mehnert waren eine Vielzahl von Strafanzeigen, die zum Teil ausführlich juristisch begründet von sich so verstehenden Tierschützern aus allen Teilen der Republik kamen. Diese waren bisweilen eingekleidet in beleidigende Äußerungen (M. sei krank, sollte selbst in Käfig etc.) bis hin zu gegen Florian Mehnert gerichteten Morddrohungen. Soweit sie Beleidigungen und Bedrohungen enthielten, waren diese Anzeigen ausschließlich per E-Mail erhoben worden. Die Anzeigen waren bei Polizeibehörden in ganz Deutschland eingereicht und von den dortigen Landeskriminalämtern an das LKA Baden-Württemberg zur weiteren Bearbeitung abgegeben worden. Das LKA wurde wegen des Wohnsitzes von Florian Mehnert im Badischen als zuständige und damit ermittlungsführende Behörde angesehen.

Am fünften Tage des Experiments hatte die Freiburger Polizei Florian Mehnert in Begleitung des Amtstierarztes aufgesucht und die Apparatur, also Käfig, Ratte, Kamera, montierte *paintball*-Waffe in Augenschein genommen. Ergebnis: Der Besitz der *paintball*-Waffe ist waffenscheinfrei, der Käfig ausreichend groß, angefüllt mit rattenspezifischen Nest-Utensilien, guter Ernährungszustand der Ratte und somit artgerechte Haltung. In diesem Stadium des Kunstexperiments war also alles in Ordnung, kein Verstoß gegen das Tierschutzgesetz und gegen das Waffengesetz und damit keine rechtliche Handhabe gegeben zum staatlichen Einschreiten. Aber:



Die steuerbare Waffe (verpixelt) von oben gesehen. Auf dem Lauf vorne ist die Webcam befestigt.

Von Seiten des ermittlungsführenden Kriminalhauptkommissars wurde Florian Mehnert bedrängt, das Kunstexperiment abzubrechen, weil man schon jetzt von einer Vielzahl von Strafanzeigen und Aufforderungen, dem Experiment ein Ende zu setzen, eingedeckt worden sei. Wenn er das nicht freiwillig tue, dann müsste die Polizei zu anderen, polizeilichen Mitteln greifen, um das Experiment auch gegen seinen Willen zu beenden. Angesichts der bereits jetzt schon erreichten öffentlichen Aufmerksamkeit folgte Florian Mehnert dieser nachdrücklichen polizeilichen Anregung. Er übergab dem Amtstierarzt die Ratte. Das Experiment war damit beendet. Ob die als sogenannte *Futter-Ratte* gekaufte Ratte schließlich als solche und damit bestimmungsgemäß geendet ist, ist unbekannt.

Die Staatsanwaltschaft hat das Verfahren gegen Florian Mehnert eingestellt. Juristische Begründung: Artgerechte Haltung und keine getötete Ratte, also kein Delikt, kein Verstoß gegen das Tierschutzgesetz! Der Versuch zu solch einer Straftat allein ist nicht strafbar. Und man hatte Florian Mehnert geglaubt, dass er die Ratte in Wirklichkeit nicht töten lassen wollte.

Aber was wäre juristisch passiert, wenn die Ratte doch zu Tode gekommen wäre? Das juristische Abwägungsprogramm zwischen Strafrecht und der verfassungsrechtlich geschützten Freiheit der Kunst (Art. 5 Abs. 3 Grundgesetz: „Kunst und Wissenschaft, Forschung und Lehre sind frei") sei in aller Kürze dargestellt.

Weil Kunst nicht durch Gesetze eingeschränkt wird, auch nicht durch Strafgesetze, sind die jenseits aller Gesetze existierenden, sogenannten *immanenten* Schranken der Verfassung zu beachten. Das heißt, in jedem konkreten Einzelfall ist eine Abwägung vorzunehmen. Und diese sieht in aller Kürze folgendermaßen aus:

Der Tierschutz ist seit 2001 in das Grundgesetz aufgenommen (Art. 20a Grundgesetz). Tierschutz ist damit auf gleicher Augenhöhe wie andere Verfassungsgüter, wie die Meinungs- und Kunstfreiheit, angesiedelt. Dass der Tierschutz das tatsächlich nicht ist, wissen wir insbesondere aus der staatlichen Billigung und Unterstützung der Massentierhaltung.

Die Tötung eines *Wirbeltieres* ist nur zulässig, wenn diese „sachlich begründet" ist (s.o. Wortlaut von § 17 TSG).

Die Rechtsprechung hat die Provokation mit der Tötung eines Tieres durchgängig nicht als sachlich begründet erachtet. Denn es gäbe noch viele andere Möglichkeiten, um seinen Protest zum Ausdruck zu bringen. Somit wäre die tatsächliche Tötung der Ratte gemäß dem Tierschutzgesetz strafbar gewesen, auch wenn diese in Berufung auf die Kunstfreiheit des Grundgesetzes erfolgt wäre.

Aber auch ohne Tötung eines Tieres, hier der Ratte, allein im der Schaffung und Öffentlichmachung des Scenario von Ratte und Luftdruckpistole, liegt bereits eine weitere Straftat vor. Der staatsanwaltliche Einstellungsbeschluss widmet sich über mehrere Seiten diesem weiteren und auch für erfüllt gehaltenen Straftatbestand:

Verstoß gegen § 111 StGB:

> *„(1) Wer öffentlich, in einer Versammlung oder durch Verbreiten von Schriften (§ 11 Abs. 3) zu einer rechtswidrigen Tat auffordert, wird wie ein Anstifter (§ 26) bestraft." – also mit einer Gefängnisstrafe bis zu drei Jahren (s.o. § 17 des Tierschutzgesetzes).*

Dieser Tatbestand ist – wie die Staatsanwaltschaft recht schnell (und richtig) darlegt – durch Florian Mehnert erfüllt. Im Einstellungsbeschluss folgen nun sechs Seiten, in denen dargelegt wird, dass ein Kunstprojekt vorliegt und wägt gegeneinander ab:

- Hier Kunstfreiheit gemäß Art. 5 Abs. 3 GG: „Kunst, Wissenschaft, Forschung und Lehre sind frei." Also nicht einschränkbar.

- Dort aber: Was ist Kunst? – Ist das Kunst?

Das Bundesverfassungsgericht hat sich hier klugerweise sehr zurückgehalten: Kunst ist nicht definierbar, eine Definition von

Kunst sei unmöglich. Kunst ist im weitesten Sinne eine Interaktion von Person, Materie und Gesellschaft, wie das Gericht in seinem wegweisenden Urteil zum sogenannten *Anachronistischen Zug* im Jahre 1982 ausgeführt hat (zur Erinnerung: Der damalige bayerische Ministerpräsident Franz Josef Strauß fühlte sich durch einen durch das Land ziehenden, von Künstlern gestalteten Umzug heftigst angegriffen und beleidigt. Ergebnis der Abwägung des Verfassungsgerichts: Beleidigung eigentlich gegeben, aber im konkreten Fall eines Kunstprojekts nicht strafbar):

Kunst plus Aufmerksamkeit plus Provokation: Das darf Kunst!

Und im konkreten Fall des Kunstexperiments des Florian Mehnert: Es liegt eine an sich strafbare Aufforderung zur Begehung einer Straftat vor, aber – Achtung Kunst! – keine Strafbarkeit!

Variation: Wenn Florian Mehnert die Ratte zunächst an seinem Ziel der „elf Tage" festgehalten hätte und die Ratte nicht der Polizei und dem Amtstierarzt ausgehändigt hätte. Womit hätte Florian Mehnert dann rechnen müssen?

Die Polizei hätte kein polizeirechtliches Verbot auf Unterlassung (versehen mit einer Zwangsgeldandrohung etc.) verhängen können, weil sie wusste, dass die Ratte nicht getötet werden sollte. Florian Mehnert hatte das der Polizei glaubhaft mitgeteilt.

Wenn die Polizei trotzdem etwas gegen die durch die Aktion ausgelöste Unruhe und öffentliche Diskussion – und die ihr hierüber verursachte Arbeit – hätte machen wollen, dann wären ihr die Hände gebunden gewesen. Insbesondere hätte sie Florian Mehnert nicht dazu zwingen können, das Experiment abzubrechen, weil er das Experiment gar nicht hatte vollenden wollen. Das einzige, was die Polizei in legaler Weise dann hätte unternehmen können, war die Öffentlichkeit selbst über die nicht bestehende Tötungsabsicht zu informieren, wie es schließlich durch eine Pressemitteilung des Landratsamts als zuständiger (Polizei-)Behörde durch Mitteilung des Abbruchs des Projekts (Zitat: „Die Ratte befindet sich an einem sicheren Ort") geschehen war.

Zu 2. Bedrohung von Florian Mehnert

Florian Mehnert erhielt über Twitter und direkt an ihn gerichtete E-Mails eine Vielzahl beleidigende schriftliche Äußerungen, die von persönlichen Bedrohungen bis hin zu Morddrohungen reichten. Auf Grund dieser Flut hatte Florian Mehnert die örtliche Polizei um Polizeischutz angefragt. Ein paar Proben des im wahrsten Sinne des Wortes sich über Florian Mehnert ergießenden *Shitstorms* machen einen solche Anfrage nachvollziehbar:

- *„warum stellst Du Dich eigentlich nicht gleich selbst in die Box, Du feige Sau?! Auch damit wär dir Aufmerksamkeit garantiert…"* (sbeer99@hotmail.com)

- *„Florian Mehnert ich hoffe Sie werden eines Tages erschossen."* (David Pella@DrunKindDOTA)

- *„Nach dem zwölften Tag wird die Waffe auf dich gerichtet sein! Egal wo du dich befindest: Im Einkaufscenter, im Laden um die Ecke oder auf der Strasse. Dir ist ein Leben ja bekanntlich nichts wert, dann soll es dir gleich ergehen."* (135ser+4ujs8ebiokzv4@guerrillamail.com)

- *„Kann man nach Ablauf der 11 Tage auch Dich elenden Dreck-Nazi per Mausklick abschiessen…?"* (Justin Schneider via Justinschnidi@gmx.ch)

- *„FlorianMehnert MURDERER. I truly hope that if that poor rat gets killed, you do too. You derserve to be shot in the head."* (Madison Olivia via twitter notify@twitter.com)

- *„…Am besten würde Man die Ratte gegen Herrn Mehnert austauschen das wäre das einzig richtige…"* (alex.mooij@hotmail.com)

- *„Wir haben auch ein schönes Spiel erfunden: Wer Dir kräftig in die Schnauze schlägt, bekommt 100 €. Wer Dir deine Knochen bricht, bekommt 200 € und wer dir dein beschissenes Gehirn rausprügelt bekommt 700 €! Wir kriegen dich, du Tierschänder!!!"* (tierfreund@re-gister.com)

- *„Sorry Florian was bist Du für ein perverses A******sowas mit der Ratte zu machen, Dich sollte man in dieses Käfig stecken!"* (Nick Home via nickswiss@gmx.ch)

- *„Christian Weltin: Wo finde ich diese sogenannten Künstler ich glaube der braucht eine Kugel durch den Kpf! Das was die da vorhaden ist echt pervers."* (via: facebook.com/christian.weltin?fref=hovercard)

Die Staatsanwaltschaft Freiburg hat – ohne eine in den Akten nachvollziehbare eigene Ermittlungstätigkeit – die „gegen unbekannt" zunächst eingeleiteten Verfahren am 29. April 2015 eingestellt mit folgender Begründung:

> *„Die Durchsicht dieser E-Mails ergab keine Ansatzpunkte für eine Ermittlung der Täter. Aus Mail-Adressen ist in aller Regel, so auch hier, der wahre User nicht erkennbar. Die Anmeldung von E-Mail-Adressen erfolgt stets über das Internet und vom heimischen PC aus. Gerade in Fällen wie den vorliegenden, wo Straftaten begangen oder angedroht werden, erfolgt die Anmeldung unter Alias-Namen, um eine Strafverfolgung nicht zu ermöglichen. Allein schon aus den verwendeten Namen der Absender ist die Verschleierungsabsicht erkennbar. Das Verfahren musste daher aus tatsächlichen Gründen eingestellt werden."*

Dagegen steht: Die Staatsanwaltschaft hat offenbar in keinem einzigen der vielen hier nur beispielhaft zitierten E-Mails eine Anfrage bei den Providern gemacht. Zumindest bei deutschen Providern hätte eine solche Anfrage zu den Anmeldedaten geführt, auch wenn in den E-Mails selbst Alias-Namen angegeben worden wären. Gleiches gilt für die Inhaber von Facebook-Accounts. Ich halte es für nicht zulässig, von vorneherein auf jegliche Ermittlungen zu verzichten. In jedem Fall hätte bei den von den Providern mitgeteilten Namens-und Adressangaben weiter ermittelt werden können, ob es sich tatsächlich um fiktive Anmeldedaten gehandelt hat. Hiervon kann gerade nicht von vorneherein ausgegangen werden. Dies widerspricht jeder kriminalistischen Logik. Die gegebene Begründung kann nur als

vorgeschoben bezeichnet werden. Ganz offenbar wollten Polizei und Staatsanwaltschaft hier keine weiteren Ermittlungen anstellen, um der Aktion nicht über deren Beendigung hinaus weitere Öffentlichkeit zu verschaffen.

Ist das Internet also doch ein faktisch rechtsfreier Raum? Der Freiburger Oberstaatsanwalt Mächtel hat erst kürzlich in einem Zeitungsinterview dazu aufgefordert, im Internet geäußerte ausländerfeindliche Hass-Kommentare zu dokumentieren und der Polizei zu übergeben, damit diese weitere Ermittlungen durchführen kann (Freiburger Wochenzeitung vom 11. November 2015). Wenn diese so erfolgen wie im hier vorliegenden Fall, dann wird das Internet wirklich zum rechtsfreien Raum.

Zu 3. Drohnen im militärischen Bereich

Die Tötung eines Menschen ist in jedem Falle strafbar, ob unmittelbar oder durch Einsatz einer Drohne, die durch einen Stick elektronisch gesteuert wird.

Wenn aber nach unserer Rechtsordnung das Töten eines Menschen erlaubt ist, dann ist es dies mit oder ohne Drohne:

In Deutschland ist die militärische Tötung von Menschen nur bei völkerrechtlich zulässigem Militäreinsatz erlaubt, also bei einem UN-Mandat oder im sogenannten *Verteidigungs- bzw. Bündnisfall*.

Anders sieht das die USA: dort werden außerhalb von völkerrechtlich zulässigem Militäreinsatz Drohnen zur Tötung von Menschen eingesetzt. Dies sind nach unserer deutschen Rechtsansicht extra-legale, illegale Tötungen. An solchen teilzunehmen, etwa durch Hilfestellung bei Aufklärung und Observation bzw. Zurverfügungstellung von eigenem Aufklärungsmaterial für Zwecke der USA und deren Drohneneinsatzes, ist nach deutschem Recht strafbar und deutschen Stellen verboten. Die soeben beschlossene logistische Beteiligung von deutschen Aufklärungsflugzeugen in Syrien ist – ohne UN-Mandat, ohne den Verteidigungs- und Bündnisfall – ein Verstoß gegen das strafrechtliche Verbot auch nur der Vorbereitung eines Angriffskrieges (§80 StGB). Oder: Wir sind schon im Krieg, aber wer gegen wen?

Zu 4. Drohnen im innerstaatlichen Einsatz

Der Polizei ist im innerstaatlichen Einsatz die Befugnis zur Tötung eines Menschen nur im einzigen Ausnahmefall, dem sogenannten *finalen Rettungs- oder Todesschuss*, erlaubt, wie er in den meisten Polizeigesetzen der Länder normiert ist. Der Einsatz von Drohnen durch die Polizei müsste, da bisher nicht vorgesehen, zusätzlich und ausdrücklich in die Polizeigesetze aufgenommen sein. Drohneneinsätze finden aber schon und insbesondere zur Aufklärung statt. In der Schweiz hatte vor einigen Jahren der Fal schlagartig erste öffentliche Aufmerksamkeit erlangt, in dem die Polizei bei der Drohnenüberwachung eines Waldstückes zur Verfolgung von vermeintlichen Wilderern ein Pärchen beim verbotenen Cannabis-Rauchen entdeckt hat. Es dürfte nicht beim Einzelfall bleiben. Der Einsatz von Drohnen zur heimlichen Beobachtung von oben wird mehr und mehr Bedeutung im polizeilichen Handlungsscenario erlangen. Die polizeiliche Überwachung ist aber nicht ohne konkrete Verdachtsmomente zulässig. Dass diese Voraussetzung eine für die Polizei leicht zu überwindende Hürde ist, zeigt die Praxis der polizeilichen Video-Erfassung von Demonstrationen. Das ist seit Jahren längst polizeilicher Alltag und in den Polizeigesetzen verankert.

Es wird wohl nicht mehr lange dauern, dass über das Ausspähen hinaus der Einsatz von Tränengas von oben ebenfalls zum polizeilichen Handlungsspektrum gehören wird.

- *Geheimdienste:* Hierüber ist nichts bekannt. Ich würde aber nur zu gerne wissen, wie viele Drohnen die Verfassungsschutzbehörden aktuell schon besitzen oder deren Anschaffung in Auftrag gegeben haben.

- *Private:* Der Einsatz von Drohnen ist durch jedermann und jedefrau in gleichem Maße zulässig, wie dies etwa der Einsatz von Modellflugzeugen ist oder das Drachensteigenlassen. Es ist sich an die Höhengrenzen des Flugsicherheitsvorschriften zu halten. Vor allem aber ist beim Einsatz von privaten Spähdrohnen darauf zu achten, dass hierdurch nicht die Rechte Dritter berührt werden. Werden Aufnahmen bzw. Daten von Dritten erfasst, dann ist dies nur zulässig, wenn hierdurch nicht deren Persönlichkeitsrechte verletzt werden. Hierbei sind die Vorschriften des Bundesdatenschutzgesetzes zu beachten. Jede Erfassung von personenbezogenen und personenbeziehbaren Daten, darunter fallen auch Grundstücke, bedarf der vorherigen Erlaubnis der betroffenen Person. Der Verkaufspreis ab € 50,– je nach Modell könnte mit dafür sorgen, dass daraus ein Volkssport wird – und Lüsternheiten jeglicher Art auf Befriedigung hoffen. Viel Arbeit für die Gerichte...

Wo bleibt die Privatsphäre?

Dass der Künstler Florian Mehnert hier immer schon vorausschauende Sensibilität hat, beweist seine Abhör-Installation zur Belauschung von Spaziergängern im Walde. Das ist heute schon Privaten möglich, und erst recht natürlich auch dem Staat. Das führt letztlich zu dem traurigen Befund: Es gibt keine sicheren Orte, keine Privatsphäre mehr, nur Orte, Sphären, auf die sich – gerade – keine Begehrlichkeiten richten.

Udo Kauß

Dr. **Udo Kauß** ist Rechtsanwalt in Freiburg, spezialisiert auf das Recht der Inneren Sicherheit und Datenschutz; Vorsitzender der Bürgerrechtsvereinigung *Humanistische Union,* Landesverband, Baden-Württemberg; Mitautor des 2013 veröffentlichten Memorandums der Bürgerrechtsgruppen *Brauchen wir den Verfassungsschutz? Nein!*

Britta Schinzel

NGOs – wir klagen an und fordern auf

Das Projekt 11 TAGE *berührt die Intentionen des FIfF und anderer gegen Überwachung, Cyberwar und Drohnenkrieg agitierender NGOs auf vielfältige Weise. Der virtuelle Angriff auf die Ratte aus dem Internet simuliert die Drohnen-Zielfindung; das von Florian Mehnert verwendete Mittel von Egoshootern aus der Spielewelt verweist auf die Vermischung der Gamification mit dem Training an modernen Waffensystemen; die Überwachung ist essentieller Teil von Cyberwar und Drohnenkrieg. Nicht zuletzt sind auch die gegen Mehnert instanziierten Shitstorms und Morddrohungen wichtige Themen für NGOs, die sich mit dem IT-Bereich beschäftigen. Hier werden einige dieser Punkte aufgegriffen.*

Einleitung

Es scheint zunehmend nötig, gegen Krieg, Waffenproduktion, und Überwachung zu agitieren, gesellschaftliches Bewusstsein herzustellen bzw. zu schärfen, mehr noch, Einfluss auf Parlamentarier und die Regierung zu nehmen und sogar Verfassungsklagen anzustrengen.

Wer kann in einer Demokratie außerparlamentarisch Einfluss auf die Politik nehmen?

Solche Akteure sind einmal die Medien, zum anderen die Wissenschaften mit Veröffentlichungen, und wie im vorliegenden Fall die Kunst, indem sie Finger in die Wunden legen und Aufmerksamkeit erzeugen. Schließlich können Verbände, Vereine, NGOs mit Demonstrationen, Kampagnen, Veröffentlichungen und Pressemitteilungen zur Bürgerbeteiligung im Internet und auf der Straße aufrufen und Gerichte anrufen. Die FIfF-Kampagnen gegen Überwachung, TTIP, CETA, TISA, u.s.w., sowie jene für Cyberpeace sind dafür gute Beispiele. Ja, die Bundesregierung verlässt sich inzwischen mit ihren zu stark vom Lobbyismus geprägten Gesetzen auf das Korrektiv der Bürgerinitiativen und ihrer Verfassungsklagen, wie sie *Humanistische Union* und *Deutsche Vereinigung für Datenschutz* durchführen. Auch auf EU-Ebene will beispielsweise *European Digital Rights* (EDRi) der Überwachung, dem Cyberkrieg und dem Lobbyismus im Bereich der Informationstechnik entgegenwirken.

Informationstechnik und Krieg:

Krieg, der 2. Weltkrieg, war der erste wesentliche Anschub für die Entwicklung von Computern. Weitere Verwendung fanden Mainframes für den industriellen Komplex, bis Computer mit der Einführung von Homecomputern Mitte der 1980-er Jahre in den privaten Bereich diffundierten. Mittlerweile jedoch werden militärische Anwendungen auf zivile Technologien bzw. auf *dual-use*-Anwendungen aufgesetzt. Informatik-Entwicklungen, die für das Militär mit verwendet werden, sind Bilderkennung und -verarbeitung, Sensoren und Aktuatoren, Robotik. Netzwerke, Datenbanken, Kryptographie und Dekryptierung, Big Data, Künstliche Intelligenz, etc. All dies wird u. a. für die Entwicklung von Killerdrohnen benötigt.

Die derzeit im Einsatz befindlichen UAV *(unmanned area vehicles)* der USAF und der CIA sind die *General Atomics MQ-1 Predators*[1]. Der Predator trägt Kameras, Sensoren und lasergesteuerte Hellfire Luft-Boden Raketen oder andere Munition für ‚Hunt and kill'-Operationen. Er ist verbunden mit einer Bodenkontrollstation in Nähe zum Einsatzgebiet, von wo aus er mittels Sichtdatenlink kontrolliert wird, und einer Satelliten-Kommunikationsverbindung für Operationen ausser Sichtweite. In der Bodenkontrollstation sitzt ein Pilot, der das System fernsteuert und auf der Militärbasis in Nevada oder Ramstein im Pfälzerwald[2] vor ihren Bildschirmen 2 Sensoroperatoren zur Bedienung der Kameras, Sensoren und Radare, und für die Datenanalyse und Kommunikation. Das Fluggerät besitzt ein Multispektral-Zielsystem, eine TV-Kamera und eine thermographische Kamera, die volle Bewegungsvideos produzieren. Es kann bis zu 14 Stunden in der Luft bleiben, bis zu 15 km hoch fliegen, in einem Einsatzradius von 750 km und zurück zur Basis. Die neuere Produktionsserie *MQ-1B* enthält u. a. Verbesserungen des Radarsystems, der Software, der Motoren und der Einspritzung und der Navigation, längere Flügel und duale Alternatoren.

Seit 1995 wurden diese Waffen über Afghanistan, Pakistan, Bosnien, Serbien, Iraq, Yemen, Libyen, Syrien und Somalia eingesetzt. Die Planungen für verbesserte Systeme erweitern die Möglichkeiten bis zur fast vollkommenen Selbständigkeit.

Die Obama-Regierung hat – völkerrechtswidrig – den Einsatz der Killerdrohnen im Vergleich zur Bush-Regierung verfünffacht und nicht nur die Einsatzgebiete, sondern auch die Angriffsziele erweitert. Seither werden nicht nur auf einer Todesliste stehende Terrorverdächtige verfolgt, sondern auch Personen und Gruppen von Personen, die aufgrund von Signaturanalysen unter Verdacht geraten. Signaturen entstehen automatisiert aus Überwachungsdaten, die aufgrund von (geheim gehaltenen) Merkmalen zur Profilbildung von Verdächtigungen dienen. Es überrascht nicht, dass die so genannten Kollateralschäden einer solchen Zielermittlung hoch sind. Die Zahl der so Getöteten liegt im vier bis fünfstelligen Bereich, davon sind vermutlich gut die Hälfte zivile unschuldige Opfer, eine weitere Mehrzahl durch die Signaturmethode unschuldig Verdächtigter, sowie eine kleine Zahl solcher, die tatsächlich Gefährder waren. Ihnen allen ist jedes Recht genommen, das einer Anklage, einer Gerichtsverhandlung, oder auch nur das letzte Menschenrecht, das der Kapitulation.

Tatsächlich sind viele Drohnenpiloten sehr gestresst und unzufrieden mit dieser Art Kriegführung. Viele leiden an posttraumatischen Belastungsstörungen, wenn sie erkannt haben, welche Schuld mit ihrer Rolle beim Ermöglichen dieses systematischen Zerstörens unschuldiger Leben einherging. Am 18. November 2015 kritisierten vier namentlich unterzeichnende ehemalige US-Drohnen-Piloten (drei von ihnen *MQ-1B-Predator*-Piloten) in einem offenen Brief an die US-Regierung den Drohnenkrieg

überdies als ein Terroristen-Rekrutierungsprogramm[3]. Sie hatten jahrelang unter anderem im Irak und in Afghanistan tödliche Drohnen gegen angebliche Terroristen eingesetzt. Sie klagen jetzt in einem offenen Brief diesen Drohnenkrieg als einen einzigen Irrweg an, als eine der verheerendsten Triebfedern des Terrorismus und der Destabilisierung weltweit. Sie fordern die US-Regierung auf, ihre Perspektive zu überdenken, auch wenn ihnen eine solche Bitte angesichts der beispiellosen Verfolgung von Whistleblowern, die ihnen vorangegangen sind – wie zum Beispiel Chelsea Manning, Julian Assange und Edward Snowden – womöglich vergeblich erscheint.

Leider hat Frau von der Leyen bzw. die Bundesregierung beschlossen, in der Bundeswehr ebenfalls Drohnen einzuführen.

Cyberwarfare

Die Snowden-Leak haben nicht nur die Ausspähung unserer Privatsphäre sondern auch deren militärische Dimension gezeigt[4]. Eine der veröffentlichten Folien stellt die *Information Superiority* durch technologischen Fortschritt als wichtigste Voraussetzung für die militärische Überlegenheit der USA auf der Welt dar. Nachgeordnet sind die oben erwähnten, IT-unterstützten konventionellen Waffensysteme. Wichtiger noch sind die neuen Angriffe im Netz, die von Spionage über Informationsmanipulation, der Destabilisierung lebenswichtiger Infrastrukturen bis hin zu vernetzten kriegerischen Operationen reichen. Die Ausspähung des Mobilfunks zur Zielermittlung für Drohnenangriffe gegen Terrorverdächtige verbindet die Cyberwaffen mit dem Drohnenkrieg. Die Möglichkeiten von Cyberangriffen beruhen auf absichtlich installierten oder unabsichtlich fehlerhaftem Code mit offenen Schwachstellen, die für kriminelle Zwecke missbraucht werden können. Da diese geheim gehaltenen Angriffe in den zivilen Informationsströmen mitschwimmen, gefährden sie alle und alles, und den inneren und äußeren Frieden. Auch die gleichzeitig mitbetriebene Industriespionage hat im Hinblick auf die angestrebte strategische Überlegenheit und die technologische Hochrüstung große Bedeutung. Dabei werden Grundrechte ausgehebelt, IT-Sicherheitsstandards mit staatlicher Billigung unterlaufen und unsere informationelle Privatsphäre verletzt.

Viel besser wäre es, die Schwachstellen zu veröffentlichen, damit sie schnell geschlossen werden können. Insbesondere öffentliche Stellen müssen die Integrität von Informationssystemen bewahren. Dies folgt aus dem Grundrecht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Dadurch könnte das öffentliche Bewusstsein und Vertrauen in defensive Sicherheitsstrategien erhöht werden. Unsere Kampagne Cyberpeace hat u. a. dies zum Ziel.

Ein anderes Anliegen der Cyberpeace-Kampagne ist eine klare Sprache, da unklare Sprache zur Eskalation von Konflikten beitragen und unberechtigt kriminalisieren kann. So ist beispielsweise ein Wandel des Sicherheitsbegriffs zu beobachten: von sicheren Infrastrukturen, Datenschutz, Personenschutz, Schutz vor Überwachung und sicherem Bewegen im Internet, hin zu: Sicherheit vor Terrorismus. Dies bedeutet eine Umkehrung des obigen Sicherheitsbegriffs. Die USA hingegen – und nicht nur sie – begründen mit dem Begriff *Sicherheit* ihre NSA-Aktivitäten, den Zwang der Computerfirmen zur Lieferung ihrer Daten an die NSA, die Obstruktion aller Kryptosysteme, usw. Ein neues Gesetz ist in der Pipeline zu solcher Einrichtung der Hardware, die verhindert, dass Benutzende Open Source-Firmware für ihre Geräte nachladen können, was z. B. den sicheren *port 22* mit *ssh* unterbindet.

Überwachung

Sie geschieht in Deutschland nicht nur durch durch äußere Mächte, die NSA, GCHQ, usw., sondern auch durch die deutschen Geheimdienste, Verfassungsschutz, BND, BKA, und die LKAs. Die Fluggastdatenspeicherung wurde durchgewinkt und selbst höchstrichterliche Urteile des BVG und des EuGH gegen die Vorratsdatenspeicherung haben ihre Durchsetzung nicht verhindert.[5]

Tatsächlich wurde in beiden Teilen Deutschlands der Post- und Fernmeldeverkehr seit dem 2. Weltkrieg überwacht[6], ab 1949 in der BRD unter Siegerrecht, ab 1951 unter alliiertem Besatzungsrecht, und 1954 unter Vorbehaltsrecht. Begründet wurde dies mit der Strategie der „doppelten Eindämmung der deutschen und der sowjetischen Gefahr". Die Abhöraffäre 1963/64 brachte die bundesrepublikanische Überwachung des Post- und Fernmeldeverkehrs aus der DDR an den Tag, sowie Informationen über die Zusammensetzung des Verfassungsschutzes mit ehemaligen SS-Angehörigen und Nazigrößen (12 von 16 Leitern des Verfassungsschutzes) – in Umkehrung des Auftrags der doppelten Eindämmung, jedenfalls der Eindämmung von Naziaktivitäten in der Bundesrepublik. 1968 wurde auf die Notstandgesetze das G10-Gesetz zur Beschränkung des Post- und Fernmeldegeheimnisses still und

Britta Schinzel

Britta Schinzel stieg nach ihrem Studium der Mathematik und Physik in die Compiler-Entwicklung in der deutschen Computerindustrie ein. Von dort wechselte sie in die Theoretische Informatik an der TH Darmstadt und habilitierte dort. Im Rahmen ihrer Professur für Theoretische Informatik an der RWTH Aachen arbeitete sie in verschiedenen Gebieten der Künstlichen Intelligenz, initiierte eine Reihe interdisziplinärer Projekte mit Soziologie, Linguistik, Biologie und Medizin und begann sich, zunächst nur in der Lehre, später auch in der Forschung, mit Informatik und Gesellschaft zu beschäftigen.

leise aufgesetzt. Somit wurden 1968 die alliierten Forderungen deutsches Recht und Verfassungsrecht, und jede Bundesregierung verpflichtet, auch ohne Überwachungsvorbehalt der Alliierten deren Überwachungswünsche weitestgehend zu erfüllen. Obgleich es ein ähnliches Gesetz in keinem westlich demokratischen Staat gibt, wurde es nicht öffentlich diskutiert, da die Überwachung nach Anordnung der Alliierten einer strikten Geheimhaltungspflicht unterliegt, die auch mit rigiden Anordnungen rechtlich verankert und mit dem Schutz der Sicherheit der alliierten Streitkräfte begründet wurde. Das Geheimhaltungsgebot sah drastische Strafen dafür vor, dass Informationen zur Überwachung an die Öffentlichkeit gelangten, indem Verstöße mit Landesverratsprozessen, unbegrenzt hohen Geldstrafen, Gefängnis, bis hin zur Aberkennung des aktiven und passiven Wahlrechts bedroht wurden. Kein.e Abgeordnete.r konnte etwaige Verstöße gegen das Grundgesetz auch nur erwähnen. Die Folge war, dass Anträge der Alliierten auf Überwachung im Parlament – und das bis heute – einfach durchgewunken wurden. Das folgende Urteil des Bundesverfassungsgerichts zum G10-Gesetz definierte nicht mehr die Grundrechte als *höchstes Rechtsgut*, sondern den Staatsschutz als *überragendes Rechtsgut*, „zu dessen wirksamem Schutz Grundrechte, soweit unbedingt erforderlich, eingeschränkt werden können."[7] Das G10-Gesetz wurde durch die mehrfach erweiterte Ergänzung zum NATO-Truppenstatut von 1951 ebenfalls erweitert. Die Gelegenheit, die deutsche Wiedervereinigung zur Einstellung der Überwachungspraxen zu nutzen und wirklich einen souveräneren deutschen Staat mit seiner freiheitlichen Verfassung zu etablieren, waren bei den Zwei-plus-Vier-Verhandlungen 1990 nicht durchsetzbar. Die Westmächte waren nicht bereit, die Zusatzvereinbarungen zum G10-Gesetz noch zum NATO-Truppenstatut aufzuheben, vielmehr wurde 1994 insbesondere die Gültigkeit für die Neuen Bundesländer festgeschrieben.

Daher ist die Unterstützung des Drohnenkrieges durch die Bundesrepublik von Ramstein aus gleichzeitig verfassungswidrig und geheim legal.

Der NSA-Skandal bringt mit den Snowden-Leaks laufend neue Enthüllungen zutage, die Massenüberwachung und die Hacking-Aktivitäten der NSA und CGHQ. Die bekannteren Programme PRISM, TEMPORA and XKeyscore werden ergänzt durch das Überwachungsprogramm des Geldtransfers *Tracfin DB*, der Geolokations-Datenbank *Fascia*, dem Telefonüberwachungsprogramm *Mystic retro* oder dem SMS-Überwachungsprogramm *Dishfire*, das 194 Mio. SMS pro Tag abgreift[8]. Unterstützt werden die staatlichen Überwachungsprogramme durch jene der großen Datenzentren und Clouds der privaten Firmen Google, AT&T, Vodafone, Yahoo etc. Die so erfassten riesigen Datenströme werden beispielsweise von der Firma *Narus* mit einem spezialisierten High-Speed-Programm *Narus STA 6400* in Realtime semantisch analysiert.[9] Die Programme *Marina* and *XKeyscore* analysieren die Metadaten und rekonstruieren die Inhalte zum Lesen. Die Konsolidierung dieser neuen Datenflüsse scheint zunächst das reguläre Internet nicht zu stören. Narus jedoch spricht von *actionable information*, da die so gewonnenen Einsichten für politische und ökonomische Vorteile genutzt werden, wie es traditionell die Spionage tut. Die NSA kann ihre autoritäre Position im Netz dazu verwenden, in Kommunikationsflüsse zu intervenieren, Cyberattacken zu starten. Die Programme *MonsterMind* und *Quantumtheory* manipulieren Internetkommunikation mit *deep packet injection*. Damit können Pakete geöffnet, verändert, einzelne Computer infiziert, aber auch kulturelle Codes definiert werden, indem Standardisierungskommittees kontrolliert und beeinflusst werden können. Die NSA markiert Ziele, definiert Signaturen durch Markierungen und kann sie aktivieren, wenn eine Person eine spezielle Seite besucht, eine bestimmte Person kontaktiert oder einen speziellen Service, wie etwa den *Tor*-Browser benutzt. Das Bewusstsein der Menschen, überwacht zu werden, wird sie zu einem veränderten Verhalten veranlassen. So wird globale Politik einseitig und geheim ausgeübt, ohne demokratische Beteiligung, mit der Rechtfertigung, dass Amerika als einzige Supermacht der Welt spezifische Verantwortung trage.

Beabsichtigte Folgen der Überwachung sind die Zerstörung aller Sicherheitsinfrastrukturen durch die NSA. Sie bedroht nicht nur die Privatsphäre, sondern alle IT-unterstützten Infrastrukturen, was zu Angst und Vertrauensverlust führt. Sie unterminiert aber auch demokratische Strukturen und Regierungsaktivitäten. Die NSA-Überwachung ist auch deshalb besonders problematisch für die Demokratie, da sie im Interesse eines einzelnen Staates als *the world's telecommunication backbone* operiert und Technopolitik betreibt. Politik wird also durch Technik und durch Manipulation der (technologischen) Internet-Infrastruktur gemacht, von uns nicht wahrnehmbar. Dies führt zu Vertrauensverlust, verändert unser Verhalten, führt zur Selbstkontrolle und dadurch zum Verlust von Freiheit. Wir befinden uns als Teil eines zentralisierten Überwachungsnetzwerks, dessen Regeln und Zwecke wir nicht kennen, in einer kafkaesken Situation. Das verunsichert, erzeugt Angst und Aggressionen, die sich gegen Stellvertreter entladen, beispielsweise in Shitstorms. Hierfür ist Florian Mehnerts Kunstaktion ein exemplarisches Beispiel.

Giorgio Agamben bezieht sich in seinen Bänden *Homo sacer*[10] (in der Doppelbedeutung von heilig bzw. ausgestoßen als jemand, der – in der souveränen Sphäre – zwar getötet, aber nicht geopfert werden darf), auf Carl Schmitt: Souverän ist, der den Ausnahmezustand ausrufen kann. Agamben sieht darin das politische Paradigma der Moderne: als den permanenten Ausnahmezustand, „der Versuch, die Ausnahme in die Rechtsordnung selbst einzuschließen, durch die Schaffung einer Zone der Unbestimmtheit, in der Tatsache und Recht zusammenfallen". Souverän also ist die Sphäre, in der man töten kann, ohne einen Mord zu begehen, und ohne ein Opfer zu zelebrieren, und heilig, also tötbar, aber nicht opferbar, ist das Leben, das in diese Sphäre eingeschlossen ist. Heiligkeit bezieht sich in diesem Kontext nicht auf das Religiöse, sondern auf die ursprüngliche Einbeziehung des nackten Lebens in die juridisch-politische Ordnung, und das Syntagma *Homo sacer* benennt etwas wie die ursprüngliche „politische" Beziehung, d. h. das Leben, insofern es in der einschließenden Ausschließung der souveränen Ausnahme als Bezugsgröße liegt. Das „Lager" hat Agamben zum exemplarischen Raum des Homo sacer ausgemacht, da es sich zum Ausnahmezustand materialisiert hat, wo die Existenz auf das „nackte Leben" reduziert wird, die Grundrechte nicht eingehalten, die Rechte auf Gesundheit, Privatsphäre und Würde eingeschränkt sind.

Mit dem *war on terror* wird der (nicht legitimierte und nicht explizierte)[11] Ausnahmezustand jedoch sukzessive über die Lager

hinweg ausgeweitet: Drohnenkrieg, Cyberkrieg, geheimdienstliche Massenüberwachung, die Schaffung rechtsfreier Räume, Folter in Lagern, staatlich-technische Zerstörung der Datenschutzinfrastrukturen: hier wird die Ausnahme zur Regel, zur Norm.

Und wer wird nunmehr zunehmend zum Souverän? Es sind die Maschinen, die Programme, die Algorithmen, Datenanalyse-Programme auf ungeheueren Datenmengen, zunehmend selbst lernend, von Menschen nicht mehr rationalisierbar! Und wer kontrolliert sie???

Doch Mehnerts Projekt zeigt auch die Chancen, die der digitale Raum bietet: die einer Gegenöffentlichkeit, eines Mediums zur Aufklärung, und – vermittelt – hoffentlich nicht nur die Utopie struktureller und rechtlicher Revisionen.

Anmerkungen

1 *vgl. https://en.wikipedia.org/wiki/General_Atomics_MQ-1_Predator*
2 *die deutschen G10-Gesetze erlauben dies den USA*
3 *veröffentlicht in ZEIT online*
4 *vgl. Sylvia Johnigk: Let's Clear up the Debris; What the Snowden Leaks Mean for Your IT Security; Vortrag IS4IS Wien, 6th June 2015*
5 *Dabei wird eingeräumt, dass die ganzen Überwachungsmaßnahmen Anschläge wie den jüngsten in Paris nicht verhindert haben, dass sie allenfalls zur Nachbearbeitung solcher katastrophalen Ereignisse nützlich sind.*
6 *wie Josef Foschepoth in seinem Buch „Überwachtes Deutschland – Post- und Telefonüberwachung in der alten Bundesrepublik", Verlag Vandenhoeck & Ruprecht, November 2012 dargelegt hat.*
7 *BVerfGE 30 15.12.1970, S 18, Zitat S 199*
8 *vgl. Sylvia Johnigk: Let's Clear up the Debris; s.o.*
9 *vgl. Laura Fichtner: Scientia est Potentia: Techno-Politics as Network(ed) Struggles, Masterthesis an der Universität Twente, Niederlande.*
10 *Giorgio Agamben: Homo sacer. Souveräne Macht und bloßes Leben; Suhrkamp Verlag, Frankfurt am Main 2002, ISBN 9783518120682*
11 *im Unterschied zum von Hollande gerade für Paris ausgesprochenen 3-monatigen Ausnahmezustand*

Christa Karpenstein-Eßbach

Florian Mehnerts *11 TAGE*:

Zwischen Provokation und Medienästhetik

Dieser Beitrag reflektiert Florian Mehnerts 11 TAGE *aus der Perspektive auf Konkurrenzen zwischen Kunst und Medien unter fünf Gesichtspunkten: mediale/ästhetische Wirkungspotenziale; Krieg und Medien; Realitätsaffinitäten, Fiktion, Simulation; Publikumsbeteiligung; Fragen des ästhetischen Werts.*

Wie ist engagierte Kunst unter den Bedingungen von Medienkonkurrenz möglich? Dieser Frage will ich im Folgenden nachgehen. Mit Medienkonkurrenz meine ich, dass die Künste seit längerem genötigt sind, mit Medien – so verschieden sie sind – um Wirkungsintensitäten und neue Wahrnehmungspotenziale zu konkurrieren. Technische Medien sind nicht das ferne Jenseits der Künste. Florian Mehnerts Kunstprojekt *11 TAGE* nutzt die Möglichkeiten des Internet und der Web-Kommunikation, verbunden mit Anleihen an den Ego-Shootern von Videospielen, also eine Kombination von Information, Kommunikation, Unterhaltung und Spiel. Auf fünf Punkte möchte ich knapp eingehen, um meine Frage aufzufalten.

Wirkungspotenziale

Medien im Sinne von Verbreitungsmedien verlangen nach Aufmerksamkeit und brauchen Einschaltquoten. Dazu gehören verschiedene wirkungsästhetische Strategien. Grob skizziert: die Neigung zu sich überbietendem Sensationismus, die Inszenierung von Präsenz und emotionaler Beteiligung bis hin zum Management der Gefühle, die Evokation von Näheverhältnissen über Entfernungen hinweg und – nicht zu vergessen – die Dominanz des Visuellen und die Unmittelbarkeit der Bilder. Dabei partizipieren Medien am Wirkungspotenzial des Ästhetischen, um neue Ausdrucksweisen, Faszinationen und Intensitäten zu erzeugen. Sie adaptieren künstlerische Traditionen und können sie sich anverwandeln, so wie beispielsweise der frühe Film die Ausdrucksmittel des Theaters adaptierte, so dass das Theater wiederum genötigt war und bis heute wird, sich seinerseits so zu verändern, dass es auf neue technische Medien eine Antwort findet. Im Bereich des Visuellen scheinen die rasanten Tempofolgen der Bilder und ihre senso-motorischen Aufladungen von ästhetischen Artefakten kaum noch überboten werden zu können, und gerade hier könnte es die Kunst im Kampf um Aufmerksamkeit besonders schwer haben. Wie in vielen Video-Kunstwerken, die die Geduld des Betrachters auf eine harte Probe stellen, hebt sich Florian Mehnerts Projekt von der medialen Zeitökonomie des Tempos deutlich ab, denn für die Dauer von elf Tagen soll gar nichts passieren. Man könnte darin eine Zeit der erzwungenen Kontemplation sehen – eine künstlerische Praxis, die nur dann in ihrer Eigenart verständlich wird, wenn man sie in Relation zu den medialen Praxen von Sensation und Tempo sieht. Der Komplex, in dem senso-motorische Aktion, emotionale Beteiligung und Nähe über Ferne hinweg miteinander verschaltet werden, ist auf das Ende verschoben: man muss *durchhalten*. Insofern handelt es sich um einen Sensationismus medial-ästhetischen Zeitmanagements mit abzuwartender Entladung.

Krieg und Medien

Medien sind nicht nur Verbreitungsmedien – sie haben auch eine wichtige technische Seite. Diese Seite führt uns zum Zusammenhang von Krieg und Medien. Zum einen haben Medien eine eminente Funktion im Rahmen von Kriegsberichterstattung und Propaganda. Aber technische Medien haben darüber hinaus eine militärische und kriegerische Genealogie, sie sind (wenn

auch nicht in allen Fällen von Anfang an) Erfindungen von Mitteln zur Kriegsführung. Damit sind nicht Waffen im strengen Sinn gemeint, sondern Geräte und Technologien des Speicherns, Übertragens und Bearbeitens von Informationen zum Zwecke der Kriegsführung, also etwa drahtlose Sprechverbindungen, ohne die kein Kampfflugzeug fliegen und kein U-Boot tauchen, oder Computer, ohne die keine Drohne gesteuert werden könnte. Die knappe Diagnose des illusionslosen Medientheoretikers Friedrich Kittler lautet denn auch: beim zivilen Gebrauch von Medien handelt es sich um einen „Mißbrauch von Heeresgerät". Das gilt für das Radio ebenso wie für Computer oder Internet.

Die Ratte von Florian Mehnert ist nun gewiss kein Kriegsgerät. Aber welchen künstlerischen Missbrauch von Heeresgerät hat Florian Mehnert mit seinem Videoprojekt und ferngesteuertem Schießeisen betrieben? Nun, Mehnert hat die Militärtechnik des Drohneneinsatzes den Leuten als Vergnügungsspiel angeboten, er hat das Amalgam von Medien, Krieg und Unterhaltung nicht dem Dunkel des täglichen Missbrauchs überlassen, sondern ins Licht einer künstlerischen Aktion gestellt.

Fiktion und Simulation

Hier geht es mir um Wirklichkeitsverhältnisse, um Realität, Schein, Fiktion, Simulation. Das ist ein Problem, das sich mit der universellen Maschine Computer und ihren ebenso universell anwendbaren 0-1-Rechenoperationen noch einmal verschärft hat. Wir misstrauen deshalb vielleicht auch manchmal den Bildern. Simulationen kann man als die Erzeugung eines perfekten Scheins bezeichnen, und zwar eines Scheins, dem man eben nicht mehr ansieht, dass es Schein ist, weil er wie das Reale ist. Bei der Fiktion ist das anders: weil die Fiktion als solche kenntlich ist, weiß man, dass sie vom Realen getrennt, ihm gegenüber autonom ist. Simulationen sind hingegen realitätsaffin.

Sie alle kennen vermutlich die Fernsehsendung *Verstehen Sie Spaß?* Hier geraten Leute in eine Situation, in der sie etwas für wirklich nehmen, was es nicht ist – so unwahrscheinlich die Situation auch sein mag. Vielleicht sind die Mitspieler in dieser Sendung auch einfach an die informationstheoretische Regel gewöhnt, die lautet: je unwahrscheinlicher, desto informativer. Wichtig ist hier: der Schein wird verborgen, man wird getäuscht, aufs Glatteis geführt. Ich weiß nicht, ob Florian Mehnert an diese Fernsehsendung gedacht hat. Was aber wäre geschehen, wenn ein Hinweis auf das Sendeformat von *Verstehen Sie Spaß?* in die Kunstaktion eingebaut worden wäre? Ohne solchen Hinweis hingegen lassen sich die *11 TAGE* als eine entwendende Verwendung von geläufigen Medienpraxen verstehen, durch die dem Fernsehen die bloße Unterhaltung durch die Simulation des Realen streitig gemacht wird.

Nun verlaufen die Konkurrenzlinien zwischen Künsten und Medien nicht nur so, dass in künstlerischen Artefakten solche entwendenden Verwendungen von Medien stattfinden, sondern auch umgekehrt: die Künste sind ihrerseits ein Reservoir, aus dem sich Medien bedienen. Eine bemerkenswerte mediale Parallele zu *11 TAGE* war in der *Heute-Show* von Oliver Welke, einer Polit-Comedy, am 27. November 2015 zu sehen. Als Geschenkvorschlag für Kinder zum Weihnachtsfest wurde ein Versuchsbaukasten zum Thema Klimawandel vorgestellt, der dazu verhelfen soll, das ökologische Verantwortungsbewusstsein zu schärfen. Präsentiert wird ein Versuch: in einer durchaus speziesadäquat hergerichteten, nach oben offenen Glaskugel befindet sich eine Maus. Erfahrbar gemacht werden soll, was geschieht, wenn der Meerwasserspiegel steigt. Dazu, so die Versuchsanleitung, wird aus einem großen Gefäß Wasser in die Kugel gegossen. Der Moderator führt diesen Versuch in der Sendung nicht aus, sondern empfiehlt ihn für die spätere häusliche Aktion: Das können Sie zu Hause mit Ihren Kindern ausprobieren. Die strukturellen Ähnlichkeiten – Ratte/Maus, Töten des Tieres, dringlicher politischer Kontext (Drohnen/Klimawandel), experimenteller Charakter, Selbstbeteiligung, Realitätsaffinität – sind bemerkenswert. Eine Affinität liegt ebenso darin, dass der Test testet, wie hoch die Mitmachbereitschaft selbst ist – hierin wiederum dem Milgram-Experiment ähnlich, das die Gehorsamsbereitschaft von Probanden gegenüber Autoritäten, die das Zufügen von Stromschlägen befehlen, testete. Der Unterschied zwischen Sendungen wie *Verstehen Sie Spaß?* oder der *Heute-Show* und den *11 TAGE*n liegt jedoch genau darin, dass jene Sendungen mit einer spezifischen Rahmung versehen sind, die sie in einem *Format* situiert, d. h. situativ eingrenzt und die Rezeption damit steuert. Mehnert hat auf solche Rahmung – etwa in der Form einer Bemerkung, es handele sich um Kunst – verzichtet.

Publikumsbeteiligung

Diese vorangegangenen Überlegungen führen zum vierten Punkt. Wie viele andere Kunstaktionen wird auch die von Florian Mehnert erst durch die Beteiligung des Rezipienten als, wenn man so will, *Werk* vollendet. Dass das Publikum als anwesender Mitmacher und nicht nur als passiver Konsument konstitutiv dabei ist – das kennen wir aus den verschiedensten Medienproduktionen und Sendungen. Hier funktioniert das zumeist weitgehend reibungslos, und diese Beteiligung ist vor allem schon im Programmablauf eingeplant. Ein Künstler aber muss

Christa Karpenstein-Eßbach

Christa Karpenstein-Eßbach, geb. 1951, ist apl. Professorin für Neuere deutsche Literaturwissenschaft an der Universität Mannheim. Wichtigste Veröffentlichungen neben zahlreichen Aufsätzen: Einführung in die Kulturwissenschaft der Medien (2004); Orte der Grausamkeit. Die Neuen Kriege in der Literatur (2011), Deutsche Literaturgeschichte des 20. Jahrhunderts (2014).

sich darum sorgen, ob er sein Publikum findet. Die Beteiligung, die die Kunstaktion vollendet, muss provoziert werden. Aber welche Beteiligung wäre in diesem Fall die richtige gewesen? Eine Reaktion, die statt der Ratte den Künstler ins Visier nimmt? Eine andere, die sich an die Spielregel hält und nach elf Tagen auf die Ratte schießt? Oder noch eine andere, die sich gleichgültig oder befremdet abwendet – also eine Nicht-Reaktion? Vielleicht sind noch andere denkbar. Die Struktur der Provokation von Beteiligung läuft hier darauf hinaus, dass sie weniger auf homogene emotionale oder intellektuelle Reaktionen zielt, sondern qua Provokation Spaltungen des Publikums provoziert. Die *11-TAGE*-Aktion Florian Mehnerts hat in meinen Augen eine gewisse Affinität zu neuen Theaterformen – Stichwort *Theater des Performativen* –, bei denen provozierte Mitmachreaktionen des Publikums häufig auch zu dessen Spaltung führen. Anders als Walter Benjamin, der im Blick auf den Film bemerkte, dass hier die Wahrnehmungskapazität der Filmzuschauer getestet und trainiert werde, haben wir es bei den *11 TAGE*n mit einem provokativen Test zu tun, der die Reaktionen auf einen Test testet.

Fragen des ästhetischen Werts

Schließlich mein letzter Punkt: die Frage des ästhetischen Werts. Engagierte Kunst kommt ohne die Verknüpfung von Ethik und Ästhetik nicht aus, sie hat ein Ethos, das sie ästhetisch in Szene setzt. Würde sie völlig ungebrochen einen moralischen Wert propagieren, wäre sie bestenfalls pastoral, schlimmstenfalls banal. Wenn sie einen ästhetischen Wert haben will, ist engagierte Kunst genötigt, möglichst viele außerästhetische Werte in konfliktreiche Konstellationen zu bringen.

Woher kommt in Florian Mehnerts Kunstaktion der Werte-Konflikt, der der Aktion einen ästhetischen Wert verleiht? Mein Eindruck: er kommt aus den Reaktionen der Rezipienten, und zwar ausschließlich aus falschen Reaktionen. Um es genauer zu sagen: das Publikum dieser Aktion konnte nur alles falsch machen. Das Publikum hat einem Schein geglaubt, dessen Scheinhaftigkeit es nicht erkannt hat. Und: das Publikum hat eine Wirklichkeit angenommen, dabei aber die richtige verfehlt – statt Medien, Krieg und Drohnen lag ihm die Wirklichkeit einer Ratte am Herzen. Wer mehr oder minder empört das Lebensrecht der Ratte in Schutz nimmt, macht sich schuldig, das Lebensrecht der Drohnenopfer vergessen zu haben. Wer sich zum Schuss auf die Ratte entschließen sollte, macht sich nicht nur schuldig, ein armes Tier zu töten, ohne die Lizenz eines Kammerjägers zu haben, sondern zieht den Verdacht auf sich, eine weitergehende, sei es spaßige oder kaltblütige Tötungsbereitschaft an den Tag zu legen und einem Drohnenschützen zu ähneln. Es handelt sich um eine Situation, die klassischerweise als *Double-Bind* bezeichnet wird und die bekanntlich nach keiner der beiden Seiten hin eine *richtige* oder angemessene Auflösung finden kann. Unzutreffend wäre es auch, die *11 TAGE* als einen einfachen Test aufzufassen, denn zum Test gehört die Möglichkeit, ein annährend richtiges Ergebnis erzielen zu können; hier aber testet der Test, und das ist das *Ergebnis*. Sollte sich hingegen jemand auf die Probe gestellt sehen, so bliebe er im Zweifel, was der Grund seiner Probe und der Modus des Sich-Bewährens wäre. Und schließlich – wenn das Publikum all dies nicht falsch gemacht haben sollte: es hätte immerhin noch die Dummheit begehen können, sich an einem Spiel zu beteiligen, das keines war. Man könnte daraus den Schluss ziehen, dass engagierte Kunst unter Bedingungen von Medienkonkurrenzen nicht aufs Richtige setzen, sondern nur Falsches aufs Korn nehmen könnte.

Ulrich Bröckling

Drohnen und Helden[1]

Am 4. Februar 2002 feuerte eine Drohne vom Typ Predator *eine* Hellfire*-Rakete auf drei Männer in der Nähe der afghanischen Stadt Khost und tötete sie. Man vermutete, die CIA habe einen der drei, wegen seiner Körpergröße und seiner grauen Haare, für Osama bin Laden gehalten. Ein offensichtlicher Irrtum, wie sich bald herausstellte. Ein Pentagon-Sprecher erklärte im Nachhinein, „[w]e're convinced that it was an appropriate target," musste jedoch einräumen, „[w]e do not know yet exactly who it was."*[2] *Journalisten berichteten später, bei den Getöteten habe es sich um Zivilisten gehandelt, die auf dem Gelände eines verlassenen Mudjaheddin-Camps nach Altmetall suchten.*

Bei dieser Tötungsaktion handelte sich um die erste bekannt gewordene Operation einer bewaffneten Drohne. Zu Aufklärungszwecken waren die Predators schon seit 1994 eingesetzt worden, mit einem Waffensystem hatte man sie allerdings erst kurz zuvor ausgerüstet. In der Testphase hatten Experten befürchtet, der rückwärtige Feuerstrahl der Raketen könne die Leichtfluggeräte zerstören. Das geschah nicht, und damit begann der rasante Aufstieg der *Remotely Piloted Aircraft* oder *Unmanned Combat Air Vehicles (UCAVs),* so die offizielle Bezeichnung.

Die Bush-Regierung setzte in der Folge bewaffnete Drohnen in Afghanistan und Pakistan zunächst zur Tötung sogenannter *high-value targets* ein, die Angriffe richteten sich gegen bekannte Talibanführer oder Mitglieder von Al Qaida. Unter Obama wurde das Programm massiv ausgebaut, allein während seiner ersten Amtszeit zählte man fünfmal so viele Angriffe wie in den acht Jahren der Bush-Präsidentschaft. Inzwischen machen Drohnen ein Drittel der US-amerikanischen Kriegsluftflotte aus.[3] Die US-Regierung betreibt zwei Drohnenprogramme: ein militärisches, das feindliche Kräfte in den Kriegsgebieten in Afghanistan und dem Irak bekämpft, und ein geheimes unter Verantwortung der CIA, das sich gegen Terrorverdächtige in der gesamten Welt richtet und auch in Gebieten operiert, in denen keine US-Truppen stationiert sind.[4] Dokumentiert sind verdeckte Drohnenangriffe vor allem im Jemen, in Somalia und Syrien. Die Obama-Regierung weitete indes nicht nur die Einsatzgebiete aus, sondern sie erhöhte auch die Anzahl der Ziele. Neben der Tötung namentlich bekannter Terrorverdächtiger, die auf einer vom Präsidenten unterzeichneten Todesliste aufgeführt sind, setzt sie auf *signature strikes.* Diese richten sich gegen „groups

of men who bear certain signatures, or defining characteristics associated with terrorist activity".[5] Die Identität der Zielpersonen ist zunächst noch unbekannt, *signiert* werden sie aufgrund ihres Verhaltens. Anhand einer Lebensmusteranalyse *(pattern of life analysis)* werden persönliche Profile angelegt, die sich aus den von den Überwachungskameras der Drohnen gesammelten Bewegungsmustern speisen, aber auch aus anderen Daten, beispielsweise aus der Auswertung von Mobilfunkverbindungen. In der Summe ergibt das Profiling ein Gesamtbild der zeitlichen, räumlichen und sozialen Verhaltensparameter eines Menschen. Auf diese Weise wird das Töten sukzessive automatisiert; Algorithmen entscheiden, wer sterben muss.[6] Welche Merkmale die Zielpersonen im Einzelnen als Verdächtige ausweisen, das bleibt geheim. Zivile Opfer werden kurzerhand wegdefiniert: Nachdem John Brennan, Obamas Berater in Sachen Terrorbekämpfung, 2011 stolz verkündet hatte, die Technik sei inzwischen so weit fortgeschritten, dass es im Jahr zuvor so gut wie keinen kollateralen Todesfall gegeben habe, deckte die New York Times auf, dass die amtlichen Dokumente alle Männer im wehrfähigen Alter, die sich im Gebiet des Drohneneinsatzes aufhalten, pauschal als Kombattanten einstuften. Korrigiert wurde dies, sofern explizite Hinweise auf die Unschuld der Getöteten auftauchten, allenfalls posthum.[7]

Recherchen unabhängiger Journalisten belegen demgegenüber einen hohen Anteil getöteter Zivilisten; ihr Anteil bewegt sich zwischen 12 und 35 Prozent. Allein für Pakistan gehen sie – Stand Anfang Mai 2015 – von 423 bis 962 zivilen Drohnenopfern aus, darunter zwischen 172 und 207 getötete Kinder, bei einer Gesamtzahl der Getöteten zwischen 2449 und 3949.[8] Rechtlich gesehen ist die Politik der gezielten Tötungen höchst umstritten: Selbst Juristen, die solche Aktionen im Rahmen bewaffneter zwischenstaatlicher Konflikte durch das Völkerrecht gedeckt sehen, stufen Drohnenangriffe auf dem Gebiet von Staaten, mit denen man sich nicht im Kriegszustand befindet, als völkerrechtswidrig ein.

Die *präemptive* Tötung Verdächtiger ohne Anklage und Gerichtsurteil, die mit dem zynischen Euphemismus eines Kollateralschadens belegten Opfer unter der Zivilbevölkerung, die Traumatisierung der gesamten Bevölkerung in den betroffenen Regionen, die täglich 24 Stunden die Drohnen über sich kreisen hören und sehen und die jederzeit fürchten müssen, ohne Vorwarnung unter Raketenbeschuss zu geraten, all das gerät zum Skandal.

Geführt wird der Drohnenkrieg von US-amerikanischer Seite derzeit vor allem mit dem *MQ-9 Reaper*, einer Weiterentwicklung der Predator-Drohne, die für *hunt and kill* Operationen ausgelegt ist. Mit einer Länge von elf und einer Flügelspannweite von zwanzig Metern kann diese Drohne bis zu dreißig Stunden in der Luft bleiben; sie fliegt in einer Höhe von bis zu 15.000 Metern und deckt dabei einen Einsatzradius von mehr als 3000 Kilometern ab. Bestückt ist sie zum einen mit *Hellfire* Luft-Boden-Raketen und lasergesteuerten Präzisionsbomben, zum anderen mit dem Aufklärungssystem *Gorgon Stare*, das zahlreiche Infrarot- und Videokameras sowie Richtlaser kombiniert, bis zu 65 Streaming-Bilder gleichzeitig an unterschiedliche Adressaten sendet und es ermöglicht, eine Fläche von vier mal vier Kilometern in hoher Bildauflösung aus unterschiedlichen Blickwinkeln zu überwachen. Aus einer Flughöhe von 3,2 Kilometern lassen sich damit Nummernschilder entziffern. Das noch in der Planung befindliche Nachfolgesystem heißt *Argus IS*.

Neben einem Bodenteam, das für Start und Landung der Drohne zuständig ist, sind drei Personen für ihren Einsatz erforderlich. Diese Crew besteht aus einem Piloten, der das System fernsteuert, einem *Sensor Operator,* der die verschiedenen Kameras, Radargeräte und Sensoren bedient, und einem *Mission Intelligence Coordinator,* der die Kommunikation mit Analysten, Datenbanken und anderen Crews übernimmt.[9] Während das Bodenteam auf einem Flughafen in regionaler Nähe zum Einsatzgebiet stationiert ist, sitzen die Operatoren im Schichtdienst auf einer Tausende von Kilometern entfernten Militärbasis in Nevada oder im Pfälzerwald vor ihren Bildschirmen. Die Daten werden ihnen in Echtzeit per Satellit übermittelt. Die räumliche Distanz geht allerdings einher mit einer virtuellen Nähe: Mit dem ferngesteuerten Super-Zoom verfolgen die Drohnen-Operatoren ihre Zielpersonen über Tage, Wochen, manchmal Monate, rund um die Uhr. Sie registrieren, wann diese das Haus verlassen, wohin sie gehen, mit wem sie sich treffen. So entsteht eine einseitige, aber geradezu intime soziale Beziehung. Und wenn sie die Hellfires abgefeuert haben, sehen sie aus ebenso großer Nähe, was diese anrichten: Tod und Zerstörung in einem Umkreis von mindestens fünfzehn Metern. Anders als Bomberpiloten, die nach einem Abwurf weiterfliegen und den Schrecken, den sie bringen, niemals zu Gesicht bekommen, bleibt das elektronische Auge nach dem Treffer weiterhin auf den Punkt gerichtet, an dem die Opfer vernichtet wurden.

Es ist diese Virtualität des Tele-Kriegs, es ist der geografische Abstand zwischen waffenbewehrtem Flugobjekt und Bedienungspersonal und damit verbunden die Diskrepanz zwischen der tödlichen Gewalt, denen die Opfer der Drohnenangriffe ausgesetzt sind, und der Sicherheit der Crews in ihren Operation Rooms, welche diese Form der Kriegführung anstößig erscheinen lässt. Kritik kommt nicht zuletzt von militärischer Seite: Der Drohnenkrieg sei ein „‚virtueless war,' requiring neither courage nor heroism", zitiert ein Artikel im New Yorker den vormaligen British Air Chief Marshall Sir Brian Burridge.[10] Ein 19-jähriger Drohnenpilot berichtet von seinem ersten Angriff, bei dem er Fahrer und Beifahrer eines mit Maschinengewehr bestückten Pickups tötete, die eine Patrouille amerikanischer Bodentruppen in Südafghanistan beschossen: „You feel bad. You don't feel worthy. I'm sitting here safe and sound, and those guys down there are in the thick of it, and I can have more impact than they can. It's almost like I don't feel like I deserve to be safe."[11] Die Strategie des gezielten Tötens widerspricht dem soldatischen Ethos mit seiner Idee eines *gerechten Kampfs*. Das Verdikt der Feigheit impliziert auch eine sexuelle Depotenzierung. So hat die offizielle Bezeichnung für die ferngesteuerten Waffensysteme – *Unmanned Combat Air Vehicles* – einen die Männlichkeit anzweifelnden Doppelsinn: *Unmanned* bedeutet im Englischen nicht nur unbemannt sondern auch entmannt.[12]

Militärische Disziplinierung, die Fabrikation gehorsamer Soldaten, muss beides wecken, die Bereitschaft zu töten und die zu sterben, und zu diesem Zwecke werden diejenigen, die zum einen wie zum anderen willens und in der Lage sind, zu Vorbildern erhoben und als Helden verehrt. Das Ethos des fairen Kampfes liefert dafür das normative Gerüst: Die Gefahr, selbst getötet zu werden, suspendiert das allgemeine Tötungsverbot. Nur weil

der Gegner mir ans Leben will und kann, so das militärische Ethos, darf und muss ich ihm das seine nehmen. Mit der kriegerischen Wirklichkeit hatten die Beschwörungen militärischen Heldentums indes niemals viel zu tun. Das Letzte, was sich Soldaten auf dem Schlachtfeld wünschen, ist ein fairer Kampf.[13] Sie wollen überleben, keine Verletzungen davon tragen, nicht in Gefangenschaft geraten, vielleicht Beute machen, sich rächen, ihre Gegner außer Gefecht setzen oder einfach nur töten, und sie werden deshalb alles tun, um auf jeden Fall zu den Stärkeren gehören. Die Geschichte militärischer Rüstung lässt sich als ein einziger Versuch lesen, die Symmetrie der Konfrontation durch technische Überlegenheit zu asymmetrisieren, was durch immer neue Resymmetrisierungsversuche konterkariert wird, die wiederum neue Asymmetrisierungsanstrengungen in Gang setzen und so weiter.[14]

Die Drohnenkriegführung treibt die Asymmetrie von Kampf und technischer Effizienz so weit ins Extrem, dass die eine Seite ganz verschwindet. Die Spielregeln wandeln sich radikal: „Das Paradigma ist nicht jenes von zwei Kämpfern, die einander gegenüberstehen, sondern ein anderes: ein Jäger, der seinen Vorstoß macht, und eine Beute, die flieht oder sich versteckt."[15] Der Krieg wird zur präventiven Menschenjagd: „Es geht weniger darum, spezifische Angriffe zu erwidern, als vielmehr die Entstehung neuer Bedrohungen durch die frühzeitige Ausschaltung ihrer potenziellen Agenten zu verhindern."[16] Drohnen machen keine Gefangenen, und sie erlauben keine Kapitulation.

Das Besondere der *Drohnisierung* des Krieges liegt nicht in der imperialen Machtüberlegenheit, sondern im offiziellen Übergang „von einer Ethik der Aufopferung und Tapferkeit zu einer Ethik der Selbsterhaltung und mehr oder weniger akzeptierten Feigheit".[17] Für die westliche Militärpolitik wird der Schutz des Lebens der eigenen Soldaten zum absoluten Imperativ. Schon eine begrenzte Anzahl von Gefallenen – gemeint sind selbstverständlich nur Tote auf der eigenen Seite – würde die öffentliche Zustimmung zu einem Kriegseinsatz gefährden, so die militärische Begründung für die Umwertung militärischer Werte. Smarte Technologie soll deshalb übernehmen, wofür bisher Kampfeswille und Opferbereitschaft mobilisiert werden mussten.

In der Geschichte des Krieges führten neue und besonders wirkmächtige Waffen häufig auch zur Heroisierung derjenigen, die sie trugen oder lenkten – man denke nur an die Fliegerhelden des Ersten und Zweiten Weltkriegs. Für die Drohnenpiloten trifft das Gegenteil zu: Sie sehen sich dem Vorwurf ausgesetzt, unverbesserliche *Nerds* zu sein, die ihrer puerilen Leidenschaft für Computerspiele nachgehen und vom sicheren Sessel aus die Raketen schon deshalb ohne Skrupel abfeuern, da sie zwischen virtueller und realer Welt kaum mehr zu unterscheiden wüssten. Der *Gamifizierung* des Krieges entspreche eine Playstation-Mentalität der *chair-borne rangers*, die ihre prospektiven Opfer nur als bewegte Bilder auf den Monitoren sähen. Die Air Force klagt über ein *drone stigma*, dem die Crews ausgesetzt seien, und hat Mühe ausreichend qualifiziertes Personal zu finden: „Most pilots don't enjoy flying from a box."[18]

Die militärischen Instanzen betonen inzwischen die besonderen psychischen Belastungen, denen die Drohnen-Operatoren ausgesetzt sein sollen. Die permanente Sorge, versehentlich Unschuldige zu treffen, sowie das emotionale Wechselbad, in der Nachtschicht per Fernsteuerung verdächtige Terrorkämpfer zu töten und am nächsten Morgen die Kinder zur Schule zu bringen, stellen demnach außergewöhnliche Stressoren dar und erhöhen das Burnout-Risiko.

Bedeutet Postheroismus also die Delegation heldenhafter Tugenden an Maschinen, die möglicherweise bald auch auf die menschliche Fernsteuerung verzichten werden? Phantasmen einer Kriegführung ohne tötende Gewalt gleichermaßen als technisches Substitut wie als geradezu hegelianische Aufhebung militärischen Heldentums. Der „prometheischen Scham", dem unhintergehbaren Inferioritätsgefühl der Menschen angesichts der Überlegenheit der von ihnen geschaffenen technischen Werkzeuge, das der Philosoph Günther Anders den Menschen des Atomzeitalters attestierte,[19] korrespondiert die ehrfürchtige Bewunderung ebendieser Werkzeuge.

Helden erzeugen die Drohnen allerdings auf ganze andere Weise: Das ferngesteuerte *targeted killing* führt dem globalisierten Dschihadismus fortlaufend neue Kämpfer zu. Sie setzen der Risikoaversion westlicher Kriegführung die Unbedingtheit ihres Todeswillens entgegen und finden dafür begeisterte Anhänger. Der *suicide bomber* ist die feindliche Komplementärfigur des Drohnenpiloten: „Auf der einen Seite das vollkommene Engagement, auf der anderen die absolute Distanzierung." Während im Selbstmordattentat „der Körper des Kämpfers vollständig mit seiner Waffe verschmilzt, garantiert die Drohne die radikale Trennung der beiden."[20] Der postheroische Traum einer sauberen Kriegführung gebiert heroische Ungeheuer.

Die Diagnose des postheroischen Zeitalters bedeutet daher keinesfalls ein Ende heroischer Anrufungen. Solange politische oder religiöse Mächte auf die Bereitschaft zum Selbstopfer angewiesen sind und sie schüren, wird man Helden suchen und

Ulrich Bröckling

Ulrich Bröckling ist Professor für Kultursoziologie an der Albert-Ludwigs-Universität Freiburg. Seine Forschungsschwerpunkte sind die Soziologie der Sozial- und Selbsttechnologien, Gouvernementalitätsanalysen und die Soziologie des Krieges und des Militärs. Aktuelle Veröffentlichungen: The Entrepreneurial Self. Fabricating a New Type of Subject, London 2016; Das Andere der Ordnung. Theorien des Exzeptionellen, Hg. zus. mit Christian Dries, Matthias Leanza und Tobias Schlechtriemen, Weilerswist 2015.

finden. Der Streit darüber, ob militärischer Heroismus antiquiert ist und wir in der Ära des Postheroismus angekommen sind, führt deshalb nicht weiter. Schon die Frage ist falsch gestellt. In Abwandlung des bekannten Buchtitels von Bruno Latour[21] müsste man stattdessen konstatieren: Wir sind nie heroisch gewesen. Wir sollten es immer nur sein. Und viel zu oft wollten wir es auch.

Anmerkungen

1 *Erweiterte Fassungen des vorliegenden (von B. Schinzel gekürzten) Beitrags erscheinen in Achim Aurnhammer/Ulrich Bröckling (Hrsg.): „Vom Weihegefäß zur Drohne. Kulturen des Heroischen und ihre Objekte", Würzburg: Ergon Verlag 2016, und in der Ausgabe 2/2015 der Online-Zeitschrift Behemoth. A Journal on Civilization zum Thema „Game Changers? Drones at the intersection of military and civilian use" (https://ojs.ub.uni-freiburg.de/behemoth/).*

2 *John Sifton: A Brief History of Drones, in: The Nation, 27.02.2012.*

3 *Asawin Suebsaeng: Drones. Everything You Ever Wanted to Know But Were Always Afraid to Ask, in: Mother Jones, 05.03.2013.*

4 *Jane Mayer: The Predator War. What are the risks of the C.I.A.'s covert drone program?, in: The New Yorker, 26.10.2009.*

5 *Daniel Klaidman: Kill or Capture. The War on Terror and the Soul of the Obama Presidency, New York 2012, S. 41.*

6 *Vgl. Nils Markwardt: Drohnenkrieg. Überwachen und vernichten, in: Die Zeit, 27.10.2014.*

7 *„Mr. Obama embraced a disputed method for counting civilian casualties that did little to box him in. It in effect counts all military-age males in a strike zone as combatants, according to several administration officials, unless there is explicit intelligence posthumously proving them innocent" (Jo Becker / Scott Shane: Secret 'Kill List' Proves a Test of Obama's Principles and Will, in: New York Times, 29.05.2012).*

8 *Das Bureau of Investigative Journalism in London dokumentiert die Zahl der Toten und Verletzten seit 2004, http://www.thebureauinvestigates.com/category/projects/drones/drones-graphs/, 02. Mai 2015.*

9 *Peter M. Asaro: The labor of surveillance and bureaucratized killing: new subjectivities of military drone operators, in: Social Semiotics 23.2, 2013, S. 196–224.*

10 *Mayer, Predator War (Anm. 3).*

11 *Mark Bowden, The Killing Machines. How to Think About Drones, in: The Atlantic, Sept. 2013.*

12 *Vgl. Grégoire Chamayou: Ferngesteuerte Gewalt. Eine Theorie der Drohne, Wien 2014, S. 110. Die folgenden Ausführungen verdanken Chamayous Buch zahlreiche Anregungen.*

13 *„As anyone who has ever been in combat will tell you, the last thing you want is a fair fight" (Bowden, Killing Machines, Anm. 13).*

14 *Vgl. Herfried Münkler: Der Wandel des Krieges. Von der Symmetrie zur Asymmetrie, Weilerswist 2006.*

15 *Chamayou, Ferngesteuerte Gewalt (Anm. 16), S. 44.*

16 *Ebd.: S. 46.*

17 *Ebd.: S. 112.*

18 *Lee Ferran: Drone 'Stigma' Means 'Less Skilled' Pilots at Controls of Deadly Robots, in: ABC News, 29.04.2014, http://abcnews.go.com/Blotter/drone-stigma-means-skilled-pilots-controls-deadly-robots/story?id=23475968, 02. Mai 2015.*

19 *Günther Anders: Über prometheische Scham, in: Die Antiquiertheit des Menschen, Bd. 1. Über die Seele im Zeitalter der zweiten industriellen Revolution, München 61983, S. 21–95.*

20 *Chamayou, Ferngesteuerte Gewalt (Anm. 16), S. 95–96.*

21 *Bruno Latour, Wir sind nie modern gewesen. Versuch einer symmetrischen Anthropologie, Frankfurt a. M. 1998.*

Quelle: Florian Mehnert – Das Kunstexperiment 11 Tage, Vortrag FIfFKon 2015

Kommerzialisierung des Sozialen – Markt und Macht im Zeitalter digitaler Kompletterfassung

FIfF-Konferenz vom 6. bis 8. November 2015 an der Universität Erlangen-Nürnberg

Im Zentrum der 31. FIfF-Konferenz, die vom 6. bis 8. November 2015 unter dem Motto *Kommerzialisierung des Sozialen – Markt und Macht im Zeitalter digitaler Kompletterfassung* an der Universität Erlangen-Nürnberg stattfand, stand die Auseinandersetzung mit digitaler Sensorik, die zunehmend unser Leben durchdringt und unaufhörlich Daten generiert und speichert, von deren Existenz wir oft gar nichts wissen. Die Daten entstehen in Computern und Smartphones, aber auch in Navigationsgeräten, Fitnesstrainern und digitalen Implantaten. Jeder Mensch und jede menschliche Interaktion hinterlässt dadurch digitale Spuren, ein Umstand, den nicht nur Suchmaschinen und soziale Netzwerke zu einem Geschäftsmodell gemacht haben. Nachdem der Mensch als Arbeitskraft und Konsument umfassend überwacht, analysiert und kommerzialisiert worden ist, folgt mit dem Internet der Dinge nun die Kommerzialisierung des privaten und sozialen Lebens? Welchen Wert haben unsere privaten und sozialen Daten und wer verdient an ihnen? Welche Konsequenzen haben Likes, LifeStyle-Apps und das Internet der Dinge auf das Machtgefüge der Gesellschaft?

Ein weiteres Thema der Konferenz war die Kampagne *Cyberpeace* des FIfF, zu der ein (Zwischen-)Fazit gezogen und die Frage diskutiert wurde, wie sie weitergeführt werden soll. Derzeit wird die Kampagne durch die *Stiftung Bridge* gefördert.

Felix Freiling, Professor für Informatik an der Universität Erlangen-Nürnberg und Gastgeber der Konferenz, begrüßte die Teilnehmer.innen am Freitag Abend. Darauf folgten zwei Vorträge: *Miika Blinn*, Referent für Digitales und Medien beim *Verbraucherzentrale Bundesverband* (vzbv) sprach zum Thema *Individuelle Preise – Eine Herausforderung für Verbraucher.* Der Einsatz von Big Data, so Blinn, verändere Wettbewerb und Marktprozesse fundamental. Wenn zunehmend selbstlernende Algorithmen auf Basis von Big Data Preise gestalten, führe dies zu einer erheblichen Informations-Asymmetrie zugunsten der Anbieter. Wenn sich Preise auf Grund nicht nachvollziehbarer Mechanismen im Minutentakt ändern, könne dies die Verbraucher stark verunsichern.

Smart-TVs im Fokus der Datenschutzaufsichtsbehörden war das Thema von *Andreas Sachs,* dem Leiter des technischen Referats beim Bayerischen Landesamt für Datenschutzaufsicht in Ansbach. Als eine der letzten Bastionen des analogen Zeitalters erfahre das Fernsehen durch die (breitbandige) Internetanbindung der aktuellen Geräte, der Smart-TVs, tiefgreifende Veränderungen. Stichworte wie *Konvergenz der Medien* lösen das lineare Rundfunksignal – und damit das anonyme Fernsehen – ab und bieten den Bürgern Angebote wie HbbTV, Mediatheken, personalisierte Dienste und Apps auf dem Fernsehgerät an. Unter der Federführung des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA) haben die Datenschutzaufsichtsbehörden der Länder im Winter 2014/15 ein technisches Prüfprojekt zu den Datenflüssen bei Smart-TVs durchgeführt, mit dem Ziel, eine Basis für eine rechtliche Bewertung und einen aufsichtlichen Vollzug zu schaffen. Im Vortrag wurde neben den technischen Aspekten der Prüfung auch auf die rechtlichen Gegebenheiten und Probleme und die Möglichkeiten der aufsichtlichen Kontrolle bei Smart-TVs eingegangen.

Der deutsche Künstler *Florian Mehnert* erlangte mit mehreren Kunstprojekten und Ausstellungen zum Thema Überwachung international Aufmerksamkeit. Bereits im Rahmen des Schwerpunkts in der FIfF-Kommunikation 3/2015 hatte er von seinem Kunstexperiment *11 TAGE* berichtet, in dem er den Einsatz von ferngesteuerten bewaffneten Drohnen als Folge der Überwachung untersuchte. Die internationalen Reaktionen auf das Projekt waren extrem kontrovers, es folgten ein Shitstorm und Morddrohungen, die Behörden reagierten nervös. Eine Aufarbeitung des Projekts hinsichtlich seiner Reaktionen und aufgeworfenen Fragen bildete den Schwerpunkt von Mehnerts Vortrag. Ergänzend berichtete er von weiteren Kunstprojekten, wie beispielsweise dem Projekt *Waldprotokolle,* in dem er Wege und Lichtungen in Wäldern mit Mikrofonen verwanzte, die vorbeigehende Passanten abhörten. (In der aktuellen Ausgabe der *FIfF-Kommunikation* wird im Rahmen eines Schwerpunkts von einer Veranstaltung in Freiburg berichtet, in der ebenfalls das Kunstprojekt *11 TAGE* Thema war und aus unterschiedlichen

Blickwinkeln – medientheoretisch, kunsttheoretisch, juristisch, soziologisch und zivilgesellschaftlich – beleuchtet wurde.)

Sebastian Hahn bei seinem Vortrag (The Tor Project) – Privacy by Design in a digital World

Sebastian Hahn, Student an der Universität Erlangen-Nürnberg und seit 2008 am *Tor*-Projekt beteiligt, berichtete über *Privacy by Design in einer digitalen Welt.* Historisch betrachtet war das Internet nie dazu gedacht, die Daten seiner Nutzer zu schützen. Die Protokolle, die im Internet Verwendung finden, müssen daher mühevoll erweitert oder ersetzt werden, um die informationelle Selbstbestimmung möglich zu machen. Gleichzeitig werden die Qualitätsprobleme unserer Software-Infrastruktur immer deutlicher sichtbar, ein neuer, ganzheitlicher Ansatz würde der digitalen Welt gut tun. Am Beispiel von *Tor* wird aufgezeigt, welche Probleme Overlaynetzwerke lösen können und wo sie versagen, welche typischen Fehler im Entwicklungsprozess auftreten können und wie versucht wird, diese zu identifizieren und zu beheben, bevor ein Schaden entstehen kann.

Den Abschluss bildete am Sonntag Morgen der Vortrag von *Sebastian Jekutsch: Was gibt's Neues in Sachen Faire Computer?* Sebastian Jekutsch recherchiert und informiert seit nun fünf Jahren über sozialverträgliche IT-Produktion. Er ist Sprecher der AG *Faire Computer* des FIfF und Initiator des *blog.faire-computer.de*. In seinem Vortrag berichtete er davon, was in den letzten Jahren im Bereich der sozialverträglichen IT-Produktion geschehen ist und in welche Richtung sich die Szene entwickelt. Nach einer kurzen Einführung ging es zur Sache: Apple und Samsung, ein Siegel und viele Rankings, Konfliktfreiheit und Sklavenarbeit, Unternehmens- und Konsumentenverantwortung, Fairphone und die faire Nager-IT-Maus. Man erkennt, dass praktisch alle Fortschritte auf Druck aus der Zivilbevölkerung und aus professionell arbeitenden Nichtregierungsorganisationen zustande kamen. Sebastian Jekutsch stellte die Szene vor, in der sich auch das FIfF bewegt. Es folgten Hinweise, wie man sich als Konsument und Aktivist beteiligen kann, wenn einem Fairness wichtig ist. Am Schluss stehen Forderungen, aber nicht an die Hersteller oder uns Konsumenten, sondern an die, die tatsächlich die Macht haben: an die Politik.

Arbeitsgruppen befassten sich mit den Themen *Internet der Dinge*, *Teilhabe an der allgegenwärtigen Kommunikation* und *Grenzen der Biometrie*. Zwei Arbeitsgruppen gab es zur Kampagne *Cyberpeace:* Auf die bisherige Kampagne wurde Rückschau gehalten und davon ausgehend diskutiert, wie sie weitergeführt werden kann. Die Teilnehmenden waren sich einig, dass dieses Thema über den Zeitraum der Förderung durch die *Stiftung Bridge* hinaus zentrales Thema des FIfF bleiben soll und auch künftig – ggf. in abgewandelter Form – auch weitergeführt wird. Ein zweiter, praxisorientierter Workshop hatte zum Ziel, das *Cyberpeace*-Kampagnenlogo zum Blinken zu bringen – dadurch haben wir jetzt einen echten Blickfang für weitere Aktionen der Kampagne.

Bereits am Samstag Abend wurde zum fünften Mal der *FIfF-Studienpreis* verliehen. Die Laudatoren Britta Schinzel und Stefan Hügel gratulierten *Christian Kühne* aus Berlin zum ersten Preis für seine Arbeit *GNUnet und Informationsmacht: Analyse einer P2P-Technologie und ihrer Folgen*, *Laura Fichtner* aus Twente zum Preis für ihre Arbeit *Scientia est Potentia: Techno-Politics as Network(ed) Struggles* und *Angela Meindl* aus Bremerhaven zum Preis für ihre Arbeit *Internet-Profiling. Umfang, Risiken und Schutzmaßnahmen am Beispiel von Google*.

Auf der abschließenden Mitgliederversammlung des FIfF wurde nach dem alljährlichen Rechenschaftsbericht ein neuer Vorstand gewählt. Kern des Vorstandsberichts waren ebenfalls die Kampagnen zu *Cyberpeace* und *Faire Computer,* mit einer beeindruckenden Anzahl von Aktivitäten und Publikationen.

Bei der Vorstandswahl wurden Stefan Hügel als Vorsitzender und Dietrich Meyer-Ebrecht als sein Stellvertreter bestätigt. Als Beisitzer.innen wurden Anne Schnerrer und Benjamin Kees (beide Berlin) sowie Michael Ahlmann (Bremen) neu gewählt und die bisherigen Mitglieder Sylvia Johnigk, Hans-Jörg Kreowski, Kai Nothdurft, Rainer Rehak, Jens Rinne, Britta Schinzel, Ingrid Schlagheck, Werner Winzerling und Eberhard Zehendner bestätigt. Herzlichen Glückwunsch.

Der Veranstaltungsort, die Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)

FIfF-Studienpreis 2015

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

das FIfF verleiht heute seinen Studienpreis 2015.

In einer Zeit, in der die Durchdringung der Gesellschaft mit Produkten der Informatik unvermindert zunimmt, ist die akademische Auseinandersetzung mit ihren Folgen in der Gesellschaft weiter auf dem Rückzug. Informatiksysteme sind geronnene Machtstrukturen. Bei ihrer Konzeption und Implementierung werden Entscheidungen getroffen, die diese Machtstrukturen festlegen und verfestigen. Das Internet, bereits zu Beginn durch das Militär und für das Militär konzipiert, ist zur größten Überwachungsinfrastruktur geworden, die es in der Geschichte gegeben hat – auch wenn freilich das heutige Internet mit dem Netz, das 1969 drei Großrechner miteinander verband, nicht mehr vergleichbar ist.

Das FIfF will seine Möglichkeiten nutzen, dem Abbau des Fachgebiets auf der einen Seite und der militärischen Kolonisierung der Informationsinfrastruktur, die zur Basis unseres Zusammenlebens geworden ist, entgegenzuwirken. Wir tun dies durch unsere inhaltliche Arbeit, durch unsere Kampagnen, Publikationen, Konferenzen und durch unsere Stellungnahmen. Und wir verleihen nun zum fünften Mal den FIfF-Studienpreis.

Mit unserem Studienpreis wollen wir:

1. hervorragende Abschlussarbeiten aus diesem Gebiet auszeichnen und die dahinterstehende Leistung würdigen
2. Aufmerksamkeit für Themengebiete schaffen, die wir für die Entwicklung einer digitalen Gesellschaft für essentiell wichtig halten

Technik ist von der historischen Entwicklung her auf militärische, industrielle und wirtschaftliche Zwecke ausgerichtet. Technik, die funktioniert, wird stets auch hergestellt und angewendet – unabhängig von ihrer Rechtmäßigkeit. Ein aktuelles Beispiel dafür ist die vom EuGH und vom Bundesverfassungsgericht verworfene Vorratsdatenspeicherung, der selbst höchstrichterliche Entscheidungen offenkundig nichts anhaben können – auch hier entscheidet die- oder derjenige, der Macht ausüben kann. Doch es ist die gesellschaftliche Aufgabe der Informatikerinnen und Informatiker, technische Systeme auch von ihren ethischen und rechtsstaatlichen Anforderungen her zu denken, um eine Technik zu verhindern, die zum Selbstzweck wird und schädliche Nutzung als „Sachzwang" etabliert. Mit unserem Studienpreis wollen wir Arbeiten auszeichnen, die dieser Aufgabe gerecht werden.

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

- Professorin **Britta Schinzel** aus Freiburg,
- Professor **Jochen Koubek** aus Bayreuth,
- **Rainer Rehak** aus Berlin,
- **Johannes Starosta** aus Braunschweig
- und mir selbst, **Stefan Hügel** aus Frankfurt am Main

hat aus den sehr guten Einreichungen drei Arbeiten ausgewählt, die wir heute hier prämieren werden.

1. Preis	**Christian Kühne** **Humboldt-Universität zu Berlin** *GNUnet und Informationsmacht: Analyse einer P2P-Technologie und ihrer Folgen*	Laudatio: Stefan Hügel
3. Preis (1)	**Laura Fichtner** **Universiteit Twente** *Scientia est Potentia: Techno-Politics as Network(ed) Struggles*	Laudatio: Britta Schinzel
3. Preis (2)	**Angela Meindl** **Hochschule Bremerhaven** *Internet-Profiling. Umfang, Risiken und Schutzmaßnahmen am Beispiel von Google*	Laudatio: Stefan Hügel

Die Preisträger.innen im Überblick

Stefan Hügel – Laudatio

Christian Kühne: GNUnet und Informationsmacht – Analyse einer P2P-Technologie und ihrer Folgen

Diplomarbeit an der Humboldt-Universität zu Berlin

Technik durchzieht unser gesamtes Leben. Sie beeinflusst, wie wir handeln und agieren, und immer mehr auch, wie wir denken. In Technik spiegeln sich Machtstrukturen wider, durch Technik wird Macht ausgeübt – das sollte uns nicht erst seit den Snowden-Enthüllungen bewusst sein.

Viele halten Technik dagegen immer noch für unpolitisch, manche behaupten das wider besseres Wissen. „Die grundlegende Fragestellung der Informatik ist: Was kann effizient automatisiert werden?“, so schrieb 1989 eine Task Force der ACM, der Association for Computing Machinery. Längst wissen wir, dass diese Formel zu kurz greift. Technik ist politisch, sie muss auch die Frage stellen: „Was *soll* effizient automatisiert werden?“ Und sie muss die Antwort darauf offenlegen.

Mit Technik wird Macht ausgeübt – das ist der Ausgangspunkt der Arbeit *GNUnet und Informationsmacht: Analyse einer P2P-Technologie und ihrer Folgen* von Christian Kühne, die an der Humboldt-Universität zu Berlin verfasst wurde. Die Jury des FIfF-Studienpreises und der Vorstand des FIfF zeichnen diese Arbeit heute mit dem FIfF-Studienpreis 2015 aus. Die Arbeit untersucht die emanzipatorischen Potenziale mit Blick auf Formen informationeller Macht und daran anschließend die Machtverschiebung in der Informations- und Kommunikationsverarbeitung.

„Die konkreten negativen Auswirkungen ungebändigter Informationsmacht … sind vielfältig: angefangen bei subtilen Formen wie der Manipulation ökonomischer Präferenzen oder künstlicher Bedürfnisgenerierung durch verführerische Werbung, die Manipulation ‚digitaler Öffentlichkeit‘, Wirtschaftsspionage, die Hintergehung politischer Institutionen … bis hin zu mörderischen Härtefällen von Drohneneinsätzen“, so heißt es in der Arbeit einleitend. Für Nutzerinnen und Nutzer und erst recht für indirekt von der Technikanwendung Betroffene sind die dahinterstehenden Machtstrukturen meist nicht erkennbar, geschweige denn beeinflussbar.

Die Arbeit analysiert das politische Potenzial des GNUnet – eines Projekts mit dem Ziel, langfristig das Internet als Basistechnologie moderner Gesellschaften durch eine emanzipatorische Plattform zu ersetzen – auf geisteswissenschaftlicher und informatischer Basis. Sie setzt sich mit den Ideen und der Geschichte des GNUnet-Projekts und dem GNUnet als Peer-to-Peer-Netzwerktechnologie auseinander. Außerdem stellt sie die Verbindung zum *kritischen Datenschutzprojekt* her und analysiert das konstruktive Zusammenspiel beider Projekte.

Dazu werden zunächst Selbstbild und Identität des Projekts untersucht, und wie sich Selbstverständnis und Wertesystem des Projekts auf die Technik auswirken. Danach folgt die Untersuchung der sozialen Wirkung, besonders der resultierenden Machtverschiebungen, die als Folgenabschätzung beschrieben werden. Eine alternative Problemperspektive bietet das Datenschutzprojekt, das dem Projekt GNUnet gegenübergestellt wird. Der Abschnitt schließt mit einem Vorschlag zur Einordnung und Bewertung des GNUnet.

Christian Kühne bei Entgegennahme des Studienpreises
Foto: Kai Nothdurft

Der Autor erwartet, dass die Zielsetzung des GNUnet-Projekts erreicht wird: „Vor allem dort, so die gewonnene Erkenntnis, wo Organisationen reine Internetdienste anbieten oder Organisationen als technische Vermittler Einfluss auf physische Netze haben, können starke Machtverschiebungen durch den Einsatz des GNUnets auftreten“, schreibt er zusammenfassend.

Die Arbeit ist, nicht nur für einen Informatiker, sprachlich auf hohem Niveau, der Stil ist ein wenig ausschweifend, das Gesamtwerk aber ist kritische Informatik im besten Sinne. Der Verfasser beweist große wissenschaftliche Kreativität, ihm gelingt es, unterschiedliche Strategien im Umgang mit personenbezogenen Daten konzeptuell zu fassen und damit einem kritischen Vergleich zugänglich zu machen. Aus medienwissenschaftlicher Sicht ist sein Ansatz beeindruckend, die politischen Aussagen von Informationstechnologie herauszuarbeiten und damit die Unschuldsvermutung von informatischen Systemen und Algorithmen einmal mehr aufzuheben.

Derartige Technologien sind immer auch Ausdruck einer Sichtweise ihrer Gestalter, in diesem Fall auf Macht und Herrschaftsstrukturen, auf Staaten und Organisationen sowie auf Individuen, Persönlichkeitsrechte und Privatheit.

Der Datenschutz und das GNUnet verfolgen hier gänzlich unterschiedliche Ansätze, der Datenschutz versucht, die in der Verfassung garantierten Grundrechte inklusive ihrer Einschränkungen im Rahmen des Rechtssystems durchzusetzen, das GNUnet implementiert eine grundlegende Kritik an zentralisierten Herrschaftsstrukturen im Namen eines radikalen Freiheitsbegriffs.

In einem Epilog, der diesen Titel wirklich verdient, fasst der Verfasser seine Arbeit in zwei wichtigen Begriffen zusammen: Zum einen *Informatische Politik* als Menge der Handlungen, die durch den Einsatz von Informationstechnologien auf die politische und soziale Wirklichkeit Einfluss zu nehmen suchen. Zum anderen *Politische Informatik* als theoriegeleitete, kritische Entwicklung und Anwendung von Informations- und Kommunikationstechnologien. Die Arbeit schließt mit dem Satz: „Die große politische Idee des GNUnet-Projekts ... ist vielleicht keine so neue, aber für das radikaldemokratische Projekt ein wichtiger Baustein: das Ersinnen und Etablieren herrschaftsfreier kooperativer Internetdienste." Nicht nur die heute immer offensichtlichere Entwicklung des Internet von einem Instrument der Kooperation und Völkerverständigung hin zu einer militarisierten Infrastruktur für Cyberkrieg, Überwachung und Kommerz zeigt, wie wichtig das ist.

Es wäre zu wünschen, dass es mehr Informatikerinnen und Informatiker gäbe, die über die Kompetenzen verfügten, sowohl den politischen Kern ihrer Technologien zu verstehen und diese andererseits bewusst in sozialen Handlungen einzusetzen.

Die Jury des FIfF-Studienpreises hat sich einhellig für die Auszeichnung der Arbeit entschieden.

Herzlichen Glückwunsch, Christian Kühne, zum FIfF-Studienpreis 2015.

Britta Schinzel – Laudatio

Laura Fichtner: Scientia est Potentia – Techno-Politics as Network(ed) Struggles

Masterarbeit in Science Technology Studies an der Universiteit Twente

Im Anschluss an die durch Whistleblower bekannt gewordenen Überwachungsskandale unternimmt es Frau Fichtner, herauszuarbeiten, wie technologische Infrastrukturen zur politischen Governance dienen. Die Möglichkeiten des Internet werden ja von politischen Akteuren auch dazu genutzt, an demokratischen Prozessen vorbei weit reichende gesellschaftspolitische Steuerungen zu implementieren und damit die politische Agenda festzusetzen. Die Arbeit behandelt die Überwachung aus dem Blickwinkel der politischen Philosophie, ist jedoch informationstechnisch und mit Bezug auf die Snowden-Leaks genau und kenntnisreich ausgearbeitet. Die durch die NSA infiltrierten IT-Netzwerke können als Prototypen für Gilles Deleuze's Kontrollgesellschaften angesehen werden, bei denen die Disziplinierung in die Protokollregeln eingebettet ist. Dabei führt aber die Besonderheit des Geheimen, das diffuse Wissen darüber, Teil eines zentralisierten Überwachungsnetzwerks zu sein, ohne seine genauen Zwecke zu kennen, zu einer kafkaesken Situation, in der wir kaum Möglichkeiten haben uns zu verhalten, um unangenehme Folgen zu vermeiden.

Frau Fichtner analysiert sehr genau auf Hardwareseite die durch Snowden bekannt gewordenen Eingriffe der NSA in das Netz, etwas weniger jene auf Seiten der Protokolle, und noch weniger die auf Applikationsebene. Sie verweist dabei auf die Wichtigkeit der materiellen Seite der Vernetzung, des Abfangens an den verlegten Kabeln und Knoten, sowie damit verbunden, deren Lokalisierung. Das Verspechen, die durch die Überwachung ermöglichte bzw. erfolgte technopolitische Steuerung aufzudecken, wird nur partiell erfüllt. Das liegt vor allem daran, dass die Aktionen der NSA im Geheimen erfolgen und somit schwer zu erraten sind. So kann sie die politischen Eingriffe vorwiegend in ihren Potenzialen darstellen, über solches Wissen Druck aufzubauen, zu erpressen usw. Bekannte Eingriffe sind etwa die Markierung von Signaturen und das für Drohnenangriffe genutzte Profiling, um Zielpersonen für nicht deklarierte Kriege auszumachen. Oder die Nutzung des Vorwissens über Grenzen der Verhandlungsfreiheit von Verhandlungspartnern, etwa bei Verhandlungen über Klimaziele, die zu deren Scheitern führte.

Laura Fichtner, Foto: Kai Nothdurft

Frau Fichtner entwickelt eine theoriegeleitete Methode zur Analyse solcher Governance über technische Netzwerke. Sie verwendet dafür zunächst die pragmatische Demokratie-Theorie von Dewey, zusammen mit den Theorien von Castells und Hickman, die die Rolle technologischer Strukturen in der Politik untersucht haben. Diese sehen die technischen Infrastrukturen als hauptsächlich mit der Regulierung der Kanäle für Interaktionsflüsse befasst, also extrinsisch wirkend. Weiter zurückgreifend auf die Arbeiten der kanadischen Gender-/Technikforscherin Susan Leigh Star über Infrastrukturen, von Alexander Galloway's Analyse der Internet-Netzwerkdiagramme und Manuel Castells' Konzept von Räumlichkeiten für Flüsse wird deutlich gemacht, wie mittels der verschiedenen informationstechnologischen Netzwerke neue Räume geschaffen wurden. Räume, in denen Informations-, Organisations- und Regulierungsflüsse weitgehend unbemerkt und ohne demokratische Beteiligung in sozio-politische Strukturen eingebettet werden. So kann sie zeigen, wie technologische Steuerung und Überwachung inzwischen sogar leitend für politische Prozesse genutzt werden. In solcher Technopolitik spielt die Überwachung durch die NSA eine zentrale Rolle. Fichtner nutzt das empirische Material von Edward

Snowden, um zu zeigen, wie Überwachungstechnologie auf und in der Internet-Infrastruktur operiert, und so deren machtvolle konsolidierende Möglichkeiten für Politik nutzt. Da politische, aber auch kommerzielle Akteure durch Gestaltung der materiellen Infrastrukturen und Strukturierung der Kommunikationskanäle bestimmte soziale Strukturen und Kontrollmechanismen regulieren, bestimmen sie nun auch intrinsisch Politiken in einer Weise, die traditionell durch Legislatur und demokratische Politiksteuerung betrieben wurde.

Die physikalische Ebene, die Protokollebene und die Applikationsebene mit dem User Interface erzeugen strukturierte Räume für soziale Interaktionen. Der obersten Schicht, in der Nutzende sich erfahren, unterliegt eine den meisten unsichtbare Schicht, die nun Edward Snowden sichtbar gemacht hat. Auch wenn das Internet global operiert und geographische Orte somit unwichtig erscheinen, spielen die lokalen Territorien der Orte und Flüsse der NSA-Überwachungsprogramme wie PRISM und ihre zentralisierte hierarchische Organisation eine große Rolle, wie die aus den Snowden-Leaks bekannten Bilder der NSA-Kommunikationskanäle zeigen: die USA sind dort definiert als „the world's telecommunication backbone". Ein anderes Bild bestimmt die globale *information superiority* als erstes Ziel der US-policy zum *war on terror*. Die NSA setzt sich in zentrale Position, indem sie ein geheimes zentralisiertes Netzwerk auf das öffentliche, verteilte Netzwerk aufsetzt, das die Internetprotokolle kreieren. Weiter zielt die NSA auf einen unidirektionalen Informationsfluss hin zu sich, ohne selbst daran teilzunehmen. Die bekanntesten Programme *Upstream* für das Anzapfen des Internetverkehrs auf der physikalischen Ebene von Kabeln und *hubs* und PRISM für die Sammlung von Daten durch die großen amerikanischen Firmen kooperieren für die Datenerfassung. Auch die materielle Zusammensetzung der Kabel ist wichtig, da Glasfaserkabel direkt angezapft werden müssen, weil sie nicht von außen über ihre elektromagnetischen Felder beobachtbar sind, so mittels eines Splitters in einem speziellen Raum *641A* bei AT&T. Überwachungsassemblagen müssen das Erfasste in diskreten Datendoubletten reorganisieren, damit sie untersucht und für gezielte Intervention vorbereitet werden können. In spezifischen hierarchisierten Netzwerken werden die Daten und Flüsse gesammelt und vergleichbar gemacht. Ein wichtiges High-Speed-Programm ist dabei *Narus STA 6400*, das die semantische Analyse riesiger Mengen von Datenverkehr in Realtime leistet, installiert in einem speziellen Raum der Firma Narus. Die NSA speichert in Maryland und Utah riesige Datenmengen von 12.000 Petabyte pro Monat. Sie werden analysiert, dekodiert und semantisch aufbereitet. Die Programme *Marina* and *XKeyscore* analysieren Metadaten und rekonstruieren die Inhalte zum Lesen. Die Konsolidierung dieser neuen Datenflüsse scheint zunächst das reguläre Internet nicht zu stören. Narus jedoch spricht von *actionable information*, da die so gewonnenen Einsichten für politische und ökonomische Vorteile genutzt werden, wie es traditionell die Spionage tut. Die NSA kann ihre autoritäre Position im Netz dazu verwenden, in Kommunikationsflüsse zu intervenieren und Cyberattacken zu starten. Die Programme *MonsterMind* und *Quantumtheory* manipulieren Internetkommunikation, indem sie nicht nur *deep packet inspection*, sondern auch *deep packet injection* betreiben. Damit können Pakete geöffnet, einzelne Computer infiziert, aber auch kulturelle Codes definiert werden, indem Standardisierungskommittees kontrolliert werden können. Die NSA markiert Ziele, definiert Signaturen durch Markierungen und kann sie aktivieren, wenn eine Person eine spezielle Seite besucht, eine bestimmte Person kontaktiert oder einen speziellen Service, wie etwa den Tor-Browser benutzt. Sie erzeugt so verbotene Bereiche, die man besser meiden möchte, wenn man ihre Markierungen denn kennt. Auch kann das Bewusstsein der Menschen, überwacht zu werden, sie zu einem veränderten Verhalten veranlassen. Einseitigkeiten zeigen sich auch darin, dass die informationstechnischen Infrastrukturen geographisch andere Bereiche tangieren als jene, von denen sie ausgehen – in den USA darf nicht in gleicher Weise überwacht werden wie es die NSA, unterstützt durch die *five eyes,* auf der ganzen übrigen Welt tut. Globale Politik wird einseitig und geheim ausgeübt, ohne demokratische Beteiligung, mit der Rechtfertigung, dass Amerika als einzige Supermacht der Welt spezifische Verantwortung trägt. Jedoch war das World Wide Web auf der zweiten und dritten Internet-Ebene ursprünglich als ein verteiltes Netzwerk gedacht, ohne zentrale Autorität, in dem alle Teilnehmenden gleiche Rechte und gleiches Gewicht haben sollten.

Frau Fichtner widmet sich auch der Gegenüberwachung. Diese operiert vor allem auf der Protokollebene. Kryptierung kann die Inhaltsdaten schützen, aber nicht die Metadaten. Letztere können durch das Tor-Netzwerk verschleiert werden. Tor versucht die räumliche Ordnung durcheinander zu bringen und das verteilte Netzwerk zu stärken. Doch auch das verteilte Netzwerk hat keinen demokratischen, sondern eher anarchischen Charakter. Die NSA versucht auch eine Gegen-Gegenüberwachung, indem sie die Kryptierung kompromittiert, sich illegal der Schlüssel bemächtigt, ebenso wie sie Tor-Protokolle kompromittiert und die Kryptierstandards definieren will. Ja, es gelingt ihr, die US-Regierung und nun wohl auch die EU zu Gesetzen zu bewegen, die auf allen *Layers* Sicherheitslücken für sie zur Einführung von Spionagetools offen lässt. Und die alle wichtigen Softwarestandards setzende Firma Microsoft führt *backdoor by design* ein. All dies führt nicht nur zu einem Kampf um die Bedeutung von Werten wie Freiheit und Sicherheit, sondern zu einem technopolitischen Kampf um die intrinsische Regulierung der Kanäle für Interaktionen im Netz. Sowohl die NSA als auch Internet-Aktivisten formen durch Technik spezifische soziale Strukturen und machen so Politik. Die Souveränität der Staaten wird dadurch unterminiert, ebenso wie demokratische Strukturen und Prozesse in der Komplexität der delokalisierten Einflüsse untergehen. Politiker können nicht mehr unbeeinflusst vom anarchischen Charakter der Informationsnetzwerke für die Öffentlichkeit agieren, die sie eigentlich repräsentieren, was in einem Zirkel Überwachung und Governance wünschenswert erscheinen lässt, wie wir dies erleben. Doch Unsichtbarkeit und Geheimhaltung erhöhen die Komplexität, erlauben Machtausübung durch versteckte Zwänge, wohingegen Transparenz, freie Information und freier Kommunikationsfluss die Demokratie stärken könnten.

Die Arbeit verwendet kenntnisreich die philosophische ebenso wie die technische und kritische Literatur und ist in guter englischer Sprache geschrieben. Etliche Wiederholungen allerdings hätten vermieden werden können.

Die Arbeit bereichert unser Wissen über die Technopolitik der NSA, **weshalb wir ihr einen dritten FIfF-Studienpreis verleihen. Wir gratulieren Frau Fichtner herzlich dazu!**

Stefan Hügel – Laudatio

Angela Meindl: Internet-Profiling. Umfang, Risiken und Schutzmaßnahmen am Beispiel von Google

Bachelorarbeit an der Hochschule Bremerhaven

Wenn wir uns im Internet bewegen, hinterlassen wir Spuren, denen Staaten und Unternehmen nur zu gerne folgen. „Daten sind das Öl des 21. Jahrhunderts" – das ist inzwischen ein geflügeltes Wort.

Wirtschaftsunternehmen, große Konzerne wie kleine Start-Ups, bieten Services kostenlos an – *kostenlos* meint hier: ohne dass wir mit Geld bezahlen müssen. Stattdessen bezahlen wir mit unseren Daten, wir werden durch die ganze Welt verfolgt, die Informationen über uns, unsere Vorlieben, unser Verhalten werden immer mehr und immer genauer beobachtet. Detaillierte Profile über uns werden angelegt, und es ist fast unmöglich, sich dem zu entziehen. „*Wenn etwas im Internet kostenlos ist, dann bist Du wohl nicht der Kunde, sondern das Produkt.*"

Die Arbeit *Internet-Profiling – Umfang, Risiken und Schutzmaßnahmen am Beispiel von Google* von Angela Meindl, die an der Hochschule Bremerhaven entstanden ist, setzt sich mit der Problematik dieses Internet-Profilings aus verschiedenen Blickwinkeln auseinander.

Dabei wird anhand von Google auf das technisch Machbare und das datenschutzrechtlich Erlaubte eingegangen. Ein besonderes Augenmerk gilt dem Recht auf informationelle Selbstbestimmung, möglichen Gefährdungspotenzialen und möglichen Schutzmaßnahmen. Die Autorin ist in der Praxis verankert, betreibt einen eigenen Web-Shop und möchte die Nutzung von Shops analysieren, ohne Profile ihrer Nutzer.innen anzulegen – oder Diensteanbietern wie Google die Möglichkeit dazu zu geben.

Webshop der Preisträgerin mit den Datenschutzbestimmungen
Quelle: www.naturkosmetik-deutschland.de

In einem Praxisprojekt wird gezeigt, dass das Ziel der Analyse von Zugriffen auf Webangebote auch ohne umfassendes Profiling erreicht werden kann. Möglichkeiten zur Ausübung des Rechts auf informationelle Selbstbestimmung trotz Profiling bilden den Abschluss der Arbeit.

Im Zentrum der Arbeit stehen Datenanalysen, die nicht in Form eines Angriffs Unbefugter erfolgen, sondern durch die Verarbeitung von Daten durchgeführt werden, die bei der Nutzung von Services im normalen Betrieb anfallen. Daten werden analysiert, auf Basis dieser Analysen werden Prognosen erstellt, um den Nutzer.innen Empfehlungen zu geben. Gleichzeitig ergibt sich ein sehr weitgehendes Persönlichkeitsbild der betroffenen Personen, aus dem weitgehende Schlüsse gezogen werden können. Dabei können sich sowohl korrekte Schlüsse ergeben – damit weiß Google eventuell besser über uns Bescheid als wir selbst – oder es ergeben sich falsche Schlüsse, die sich nachteilig auswirken können, wenn beispielsweise aufgrund der Daten (falsche) Verbindungen zu Terrorismus hergestellt werden.

Zusätzlich wird unser Persönlichkeitsbild auch öffentlich – die durch Google gefundenen Ergebnisse sind für alle Nutzer.innen des Internets einsehbar und machen es auch diesen möglich, sich weit gehende Urteile und Vorurteile zu bilden, beispielsweise Bekannten oder potenziellen Arbeitgebern. Solche Informationen können auch für Mobbing oder Stalking genutzt werden.

Im praktischen Teil der Arbeit werden an einem Online-Shop Möglichkeiten untersucht, für die Betreiber.in notwendige Analysen durchzuführen, ohne die Persönlichkeitsrechte der Nutzer.innen übermäßig zu gefährden. Das bedeutet zweierlei:

- Der Umfang der erhobenen Daten ist minimal, d. h. er geht nicht über das für eine Analyse der Shop-Nutzung durch den Betreiber erforderliche Maß hinaus.

- Die Daten bleiben beim Shop, d. h. sie werden nicht beim Anbieter des Analyse-Service zusammengeführt.

Gegen die zweite Anforderung verstößt beispielsweise *Google Analytics* – mit den Analysen eines Shopbetreibers werden die Daten auch bei Google gesammelt, zusammengeführt und stehen Google dann für weitreichende, übergreifende Analysen zur Verfügung.

Die Autorin untersucht dafür als Alternativen das Analysewerkzeug *Piwik* und den AdServer *Revive* und stellt deren Nutzung dar. Sie kommt dabei zu dem Ergebnis, dass diese Werkzeuge eine vergleichsweise datenschutzfreundliche Alternative zu Google darstellen. Den Abschluss der Arbeit bildet ein kurzer Vergleich der Datenschutzbestimmungen in Deutschland und den USA.

Abschließend stellt die Autorin fest, dass gezielte Werbung ein legitimes Anliegen sei. Dabei muss aber geltendes Recht berücksichtigt und die Sicherheit der Nutzer.innen respektiert werden. Aus ihrer Sicht sind diese Bedingungen in der Praxis häufig nicht erfüllt – die Risiken, die daraus erwachsen, wurden bereits dar-

gestellt. Insbesondere muss es für Nutzer.innen möglich sein, Webangebote ohne Tracking nutzen zu können.

Die Arbeit gibt einen umfassenden Überblick über die heutige Praxis des Internet-Profiling und stellt alternative Möglichkeiten anhand eines Praxisbeispiels dar. Die Arbeit basiert auf der Auswertung einschlägiger Literatur und einem Experteninterview, das mit einem Vertreter des *Chaos Computer Club* geführt wurde.

Durch die Darstellung der Gefährdungen am verbreiteten Beispiel Google, in Verbindung mit einem praktischen, vergleichsweise datenschutzfreundlichen Alternativszenario, stellt die Arbeit eine überzeugende Verbindung von Informatik und ihren gesellschaftlich relevanten Auswirkungen dar. Sie zeigt eine kritische Analyse des Themas und enthält eine umfassende Analyse. Durch die Untersuchung der Alternativen im Praxisbeispiel zeigt sie einen Weg auf, Analysen datenschutzfreundlich durchzuführen und bietet damit eine Alternative zu den verbreiteten Analysetools von Google, die aus datenschutzrechtlicher Sicht bedenklich sind und das Persönlichkeitsrecht der Nutzer.innen gefährden.

Die Autorin betreibt einen eigenen Web-Shop, der die Arbeit motiviert hat und einen starken Bezug zur Praxis herstellt. Wir würden uns wünschen, dass sich die Betreiber von Angeboten im Internet häufiger so intensiv mit den Wirkungen ihres Tuns auseinandersetzten.

Unter all diesen Aspekten hat sich die Jury des FIfF-Studienpreises für die Auszeichnung der Arbeit entschieden.

Herzlichen Glückwunsch, Angela Meindl, zum FIfF-Studienpreis 2015.

FIfF e.V.

Mitgliederversammlung (MV) des FIfF

Erlangen, 8. November 2015, 11:50 – 14:25 Uhr

– Beschlussprotokoll[1] –

Sitzungsleitung: Stefan Hügel als Vorsitzender des FIfF.

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

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

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

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

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

   Stefan Hügel berichtet über die kontinuierliche Arbeit des FIfF seit der letzten MV und über den Haushalt mit Stand 5.11.2015. Außerdem berichten Vertreter der Regionalgruppen. Es wurden keine Beschlüsse gefasst.

4. **Bericht der Kassenprüfer**

   Für die am 10.6.2015 in Bremen durchgeführte Kassenprüfung durch Klaus Lüttich und Kurt Fussangel berichtet Klaus Lüttich der MV. Aus dem Kassenprüfungsprotokoll: „Dem Vorstand wird eine dem Vereinszweck entsprechende, ordnungsgemäße Kassenführung bescheinigt. Einer Entlastung des Vorstandes steht nach unserer Auffassung nichts entgegen. Wir beantragen die Entlastung des Vorstandes."

5. **Diskussion der Berichte**

   Es wurden keine Beschlüsse gefasst.

6. **Entlastung des Vorstandes**

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

7. **Neuwahl des Vorstandes**

   MV wählt einstimmig Peter Bittner als Wahlleiter und Michael Ahlmann als Wahlhelfer. Es sind 22 stimmberechtigte Mitglieder anwesend.

   Wahl des **Vorstandsvorsitzenden**:

Vorschlag:		
Stefan Hügel	abgegebene Stimmen	22
	gültige	20
	ja	20
	nein	0
	enthalten	0

   Stefan Hügel ist gewählt und nimmt die Wahl an.

   Wahl des **stellvertretenden Vorstandsvorsitzenden**:

Vorschlag:		
Dietrich Meyer-Ebrecht	abgegebene Stimmen	22
	gültige	21
	ja	20
	nein	0
	enthalten	1

   Dietrich Meyer-Ebrecht ist gewählt und nimmt die Wahl nach der MV an.

Wahl der **Beisitzerinnen und Beisitzer:**
Abgegeben: 22 | Gültig: 22

Vorschläge	ja/nein/enth.	Wahl angenommen
Benjamin Kees	19/2/1	ja
Ingrid Schlagheck	19/1/2	ja
Sylvia Johnigk	14/3/5	ja
Kai Nothdurft	20/1/1	ja
Jens Rinne	19/1/2	ja
Hans-Jörg Kreowski	21/0/1	ja
Michael Ahlmann	16/1/5	ja
Rainer Rehak	20/0/2	ja
Britta Schinzel	21/0/1	ja
Eberhard Zehendner	16/3/3	ja
Werner Winzerling	17/2/3	ja
Anne Schnerrer	16/2/4	ja

8. Neuwahl der Kassenprüfer

Die MV wählt im Block einmütig bei 2 Enthaltungen zu den neuen Kassenprüfern des FIfF: Peter Bittner (stimmt zu), Kurt Fussangel (lehnt die Wahl nach der MV ab), Klaus Lüttich (stimmt zu) und Gernot Lucks (stimmt nach der MV zu).

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

Kai Nothdurft erläutert seinen Vorschlag: „Der Vorstand kann Mitgliedern die Funktion der Sprecher.in des FIfF für ein Fachgebiet geben." Wird auf der nächsten Vorstandssitzung behandelt.
Benjamin Kees regt an, wo es rechtlich möglich ist, E-Mail statt Briefe zu versenden.

10. Anträge an die Mitgliederversammlung

Es lagen keine Anträge vor.

11. Verschiedenes

Es lagen keine Anträge vor.

12. Genehmigung des Protokolls

Das Protokoll wird einstimmig genehmigt.

1 Inoffizielle Fassung, redaktionell bearbeitet (Zustimmungen aktualisiert, Stand 23. Januar 2016). Die offizielle Fassung liegt in der FIfF-Geschäftsstelle vor.

Dagmar Boedicker

Aus der Regionalgruppe München

Lesen gegen Überwachung

Am 31. Oktober war auch München bei der bundesweiten Aktion Lesen gegen Überwachung *dabei. Unser neues FIfF-Mitglied Manuela hat im Olympiadorf München eine Lesung organisiert, die einen fantastischen Spannungsbogen mit überzeugender Argumentation verband.*

Vier Akteure, zwei davon Laien-Schauspieler, lasen aus Büchern von Cory Doctorow *(Little Brother),* Ilija Trojanow/Juli Zeh *(Angriff auf die Freiheit),* Stefan Aust/Thomas Ammann *(Digitale Diktatur)* und Glenn Greenwald *(Die globale Überwachung).*

Die Lesung begann mit dem *ganz normalen* überwachten Alltag, erläuterte und begründete die informationelle Selbstbestimmung als Voraussetzung der Demokratie und kulminierte in einem engagierten Plädoyer, ihre Aufrechterhaltung nicht als Selbstverständlichkeit zu verstehen, sondern sie zu verteidigen.

Der jüngste Vortragende[1] war fast im Alter des 17jährigen Helden von Doctorow. Den Roman würde ich nach dieser Leseprobe allen Jugendlichen (ab 13/14 Jahren) auf den Geschenktisch legen: Spannend, witzig und klug. Eine so überzeugende und verständliche Erklärung für *false positives* hätte ich gern schon vor Jahren gelesen.

Manuela gab die Einführung in das Thema, schilderte die Geschichte des Datenschutzes, beschrieb die Rollen von Staaten und Unternehmen bei den Überwachungs-Aktivitäten und beschloss die Veranstaltung mit der Aufforderung Zehs/Trojanows an uns alle, diejenigen nicht zu vergessen, die dafür gekämpft haben, dass wir heute frei diskutieren, auf die Straße gehen oder eine Regierung abwählen können. – Manche bezahlten den Kampf mit ihrem Leben. Heute ist jeder aufgefordert, an den demokratischen Prozessen teilzunehmen und auf seine gewählten Abgeordneten einzuwirken.

Manuela, Manja Evers und Fritz Götz trugen in wechselnden Rollen aus *Angriff auf die Freiheit* vor, im Wechsel mit dem begabten jugendlichen Vorleser mit Stellen aus Doctorows *Little Brother,* was eine angenehme, abwechslungsreiche Form war. Es kam nicht eine Minute Langeweile auf, obwohl sicher nicht alle Zuhörerinnen und Zuhörer den Datenschutz als Leidenschaft betreiben. Alle wünschten sich eine weitere Lesung zum Thema im nächsten Jahr. Beim anschließenden Gespräch interessierten sich auch viele für das FIfF, insbesondere die Cyberpeace-Kampagne.

Anmerkung

1 hier aus Datenschutzgründen nicht mit Foto und Namen vorgestellt

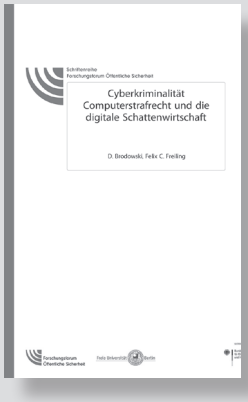
Eberhard Zehendner

Dominik Brodowski und Felix Freiling: „Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft“

Nicht selten würzen Darlegungen zum Thema *Cybercrime* eine dürftige Faktenlage mit spektakulären Fallbeschreibungen, Mutmaßungen und angsteinflößenden Bildern, die mit tatsächlichen Gefahren wenig zu tun haben. Ganz anders die von dem Rechtswissenschaftler Dominik Brodowski und dem IT-Sicherheitsexperten Felix Freiling gemeinsam verfasste, thematisch perfekt verzahnte Studie: Unaufgeregt, ohne die üblichen reißerischen Aufmacher und Übertreibungen, streng auf wissenschaftlicher Literatur und eigenen Erfahrungen der Autoren beruhend, so präsentiert sich das Werk, das klären, erklären, aufklären möchte – das Thema aus vielen Richtungen beleuchtend und mitunter keine leichte Kost.

Eingangs verdeutlichen die Autoren im amüsant geschriebenen Grundlagen-Kapitel *Informationstechnische Systeme,* das von Laien wie Experten mit Gewinn gelesen werden kann, fünf Prinzipien der Informationstechnik, die *im Zusammenspiel mit krimineller Energie die heutigen und vermutlich auch die zukünftigen Trends im Bereich der Cyberkriminalität erklären* könnten: *Automatisierbarkeit, Flüchtigkeit, räumliche Entgrenzung, Kopierbarkeit und Angreifbarkeit.* Sehr plastisch bedeutet z. B. räumliche Entgrenzung, *dass im Internet jeder eines jeden Nachbarn ist, man also nicht wie in der realen Welt versuchen kann, in einer »besonders sicheren Gegend« zu wohnen.* Überdies finden sich bereits in diesem Kapitel (unerwartet) programmatische Überlegungen, was sich schon im einleitenden Satz zeigt: *Ohne Zweifel ist die moderne Informationstechnologie ein wesentlicher Antrieb für neue Formen der Kriminalität.* Der aktuelle Zustand des *Cyberspace* wird als *mit all seinen Unsicherheiten zu einem gewissen Grad unvermeidbar* dargestellt, als historische Folge der technischen Rahmenbedingungen. Dass es *unmöglich ist, Software zu schreiben, die keine Fehler enthält,* und *unser Wissen über die prinzipiellen Ursachen und die Natur von Systemschwachstellen heute noch sehr gering* ist, kann dabei nicht oft genug betont werden.

Auf die *Unkundigkeit vieler Benutzer* und *unzureichende Erfahrung der gesamten Gesellschaft im Umgang mit vernetzten Computersystemen* gehen die Autoren anschließend bewusst nicht weiter ein, da sie die *Schwachstelle Benutzer* nicht als ursächlich ansehen. Wohl aber als problemverstärkend, denn der Wunsch nach immer mehr *Features* von Software führt typischerweise zu höherer Komplexität und damit zu mehr Schwachstellen. Ob in der Praxis tatsächlich *qualitativ kaum mehr ein Unterschied zwischen der Komplexität, die man von der realen Welt kennt, und der des Cyberspace besteht,* mag bezweifelt werden, doch die *Erkenntnis, dass es bei einer hinreichenden Komplexität des zugrunde liegenden informationstechnischen Systems im Cyberspace genauso wenig die spurenlose Straftat gibt wie in der realen Welt,* beleuchtet die Bedeutung der Computerforensik für die Strafverfolgung: Der Cyberspace, obwohl vielfach als virtuell verstanden, ist *schlussendlich doch wieder Teil der realen Welt;* Handlungen im Cyberspace können *auf Handlungen in der realen Welt zurückgeführt werden,* was *die rechtliche Erfassung und forensische Auswertung von Straftaten im Internet* ermöglicht.



Dominik Brodowski und Felix C. Freiling:
Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft.
Schriftenreihe Sicherheit, Nr. 4.
Berlin: Freie Universität Berlin, Forschungsforum Öffentliche Sicherheit, 2011.
ISBN 978-3-929619-66-9
Kartoniert, 222 Seiten

Bestellung und Download:
www.sicherheit-forschung.de/publikationen/schriftenreihe/
Liegt z. B. unter *www.sicherheit-forschung.de/publikationen/schriftenreihe/sr_v_v/sr_4.pdf*

Im Kapitel *Cyberkriminalität und Computerstrafrecht als ungeklärte Begriffe* führen die Autoren sodann aus, dass Begriffe wie *Cyberkriminalität, Computerkriminalität, Computerstrafrecht* oder *Internetstrafrecht* in der deutschen Strafrechtsordnung gesetzlich nicht definiert sind, im Recht der Europäischen Union uneinheitlich (und außerhalb juristischer Fragestellungen regelmäßig unpräzise) verwendet werden und daher erst zu erschließen sind. Denn mit diesen Begriffen muss ein weites Feld von Konstellationen erfasst werden, in denen die Verwendung informationstechnischer Systeme das Strafrecht vor neue Herausforderungen stellt. Aus dem Blickwinkel der Rechtswissenschaft werden informationstechnische Systeme einerseits als Mittel zur Vorbereitung oder Begehung herkömmlicher Straftaten betrachtet. Computer- und Internetdelikte im engeren Sinne (Ausspähen und Abfangen von Daten, Computersabotage, Computerbetrug u. a. m.) sehen informationstechnische Systeme dagegen als (unmittelbares) Angriffsobjekt vor, auch wenn die Strafnormen mittelbar Zwecken wie dem Vermögens- oder Geheimnisschutz dienen.

Die Informatik interessiert sich mehr für die Rolle der Technik als für die Begehungsmodalität; nicht scharf, aber für die Strafverfolgung nützlich, wird technikorientierte von menschenorientierter Cyberkriminalität unterschieden. *Technikorientierte* Cyberkriminalität (u. a. Phishing, Computersabotage, Datenmanipulation,

Botnetze) benutzt Schadsoftware und korrespondiert weitgehend zur Begehungsmodalität des Computers als Angriffsobjekt, obwohl teilweise auch Social-Engineering-Angriffe darunter fallen. *Menschenorientierte* Cyberkriminalität (wie Cyberstalking oder eBay-Betrug) basiert auf technisch unterstützter Kommunikation zwischen Menschen und entspricht eher dem Computer als Begehungsmittel, was *kriminalistisches Gespür* erfordert und der traditionellen Ausbildung vieler Strafverfolger entgegenkommt. In der Informatik ausgebildete IT-Sicherheitsexperten können ihre Stärken dagegen besser gegen technikorientierte Cyberkriminalität einsetzen. Die Autoren vertreten daher die Auffassung, dass es zur Bekämpfung technik- wie menschenorientierter Cyberkriminalität erforderlich ist, die Strafverfolgungsakteure (unterschiedlich gewichtet) sowohl sozial-kriminalistisch als auch technisch-kriminalistisch adäquat auszubilden.

Für ihr Werk wählen die Autoren nun eine (im juristischen Sinne) materielle Sichtweise: Cyberkriminalität wird verstanden als *alle sozialethisch erheblich zu missbilligenden, sozialschädlichen Verhaltensweisen, die verfassungskonform unter Strafe gestellt sind oder unter Strafe gestellt werden könnten, und die entweder als Angriffsobjekt oder als Begehungsmittel informationstechnische Systeme einsetzen; Computerstrafrecht als Oberbegriff für alle Aspekte des Straf- und Strafprozessrechts, welche eine Cyberkriminalität betreffende Strafdrohung anordnen und durchzusetzen versuchen.* Dies lenkt den Blick auch auf zukünftig erst noch als Delikt zu verstehende Praktiken sowie daran angepasste Methoden der Ermittlung und Strafverfolgung – einschließlich einer Bewertung von Sinnhaftigkeit, Nutzen und Risiken bestehender Strafnormen und zukünftiger Veränderungen. Verfassungsrechtliche Grenzen des materiellen wie auch des prozessualen Computerstrafrechts sowie mögliche Regelungsmodelle des Öffentlichen, Zivil- und Strafrechts zur Steuerung von Cyberkriminalität werden ausführlich im Kapitel *Cyberkriminalität: Verfassungsrecht, Regelungsmodelle und Alternativen* diskutiert.

Durch immer stärkere Nutzung des Cyberspace für bereits vorher übliche Aktivitäten treten darauf bezogene *klassische* Delikte wie Betrug oder Erpressung nun auch (in entsprechender Form und häufig vergrößerter Dimension) als Cyberkriminalität auf. Hinzugekommen sind aber auch qualitativ neue Delikte, die typisch für den Cyberspace sind, aus den dort veränderten Rahmenbedingungen resultieren und mit spezifischen technischen und juristischen Mitteln verfolgt werden müssen. Im Kapitel *Von klassischer Kriminalität zur Cyberkriminalität* werden diese Entwicklungen nachgezeichnet und damit verbundene Herausforderungen eng auf die eingangs erwähnten fünf Prinzipien der Informationstechnik bezogen erklärt. Hinsichtlich der Täter, der Cyberkriminellen, über die es insgesamt wenig gesicherte Erkenntnisse zu geben scheint, interessieren die Autoren sich vorwiegend für solche mit finanziellen Motiven und charakterisieren diese im spannenden Kapitel *Wertschöpfungsprozesse, Akteure, Schäden.* Die Tätergruppen zu klassischen Delikten scheinen beim Übergang ins Internet unverändert, IT-Sicherheitsvorfälle in Unternehmen und Behörden häufig von in deren Bereich Beschäftigten verursacht. Darüber hinaus fallen neben einer zunehmenden Zahl von Einzeltätern, die ohne besondere Kenntnisse mit frei im Netz verfügbaren Angriffswerkzeugen Straftaten im Netz begehen, vor allem weltweit vernetzte kriminelle Gruppen auf, die in ihrer Gesamtheit durch den Begriff *Schattenwirtschaft* zutreffend beschrieben werden, deren Organisationsformen sich aber stark von denen der klassischen organisierten Kriminalität unterscheiden. Im weiteren Verlauf des Kapitels werden Mechanismen der Arbeitsteilung und Wertschöpfung dieser Schattenwirtschaft sowie daraus entstehende Schäden prinzipiell dargestellt sowie an Beispielen verdeutlicht. Als wichtige Schlussfolgerung erscheint das individuell, in der Öffentlichkeit und auch in Institutionen bestehende Bild von Cyberkriminalität verzerrt, da von Überschätzung der Relevanz einzelner Tatbestände und gleichzeitig (durch hohe Dunkelziffern) einer Unterschätzung des Gesamtproblems geprägt.

Um Verunsicherung und Hilflosigkeit nicht unnötig Raum zu geben, beantworten die Autoren nun in einem umfangreichen handlungsorientierten Teil der Studie die Frage: *Was kann jeder Einzelne, was kann jedes Unternehmen und was kann Deutschland tun, um der Cyberkriminalität wirksam entgegen zu treten?* Im Kapitel *Schutz »im Kleinen«: Selbstschutz und nationale Strafverfolgung* stellen sie dazu eine Vielzahl möglicher Maßnahmen des technischen und organisatorischen Selbstschutzes für Privatpersonen, Unternehmen und Behörden dar – die allerdings intensiver umgesetzt werden müssten. Das deutsche Straf- und Strafprozessrecht scheint – rechtlich gesehen – gut gerüstet zur Verfolgung der meisten Delikte von Cyberkriminalität, bei den Strafverfolgungsbehörden bestehen diesbezüglich aber noch Defizite hinsichtlich Qualifizierung und Rekrutierung. Da Cyberkriminalität häufig auch Staatsgrenzen überschreitet, wird im Kapitel *Schutz »im Großen«: Strafverfolgung und Transnationalität* deren internationale Dimension betrachtet. Neben zahlreichen positiven Beispielen informeller internationaler Kooperation wird die (weltweite!) Bedeutung der Cybercrime-Konvention des Europarats für die internationale Harmonisierung des Strafrechts hervorgehoben. Dagegen werfen extraterritoriale Strafverfolgung und internationale justizielle Zusammenarbeit in Strafsachen eine Reihe bisher ungelöster Probleme auf.

Wer sich einen schnellen Überblick über die Ergebnisse der Studie verschaffen möchte, sei auf das Kapitel *Handlungsempfehlungen: Neun Thesen* verwiesen. Ein umfangreiches Literaturverzeichnis unterstützt das Nachprüfen getroffener Feststellungen sowie das Weiterlesen und Vertiefen zu einzelnen Fragestellungen; auch auf Ausgespartes wird kompetent weiterverwiesen. Und noch eine angenehme Überraschung: Das Werk kann kostenlos im Internet heruntergeladen werden. Die gedruckte Ausgabe ist gegen Portokostenersatz erhältlich.

Eberhard Zehendner

Eberhard Zehendner ist Professor für Technische Informatik an der Friedrich-Schiller-Universität Jena, wo er u. a. im Bereich *Informatik & Gesellschaft* lehrt. Seit 2013 gehört er dem FIfF-Vorstand an.

Stefan Hügel

Log 4/2015

Ereignisse, Störungen und Probleme der digitalen Gesellschaft

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

Aus Platzgründen beschränken wir uns in dieser Ausgabe auf den August 2015. Die Fortsetzung erscheint in der nächsten Ausgabe.

August 2015

4. August 2015: Nachdem Generalbundesanwalt Harald Range das Bundesjustizministerium im Zusammenhang mit dem Verfahren wegen Landesverrats gegen *netzpolitik.org* scharf angegriffen hatte, wird er am selben Tag durch Bundesjustizminister Heiko Maas in den einstweiligen Ruhestand versetzt. Range hatte seinem Dienstherrn einen „unerträglichen Eingriff in die Unabhängigkeit der Justiz" vorgeworfen, nachdem dieser ihn angewiesen hatte, den Auftrag zu einem Gutachten zu der Affäre zurückzuziehen. Das Ministerium bezeichnete die Äußerungen Ranges als „nicht nachvollziehbar". Nachfolger Ranges soll der Münchener Generalstaatsanwalt Peter Frank werden. Der Fortgang des Verfahrens gegen netzpolitik.org ist zu diesem Zeitpunkt noch unklar (Quelle: netzpolitik.org, Heise).

5. August 2015: Die chinesische Regierung verstärkt die Internetüberwachung. Bei Betreibern großer Web-Dienste soll künftig eine Polizeiwache eingerichtet werden, um damit schneller auf Online-Kriminalität reagieren zu können. Dabei geht es nicht nur um Delikte wie Onlinebetrug oder Datendiebstahl, sondern auch um das „Verbreiten von Gerüchten". Die Menschenrechtsorganisation *Human Rights Watch* kritisiert die Pläne (Quelle: Heise).

7. August 2015: Die NDR-Journalistin Anja Reschke fordert die Öffentlichkeit in ihrem Tagesthemen-Kommentar auf, Haltung gegenüber Hasskommentaren im Internet zu zeigen, die gegen Flüchtlinge gerichtet sind. „Wenn man also nicht der Meinung ist, dass alle Flüchtlinge Schmarotzer sind, die verjagt, verbrannt oder vergast werden sollten, dann sollte man das ganz deutlich kundtun", erklärt sie dazu. In einem nachfolgenden Interview mit *tagesschau24* fordert sie auch von Politiker.innen, klar Stellung zu beziehen. Ihrer Beobachtung nach verstecken sich *Hater* anders als früher häufig nicht mehr hinter Pseudonymen und erhalten teilweise begeisterten Zuspruch. Der Kommentar löst weitere Hasskommentare, aber auch viel Zuspruch aus (Quelle: Tagesthemen, tagesschau24, Heise).

7. August 2015: Sicherheitsforscher finden eine Reihe kritischer Sicherheitsschwachstellen in Fahrzeugen des Herstellers Tesla. Sie waren in der Lage, bei geringem Tempo das Auto zum Stehen zu bringen und zu entriegeln, mussten sich dazu aber vorher Zugang zu dem Wagen verschaffen. Die Schwachstelle wurde von Tesla mittlerweile behoben, Besitzer sollen ein Update über WLAN und Mobilfunk erhalten (Quelle: Financial Times, BBC News, Heise).

10. August 2015: Entgegen der Ansicht von Bundesjustizminister Heiko Maas hat sein Ministerium Zweifel an der Rechtmäßigkeit der geplanten Vorratsdatenspeicherung. Der Beschluss des Europäischen Gerichtshofs (EuGH) lasse möglicherweise nur noch eine anlassbezogene Speicherung von Verbindungs- und Standortdaten zu, beispielsweise für einen bestimmten Personenkreis. Juristen des Ressorts kommen zu dem Ergebnis, dass es nach dem EuGH-Urteil einen Zusammenhang zwischen den zu speichernden Daten und einer Bedrohung der öffentlichen Sicherheit geben müsse. Maas selbst ist der Ansicht, dass die Initiative der Bundesregierung die Vorgaben des Bundesverfassungsgerichts und des Europäischen Gerichtshofs erfülle (Quelle: Spiegel, Heise).

10. August 2015: Die Ermittlungen gegen netzpolitik.org wegen Landesverrats werden eingestellt. Bundesanwaltschaft und Bundesjustizministerium gehen nunmehr davon aus, dass es sich bei den veröffentlichten Inhalten um keine Staatsgeheimnisse handelt. Gegen die Quellen der Dokumente wird jedoch weiter wegen Verletzung des Dienstgeheimnisses ermittelt (Quelle: Heise).

11. August 2015: Mobilfunkdaten können bei Facebook massenhaft ausgelesen werden. Ein britischer Softwareentwickler hat mit einem Skript zufällige mobile Telefonnummern an die Programmierschnittstelle des sozialen Netzwerks geschickt und darauf die Profile von Facebook-Nutzern erhalten, wenn dem Profil die entsprechende Nummer zugeordnet war. Die Suche anhand der Mobiltelefonnummer ist in den Datenschutzeinstellungen von Facebook standardmäßig freigegeben. Als Facebook über die Schwachstelle informiert wurde, habe das Unternehmen erklärt, es handele sich dabei nicht um eine Sicherheitsschwachstelle; auffällig häufige Abfragen der Programmierschnittstelle würden aber überwacht, um Missbrauch zu verhindern (Quelle: Heise).

12. August 2015: Einem Mitarbeiter von US-Präsident Barack Obama zufolge hat die US-Regierung die Weitergabe der Liste der NSA-Selektoren zur Kommunikationsüberwachung nicht untersagt. Sie habe auch nicht damit gedroht, die Geheimdienstkooperation einzustellen. Es seien lediglich Bedenken geäußert worden. Die Bundesregierung hatte das Verbot behauptet und damit begründet, die Liste nicht an Untersuchungsgremien weiterzugeben. Mit der Durchsicht der Listen wurde der ehemalige Bundesrichter Kurt Graulich als Sonderermittler beauftragt, der seine Erkenntnisse an den Untersuchungsausschuss weitergeben soll (Quelle: Zeit, Heise).

12. August 2015: Deutsche Geheimdienste sollen weiterhin bei Banken, Fluggesellschaften, Reisebüros, Post- und Telekommunikationsdienstleistern Auskünfte über „Terrorverdächtige" einholen und IMSI-Catcher zur Überwachung des Mobilfunkverkehrs einsetzen. Die Bundesregierung will dazu Anti-Terror-Befugnisse gemäß dem Terrorismusbekämpfungsergänzungsgesetz erneut verlängern, dieses Mal bis 2021. Das Gesetz, das 2007 in Kraft trat, wurde bereits 2011 einmal verlängert und erweitert. Datenschützer kritisieren, dass es das verfassungsrechtliche Trennungsgebot zwischen Polizei und Geheimdiensten unterlaufe (Quelle: Heise).

17. August 2015: Die Anzahl der Drohneneinsätze soll nach Plänen des US-Verteidigungsministeriums bis 2019 um 50 %, von 61 auf 90, erhöht werden. Die meisten der Flüge dienten der Aufklärung, es soll aber auch die Zahl der tödlichen Luftschläge steigen. Für Aufklärungsflüge sollen auch Privatfirmen eingesetzt werden. Nach Zahlen des britischen *Bureau of Investigative Journalism* gab es seit Juni 2004 allein in Pakistan 419 Einsätze mit einer möglichen Zahl an Todesopfern zwischen 2467 und 3976 (Quelle: Bureau of Investigative Journalism, Wall Street Journal, Heise).

19. August 2015: 15.000 Menschen haben chinesische Behörden in Verbindung mit Internetkriminalität festgenommen. Gleichzeitig wurden 66.000 Websites unter anderem wegen „illegaler und gefährlicher Informationen" geschlossen. Im Vormonat hatten die Behörden eine sechsmonatige Kampagne zur „Reinigung des Internets" angekündigt (Quelle: Chinesisches Ministerium für öffentliche Sicherheit, Heise).

20. August 2015: Aufgrund des Hackerangriffs auf den Deutschen Bundestag, bei dem ein Trojaner eingeschleust worden war, werden dessen Computersysteme zur Behebung der Schäden abgeschaltet. Damit ist der Bundestag für mehrere Tage vollständig offline. Über Details wurde „aus Sicherheitsgründen" nichts bekannt. Der Vorfall wird als „schwerwiegender Angriff" bezeichnet; der netzpolitische Sprecher der Grünen, Konstantin von Notz bezeichnete die Informationspolitik der Bundestagsverwaltung als „völlig unzureichend" (Quelle: Heise).

21. August 2015: Aufgrund des „Rechts auf Vergessenwerden" muss Google in Großbritannien auch Links zu Artikeln löschen, die das vorherige Löschen anderer Artikel zum Inhalt haben. Hintergrund sei, dass in diesen Artikeln die Vorwürfe gegen betroffene Personen erneut wiedergegeben würden, so Vize-Datenschutzkommissar David Smith (Quelle: Heise).

21. August 2015: Bundeswirtschaftsminister Sigmar Gabriel kritisiert die neuen Beschlüsse der EU-Kommission, Berichte zu aktuellen Verhandlungsrunden bei TTIP den Mitgliedsstaaten nicht mehr schriftlich zukommen zu lassen. In einem Brief an Handelskommissarin Cecilia Malmström bezeichnet er es als einen „bedauerlichen Rückschritt in unseren gemeinsamen Bemühungen um größtmögliche Transparenz". Zuvor hatte die Plattform *correctiv.org* Verhandlungsdokumente veröffentlicht, die als Verschlusssachen eingestuft waren (Quelle: correctiv.org, Heise).

23. August 2015: Weil sie „von Frauenverbänden und Gleichstellungsbeauftragten als unseriös" angesehen wurde, hat der WDR eine umstrittene Ausgabe der Sendung „Hart aber fair" aus der Mediathek entfernt. Die Auswahl der Gäste und die Gesprächsleitung seien für die Ernsthaftigkeit des Themas nicht ausreichend gewesen. Es seien aber keine Programmgrundsätze verletzt worden (Quelle: Bild, Heise).

Trauer um Peter Strutynski

Am 27. September 2015 starb Peter Strutynski.

Peter Strutynski kannte ich viele Jahre, nicht als Privatmenschen, sondern als „Macher" und als Mahner wider die unfriedlichen Entwicklungen.

Er war Mitorganisator des Friedensratschlages in Kassel und setzte dort mit seinem Einleitungsreferat – pointiert, kompromisslos friedensorientiert, ungebeugt links, stilistisch brilliant – jedes Jahr aufs Neue den thematischen Rahmen für dieses größte regelmäßige Treffen der deutschen Friedensbewegung seit Mitte der 1990er-Jahre. Er formulierte zahlreiche friedenspolitische Aufrufe, Presseerklärungen und Stellungnahmen des Bundesausschusses Friedensratschlag. Vor Ort im Kasseler Friedensforum beteiligte er sich engagiert an konkreten Aktionen, z. B. vor lokalen Rüstungsunternehmen oder während der documenta. Er initiierte an der Gesamthochschule (später Universität) die Arbeitsgemeinschaft Friedensforschung und sorgte so dafür, dass die Friedensforschung und -wissenschaft in Kassel auch in der Lehre ihren Platz fand. Als Autor und (Mit-)Herausgeber publizierte er zahlreiche Bücher, darunter jeden Herbst einen Sammelband zum Ratschlag des vorherigen Jahres, und schrieb Artikel – seit 25 Jahren auch für W&F. Dabei fand er noch Zeit, regelmäßig die Website der AG Friedensforschung zu bestücken – ein staunenswertes Kompendium für alle nur denkbaren friedenspolitischen Themen, Artikel, Dokumente und Publikationen seit dem Jahr 2000.

Selbst während seines ganz persönlichen Kampfs gegen den Krebs in den letzten drei Jahren zog er sich keineswegs ins Privatleben zurück, sondern nutzte seine guten Phasen u. a. für die Publikation neuer Bücher zu Kampfdrohnen und zur Ukraine.

Er wird beim Friedensratschlag fehlen – und nicht nur dort.

Regina Hagen
Wissenschaft & Frieden

Trauer um Andreas Buro

Prof. Dr. Andreas Buro, Friedensforscher und jahrzehntelang Vordenker der deutschen Friedensbewegung, ist am Dienstag, dem 19. Januar 2016, im Alter von 87 Jahren nach kurzer, schwerer Krankheit verstorben.

Andreas Buro gehörte zu den Mitbegründern der Ostermärsche der 1960er-Jahre. Er blieb bis wenige Tage vor seinem Tode friedenspolitisch aktiv. Er war Mitbegründer und bis zuletzt friedenspolitischer Sprecher des Komitees für Grundrechte und Demokratie. Große Verdienste erwarb er sich in der Entwicklung der Zivilen Konfliktbearbeitung (ZKB) als realistische Alternative zu militärischem Vorgehen. Seit dem Jahr 2006 gab er in Zusammenarbeit mit der Kooperation für den Frieden, einem Zusammenschluss von mehr als 50 Organisationen der deutschen Friedensbewegung, die Monitoring-Dossiers heraus, in denen ausdifferenzierte Vorschläge zur zivilen Konfliktbearbeitung in bestimmten internationalen Konflikten ausgearbeitet sind.

Andreas Buro wurde für seine friedenspolitische Arbeit 2008 mit dem Aachener Friedenspreis und 2013 mit dem Göttinger Friedenspreis ausgezeichnet.

Wir trauern um einen großartigen Wegbegleiter, der es zu seiner Lebensaufgabe gemacht hatte, Frieden zu fördern und Krieg zu überwinden, der die friedvollen Möglichkeiten sah und ergriff und der herrschenden Machtpolitik die Stirn bot.

http://www.friedenskooperative.de/Andreas_Buro.pdf

Wissenschaft und Frieden 4/2015 – „Deutsche Verantwortung – Zäsur oder Kontinuität?“

Auf der Münchner Sicherheitskonferenz 2014 hielten drei deutsche PolitikerInnen programmatisch anmutende Reden, in denen sie das veränderte Gewicht Deutschlands in Europa und der Welt beschworen und daraus ein ‚Mehr an Verantwortung‘ ableiteten. Was aber heißt ‚mehr Verantwortung‘ konkret? Und ist in der deutschen Außenpolitik eher eine Zäsur oder doch Kontinuität zu erkennen?

In W&F schreiben dazu Gunther Hellmann, Hanns W. Maull, Ingar Solty und Norman Paech, *Vier verschiedene Blicke auf ‚Außenpolitik im Wandel – Zäsur oder Kontinuität des deutschen Handelns?‘*, Stephan Klecha, *Außenpolitik deutscher Kanzler seit der Einheit*, Sabine Jaberg, *Das ‚Weißbuch 2016‘ – Kontinuität oder Kurswechsel?*, Jürgen Wagner, *Agenda Rüstung – Stärkung der Waffenindustrie und staatliche Machtpolitik*, Christiane Lammers, *Bundeshaushalt 2016 und die ‚neue‘ internationale Verantwortung Deutschlands*, Uli Cremer, *Die NATO Response Force – Eine hybride Truppe*, Hans-Georg Ehrhart, *Deutsch-französische Achse schwächelt – Quo vadis Europa?* und Velten Schäfer, *Zivile Aggression – Die Ukraine, die deutsche Außenpolitik und die Friedensbewegung*.

Außerhalb des Schwerpunktes geht es unter anderem um die Wahlen in der Türkei, um eine kritische Bestandsaufnahme in Afghanistan, um die Rolle von OSZE und Open Skies bei der Rüstungskontrolle in der Ukraine und um den Umgang der Evangelischen Kirche in Deutschland mit der Friedensfrage.

W&F liegt das Dossier *Feindbilder und Konflikteskalation* bei. Bis zum Frühjahr 2011 galt der syrische Präsident Bashar al-Assad in seinem eigenen Land ebenso wie international als Hoffnungsträger für einen Aufbruch im Land. Inzwischen haben sich die vorherrschende Syrienberichterstattung und damit die öffentliche Wahrnehmung ganz auf die Dämonisierung seiner Person zugespitzt; er gilt nun als ‚Schlächter von Damaskus‘, und viele glauben, der Syrienkonflikt wäre schon fast gelöst, würde Assad rasch das Schicksal von Saddam Hussein und Muammar Ghaddafi teilen. Das W&F-Dossier untersucht die Produktion und Funktion solcher Feindbilder und welche Konflikt-eskalierenden Folgen diese mit sich bringen unter friedenspsychologischen und medienanalytischen Aspekten sowie anhand der Beispiele Bashar al-Assad und ‚Islamischer Staat‘.

Wissenschaft & Frieden 4/2015 **„Deutsche Verantwortung – Zäsur oder Kontinuität?“**, 7,50 € plus Porto.

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

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

FIfF e.V.

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

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

FIfF-Mailinglisten

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

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

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

FIfF online

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

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

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

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

FIfF-Beirat

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

FIfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Prof. Dr. **Dietrich Meyer-Ebrecht** (stellv. Vorsitzender) – Aachen
Michael Ahlmann – Bremen
Sylvia Johnigk – München
Benjamin Kees – Berlin
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
Anne Schnerrer – Berlin
Prof. Dr. **Werner Winzerling** – Fulda
Prof. Dr. **Eberhard Zehendner** – Jena

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – 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, Eberhard Zehendner
Schwerpunktredaktion	Eberhard Zehendner (Cybercrime) Britta Schinzel (Kunstprojekt *11 TAGE*)
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	Valid street photography, Foto: Isengardt (li.) Kunstprojekt 11 TAGE, Florian Mehnert (re.)
Druck	Meiners Druck, Bremen

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

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

Aktuelle Ankündigungen

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

32. FIfF-Konferenz FIfFKon 2016
November 2016 in Berlin

FIfF-Klausur mit Vorstandssitzung
18.-20. März 2016 in Bad Hersfeld

FIfF-Kommunikation

1/2016 »31. FIfF-Konferenz 2015«
Felix Freiling, Stefan Hügel u. a.
Redaktionsschluss: 5. März 2016

2/2016 »Transhumanismus«
Karsten Wendland, Britta Schinzel
Redaktionsschluss: 6. Mai 2016

W&F – Wissenschaft & Frieden
1/15 – Afrika (mit Dossier 77: Rechter Terror in Deutschland)
2/15 – Technikkonflikte (mit Dossier 78: Zivilklauseln)
3/15 – Friedensverhandlungen (mit Dossier 79: Kriegführung im Cyberspace)
4/15 – Deutsche Verantwortung – Zäsur oder Kontinuität (mit Dossier 80: Feindbilder und Konflikteskalation)
1/16 Für den Frieden forschen? (mit Dossier 81: Rüstungsexporte)
2/16 Stadt und Krieg (mit Dossier 82: Türkei)
3/16 Islamisierung

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik
#210/211 Gesetzgebung zum Verbot der Suizidbeihilfe
#212 Reflexhaftes Strafrecht
#213 10 Jahre Versammlungsrecht der Länder

DANA – Datenschutz-Nachrichten
3/15 – Rote Linien zur EU-DSGVO
4/15 – Sichere Häfen
1/16 – Innere Sicherheit

Das FIfF-Büro

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

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

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

Schluss FIfF

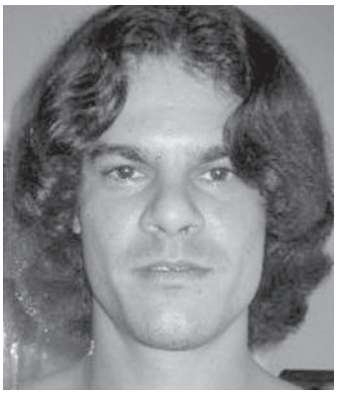
Eberhard Zehendner

Doppelleben im Doppelleben

Gestatten: Albert Gonzalez. Erfolgreichster Hacker der Welt. Nie von mir gehört? Äußerst bedauerlich! Leihen Sie mir für einige Minuten Ihr Ohr – und ich erzähle Ihnen die bemerkenswerte Geschichte meines Lebens, oder sagen wir besser: meiner Leben.

Computer haben mich immer fasziniert. Meinen ersten PC kaufte ich mit 12 von meinem eigenen Geld. Abends nahm Mutter das Kabel mit, damit ich schlafen ging; morgens saß ich um 6 schon wieder dran. Später ging ich mit meiner Freundin aus – und grübelte dabei, was ich online alles machen könnte. Ich hatte mir einen Computer-Virus eingefangen, begann mich für IT-Sicherheit zu interessieren. Alles musste ich mir selbst beibringen, doch mit 14 wusste ich genug, um einen NASA-Computer zu knacken. Das FBI kam in meine Schule, aber warum hätte ich damit aufhören sollen? Ich galt was unter *Black Hats* und mit geklauten Kreditkartendaten kaufte ich Klamotten und Musik im Netz.

Mit der Zeit lernte ich, illegal zu surfen, stahl Zugangsdaten von Managern, fand auf ihren Computern Informationen zur Systemarchitektur. Ich fühlte mich fast als Angestellter dieser Firmen; eine holte mich sogar ins Sicherheitsteam.



Ich brachte es zum Moderator bei *Shadowcrew* – einer Art eBay für Cybercrime, da wurden Daten von Kredit- und Bankkarten gehandelt und Geräte zum Fälschen von Karten. Mit 22 wurde ich dann beim „Abheben“ mit gefälschten Bankkarten erwischt. Da hätte ich mit all dem aufhören sollen – aber ich konnte einfach nicht. Der *Secret Service* fand raus, dass ich Millionen von Kartendaten hatte, und ich erklärte denen, wie ich es gemacht hatte. Die waren eindruckt, auch was Shadowcrew betraf! Ich half dann, etliche große Figuren bei Shadowcrew auffliegen zu lassen, das war nicht schön, aber eine echte Alternative zu 20 Jahren Knast. Die Agenten waren fair, ließen mir die Drogen, die ich zum Wachbleiben und Entspannen brauchte, wollten mein Vertrauen gewinnen. Es dauerte nicht lange, da hatte ich *ihr* Vertrauen!

Ich war enorm erfolgreich, wurde für meine Dienste bezahlt, sprach auf Konferenzen, arbeitete im Hauptquartier des *Secret Service* – der Direktor schüttelte mir persönlich die Hand. Die hatten wirklich nicht den geringsten Verdacht. Jetzt sind sie sauer auf mich, schimpfen mich Doppelagent. Aber ich brauchte mehr Geld, 75.000 $ pro Jahr waren nicht genug. Also heuerte ich einen Freund zum *Wardriving* an – im Auto herumfahren und dabei mit Laptop und Antenne Zugangsdaten für schlecht gesicherte drahtlose Netze ausspähen. Davon gab es viele! Damit haben wir dann Daten zu 40 Millionen Karten aus Datenbanken der angezapften Firmen abgeschöpft. Da war nichts geschützt oder verschlüsselt – sobald wir im System waren, lag alles offen, auch bei großen Unternehmen. Später kamen wir mit *SQL Injection* noch leichter an Daten, wir mussten nicht einmal in die Nähe der Unternehmen.

Daten von 180 Millionen Karten – der Hälfte der US-Bevölkerung – sollen wir gestohlen haben. Mag sein, ich habe sie nicht gezählt. TJX, Heartland und all die anderen spielten das Ausmaß herunter, 400 Millionen Dollar Schaden, sagt man. Dafür sitze ich nun 20 Jahre ab, übrigens auch das ein Rekord: kein Amerikaner bekam jemals eine härtere Strafe für Cybercrime! 2025 komme ich wohl raus, mal sehen, welche Angebote dann auf mich warten.

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