H 7625

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

35. Jahrgang 2018 Einzelpreis: 7 EUR 1/2018 – März 2018

#FIfFKon17

TRUST

Wem kann ich trauen im Netz und warum?

ISSN 0938-3476

• Tihange Doel Radiation Monitoring • Abrüstungsverifikation • Hessentrojaner •

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

Titelbild: Tagungsplakat der FIfFKon 2017 (Ausschnitt) von Benjamin Kees und Lena Schall

Inhalt

Ausgabe 1/2018

inhalt

Forum

Lesen & Sehen

Retrospektive

Rubriken

Schwerpunkt „TRUST"

Editorial

Es ist mittlerweile Tradition: Die erste Ausgabe im neuen Jahr ist der FIfF-Konferenz des Vorjahrs gewidmet. Vom 20. bis zum 22. Oktober 2017 trafen wir uns in Jena unter dem Leitmotiv *TRUST – Wem kann ich trauen im Netz und warum?*

Vertrauen ist die Basis, auf der unsere Gesellschaft aufgebaut ist. Wenn wir einander nicht mehr vertrauen können, funktioniert unser Zusammenleben nicht – das gilt auch im Netz. Wenn wir Dienste im Internet nutzen, müssen wir den Anbietern vertrauen können, dass sie die entsprechenden Leistungen erbringen und die Daten, die wir ihnen senden, verantwortungsvoll verwenden. Die Bedeutung des Vertrauens thematisierten wir im Verlauf der Tagung, und wir thematisieren sie in dieser Ausgabe in einem umfassenden Schwerpunkt. Beides verdanken wir *Eberhard Zehendner,* der mit seinem Team die Konferenz organisiert und danach den Schwerpunkt dieses Heftes gestaltet hat. In einem eigenen Schwerpunkteditorial führt er gemeinsam mit *Hans-Jörg Kreowski* in den Schwerpunkt ein und gibt einen Überblick über die darin enthaltenen Beiträge.

Zuvor enthält diese Ausgabe aktuelle Beiträge in der Rubrik *Forum.* Der erste, ein Bericht des von *Dietrich Meyer-Ebrecht* geleiteten Projektteams über *TDRM – Tihange Doel Radiation Monitoring* – basiert auf einem Vortrag bei der FIfF-Konferenz, weist aber in seiner Bedeutung für das FIfF darüber hinaus, sodass wir uns entschieden haben, ihn dort herauszulösen und als ersten Beitrag des *Forums* dieser Ausgabe zu bringen. „Subversiv greift das Projekt dort ein, wo das Vertrauen in Behörden und Industrie verloren gegangen ist, wo ernsthafte Zweifel angebracht sind, ob die im Gefahrenbereich lebenden Bürgerinnen und Bürger frühzeitig über bedrohliche Entwicklungen informiert werden würden. So erfüllt unsere Technik ein drängendes Informationsbedürfnis der im Gefahrenbereich lebenden Menschen und unterstützt gleichzeitig den Bürgerprotest und die politische Arbeit gegen den Weiterbetrieb der maroden Atomreaktoren", so beschreiben die Autoren die Zielsetzung von TDRM. Das Projekt ist ein Beispiel dafür, wie wir Technik zum Nutzen der Zivilgesellschaft einsetzen können, wenn die eigentlich zuständigen Behörden versagen.

Mit der Messung von Radioaktivität mit anderem Ziel befasst sich der darauffolgende Beitrag von *Moritz Kütt* und *Alex Glaser: Retrocomputer für Abrüstungsverifikation und eine kernwaffenfreie Welt.* „Im Rahmen einer zukünftigen Abrüstung von Kernwaffen müssen Sprengköpfe vor ihrer Zerlegung als authentische Sprengköpfe bestätigt werden. Das erfordert vertrauenswürdige Messsysteme, die diese Identifikation anhand von radioaktiven Signaturen vornehmen können. Verschiedene solche Systeme existieren, bei allen ist jedoch die vertrauenswürdige Datenverarbeitung problematisch", so die Autoren zur Zielsetzung ihres Projekts.

Der *Hessentrojaner* ist das erste große tagespolitische Thema im neuen Jahr, das angesichts der Gefährdung der Grundrechte unserer Aufmerksamkeit bedarf. Es geht um das neue *Hessische Verfassungsschutzgesetz,* das unter anderem den Einsatz von Trojanern in Form verdeckter Quellen-TKÜ vorsieht. Das Gesetz wurde von der hessischen Regierungskoalition aus CDU und Grünen – letztere offenbar gegen erhebliche Bedenken in der eigenen Partei – initiiert und war Gegenstand einer Anhörung in Wiesbaden, zu der auch wir geladen waren. Unser Sachverständiger *Rainer Rehak* machte deutlich, welche Folgen solch ein Gesetz für die Vertraulichkeit und Integrität unserer IT-Infrastruktur haben würde. Er war mit seiner Ansicht nicht allein: von 25 Sachverständigen mochte sich nahezu niemand für das Gesetz aussprechen. Diese Ausgabe enthält unsere Pressemitteilung und eine Zusammenfassung der Anhörung, die wir *Anna Biselli* von *netzpolitik.org* verdanken. Die schriftlichen Stellungnahmen sind im Netz beim Hessischen Landtag verfügbar; unsere auch bei *fiff.de.*

Eine Bewertung der *Asilomar AI Principles* zu Künstlicher Intelligenz hat *Malte Rehbein* vorgenommen. Er bemängelt eine „… technikdeterministische[n] und rein utilitaristische[n] Sichtweise auf den Einsatz von KI-Technologien …", die viele Fragen offenlasse und fordert: „Eine ethische Bewertung, rechtliche Regelung und konsequente politische Regulierung, die sowohl den Einsatz als auch bereits die Entwicklung von KI umfassen, sind dringend geboten." Ein Bericht von einer Podiumsdiskussion der Zeitschrift Wissenschaft & Frieden – *Angriff und Verteidigung in der Ära des Cyberkriegs* – und die Forderungen der Kampagne *abrüsten statt aufrüsten* runden die Rubrik ab.

John Perry Barlow, der am 7. Februar 2018 70-jährig verstorben ist, gedenken wir mit dem Abdruck seiner *Declaration of Independence in Cyberspace* in der Retrospektive.

Zuletzt eine redaktionelle Bemerkung: Das „richtige" *Gendering* von Texten mit dem Ziel einer diskriminierungsfreien Sprache ist immer noch Diskussionsthema – natürlich auch in der Redaktion der *FIfF-Kommunikation.* In den letzten Ausgaben haben wir mit dem *Gender-Punkt* experimentiert. Dies ist nicht überall auf Zustimmung gestoßen, so dass Vorstand und Redaktion entschieden haben, zum bewährten *Binnen-I* zurückzukehren – auch um mit der Schreibweise unseres Vereinsnamens konsistent zu bleiben. Zusätzlich verwenden wir gerne auch Schreibweisen, die typographische Kunstgriffe vermeiden – beispielsweise die Verlaufsform („Studierende") oder die Auflösung in *weiblich* und *männlich* („Studentinnen und Studenten"). Diese Formen verwenden wir nun als unseren Standard, im Bewusstsein, dass es eine breite Diskussion vieler Varianten des Gendering gibt und diese Entscheidung wohl nicht endgültig sein kann. Ausdrückliche Wünsche unserer Autorinnen und Autoren – insbesondere, wenn Beiträge sich selbst mit *Gender* befassen – werden wir selbstverständlich berücksichtigen.

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

Stefan Hügel
für die Redaktion

Der Brief

Bärendienst

Liebe Leserinnen und Leser, liebe Mitglieder des FIfF,

um von eigenen Versäumnissen abzulenken, hat es sich bewährt, sinnentleerte Debatten loszutreten. Und es funktioniert ja auch: Kaum hatte die künftige Staatsministerin Dorothee Bär (CSU) einen „Datenschutz aus dem 18. Jahrhundert" bemängelt, bei dem wackere Start-Ups „Leute schicken [mussten], die [Fahrpläne] vom Bushäuschen abschreiben", von „Flugtaxis" schwadroniert und die Nutzerinnen und Nutzer von Twitter (abschließend) im Kreise der Politiker, Journalisten und Psychopathen (sic!) verortet[1], brach dort eine muntere Debatte um Nebensächlichkeiten los. Nun traue ich Frau Bär durchaus das Wissen zu, dass zur Zeit der Französischen Revolution der Datenschutz im engen Sinn eine eher untergeordnete Rolle gespielt hat. Datenschutz ist aber vor allem Schutz der Menschen und der Menschenrechte, und dass damals damit einiges im Argen lag, das ist zweifellos richtig. Und damit hat sie tatsächlich (unfreiwillig?) recht: Die Umsetzung des Daten- und Menschenrechtschutzes ist durch Telekommunikationsüberwachung, Videoüberwachung des öffentlichen Raums und missbräuchliche Datennutzung für datengetriebene Geschäftsmodelle in der Tat auch heute bedroht. Nun ist die Situation der Menschenrechte selbstverständlich nicht mit der Situation während der Terrorherrschaft der Jakobiner vergleichbar – würde aber eine solche Terrorherrschaft heute errichtet, ihre Protagonisten wären über die bestehenden Möglichkeiten der Überwachung und Kontrolle zweifellos begeistert.

Interessanter wäre zunächst die Frage gewesen, warum Frau Bär offensichtlich in ihrer bisherigen – inhaltlich wohl vergleichbaren – Rolle als Parlamentarische Staatssekretärin beim Bundesminister für Verkehr und digitale Infrastruktur bei der Weiterentwicklung der Digitalisierung nicht bereits erreichen konnte, was sie jetzt ankündigt, und wie sie das im neuen Amt zu ändern plant. Und ja, der Ausbau der Netzinfrastruktur für eine flächendeckende Versorgung mit schnellem Internet ist schon wichtig – unter Umständen auch für den Betrieb von Flugtaxis.

Das Problem ist wohl, dass diejenigen, die in der Regierung wirklich etwas zu sagen haben, die Digitalisierung immer noch in erster Linie als Bedrohung wahrnehmen, die man durch umfassende Überwachung in den Griff bekommen muss. Für die „innere Sicherheit" wird künftig Frau Bärs Parteikollege Horst Seehofer zuständig sein. Das allein lässt Böses ahnen, spielt doch Bayern bei der Überwachung eine Vorreiterrolle, wie auch der aktuell diskutierte Entwurf für ein Gesetz zur Neuordnung des bayerischen Polizeirechts zeigt. Der Journalist Detlef Borchers dazu: „Überwachungsdrohnen, DNA-Tests, Präventivhaft: Der Entwurf für Bayerns neues Polizeigesetz liest sich wie das Skript eines düsteren Science-Fiction-Films. Unter einem Innenminister Seehofer könnte dies bald für ganz Deutschland gelten."[2]

Doch schauen wir in den Koalitionsvertrag:

- „Die DNA-Analyse wird im Strafverfahren auf äußerliche Merkmale (Haar, Augen, Hautfarbe) sowie Alter ausgeweitet (§ 81e StPO)"[3] und „[…] Dazu gehört die Erarbeitung eines gemeinsamen Musterpolizeigesetzes (gemäß Innenministerkonferenz-Beschluss)."[4]

Auch sonst hat der Koalitionsvertrag – der, nebenbei, von Absichtserklärungen zur Digitalisierung durchzogen ist – einiges zu bieten. Hier ein paar Punkte, die IT-Sicherheit und Datenschutz betreffen, ohne Anspruch auf Vollständigkeit:

- Der Irrweg[5] der „intelligenten" Videoüberwachung wird fortgesetzt, wenn auch der Koalitionsvertrag hier eher schwammig formuliert: „… wollen wir die Videoüberwachung an Brennpunkten einsetzen, sie verhältnismäßig und mit Augenmaß effektiv ausbauen und dabei auch technisch verbessern. Intelligente Videoüberwachung kann dabei eine Weiterentwicklung sein. Deswegen werden wir den laufenden Modellversuch abwarten, prüfen und bewerten."[6]

- Das Betreiben „krimineller Infrastrukturen" soll unter Strafe gestellt werden: „Wo Strafbarkeitslücken bestehen, werden wir eine Strafbarkeit für das Betreiben krimineller Infrastrukturen einführen, um speziell im Internet eine Ahndung von Delikten wie z. B. das Betreiben eines Darknet-Handelsplatzes für kriminelle Waren und Dienstleistungen einzuführen."[7] Was das für die Betreiber von TOR-Knoten bedeutet, bleibt abzuwarten.

- Das viel kritisierte[8] Netzwerkdurchsetzungsgesetz wird verteidigt: „Das Netzwerkdurchsetzungsgesetz ist ein richtiger und wichtiger Schritt zur Bekämpfung von Hasskriminalität und strafbaren Äußerungen in sozialen Netzwerken."

Zum Datenschutz:

- „Die Mitte 2020 anstehende Evaluierung der Datenschutz-Grundverordnung (DSGVO) wollen wir intensiv begleiten und dabei alle Regelungen auf ihre Zukunftsfähigkeit und Effektivität überprüfen."[9] Nachdem die deutsche Bundesregierung bei der Grundverordnung offenbar eher gebremst hat, ist abzuwarten, wie sie sich dabei verhält. Dass wieder der Begriff der „Datensouveränität" gegen einen wirksamen Datenschutz in Stellung gebracht wird, lässt nichts Gutes ahnen. In diesem Kontext muss auch diese Ankündigung aufmerksam verfolgt werden: „Die Frage, ob und wie ein Eigentum an Daten ausgestaltet sein kann, müssen wir zügig angehen."[10] Eigentlich kann es darauf nur eine Antwort geben.[11]

- Eine alte Forderung von DatenschützerInnen scheint erfüllt zu werden: „Wir wollen die Öffnungsklausel in Artikel 88 der Datenschutz-Grundverordnung nutzen und prüfen die Schaffung eines eigenständiges (sic!) Gesetzes zum Beschäftigtendatenschutz, das die Persönlichkeitsrechte der Beschäftigten am Arbeitsplatz schützt und Rechtssicherheit für den Arbeitgeber schafft."[12] Doch Obacht! Die letzte Initiative[13] wurde – auch von der damaligen Oppositionspartei SPD – scharf kritisiert[14] und verschwand (zum Glück) schnell wieder in der Schublade.

- „Wir werden zeitnah eine Daten-Ethikkommission einsetzen, die Regierung und Parlament innerhalb eines Jahres einen Entwicklungsrahmen für Datenpolitik, den Umgang mit Algorithmen, künstlicher Intelligenz und digitalen Innovationen vorschlägt“,[15] – das sieht eher aus wie eine Nebelkerze. Was wir brauchen sind klare Regelungen und Verfahren, um diese Regelungen umzusetzen.

- „Die Klärung datenethischer Fragen kann Geschwindigkeit in die digitale Entwicklung bringen und auch einen Weg definieren, der gesellschaftliche Konflikte im Bereich der Datenpolitik auflöst“,[16] – und hier wird es deutlich: Es geht eher darum, für die extensive Datennutzung Akzeptanz zu schaffen. Heißt es doch an anderer Stelle ganz klar: „Daten sind der Rohstoff des 21. Jahrhunderts. Wir wollen durch neue Open-Data-Anwendungen die Mobilität der Menschen und den Transport der Waren vereinfachen.“[17] Auch Frau Bär spricht, wie viele ihrer Kolleginnen und Kollegen, lieber von „Datensouveränität“ als von wirksamem Datenschutz: „Ich finde schon den Begriff ‚Datenschutz‘ schwierig. Besser wäre es, von ‚Datensouveränität‘ zu sprechen.“[18]

Zuletzt noch zwei Punkte, die wir aufmerksam begleiten sollten, scheinen sie doch alte Forderungen aus dem FIfF abzudecken:

- „Die Hersteller und Anbieter digitaler Produkte und Dienstleistungen müssen Sicherheitslücken bekanntmachen und schnellstmöglich beheben“,[19] – warum aber nicht auch Behörden? Legislativ richtig umgesetzt würde solch eine Initiative dem Staatstrojaner-Unwesen ein Ende bereiten – bei dieser Regierung ist das aber schwer vorstellbar.

- „Wir werden klare Regelungen für die Produkthaftung in der digitalen Welt aufstellen“,[20] – das ist zu begrüßen. Wie diese ausgestaltet sein werden, bleibt aber ebenfalls abzuwarten.

Welche Bedeutung der Vertrag in der Regierungspraxis wirklich haben wird, werden wir sehen müssen. Seine Formulierungen sind häufig unverbindlich („Wir wollen …“, „Wir werden uns dafür einsetzen …“) und geben keine klare Richtung vor. Auch hier gilt: „Es ist besser, nicht zu regieren, als falsch zu regieren“ – werden Gesetze unzureichend ausgestaltet, wird es danach umso schwerer, sie wieder zu korrigieren.

Was das bedeutet, zeigt ein Blick nach Hessen: Die Novelle des Verfassungsschutzgesetzes ist grundsätzlich missraten: unter anderem sieht sie Quellen-TKÜ und Online-Durchsuchung – kurz: den Hessentrojaner – vor, und sie führt eine Gesinnungsklausel ein, die nach Überzeugung der betroffenen Organisationen zu faktischen Berufsverboten führen wird. Besonders ernüchternd – man kann es nur immer wiederholen – dass der Entwurf von einer Landesregierung unter Beteiligung der Grünen vorgelegt wurde. Auch wenn der Entwurf offenbar parteiintern umstritten ist: Eine Regierungsbeteiligung von Bündnis 90/Die Grünen kann nicht mehr als Garant dafür gesehen werden, dass die Bürger- und Menschenrechte geschützt werden.[21] Gemeinsam mit dem FIfF kritisierte die große Mehrheit der Sachverständigen in einer Anhörung im Hessischen Landtag das Gesetz scharf; an seiner Verfassungsmäßigkeit bestehen erhebliche Zweifel.[22]

Woher aber der Wind weht, macht der künftige Innen- und Heimatminister Seehofer deutlich: „[…] wenn es um den Schutz der Bürger geht, brauchen wir einen starken Staat. Dafür werde ich sorgen.“[23] Welche Bürger sollen genau wovor geschützt werden? Doch weiter: „‚Wir brauchen eine wirksame Videoüberwachung an allen Brennpunkten im Land‘, sagte der künftige Innenminister.“[24]

Das Besorgniserregende dabei: Deutschland scheint gerade langsam aber stetig nach rechts zu kippen. Sind vielleicht nicht die Rechtspopulisten selbst die größte Gefahr, sondern die gemäßigten Parteien, wenn sie ihre Politik von den Rechtspopulisten bestimmen lassen?

fragt besorgt mit FIfFigen Grüßen
Stefan Hügel

Anmerkungen und Referenzen

1 *Thomas Vitzthum, welt.de (2018): Dorothee Bär: „Facebook wird zu einem Seniorennetzwerk“, https://www.welt.de/politik/deutschland/article174401539/Dorothee-Baer-Facebook-wird-zu-einem-Seniorennetzwerk.html?wtrid=socialmedia.socialflow....socialflow_twitter&__twitter_impression=true*
2 *Detlef Borchers (2018): Minority Report. Wie Bayerns Polizei den Datenschutz aushebelt. c't 6/2018, S. 34–35*
3 *CDU, CSU und SPD (2018): Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU, CSU und SPD, S. 124*
4 *CDU, CSU und SPD (2018), a.a.O., S. 127*
5 *FIfF e. V. (2017): Verfälschte Studie zur Tauglichkeit grundrechtswidriger Techniken. FIfF-Kommunikation 3/2017, S. 10–11*
6 *CDU, CSU und SPD (2018), a.a.O., S. 127–128*
7 *CDU, CSU und SPD (2018), a.a.O., S. 129*
8 *Deklaration für die Meinungsfreiheit. https://deklaration-fuer-meinungsfreiheit.de, FIfF-Kommunikation 2/2017, S. 14*
9 *CDU, CSU und SPD (2018), a.a.O., S. 130*
10 *ebd.*
11 *Pointiert zum Kernziel des Datenschutzes Martin Rost (2017): Bob, es ist Bob! FIfF-Kommunikation 4/2017, S. 63–66*
12 *CDU, CSU und SPD (2018), a.a.O., S. 130–131*
13 *http://dipbt.bundestag.de/doc/btd/17/042/1704230.pdf*
14 *Stefan Krempl (2011): Scharfe Kritik am geplanten Arbeitnehmerdatenschutz, https://www.heise.de/newsticker/meldung/Scharfe-Kritik-im-Bundestag-am-geplanten-Arbeitnehmerdatenschutz-1199341.html*
15 *CDU, CSU und SPD (2018), a.a.O., S. 47*
16 *ebd.*
17 *CDU, CSU und SPD (2018), a.a.O., S. 80*
18 *Thomas Vitzthum, welt.de (2018), a.a.O.*
19 *CDU, CSU und SPD (2018), a.a.O., S. 45*
20 *ebd.*
21 *Nach Redaktionsschluss gab es dafür den wohlverdienten BigBrotherAward (https://bigbrotherawards.de/2018/politik-cdu-gruene-landtag-hessen).*
22 *Dazu FIfF e. V.: FIfF-Sachverständigenauskunft zum Trojanereinsatz durch den hessischen Verfassungsschutz. FIfF lehnt Hessentrojaner ab, und Anna Biselli: 25 Experten lassen kaum ein gutes Haar an hessischem Geheimdienstgesetz, in diesem Heft*
23 *Spiegel Online (2018): Horst Seehofer kündigt „Masterplan für Abschiebung“ an, http://www.spiegel.de/politik/deutschland/horst-seehofer-kuendigt-masterplan-fuer-abschiebung-an-a-1197502.html*
24 *ebd.*

Daniel Brückner, Peter Kämmerling, Gerd Krenzer, Dietrich Meyer-Ebrecht und Mike Rabald

Tihange–Doel Radiation Monitoring

Wenn das Vertrauen in Behörden und Unternehmen fehlt

„Wenn wir mit unseren Worten politisch nichts bewegen können, sollen wir das einsetzen, was wir gut können: unsere Expertise in der IT und Informatik." Mit diesem Credo stellte Philipp Gräbel das Projekt Tihange–Doel Radiation Monitoring (TDRM) *auf dem 33C3 vor. Im Gefahrenbereich der belgischen Atomkraftwerke Tihange und Doel, deren Sicherheit aufgrund ihres Alters und ihres technischen Zustandes nicht mehr garantiert werden kann, initiierte ein kleines Team der FIfF-Regionalgruppe Aachen vor etwa zwei Jahren die Entwicklung des unabhängigen Radioaktivitäts-Beobachtungsnetzes TDRM. Subversiv greift das Projekt dort ein, wo das Vertrauen in Behörden und Industrie verloren gegangen ist, wo ernsthafte Zweifel angebracht sind, ob die im Gefahrenbereich lebenden Bürgerinnen und Bürger frühzeitig über bedrohliche Entwicklungen informiert werden würden. So erfüllt unsere Technik ein drängendes Informationsbedürfnis der im Gefahrenbereich lebenden Menschen und unterstützt gleichzeitig den Bürgerprotest und die politische Arbeit gegen den Weiterbetrieb der maroden Atomreaktoren.*

Der Protest geht weiter …

Atomkraft – die zivile Nutzung der Kernspaltungstechnologie für die Energieversorgung – schien für uns kein Thema mehr zu sein, nachdem die Bundesrepublik den Ausstieg erklärt hatte. Und ihn auch – noch jedenfalls, und eher zögerlich – vorantreibt. Dabei haben wir allerdings aus den Augen verloren, dass wir von Staaten umgeben sind, die ihre Atomkraftwerke unbeeindruckt weiter betreiben. Viele ihrer Reaktoren sind bereits um die 40 Jahre und mehr in Betrieb. Und mehrere stehen unmittelbar vor unserer Haustür, vor allem an unseren westlichen Staatsgrenzen: Der älteste noch betriebene europäische Reaktor mit einer Betriebszeit von 48 Jahren arbeitet in 6 km Entfernung zur deutschen Grenze im Schweizerischen AKW Beznau, 25 km südwestlich vor Freiburg liegt das französische AKW Fessenheim und 50 km südwestlich vor Trier das AKW Cattenom. Störfälle in diesen Altanlagen gehören mittlerweile zum Betriebsalltag.

Vor unserer Aachener Haustür sind es drei Reaktorblöcke im 65 km entfernten belgischen Tihange und vier Reaktorblöcke im 150 km entfernten Doel (siehe Karte). Sie sind zwar etwas weiter entfernt, stellen aber eine akute Bedrohung dar. Die Tatsache, dass einzelne Reaktoren dieser AKWs mehrmals im Jahr aufgrund technischer Störungen heruntergefahren werden müssen, hat ihnen bereits den Titel ‚Schrottreaktoren' eingebracht. Dazu kommt – besonders bedrohlich –, dass im Mantel der Reaktordruckgefäße der jeweils ältesten Reaktoren in Tihange und in Doel, in Betrieb seit 1974 bzw. 1975, schon vor mehreren Jahren Zehntausende von Haarrissen entdeckt wurden. Und bei jeder der jährlichen Überprüfungen werden es mehr.

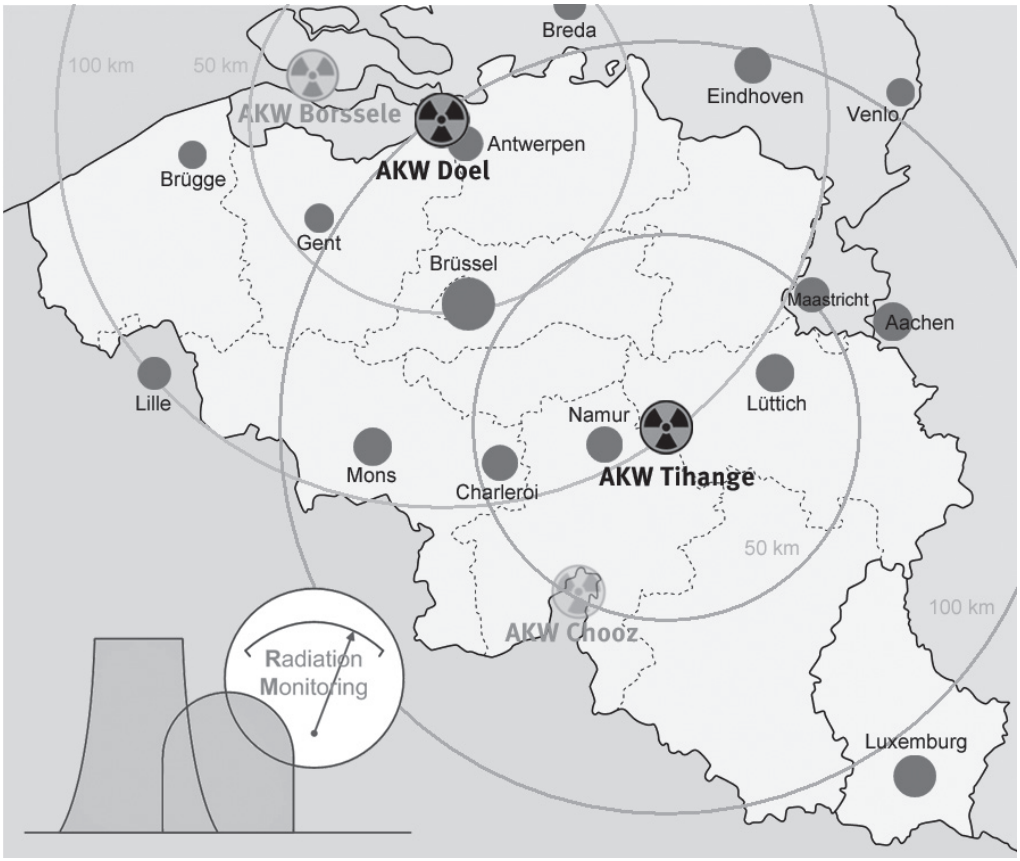


Abbildung 1: Abstand einiger Großstädte zu den AKWs Tihange und Doel, Startseite tdrm.eu Urheber: Gerd Krenzer,CC BY

Um ein Gespür für die akute Gefahr zu bekommen, muss man sich das Reaktordruckgefäß vorstellen, ein Kessel aus Schmiedestahl, gut 13 m hoch und 4,4 m im Durchmesser mit einer Wandstärke von gut 20 cm. Die Dimensionen lassen erahnen, welche Energie darin – bei einer Temperatur von 325°C und 160 Bar – eingeschlossen ist. Die akute Bedrohung besteht darin, dass der durch die vielen Haarrisse geschwächte Stahlmantel dem Druck nicht mehr standhalten kann und die Belastung ihn zum Bersten bringt. Die Explosionskraft würde unmittelbar viele Tonnen hochradioaktiven Materials in die Atmosphäre schleudern, darunter die gesundheitsgefährdenden Isotope Cs^{137}, Sr^{90} und I^{131}.[1] In einem im Auf-

trag der Städte-Region Aachen von der Universität für Bodenkultur Wien[2] angefertigten Gutachten wurden die potentiellen Folgen eines solchen GAUs bei den hier vorherrschenden westlichen bis südwestlichen Winden simuliert: Ein Landstrich von der Größe eines mittleren Bundeslandes, der den Lebensraum von 2 Mio. Einwohnern in Nordrhein-Westfalen einschließt, würde auf Dauer unbewohnbar werden.

Seit Jahren versucht das sehr aktive *Aktionsbündnis gegen Atomkraft Aachen (AAA),* die Politik zu bewegen, auf Europäischer Ebene gegen den für 16 weitere Jahre geplanten Weiterbetrieb dieser Reaktoren vorzugehen. Von der Bundesregierung wurden die Sorgen der Betroffenen lange Zeit nicht ernst genommen. Zaghafte Versuche unserer regionalen politischen Gremien werden von der belgischen Atomaufsichtsbehörde FANC wie auch vom Betreiber Electrabel, einer Tochter des französischen Energiekonzerns Engie, mit unbelegten Behauptungen über die Sicherheit der betroffenen Reaktoren abgespeist.

Wer informiert uns?

Bewegung kam erst in die Politik durch die Initiative einer Aachener Gruppe von Ärzten der *International Physicians for the Prevention of Nuclear War (IPPNW),* die die gesundheitlichen Folgen einer Havarie der Risikoreaktoren öffentlich thematisierte und dringend Vorsorgemaßnahmen der Behörden einforderte. Ihre Aufklärungsarbeit machte die Gefahren und Folgen für die Öffentlichkeit vorstellbarer, der Protest konnte sich sachlicher artikulieren, und die Behörden wurden endlich sensibilisiert. Eine Sofortmaßnahme, so die Ärzte, muss die Einnahme hochdosierter Jodtabletten sein. Sie beugen der akuten Gefahr einer Einlagerung des radioaktiven Jodisotops I^{131} in der Schilddrüse vor, und damit ist Zeit gewonnen für eine geordnete Evakuierung. (Mittlerweile werden Jodtabletten prophylaktisch an alle Haushalte verteilt.) Um aber wirksam zu sein, muss die Einnahme der Tabletten *vor* dem Eintreffen der kontaminierten Atmosphäre erfolgen, optimalerweise mit einem Vorlauf von zwei bis drei Stunden – der Zeitraum, den die atmosphärische Kontamination infolge einer Havarie in Tihange unter Südwestwind brauchen würde, um den Aachener Raum zu erreichen. Denn anders als bei einem GAU, bei dem es zu einer Kernschmelze käme, träfe uns der GAU bei einem Bersten des Reaktordruckgefäßes ohne Vorwarnzeit.

Das machte bewusst, dass völlig unklar war, wie, wann und vom wem die Öffentlichkeit über Zwischenfälle in Tihange oder Doel informiert werden würde – nicht nur in dramatischen Situationen, auch bereits bei Störfällen mit kurzzeitigem Austritt radioaktiver Gase. Ein Vertrauen, dass wir im Ernstfall unverzüglich und umfassend informiert werden, können wir den Behörden erfahrungsgemäß nicht ohne Einschränkung schenken, und schon gar nicht den Betreibern. Dies bestätigt vielfach die Geschichte der bisherigen Unfälle in kerntechnischen Anlagen – 30 ernsthafte Zwischenfälle bis schwere nukleare Unfälle seit 1950,[3] darunter die beiden bisher folgenschwersten Havarien in Tschernobyl 1986 und in Fukushima 2011. Allein in diesen beiden Fällen wurde die Öffentlichkeit erst nach Tagen informiert. Eine Beinahe-Havarie eines Forschungsreaktors im norwegischen Halden im Oktober 2016 war zwar bei Weitem weniger dramatisch, die Öffentlichkeit erfuhr davon jedoch erst nach Monaten durch die norwegische NGO Bellona.[4] Ein anderes Beispiel aus der Region: Die millionenfache Verseuchung von Eiern mit dem Insektizid Fipronil war den belgischen Behörden Wochen bekannt, bevor sie die Öffentlichkeit in Kenntnis setzten.

Nun ist die Öffentlichkeit nicht allein darauf angewiesen, dass sie von Behörden oder Unternehmen informiert wird. Es gibt öffentlich zugängliche Messdaten, die über die Intensität ionisierender Strahlung an den jeweiligen Messorten informieren. Ein gesundheitsgefährdender Störfall würde durch einen ungewöhnlichen Anstieg der Messwerte signalisiert. Diverse Organisationen, verschiedene NGOs wie auch Behörden betreiben Radioaktivitäts-Messnetze, so u. a. die Europäische Kommission das Messnetz ReMon[5]. Diese Netze sind meist sehr weitmaschig, ihre Messdaten werden teils nur mit einer Verzögerung von mehreren Stunden aktualisiert, und unklar ist, wer die Messdaten mit welchen Vorgaben kontrollieren kann. Auf nationalem Gebiet überwacht das ODL-Messnetz des Bundesamtes für Strahlenschutz mit einem sehr weitmaschigen Netz von Sensorstationen die atmosphärische Radioaktivität,[6] aber dieses nationale Netz greift natürlich nicht über Deutsches Hoheitsgebiet hinaus. Es ist offensichtlich, dass die für den regionalen Katastrophenschutz verantwortlichen Behörden nicht über verlässliche Kanäle verfügen, die frühzeitiger über Ereignisse jenseits der Bundesgrenze informieren.

Was tun? Selber machen!

Aus dieser Unsicherheit heraus wurde der Plan geboren, ein unabhängiges, bürgerbetriebenes Netz für das Monitoring der atmosphärischen Radioaktivität in der Region aufzubauen. Gestartet wurde das Projekt *Tihange–Doel Radiation Monitoring* im Frühjahr 2016. Der Impuls kam aus der Regionalgruppe des FIfF. Zwei weitere Organisationen trugen entscheidend dazu bei, dass das Projekt Fahrt aufnahm: das *Aachener Aktionsbündnis gegen Atomenergie e. V. (AAA)* und das oben schon erwähnte Ärzte-Team der IPPNW:

- Das AAA erwartet von der Existenz des Netzes, dass es den politischen Gremien und Behörden die Wachsamkeit der betroffenen Menschen signalisiert („wir schauen euch über die Schulter!“) und die Forderung nach Transparenz von offizieller Seite bekräftigt. Es sieht in TDRM eine Unterstützung seiner politischen Arbeit.

- Einen Informationsgewinn erwartet das IPPNW-Team. Mit profunder Fachkenntnis über die gesundheitlichen Folgen radioaktiver Strahlung und über die zu treffenden Vorsorgemaßnahmen werden sie von der Katastrophenschutzbehörde als Beraterinnen und Berater herangezogen. Sie unterstützen die Behörde nicht nur bei der Planung von Präventionsmaßnahmen, sondern sollen im Ernstfall auch dem Krisenstab mit ihrer Beurteilung der Lage zur Seite stehen. Der zeitliche Vorsprung, mit dem unsere Sensorstationen ungewöhnlich erhöhte Strahlungswerte registrieren würden, würde dem Team einen wertvollen zeitlichen Vorsprung in der Abschätzung der Entwicklung bieten, z. B. zur Vorhersage, wann und wo so genannte Eingreifschwellwerte überschritten werden würden.

- Und schließlich ist es uns als FIfF ein Anliegen, mit einem öffentlichen Zugang zu Strahlungsmesswerten dem Informationsbedürfnis der Menschen in der betroffenen Region Rechnung zu tragen. Wir machen die von radioaktiven Substanzen ausgehende, gesundheitsgefährdende ionisierende Strahlung, die mit unseren Sinnen nicht erfassbar ist, durch Zahlen und Grafiken gleichsam sichtbar. Wir leisten damit einen Beitrag zum Abbau unbegründeter Ängste, stärken gleichzeitig aber auch das Bewusstsein für die Risiken und für die Gefahren der Atomenergienutzung.

Für eine Idee ist schnell Begeisterung zu wecken. Wenn es an die Umsetzung geht, beginnen die Probleme – ein realisierbares Konzept aufzustellen, kompetente Akteure zu gewinnen (die auch ihre Zeit investieren wollen und können), finanzielle Ressourcen aufzubringen … Dennoch, bevor noch alle offenen Fragen endgültig geklärt waren, wurde begonnen. Nach dem Prinzip der „baubegleitenden Planung" vorzugehen, ist nicht immer der effizienteste Weg zu einer funktionierenden Lösung, aber er vermeidet, dass eine Initiative schon im Vorfeld in endlosen Diskussionen versandet.

Die Systemkomponenten

Drei wesentliche Elemente waren zu realisieren – und sind auch immer noch Gegenstand ihrer Weiterentwicklung: die Sensorstationen, die Datenbank und die Website. Eine klare Entkopplung dieser drei Elemente war (und ist) die Voraussetzung für eine verteilte Entwicklung jedes der Elemente. Beginnen wir mit der Sensorstation.

Das Ziel war es, eine mit wenig Arbeitsaufwand und unter geringen Kosten zu realisierende Lösung für ein kommunikationsfähiges Messgerät für Gamma-Strahlen zu finden. Der Kern für die Sensorstationen wurde deshalb das Open-Source-Design PiGI.[7] Es basiert auf einem Raspberry Pi, der mit einem Aufwärts-Converter für die Erzeugung einer 450 V-Spannung für den Betrieb eines Geiger-Müller-Zählrohrs ausgerüstet wird. (Als Varianten wurden auch Sensorstationen mit verschiedenen Halbleiterdetektoren ausgerüstet.) Die PiGI-Software wird mit einem von uns entwickelten Modul für die Kommunikation ergänzt. Das Kommunikationsmodul überträgt Messdaten im Minutentakt über das Internet zu unserem Server. Der aktuelle Wert repräsentiert den Mittelwert der Strahlungsintensität über die jeweils zurückliegenden 15 Minuten, siehe Kasten.

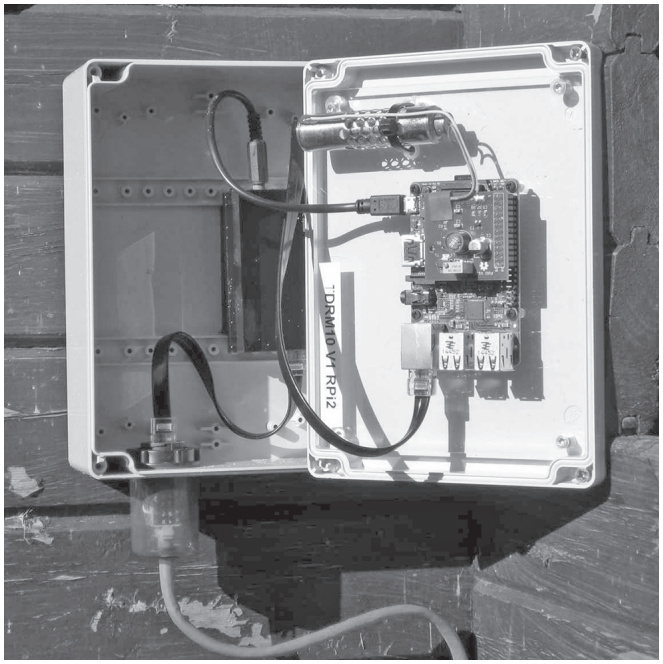


Abbildung 2: Eine der von TDRM gebauten Sensorstationen
Foto: Dietrich Meyer-Ebrecht, CC BY

Die Elektronik ist mit dem Geiger-Müller-Zählrohr zusammen in ein 10x15x20 cm messendes spritzwassergeschütztes Kunststoffgehäuse eingebaut (im Bild oben quer das Geiger-Müller-Zählrohr, darunter der Prozessor). Die Sensorstation soll möglichst außerhalb des Hauses installiert sein. Meist wird sie aus einer vorhandenen Außensteckdose mit Strom versorgt, und die Datenübertragung zum lokalen Router erfolgt über Powerline-Adapter. Eine Alternative ist die Stromversorgung über die Datenleitung mit PoE-Injektor und -Splitter (im Bildhintergrund).

An Standorten ohne Internetanschluss werden wir Funkverbindungen auf LoRaWAN-Basis einsetzen. LoRaWAN ist eine neue Kommunikationstechnologie, die für IoT-Anwendungen geschaffen wurde. Sie ermöglicht eine Datenübertragung im 868 MHz-Band über Entfernungen bis ca. 10 km mit niedriger Datenrate. Mit dieser Technologie baut die TTN-Community – TTN steht für „The Things Network"[8] – offene Netze aus Gateways zum Internet auf, die wir für die weitere Übertragung unserer Messwerte zu unserem Server nutzen. Hardware und Software für diese Erweiterung der TDRM-Sensorstation, die derzeit in Erprobung ist, wurden von einer Arbeitsgruppe an der Karel-de-Grote Hogeschool, Campus Hoboken, Antwerpen entwickelt.

Bisher wurden 20 Sensorstationen im Eigenbau erstellt. Der Materialaufwand liegt bei 200 € pro Sensorstation. Hinzu kommt für die Installation benötigtes Material wie Powerline-Adapter, Kabel etc. Die im Feld stationierten Sensorstationen bleiben Eigentum des FIfF, da ihr Material aus Spendengeldern finanziert wird, die zweckgebunden an das von der FIfF-Geschäftsstelle verwaltete TDRM-Spendenkonto fließen.

Die Messdaten der Sensorstationen laufen in unserem Server zusammen. Kern des Servers ist eine MySQL-Datenbank, die die einlaufenden Daten archiviert und sowohl für die Darstellung auf unseren Webseiten als auch für eine retrospektive Evaluation bereitstellt. Die Datenbank ist durch ein ReST-API gekapselt. Die ReST-Schnittstelle ermöglicht es, die Sensordaten als HTTPS-Pakete über die standardmäßig offenen Ports der Router Ende-zu-Ende-verschlüsselt zu übertragen. Ebenso holt sich die Website die für die anwenderseitigen Darstellungen benötigten Daten über die ReST-Schnittstelle aus der Datenbank. Datenbank und Website könnten mit Hilfe der ReST-Schnittstelle problemlos auf unterschiedlichen Servern gehostet werden. Derzeit werden sie jedoch gemeinsam auf einem für das FIfF betriebenen eigenen Server unter der Domain *tdrm.eu* gehostet.

Eine erste Website entstand im Wesentlichen im Rahmen eines Ausbildungsprojektes für angehende Fachinformatiker – eine glückliche Konstellation angesichts unserer sehr beschränkten personellen Ressourcen. Die Webseiten bieten die Darstellung der Messwerte in Übersichts- und Detailgrafiken sowie medi-

zinische und technische Hintergrundinformation. Ein wichtiges Feature ist die Viersprachigkeit – Französisch für die Wallonen, Niederländisch für die Flamen, Deutsch für die Aachener – und Englisch, denn das Projekt soll als überregionales, europäisches Angebot wahrgenommen werden.

Erreichtes und Geplantes

Die ersten Experimente und Entwicklungsarbeiten wurden vor nunmehr zwei Jahren im Frühjahr 2016 begonnen. Nach einigen Monaten Probebetrieb wurde das Netz am 13.12.2016 im Rahmen einer Pressekonferenz offiziell in Betrieb genommen und der Öffentlichkeit vorgestellt.

Mittlerweile sind fünf Sensorstationen im Umfeld des AKW Doel positioniert, ebenfalls fünf im Umfeld des AKW Tihange, drei ca. 25 km nordöstlich in Liège und Umgebung, weitere im Aachener Raum, in der Eifel und an der Hochschule Düsseldorf. Geplant ist der Ausbau auf mindestens zwei Sensorstationen in jeder der vier Himmelsrichtungen um jedes der beiden AKWs. Schwierig ist es, im immer noch sehr Atomkraft-freundlichen Belgien Menschen in der Umgebung der AKWs zu finden, die zur Installation einer Sensorstation auf ihrem Grundstück bereit sind. Schwierig ist es zudem, über die Entfernung und über die Sprachbarriere hinweg – Niederländisch in Flandern, Französisch in der Wallonie – die Installation durchzuführen und den Betrieb unterbrechungslos aufrecht zu erhalten. Mangels technischer Erfahrungen können uns die Menschen vor Ort dabei meist wenig unterstützen. So erfordern Installation und Betreuung viel Zeit und viele Fahrten.

Neben dem Aufbau weiterer Sensorstationen beschäftigt uns derzeit die Entwicklung einer von Grund auf neuen Website. Im Rahmen eines Semesterprojektes an der Hochschule Düsseldorf wurde bereits der Prototyp einer Website entwickelt, die die Darstellung automatisch an Smartphone-Displays anpasst (‚responsive design'). Ihre Entwicklerinnen und Entwickler lieferten viele Ideen für einen neuen umfassenderen Anlauf. Der wurde mit der Entwicklung einer Applikation begonnen, die auf dem CMS Joomla implementiert wird. Sie wird den Projektbeteiligten einen komfortableren Zugang für den Aufbau und die Pflege des Inhalts bieten, und sie wird vor allem weiter auf die inzwischen besser verstandenen Bedürfnisse der Nutzerinnen und Nutzer eingehen. Die Antwerpener TDRM-Arbeitsgruppe arbeitet an der Entwicklung einer Microcontroller-Version unserer Sensorstation mit geringem Energieverbrauch, die von einem Solarkollektor versorgt werden könnte.

Quo vadis, TDRM?

Natürlich fragen wir uns, was der gesellschaftliche Nutzen unseres Projektes ist. Was erwarten die Menschen von uns, die mit ihren Spenden das Projekt finanzieren? Solange keine außergewöhnlichen Situationen auftreten, solange die Strahlungsintensität im Bereich der erwarteten, immer vorhandenen Grundwerte bleibt, ist ein gelegentlicher Blick über die Zahlen und Zeitdiagramme beruhigend. Was aber, wenn aus den Messwerten ein außergewöhnlicher Störfall oder gar ein katastrophaler Unfall einer der Reaktoren gefolgert werden muss?

Ein Leichtes wäre es uns, eine Überwachungsfunktion einzurichten, die Grenzwertüberschreitungen automatisch erkennt und signalisiert. So werden wir dann auch immer wieder gefragt, warum wir nicht „eine App für Warnmeldungen" herausgeben. Vorgeworfen wurde uns bereits, dass es „un-ethisch" sei, wenn wir unsere Information für uns behielten. Jedoch, Warnmeldungen werden wir unter keinen Umständen veröffentlichen. Die Verantwortung für die Folgen könnten wir überhaupt nicht tragen. Einverständnis herrscht im Projektteam darüber, dass wir uns auch in unserem privaten Bereich keine Vorrechte herausnehmen.

Und doch haben wir eine automatische Grenzwertüberwachung vorgesehen. Allerdings ausschließlich für eine Weitergabe der Meldungen an die zuständige Behörde. Denn ihr allein obliegt in einer allgemeinen Gefahrensituation die Alarmierung der Öffentlichkeit. Der Adressat für eine Weitermeldung von Grenzwertüberschreitungen unserer Sensorstationen wäre die Leitstelle des regionalen Katastrophenschutzes. Sie trüge die Verantwortung für eine Verifizierung einer eintreffenden Meldung unter *proaktiver* Hinzuziehung aller ihr zugänglichen Informationsquellen. So würde das TDRM-Netz zu einem

D. Brückner, P. Kämmerling, G. Krenzer, D. Meyer-Ebrecht und M. Rabald

Daniel Brückner ist Systemadministrator an der RWTH Aachen. Im TDRM-Projekt ist er für die Softwareentwicklung und Administration unseres Servers verantwortlich.

Peter Kämmerling ist wissenschaftlicher Mitarbeiter im Forschungszentrum Jülich. Im TDRM-Projekt hat er die Entwicklung der Sensorstationen und deren Produktion übernommen.

Dr.Ing. **Gerd Krenzer** ist EDV-Berater. Er entwickelt ehrenamtlich die Website für das TDRM-Projekt.

Prof. Dr.-Ing. **Dietrich Meyer-Ebrecht** war Inhaber des Lehrstuhls für Messtechnik und Bildverarbeitung an der RWTH Aachen. Er ist Koordinator des TDRM-Projektes.

Michael ‚Mike' Rabald ist Immobilienmakler. In seinem ehrenamtlichen Engagement für das AAA baut er die Kontakte zu Interessenten in Belgien auf, und installiert und betreut unsere Sensorstationen.

entscheidenden Zeitvorsprung beitragen im Gegensatz zum Abwarten, bis die diesseits der Bundesgrenzen positionierten Messstellen der deutschen Behörden anschlagen oder Warnmeldungen über den grenzüberschreitenden Behördenweg eintreffen.

Unverzichtbare Voraussetzung für eine automatische Weitergabe der Information über Grenzwertüberschreitungen ist, dass wir zunächst das Netz der Sensorstationen um die AKWs genügend verdichtet haben, um Alarme durch Fehlmessungen und Störungen über Plausibilitätsprüfungen zwischen benachbarten Stationen, auch bei temporärem Ausfall einzelner Stationen, genügend sicher ausschließen zu können. Darauf arbeiten wir zur Zeit hin.

Natürlich hoffen wir, dass diese Maßnahme nie erforderlich wird. Das jedoch kann erst sicher ausgeschlossen werden, wenn alle Reaktoren in Tihange und in Doel endgültig stillgelegt sind. Unser Projekt wird, davon sind wir überzeugt, über eine informierte Öffentlichkeit den Forderungen an die Politik Nachdruck verleihen.

Resümee

Schauen wir zurück, müssen wir uns eingestehen, dass wir den zu leistenden Arbeitsaufwand, die Komplexität und die Zahl der Probleme zur Startzeit des Projektes total unterschätzt haben, insbesondere im Hinblick auf unsere sehr begrenzten personellen und finanziellen Ressourcen – und auch den Erfolgsdruck, nachdem das Projekt erst einmal wahrgenommen worden ist. Für die hohen Erwartungen schritt uns der Aufbau des Netzes viel zu langsam voran. Und doch wurde in den zwei Jahren viel erreicht. Das zeigen uns die vielen ermutigenden Zuschriften. Und die eintreffenden Spenden, mit denen wir unsere bisherigen Materialausgaben gut finanzieren konnten.

Dass wir mit unserem Projekt hohe Erwartungen der betroffenen Bürgerinnen und Bürger, nicht nur auf deutscher Seite, wecken würden, war uns schon am Anfang klar. Weniger waren wir uns bewusst, dass wir eine Verantwortung übernehmen würden, dass wir unser Projekt nicht mehr ohne Weiteres abbrechen können. Das ist schon eine Belastung. Aber Dank und Ermutigung belohnen uns, und die Bestätigung, dass wir vielen Menschen ein Bedürfnis nach Information erfüllen.

Dank

Das TDRM-Team dankt den engagierten Bürgerinnen und Bürgern, die – insbesondere im Umfeld der beiden Kernkraftwerke – eine Sensorstation in ihrem privaten Bereich installiert haben, und den vielen Spendern, die teils mit sehr großzügigen Zuwendungen geholfen haben, die Materialbeschaffung für die Produktion der Sensorstationen zu finanzieren. Wir danken Torben Müller, Lukas Tetz und David Walzer, die Datenbank und Website im Rahmen ihrer Fachinformatiker-Ausbildung entwickelt haben, Jörg Schellenberg vom AAA, der das Projekt maßgeblich mit angeschoben hat, und ganz besonders Lorenz Andriaensen und seiner Arbeitsgruppe an der Karel-de-Grote Hogeschool, die das Projekt im Raum Antwerpen vielfältig unterstützen.

Referenzen

1 *http://www.radioaktive-strahlung.org/radioaktivitaet/isotope.htm*
2 *Gufler AK, Sholly S, Müllner N. (2017) Mögliche radiologische Auswirkungen eines Versagens des Reaktordruckbehälters des KKW Tihange 2. Universität für Bodenkultur Wien, http://flexrisk.boku.ac.at/de/followup.html*
3 *https://de.wikipedia.org/wiki/Liste_von_Unf%C3%A4llen_in_kerntechnischen_Anlagen*
4 *https://www.heise.de/tp/features/Beinaheunfall-in-Norwegen-3648067.html*
5 *https://remap.jrc.ec.europa.eu/Consent/GammaDoseRates.aspx*
6 *http://odlinfo.bfs.de/DE/themen/wo-stehen-die-sonden/messstellen-in-deutschland.html*
7 *PiGI, Raspberry Pi Geiger-Müller Interface, https://apollo.open-resource.org/lab:pigi*
8 *The Things Network (TTN), thethingsnetwork.org*

Unschärfe vs. Ansprechverzögerung bei der Messung radioaktiver Strahlung

Wenn jede Minute neue Mess*daten* gesendet werden, heißt dies nicht, dass wir jede Minute einen Mess*wert* erhalten, der die Strahlungsintensität zu genau diesem Zeitpunkt repräsentiert. Radioaktive Strahlung ist ein stochastisches Phänomen. Dass ein Atom des radioaktiven Isotops in der Umgebungsatmosphäre zerfällt, ist ein Zufallsereignis, und es ist wiederum ein zufälliges Zusammentreffen, wenn das Quant oder Teilchen, das von dem zerfallenden Atom ausgesandt wird, genau auf unseren Sensor auftrifft und mit einer Interaktion dort einen Impuls auslöst. Ein Maß für die Intensität einer Strahlung kann nur gewonnen werden, wenn wir den Mittelwert der Ereignisse über ein Zeitintervall bestimmen. Je länger wir das Zeitintervall wählen, desto geringer wird die Streuung sein – desto weniger aktuell aber auch der Messwert.

Wir haben den Kompromiss zugunsten einer schnellen Anzeige außergewöhnlicher Veränderungen gewählt. Das aktuelle Messdatum ist das Ergebnis einer Impulszählung über ein mitgezogenes Zeitfenster von 15 Minuten. Wenn unsere Sensoren bei einem üblichen Grundwert der Strahlungsintensität in 15 Minuten im Mittel um die 100 Ereignisse registrieren – der *Erwartungswert* –, ist die Standardabweichung 10 (bei der zu Grunde liegenden Poissonverteilung ist die Varianz gleich dem Erwartungswert, die Standardabweichung die Wurzel daraus). D.h. bei konstanter Strahlungsintensität lägen ca. 1/3 aller unserer Messwerte außerhalb eines Bereiches von ± 10 % um den Erwartungswert.

Moritz Kütt und Alex Glaser

Retrocomputer für Abrüstungsverifikation und eine kernwaffenfreie Welt

Im Rahmen einer zukünftigen Abrüstung von Kernwaffen müssen Sprengköpfe vor ihrer Zerlegung als authentische Sprengköpfe bestätigt werden. Das erfordert vertrauenswürdige Messsysteme, die diese Identifikation anhand von radioaktiven Signaturen vornehmen können. Verschiedene solche Systeme existieren, bei allen ist jedoch die vertrauenswürdige Datenverarbeitung problematisch. Eine neuer Vorschlag für ein Messsystem basiert auf der Nutzung von Retrocomputern. Information Barrier eXperimental II *ist ein Prototyp eines solchen Systems zur Gammaspektroskopie auf Basis eines* Apple IIe *mit MOS 6502 Prozessor.*[1]

Kernwaffen sind wieder in aller Munde, und Experten schätzen das weltweite Risiko eines Einsatzes höher ein als in den letzten zwei Jahrzehnten – oder gar seit der Kubakrise vom Oktober 1962. Erst im Januar dieses Jahrs hat das renommierte *Bulletin of the Atomic Scientists* die *Doomsday Clock* auf zwei Minuten vor Mitternacht vorgestellt. Die Uhr beschreibt die Nähe der Welt zu einer globalen Katastrophe. Die neue Zeigerposition reflektiert die wachsende Bedrohung durch ein nuklear bewaffnetes Nordkorea, aber auch die öffentlichen Drohungen eines Kernwaffeneinsatzes durch US-Präsident Trump und die angespannten Beziehungen zwischen Russland und den USA.

Gleichzeitig zeigt die Doomsday Clock aber auch Versäumnisse der letzten Jahre auf. Es existieren immer noch rund 15 000 Kernwaffen im Besitz von neun Ländern. Die USA und Russland besitzen mit je rund 7000 Sprengköpfen den größten Anteil. Die Arsenale der anderen Staaten – Frankreich, Großbritannien, China, Israel, Pakistan, Indien und Nordkorea – sind deutlich kleiner. Es ist jedoch klar, dass auch ein sehr begrenzter Einsatz von Kernwaffen zu einer globalen Katastrophe führen würde, mit massiven klimatischen Auswirkungen durch den *Nuklearen Winter* und nie dagewesenen humanitären Konsequenzen sowohl für direkt betroffene Regionen als auch den Rest der Welt. Die komplette Abrüstung dieser Waffen ist nötig, vielleicht nötiger denn je.

Bestrebungen zur Rüstungskontrolle und Abrüstung gibt es prinzipiell seit dem Ende des Zweiten Weltkriegs, als die USA noch über ein Monopol über diese neuartigen Waffen verfügten. Das wichtigste Vertragswerk ist der nukleare Nichtverbreitungsvertrag (NVV), der 1970 in Kraft trat. Er verbietet die Entwicklung von Kernwaffen für Länder, die keine Kernwaffen besitzen (Nichtkernwaffenstaaten). Daneben definiert der Vertrag Kernwaffenstaaten, für die der Besitz von Kernwaffen weiterhin erlaubt bleibt (USA, Großbritannien, China, Frankreich, Russland). Kernwaffenstaaten verpflichten sich aber auch zur nuklearen Abrüstung, wenn auch ohne konkreten Zeitplan. Weitere Verträge sind der noch nicht in Kraft getretene Kernwaffenteststopp-Vertrag sowie bilaterale Vereinbarungen zwischen den USA und Russland.

In den ersten Jahren nach dem Ende des Kalten Kriegs gab es eine kurze Periode, in der weitreichende Fortschritte im Bereich der nuklearen Abrüstung möglich schienen. In diesen Jahren haben sowohl Russland als auch die USA Teile ihrer Kernwaffen-Arsenale abgerüstet und auch die Bestände an Waffenmaterialien reduziert. In der jüngeren Vergangenheit hat sich diese Entwicklung jedoch wieder eher umgekehrt. Nordkorea, Indien und Pakistan sind in den letzten 20 Jahren als neue Kernwaffenstaaten hinzugekommen. Aktuell rüstet insbesondere Nordkorea auf, indem es neben Sprengköpfen auch Tests von Langstreckenraketen durchführt, die diese Kernwaffen zu weit entfernten Zielen bringen könnten. Auch alle anderen Kernwaffenstaaten sind weit von ernsthaften Abrüstungsschritten entfernt; vielmehr modernisieren sie ihre aktuellen Arsenale, um sie für die nächsten Jahrzehnte bereit zu machen, und führen neue Waffengattungen ein.

Vor diesem Hintergrund gab es 2017 einen Lichtblick: Ein neuer internationaler Vertrag zum vollständigen Verbot von Kernwaffen *(Ban-Treaty)* ist erfolgreich verhandelt worden. Der Vertrag ist ein Versuch, eine existierende Regelungslücke zu füllen und Kernwaffen als letzte Kategorie von Massenvernichtungswaffen zu verbieten. Die Verhandlungen bauten auf Ergebnis-

Moritz Kütt und Alex Glaser

Alex und **Moritz** sind Friedensforscher und Aktivisten für eine Welt ohne Kernwaffen. Beide sind Physiker, und arbeiten am *Nuclear Futures Laboratory, http://nuclearfutures.princeton.edu* und dem *Program on Science and Global Security https://www.princeton.edu/sgs/* der Princeton University in den USA.

Ihre Forschung behandelt Verifikationstechnologien für Rüstungskontrolle und damit zusammenhängende politische Fragen. Aktuelle Projekte sind unter anderem: Nukleare Archäologie, Zero-Knowledge Protokolle, Virtual Proofs of Reality, Roboterinspektionen, Disco-Verifikation und Open Source Informationsbarrieren für Sprengkopf-Authentifizierung. Für viele der Projekte entwickeln sie eigene Software und Hardware, und nutzen Ideen aus der Maker-/Hacker-Szene.

sen von drei internationalen Konferenzen auf, bei denen die humanitären Konsequenzen des Einsatzes von Kernwaffen diskutiert wurden. Die Nichtregierungsorganisation *ICAN* (Internationale Kampagne zur Abrüstung von Kernwaffen) spielte bei den Konferenzen und den Vertragsverhandlungen eine wichtige Rolle. Ihre Arbeit des letzten Jahrzehnts wurde durch die Verleihung des Friedensnobelpreises an die Organisation im Dezember 2017 gewürdigt. Derzeit haben 56 Staaten den Verbotsvertrag unterzeichnet, 90 Tage nach der Ratifikation des Vertrags durch den fünfzigsten Staat wird der Vertrag in Kraft treten. Die Staaten, die Kernwaffen besitzen, sind den Vertragsverhandlungen erwartungsgemäß ferngeblieben. Auch fast alle NATO-Mitgliedsstaaten fehlten, Deutschland inklusive. Trotz grundsätzlicher Befürwortung von nuklearer Abrüstung sieht Deutschlands Politik aktuell weiterhin eine Rolle für Kernwaffen im Rahmen der NATO-Mitgliedschaft vor. Das zeigt sich unter anderem durch die Stationierung von 20 amerikanischen taktischen Nuklearwaffen auf einem Bundeswehrstützpunkt in Büchel, Rheinland-Pfalz. In der Vergangenheit forderten Politiker unterschiedlicher Parteien (etwa Guido Westerwelle als Außenminister oder Martin Schulz als Kanzlerkandidat) den Abzug dieser Waffen. Ein solcher Beschluss, möglicherweise verbunden mit dem Beitritt zum Kernwaffenverbotsvertrag, würde ein deutliches Zeichen setzen, und könnte auch den Beitritt einiger weiterer Staaten zum Verbotsvertrag einleiten.

Zentrale Komponente für weitere Schritte zur nuklearen Abrüstung ist die Verifikation der einzelnen Schritte. Durch solche Verifikationsmaßnahmen wird die Einhaltung der Verpflichtungen einzelner Staaten im Rahmen von internationalen Verträgen überprüft. Eine solche Überprüfung wird in der Regel durch andere Staaten oder internationale Organisationen vorgenommen, auch eine Überprüfung durch die allgemeine Bevölkerung ist vorstellbar *(Societal Verification).* Dabei gibt es verschiedene Herausforderungen. Es muss insbesondere sichergestellt werden, dass Staaten, auch solche ohne Kernwaffen, kein kernwaffenfähiges Spaltmaterial für militärische Zwecke erzeugen oder es aus dem zivilen Kernenergiesektor entnehmen. Abzurüstende Sprengköpfe müssen vor ihrer Zerlegung als wirkliche Sprengköpfe authentifiziert werden. Während und nach der eigentlichen Zerlegung muss eine lückenlose Kontrollkette gewährleistet werden, um Rückführungen von Sprengköpfen oder deren Bestandteilen in den militärischen Bereich zu vermeiden.

Sprengköpfe prüfen

Die von uns vorgestellte Technologie adressiert Probleme bei der Sprengkopf-Authentifizierung. Die Verfahren haben ein grundsätzliches Problem: Durch die Messungen werden Informationen enthüllt, die Kernwaffenstaaten als extrem sensitiv ansehen. Solche Messungen würden insbesondere das Design einer Kernwaffe preisgeben und ggf. auch auf mögliche *Schwachstellen* hinweisen. Zudem werden bei erweiterten Abrüstungsverträgen in Zukunft weitere Staaten Teil dieser Verifikationsbemühungen werden, im Rahmen des Ban-Treaty beispielsweise auch Staaten, die selbst keine Kernwaffen besitzen.

Kernwaffen lassen sich eigentlich vergleichsweise leicht anhand der von ihnen emittierten radioaktiven Strahlung identifizieren. Es gibt zwei unterschiedliche Verfahren: Beim *Attributverfahren* werden vor den Messungen gewisse Eigenschaften vereinbart, die dann durch die Messung ermittelt werden. Ein solches Attribut könnte beispielsweise die Anwesenheit von Plutonium sein; ein weiteres Attribut könnte eine festgelegte Untergrenze bestätigen, beispielsweise: Enthält das inspizierte Objekt mehr als zwei Kilogramm Plutonium? Beim *Template-Verfahren* findet die Identifizierung durch Vergleich statt. Ein Objekt wird als Muster bestimmt, alle anderen Objekte damit verglichen. Dabei ist wichtig, die Herkunft und Authentizität des Musters zuverlässig zu bestimmen, etwa durch zufällige Auswahl eines Sprengkopfs von stationierten Systemen durch Inspektoren.

Beide Ansätze werden typischerweise durch *Informationsbarrieren* ergänzt. Das sind Geräte, die komplexe Informationen verarbeiten und anschließend nur limitierte Informationen preisgeben. Eine solche, limitierte Information könnte etwa *Sprengkopf/Kein Sprengkopf* sein, häufig dargestellt durch grüne und rote LEDs. Die Analyse der komplexen Informationen erfolgt durch Datenverarbeitungssysteme. Wichtigste Voraussetzung für die Nutzung von Informationsbarrieren ist, dass beide Parteien Vertrauen in die Geräte haben. Die inspizierte Partei (Host) hat dabei ein Interesse daran sicherzustellen, dass keine sensitiven Informationen preisgegeben werden. Das könnte entweder absichtlich (etwa durch einen Nebenkanal) oder durch eine Fehlfunktion des Instruments geschehen. Die inspizierende Partei (Inspektor) fordert, dass die Informationsbarriere keinen Betrug zulässt und die angezeigten Ergebnisse die Realität korrekt wiedergeben. So könnte ein *Hidden Switch* nur dann aktiviert werden, wenn das Gerät unter bestimmten Bedingungen verwendet wird; überprüft der Inspektor das Gerät früher oder später an einem anderen Ort, würde es einwandfrei funktionieren.

Einige Gründe erschweren die Entwicklung von Informationsbarrieren: Es sind vorab wenige Informationen über das zu messende Objekt bekannt; der *Host* hat quasi unendliche Ressourcen, um einen Betrug zu vertuschen; und die Motivation zum Betrug ist hoch, denn bei Erfolg könnte der Host eigentlich abgerüstete Kernwaffen weiter besitzen. Ein weiteres Problem ist, dass nach bisherigem Stand die Hardware nach Messung an Kernwaffen beim Host verbleibt. Das schließt eine nachträgliche Überprüfung der Messelektronik durch Dritte aus.

Einige Prototyp-Informationsbarrieren wurden in den letzten Jahrzehnten entwickelt, die meisten als Forschungsarbeiten von US-amerikanischen Kernwaffenlabors. Teilweise wurden sie in Kooperation mit russischen Experten entwickelt und erprobt. Das erste und bisher einzige System, dass aus einer Kooperation eines Kernwaffenstaats und eines Nichtkernwaffenstaats hervorgegangen ist, wurde von Norwegen und Großbritannien im Rahmen der *UK-Norway Initiative* entwickelt. Die jeweiligen Entwicklungen unterscheiden sich, insbesondere bei verwendeten Mikroprozessoren und den angeschlossenen Detektoren. Trotz der zentralen Rolle solcher Geräte bei der Abrüstung gibt es jedoch bisher keine zufriedenstellenden Lösungen.

Wir schlagen daher ein alternatives Messsystem vor, das wir *Vintage Verification* nennen. Dabei werden alle informationsverarbeitenden Teile (wie Mikroprozessoren) durch alte oder *klassische* Hardware ersetzt (Retrocomputer). Alt in diesem Sinne ist Hardware aus den 70er und 80er Jahren, als der Einsatz von integrierten Schaltkreisen und Mikroprozessoren in

großem Umfang begann. Solche Hardware wäre deutlich vertrauenswürdiger als moderne Elektronik. Das hat vor allem zwei Gründe. Erstens ist solche Hardware tausendfach (oder gar millionenfach) weniger leistungsfähig. Die Implementierung betrügerischer Funktionen wird dadurch deutlich erschwert, da die Rechenleistung für solche Funktionen gar nicht zur Verfügung steht. Zweitens ist es sehr unwahrscheinlich, dass ein Mikroprozessor, der vor rund 40 Jahren gefertigt wurde, damals schon im Rahmen der Fertigung mit geheimen Betrugsfunktionen ausgestattet wurde, die speziell auf die heutige Anwendung der Abrüstungsverifikation abzielen.

Durch die Entwicklung der in Folge vorgestellten *Information Barrier eXperimental II (IBX II)* wollen wir zeigen, dass es möglich ist, mit Retrocomputern funktionsfähige Informationsbarrieren zu konstruieren. Unser Prototyp basiert auf einem Apple IIe sowie zwei neu entwickelten Erweiterungskarten (siehe Abbildung 1)[2]. Die IBX II kann zwei Objekte mit Hilfe des Template-Verfahrens als *identisch* oder *nicht identisch* klassifizieren. Wir nehmen dazu ein Gammaspektrum mit einem Sodium-Iodid-Szintillationskristall und zugehörigem Photomultiplier auf. Das ist seit vielen Jahrzehnten handelsübliche Hardware für solche Messungen. Die vergleichsweise niedrige Messauflösung kommt weiterhin dem Schutz sensitiver Informationen entgegen.

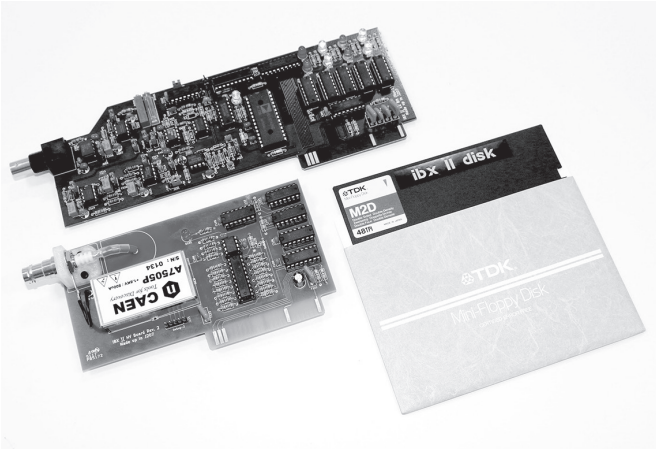


Abbildung 1: Apple IIe Erweiterungskarten und Software für IBX II, Foto A. Glaser

Die Datenverarbeitung der IBX II wird von einem Apple IIe durchgeführt. Dieser Heimcomputer, ursprünglich 1977 auf den Markt gebracht (zunächst in Version Apple II), wurde bis 1993 verkauft. Der Apple II kann als einer der *hackerfreundlichsten* Massencomputer seiner Zeit angesehen werden und war sicherlich das letzte *hackbare* Gerät aus dem Hause Apple. Im Rahmen des Designs kam es zu einem Streit zwischen den beiden Unternehmensgründern Steve Jobs und Steve Wozniak. Jobs wollte das System nur mit zwei Erweiterungssteckplätzen ausstatten. Wozniak dagegen plädierte für 8 Steckplätze, für möglichst viele von Nutzern gebaute Erweiterungskarten. Er konnte sich durchsetzen, und die Nutzergemeinde entwickelte tatsächlich viele Erweiterungskarten über Modem und Drucker hinaus – bis heute.

Herz des Apple IIe ist der MOS 6502 Mikroprozessor. Dieser 8-Bit Prozessor wurde 1975 vorgestellt, im Apple IIe läuft er mit 1 MHz. Der Prozessor war schon zu damaliger Zeit deutlich einfacher entworfen als andere Prozessoren (wie der Intel 8080 oder der Z80) und besitzt nur 3510 Transistoren. Trotz oder gerade wegen des einfachen Layouts und nur 56 Befehlen war er relativ leistungsfähig und robust. Der Prozessor wird bis heute produziert, und der aktuelle Hersteller Western Design Center schätzt, dass weltweit bis zu zehn Milliarden Einheiten dieses Chips produziert wurden. Der Prozessor ist heute quasi Open Hardware. Obwohl originale Designentwürfe nicht verfügbar sind, wurde die Struktur in mehreren Reverse Engineering Projekten ermittelt. Besonders hervorzuheben ist dabei die Arbeit von Visual 6502[3], die die elektrische Struktur durch hochauflösende Fotografien des Chips bestimmt haben. Monster 6502 hat ein funktionierendes Modell des Prozessors im Maßstab 7000:1 nachgebaut[4].

Die erste von uns für die IBX II entwickelte Erweiterungskarte versorgt den Photomultiplier mit der benötigten Hochspannung (1000 V). Sie basiert auf einer einfachen Digital-Analog-Konverter-Schaltung mit R2R-Netzwerk. Damit kann durch Software die Ausgangsspannung gesteuert werden, etwa um sie langsam von 0 auf 1000 V zu steigern bzw. am Ende wieder abzusenken und so das angeschlossene Gerät zu schonen.

Die zweite Karte *(ADC Karte)* dient der Datenaufbereitung und -digitalisierung und nutzt einen 12-Bit Analog-Digital-Konverter (ADC) des Typs AD1674 zur Digitalisierung. Ein Gammaspektrum zeigt die Häufigkeiten, mit denen Gammazerfälle bestimmter Energien gemessen werden (siehe Monitoranzeige in Abbildung 2). Einzelne Gammastrahlen, die im Szintillatorkristall detektiert werden, führen zum Aufbau von Ladung am Ausgang des Photomultipliers. Diese Ladung wird von der entwickelten Messkarte in einen Spannungspuls umgewandelt. Die Energie des Gammateilchens ist proportional zur Höhe dieses Pulses. Um daraus ein Gammaspektrum zu erzeugen, wird die Anzahl der Pulse in unterschiedlichen Energiebereichen (Kanälen) über eine gewisse Zeit gezählt. Der Datenaufbereitungsteil der ADC Karte verstärkt ankommende Pulse und verändert die zeitliche Form der Pulse, um eine bessere Digitalisierung zu ermöglichen. Eine *Peak-Detect-And-Hold*-Schaltung erkennt neue Pulse und gibt ein Signal an den Analog-Digital-Konverter, um einen Konvertierungsprozess zu starten. Während dieses Prozesses hält die Schaltung die Spannung am Eingang des ADC konstant auf der Höhe der Spitze des Pulses. Nach Abschluss der Konvertierung steht ein digitaler Wert am Ausgang

Abbildung 2: Mit Apple IIe aufgenommenes Gammaspektrum Foto A. Glaser

des ADC bereit und lässt sich durch Software auslesen. Software sortiert auch in die Kanäle.

Um die beiden Karten anzusteuern, nutzen wir ein 6502 Assembler-Programm. Eine Inspektion verläuft in vier Schritten: Zunächst wird die Hochspannung eingeschaltet, dann ein Gammaspektrum des Templates aufgenommen. Anschließend kann ein Gammaspektrum eines zu inspizierenden Objekts aufgenommen werden. Im letzten Schritt werden beide Spektren verglichen. Für diesen Vergleich werden die Daten der Spektren in je nur 12 Kanäle zusammengefasst. Die resultierenden Verteilungen werden dann mit einem Chi-Quadrat-Test verglichen. Ist das Resultat kleiner als ein Schwellwert, wird von einer hohen Ähnlichkeit ausgegangen, der Vergleich ist erfolgreich. Ansonsten ist er nicht erfolgreich. Das jeweilige Ergebnis wird entweder am Bildschirm oder über Leuchtdioden ausgegeben. Drei Faktoren beeinflussen die erzielbare Zählrate: Peak-Detect-and-Hold (dauert etwa 10–15 µs), Digitalisierung (10–15 µs) und Verarbeitung mit 6502 (35–50µs). Nach maximal 100 µs ist das Signal aufgenommen, vom 6502 verarbeitet und in den Speicher geschrieben. Theoretisch sind mit der IBX II also bis zu 10 000 Ereignisse pro Sekunde messbar. Typischerweise betreiben wir die IBX II in einem Bereich von 2000 Ereignissen pro Sekunde. Ein Spektrum kann in 1-2 Minuten aufgenommen werden.

Als Teil des Entwicklungsprozesses haben wir zu Testzwecken einen existierenden Apple II Emulator (LinApple) so erweitert, dass er auch die Funktion der beiden Erweiterungskarten enthält. Damit konnten Programmentwicklung und -tests an einem modernen Rechner durchgeführt werden. Interessierte, die unsere Arbeit testen wollen, aber nicht über die notwendige Hardware verfügen, bietet der Emulator einen guten Startpunkt (siehe Endnote 2).

Durch Entwicklung und Test der beiden Erweiterungskarten konnten wir zeigen, dass die Idee, alte Hardware zu benutzen, grundsätzlich funktionieren kann. Bisher noch als Erweiterungskarten im selbst relativ komplexen Apple IIe lässt sich ein ähnliches Design in Zukunft auch auf ein einfacheres 6502-basiertes System anpassen. So ist eine Informationsbarriere vorstellbar, die neben der Hardware der Erweiterungskarten nur einen 6502, etwas ROM für die Software und ausreichend RAM für das Template enthält. Weitere Schritte in Zukunft sind eine Optimierung des Assembler-Programms, aber auch der entwickelten Hardware. Gleichzeitig sollte versucht werden, möglichst verschiedene Wege zu finden, mit denen Alter bzw. Authentizität des verwendeten Mikroprozessors nachgewiesen werden können. Dafür sind nicht-destruktive Methoden, etwa Röntgenmikroskopie, und destruktive Methoden vorstellbar. Gerne nehmen wir Ideen und Hinweise von anderen auf. Auch wenn noch einige Schritte zu tun sind, hoffen wir, dass unser hier vorgestelltes Projekt ein kleiner Beitrag auf dem Weg zu einer kernwaffenfreien Welt ist.

Anmerkungen

1 *Inhalte dieses Artikels wurden auf dem 34c3 vorgetragen.*
2 *Software, Hardware Design und modifizierter Emulator verfügbar unter www.vintageverification.org*
3 *visual6502.org*
4 *monster6502.com*

FIfF e. V. – Pressemitteilung

FIfF-Sachverständigenauskunft zum Trojanereinsatz durch den hessischen Verfassungsschutz

FIfF lehnt Hessentrojaner ab

7. Februar 2018 – Am 8. Februar 2018 findet eine öffentliche mündliche Anhörung des hessischen Innenausschusses zum Gesetzentwurf der Fraktionen von CDU und Bündnis 90/Die Grünen für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen (HVSG) statt. Weil dem hessischen Verfassungsschutz innerhalb dieser Gesetzesnovelle auch der Einsatz von Trojanern in Form von verdeckter Quellen-TKÜ und geheimer Online-Durchsuchung erlaubt werden soll, ist das FIfF als Sachverständiger eingeladen worden. Wir empfehlen dringend, die Quellen-TKÜ und die heimliche Online-Durchsuchung ersatzlos zu streichen.

Einleitung

Geheimdienste, also staatliche Behörden, die wesentlich auf verdeckte Maßnahmen, Tarnoperationen, „Vertrauensleute“ oder verdeckte MitarbeiterInnen setzen, sind inhärent auf Intransparenz angelegt und angewiesen, da Heimlichkeit das primäre Mittel ist, die ihnen übertragenen Aufgaben auszufüllen. Ermächtigungen derartiger Dienste müssen folglich besonders kritisch analysiert werden, da einmal freigegebene Maßnahmen und ermöglichte Methoden meist nur nach Skandalen erneut zur breiten Diskussion gestellt werden (können).

Auch wenn sich die Aufgabenbereiche von Polizeien und Geheimdiensten mittlerweile gefährlich überlappen, sind dennoch die Berichts- und Transparenzpflichten von polizeilichen Behörden – im Gegensatz zu verdeckt tätigen Organisationen – zumindest grundsätzlich auf Offenheit angelegt. Wegen dieses gewichtigen Unterschieds gehen die rechtfertigenden Referenzen des Gesetzentwurfs bezüglich der Entscheidung des Bundesverfassungsgerichts zum BKA-Gesetz natürlich prinzipiell fehl. **Ein Geheimdienst ist keine Polizei und eine Polizei ist kein Geheimdienst.**

Der aktuelle Vorstoß, Geheimdiensten wie dem Verfassungsschutz die Ermächtigung zu geben, informationstechnische Systeme zu infiltrieren, ist in einen stetigen, sehr beunruhigenden Trend einzuordnen: den schrittweisen Ausbau von informationstechnischen Offensivfähigkeiten der Behörden im Sicherheitsbereich. Der Bundesnachrichtendienst (BND) hat mit seiner 300 Millionen Euro teuren *Strategischen Initiative Technik* die Fähigkeiten bekommen, technische Systeme verdeckt und offen angreifen können[1]. Aber auch die Bundeswehr wurde durch die *Strategische Leitlinie Cyber-Verteidigung* aufgerüstet, die explizit – anders als der Name impliziert – auch „offensive Cyber-Fähigkeiten" als *Wirkmittel* vorsieht.[2]

Es werden also viele hundert Millionen Euro in geheime IT-Angriffsstrategien investiert; doch beispielsweise für das *Nationale Referenzprojekt zur IT-Sicherheit in Industrie 4.0*[3] – die digitale Absicherung der Zukunft der deutschen Industrie – gibt es nur eine Finanzierung von 33 Millionen Euro; ein klares Missverhältnis. **Wir halten diese primäre Offensivausrichtung für die schlechteste aller Digitalisierungsstrategien.**

Gewährleistung der Vertraulichkeit und Integrität unserer Infrastruktur

Wenn wir von einer vernetzten Gesellschaft mit *Cloud, Industrie 4.0, Internet of Things* und *smarten* Infrastrukturen sprechen wollen, so muss immer auch die damit einhergehende gegenseitige Abhängigkeit und Verwundbarkeit mitgedacht werden. Wird also ein Hersteller oder Softwareprodukt durch bestimmte Maßnahmen und Regelungen geschützt, werden parallel dazu auch die anderswo eingesetzten Systeme, NutzerInnen und Nutzungsarten mitgeschützt. Im Gegenzug bedeutet dies jedoch auch, dass Schädigungen oder Schwächungen von bestimmten Softwarekomponenten gleichermaßen auch alle anderen Einsatzweisen schwächt und unsicherer macht. Aus diesem Grunde war es beispielsweise möglich, dass die Schadsoftware *Wannacry* sowohl private Laptops als auch ganze Krankenhaus-, Eisenbahn- und Providersysteme lahmlegen konnte.[4]

Nun nutzen alle Formen staatlichen Hackings, wie etwa die verdeckte Quellen-TKÜ oder die geheime Online-Durchsuchung – bekannte oder unbekannte – Sicherheitslücken. Doch woher kommen diese und was hat die Nutzung für Auswirkungen auf die allgemeine (IT-)Sicherheit?

Analyse der Kollateralschäden

Üblicherweise sind gerade staatliche Akteure im Sicherheitsbereich finanziell gut ausgestattet und können Sicherheitslücken am weltweiten Schwarzmarkt erwerben. Doch dadurch werden diese Unsicherheits-Märkte ganz wesentlich erzeugt, vergrößert und fatalerweise sogar demokratisch legitimiert. Gefundene Lücken werden nun zunehmend nicht mehr an Hersteller gemeldet, sondern auf den Märkten an die Meistbietenden versteigert. **In der Folge wird die gesamte IT-Infrastruktur unsicherer, da die Lücken natürlich auch Kriminellen, nicht befreundeten und auch „befreundeten" Staaten offenstehen.**

Üblicherweise verkaufen diese Sicherheitslücken-Händler ihre toxische Ware auch nicht nur an demokratische Staaten, wie man an der aktuell vom Bundeskriminalamt (BKA) beauftragten[5] deutschen Firma *Gamma/FinFisher* sehen kann. Deren Software *FinSpy* wurde damals auch von bahrainischen Behörden genutzt, um DissidentInnen zu verfolgen und den Arabischen Frühling niederzuschlagen.[6] Weitere Kunden der Firma sind Behörden in Diktaturen wie Dubai oder Katar.[7] Dabei werden auch diese Firmen immer wieder gehackt und dann deren Software, Sicherheitslücken und interne Dokumente veröffentlicht.[8]

Das ist der aktuelle katastrophale Zustand der weltweiten IT-Sicherheit. Und deutsche Behörden wollen nun weiter mithelfen, diesen Status quo zu noch weiter zu verschlechtern. Wir halten das für inakzeptabel. Das wohl bekannteste Beispiel für den Irrweg, Lücken zu behalten, war sicherlich der oben schon erwähnte Erpresserwurm *Wannacry.* Er infiltrierte weltweit zehntausende Systeme und nutzte dafür Sicherheitslücken, die der US-Geheimdienst NSA seit Jahren für eine spätere Verwendung aufgehoben hatte – und das trotz diesbezüglicher, interner Risikoabwägungsmechanismen.[9]

In der wohlwollenden Interpretation unterstützen deutsche Behörden mit Steuergeldern also schäbige Geschäftsmodelle. **In der besorgniserregenderen Deutung finanzieren deutsche Behörden Firmen, die direkt oder indirekt an der Verfolgung von DissidentInnen und MenschenrechtsverteidigerInnen in Diktaturen beteiligt sind.** Unsere Freunde von *Amnesty International* können schon jetzt vom bitteren „Erfolg" dieser Strategie berichten.[10]

Kurzum, wenn es tatsächlich um Sicherheit gehen soll, so muss die Suche nach Sicherheitslücken strukturiert, koordiniert und konsequent angegangen werden, ohne Ausnahme. Die globalisiert-vernetzte Informationsgesellschaft bedeutet mittlerweile eben auch: **Es gibt keine öffentliche Sicherheit mehr ohne IT-Sicherheit.**

Wieder *Terrorismus* als Begründung

Im Gesetzesentwurf gibt es mehrere konkrete Erwähnungen des NSU- und internationalen Terrorismus als Begründung. Der Terror soll nun noch entschlossener bekämpft werden, auch durch staatliches Hacking. Drei Beispiele aus der aktuellen Terror-Debatte seien hier einmal kurz kommentiert:

1. Gerade im skandalösen Fall des NSU und seiner (Nicht-) Aufklärung waren fehlende QKTÜ/OD-Fähigkeiten sicherlich das kleinste Problem im ganzen Debakel.[11]

2. Im Fall der rechtsextremen Oldschool Society (OSS), weitläufig bekannt durch den strittigen Telegram-Zugriff durch das BKA, waren die so erlangten Informationen vor dem Münchner Oberlandesgericht für die Verurteilung letztlich gar nicht verwendet worden.[12]

3. Der weltweit berühmte Fall um die San-Bernadino-Bomber und ihr verschlüsseltes iPhone machte zwar gute Schlagzeilen für Apple, basierte jedoch auf einem Password-Reset-Fehler der Ermittler, der dann erst den extrem teuren Hack

nötig machte. Das Öffnen des iPhones brachte im Übrigen gar keine nützlichen Informationen hervor.[13]

Insgesamt sehen wir die Begründung der neuen IT-Befugnisse in Bezug auf die im Entwurf benannten terroristischen Ereignisse also höchst kritisch. Auch wenn der Zweck *Terrorismusbekämpfung* die volle Unterstützung verdient, schießen die technischen Infiltrationsbefugnisse doch über das Ziel hinaus. Gerade bei den im Entwurf genannten Ereignissen lohnt es sich, detailliert zu durchdenken, inwiefern eine QTKÜ/OD jeweils hilfreich und zwingend notwendig gewesen wäre. Denn in einigen Fällen waren die Täter schon vorher bekannt und etwa der Anschlag am Breitscheidplatz in Berlin wurde offenbar sogar mit Involvierung von V-Leuten durchgeführt.[14] Gleiches gilt für den NSU-Fall um Andreas Temme.

Kurzzusammenfassung unserer Position zum vorliegenden Gesetzentwurf

- Speziell die Paragraphen § 6 (Quellen-TKÜ) und § 8 (Online-Durchsuchung) beziehen sich auf eine technische Ermächtigung, mit der ein informationstechnisches System infiltriert werden kann. Welche Daten letztendlich ausgeleitet werden – Kommunikation oder nicht –, ist technisch nicht automatisiert unterscheidbar und dementsprechend auch nicht sinnvoll einzuhegen. Quellen-TKÜ und OD müssen daher die gleichen Eingriffshürden und Berichtspflichten haben.

- Des weiteren gibt es technisch begründet wesentliche Zweifel an einer vertrauenswürdigen Protokollierbarkeit der Aktivitäten und Funde einer Quellen-TKÜ/OD auf einem infiltrierten Zielsystem. Die technischen Grundvoraussetzungen für verlässliches Logging und Signierung sind auf einem fremden System nicht gegeben. Eine detaillierte Dokumentation jedes Zugriffs, mindestens in Form von kompletter Quellcodevorlage und -Auditierung, ist ebenso nötig wie die rechtliche Eingrenzung auf bestimmte Zielsystemarten.

- Die heimliche Installation einer Quellen-TKÜ/OD-Software verlangt die Nutzung von Sicherheitslücken. Die dadurch entstehenden Anreize für Dritte, Sicherheitslücken nicht mehr zu melden, sondern zu verkaufen oder derartige Dienste anzubieten, schadet der allgemeinen IT-Sicherheit weltweit. Das greift langfristig die Grundlagen der vernetzten Gesellschaft an und korrodiert die digitale Infrastruktur. Zusätzlich vertreiben diese Dritten die gleichen Sicherheitslücken üblicherweise auch an Diktaturen weltweit, die damit ihre BürgerInnen kontrollieren, DissidentInnen sowie MenschenrechtsverteidigerInnen ausspähen und verfolgen. Um auf eine sichere und menschenfreundliche IT-Landschaft hinzuwirken, dürfen keine Sicherheitslücken verwendet, gehandelt oder zurückgehalten werden – insbesondere keine bislang unbekannten Lücken.

- Die These eines „Blindwerdens von Behörden“ durch Kryptographienutzung (*Going dark*) lässt sich nicht erhärten, physische Interaktionen von Kriminellen und allgemeine Effekte der Digitalisierung bieten nach wie vor hinreichende Ansatzpunkte für eine effektive Gefahrenabwehr.

- Der Verfassungsschutz ist ein Geheimdienst und per Definition ungleich intransparenter und schwerer demokratisch zu kontrollieren als etwa Polizeien. Derartig eingriffstiefe und folgenschwere Ermächtigungen wie § 6 und § 8 dürfen ihm demnach grundsätzlich nicht erteilt werden.

In der Konsequenz raten wir nachdrücklich dazu, die Paragraphen § 6 (Quellen-TKÜ) und § 8 (Online-Durchsuchung) ersatzlos zu streichen.

Material

FIfF-Sachverständigenauskunft, (PDF, 19 Seiten) https://www.fiff.de/presse/pressemitteilungen/FIfF_Stellungnahme_HVSG_Hessentrojaner.pdf

Gesetzentwurf zum Hessischen Verfassungsschutzgesetz, Drucksache 19/5412 (PDF, 57 Seiten)
http://starweb.hessen.de/cache/DRS/19/2/05412.pdf

Webseite der öffentlichen Anhörung im Innenausschuss
https://hessischer-landtag.de/node/2490

Webseite des kritischen Projekts Hessentrojaner (wir sind Unterstützer)
https://www.hessentrojaner.de

Abendveranstaltung bzw. Morgenkundgebung am 7.2. bzw. 8.2.2018
https://www.hessentrojaner.de/aufruf/

FIfF-Pressemitteilung zum Trojanereinsatz laut Strafprozessordnung (StPO)
https://www.fiff.de/presse/pressemitteilungen/entfesselter-trojaner-grosse-koalition-verhoehnt-it-sicherheit-und-demokratie

Referenzen

1 *https://netzpolitik.org/2015/strategische-initiative-technik-wir-enthuellen-wie-der-bnd-fuer-300-millionen-euro-seine-technik-aufruesten-will/*
2 *http://www.spiegel.de/politik/deutschland/bundeswehr-ursula-von-der-leyen-ruestet-an-der-cyber-front-auf-a-1042985.html*
3 *https://www.dfki.de/web/forschung/projekte?pid=945*
4 *https://www.heise.de/newsticker/meldung/WannaCry-Angriff-mit-Ransomware-legt-weltweit-Zehntausende-Rechner-lahm-3713235.html*
5 *https://netzpolitik.org/2017/geheimes-dokument-das-bka-will-schon-dieses-jahr-messenger-apps-wie-whatsapp-hacken/*
6 *https://netzpolitik.org/2014/gamma-finfisher-ueberwachungstechnologie-made-in-germany-gegen-arabischen-fruehling-in-bahrain-eingesetzt/*
7 *https://netzpolitik.org/2012/gamma-finfisher-neue-analyse-des-staatstrojaners-deutet-auf-weitere-kunden-hin/*
8 *https://netzpolitik.org/2014/gamma-finfisher-gehackt-werbe-videos-von-exploits-und-quelltext-von-finfly-web-veroeffentlicht/*
9 *https://www.wired.com/story/vulnerability-equity-process-charter-transparency-concerns/*
10 *https://www.amnesty.org/en/get-involved/take-action/free-ahmed-mansoor/*
11 *https://www.blaetter.de/archiv/jahrgaenge/2018/januar/von-aufklaerung-keine-spur-20-jahre-nsu-komplex*
12 *https://netzpolitik.org/2016/bundeskriminalamt-knackt-telegram-accounts/*
13 *https://www.washingtonpost.com/world/national-security/comey-defends-fbis-purchase-of-iphone-hacking-tool/2016/05/11/ce7eae54-1616-11e6-924d-838753295f9a_story.html*
14 *https://www.rbb24.de/politik/beitrag/2017/10/amri-von-v-mann-angestachelt-anschlag-berlin-breitscheidplatz.html*

Anna Biselli, netzpolitik.org

25 Experten lassen kaum ein gutes Haar an hessischem Geheimdienstgesetz

„Völlig unerträglich", „glasklar nicht in Übereinstimmung mit dem Bundesverfassungsgericht": So lauteten nur zwei der Bewertungen von 25 Sachverständigen im hessischen Landtag zu den Reformplänen für den Verfassungsschutz, bei denen es vom V-Leute-Einsatz bis zum Staatstrojanereinsatz viel zu besprechen gab.

Fünfundzwanzig Sachverständige bewerteten gestern vor dem hessischen Parlament in Wiesbaden einen Gesetzesentwurf[1]: das *Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen*. Es gab einiges zu besprechen: von Staatstrojanern für die Landesgeheimdienstler über die parlamentarische Kontrolle bis hin zum Einsatz von V-Leuten, bei denen künftig über Straftaten hinweggesehen werden soll.

Einmal da, werden die Begehrlichkeiten geweckt: Verfassungsschutz in Hessen soll Staatstrojaner bekommen. CC-BY 2.0 Pascal Maramis

Besonders, dass der hessische Verfassungsschutz nach dem Willen der schwarz-grünen Landesregierung in Zukunft Staatstrojaner einsetzen sollen darf, sorgte schon im Vorfeld für Kritik: Sowohl von Datenschützern und Grundrechtsaktivisten als auch aus den eigenen Reihen[2] der Grünen – die Basis hatte sich gegen den Entwurf ausgesprochen[3]. Und die bereits veröffentlichten Stellungnahmen[4] der Sachverständigen deuteten auch auf deutlich mehr Kritik als Lob hin.

Die Sachverständigen-Anhörung begann ohne viele einleitende Worte – von einer Warnung vor krawattenabschneidenden Frauen an Weiberfastnacht abgesehen – und war am Beginn vornehmlich den Juristen vorbehalten. Bei der großen Menge der Sachverständigen mahnte ein überaus resoluter Innenausschussvorsitzender, Horst Klee von der CDU, eingangs nur zur „höchsten Disziplin". Man habe sämtliche schriftliche Gutachten bereits gelesen, daher mögen sich die Experten doch knapp an den wichtigsten Punkten orientieren.

Quellen-TKÜ: schwierig, vielleicht sogar unmöglich

So stieg Jan Dirk Roggenkamp von der Hochschule für Wirtschaft und Recht Berlin gleich mit Trojaner-Problemen ein, die er bei der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) sieht. Dieser Trojaner soll nur laufende Kommunikation abhören dürfen. Er begrüßte zwar, dass eine rückwirkende Erhebung von beispielsweise Chatverläufen bei einer Quellen-TKÜ nicht zulässig sein soll. Er betonte jedoch, er glaube nicht daran, dass es überhaupt möglich sei, eine Software zu erschaffen, die nur die laufende Kommunikation abgreifen könne.

Die Software müsse unter Offenlegung des Quellcodes zertifiziert werden, so Roggenkamp. Als mögliche Zertifizierungsstelle fiel den Co-Sachverständigen Peter Löwenstein, einem IT-Unternehmer, und Hannes Federrath von der Gesellschaft für Informatik (GI) jedoch später auf Anhieb keine geeignete ein. „Mit sehr weitem Blick" könne er das beim Bundesamt für Sicherheit in der Informationstechnik vermuten, so Löwenstein.

Unsere Mitautorin Constanze Kurz, die ebenfalls als Sachverständige geladen war, hielt wie Roggenkamp eine Reduktion des Trojaners auf ausschließlich laufende Kommunikation für technisch aussichtslos. Sie führte aus, dass es in der Vergangenheit für die Quellen-Telekommunikationsüberwachung keine rechtmäßige Spionagesoftware gegeben habe, die wirklich nur das Erlaubte ausleiten könne. Rainer Rehak vom Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) hielt das ebenso für sehr schwierig, vielleicht sogar unmöglich.

Ob der Quellen-TKÜ-Trojaner nur das tut, was er darf, ist nicht nur schwer umzusetzen, es ist auch schwer zu kontrollieren. Die vorgesehenen Kontrollinstanzen wie das Amtsgericht Wiesbaden und die parlamentarische Kontrollkommission hätten keine Möglichkeit, das ernsthaft vorab einzuschätzen, so Kurz. Es sei im Gesetz nicht vorgesehen, den Quellcode zu hinterlegen, und sie kenne auch keine kommerzielle Firma, die solche Software entwickelt und sich darauf einlassen würde, ihren Quellcode an den Geheimdienst zu übergeben. Als Alternative bleibe nur eine Eigenentwicklung der Behörde.

Zu weiter Kreis möglicher Zielpersonen

Es fehle eine Eingrenzung, welche Maßnahmen unzulässig seien, um den Staatstrojaner auf die Geräte der Zielpersonen zu bringen, so Roggenkamp weiter. Darüber hinaus sollte der Zweck der Online-Durchsuchung klarer gefasst werden, also der Trojaner, der das gesamte System ausspionieren dürfe. Er verwies auf das Bundesverfassungsgericht, das geurteilt hatte, es müsse ein „überragend wichtiges Rechtsgut" betroffen sein, um heimlich informationstechnische Systeme zu infiltrieren. Zudem sei der Kreis möglicher Zielpersonen im Gesetzesentwurf zu weit gefasst.

Gerrit Hornung von der Universität Kassel formulierte seine Kritik härter, die geplanten Regelungen zum Staatstrojaner stünden „glasklar nicht in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts". Neben Roggenkamps Kritik, die er bestätigte, wies er auf die Ausnahme vom Richtervorbehalt bei Eilfällen hin – in Anbetracht des sowieso existierenden technischen Vorlaufs seien solche Eilfälle nicht plausibel. Hornung

regte schließlich gegenüber den Abgeordneten an, über einen vollständigen Verzicht auf die Online-Durchsuchung für den Verfassungsschutz nachzudenken.

Ein weiteres Argument gegen den Staatstrojanereinsatz besteht nicht nur in der möglichen Verletzung der Privat- oder Intimsphäre der Betroffenen, sondern in der Gefährdung aller, indem Sicherheitslücken offenbleiben, damit die Geheimdienstler diese gegen ihre Ziele ausnutzen können.

Gefahren durch Staatstrojaner

Hannes Federrath sieht den Staat in der Pflicht, Anreize „für die Meldung und Veröffentlichung von Sicherheitslücken zu schaffen". Durch Staatstrojaner geschehe das Gegenteil, was der „Fürsorgepflicht des Staates bei Kritischen Infrastrukturen" zuwiderlaufe. Auch beispielsweise Ampelanlagen, Energieversorger und andere wichtige Systeme seien durch offengehaltene Lücken verwundbar.

Manchmal müssen Angreifer die bewusst offengelassenen Lücken nicht einmal selbst suchen, manchmal finden sie gleich den fertigen Trojaner: Constanze Kurz berichtete von Spionagesoftware, die „befreundeten Geheimdiensten" in der Vergangenheit bereits entschwunden[5] ist und von gehackten Firmen, die Spionagesoftware herstellen. Diese Risiken habe der Gesetzgeber in keiner Weise betrachtet. Die Schäden, die dadurch entstehen können, wenn die Software in andere Hände gerät, seien „sehr viel größer, die Risiken insgesamt sehr viel höher als der Nutzen". Sie glaube auch nicht, dass der hessische Verfassungsschutz besser in der Lage sei, seine Software zu schützen als andere Geheimdienste – wie etwa die NSA.

Rainer Rehak brachte die Gefahr durch Staatstrojaner auf den Punkt: „Es ist weniger eine Abwägung von Freiheit oder Privatsphäre gegen Sicherheit, sondern von Sicherheit gegen Sicherheit: die Sicherheit in Einzelfällen gegen die Sicherheit aller Menschen in Deutschland". Rehak appellierte speziell an die regierungsbeteiligten Grünen: „Es geht auch um eine intakte digitale Umwelt. Wir brauchen Luft zum Atmen."

Substantielle Argumente *für* den Verfassungsschutz-Trojaner brachte keiner der Angehörten explizit vor. Andreas Grün von der Gewerkschaft der Polizei Hessen merkte jedoch positiv an, durch doppelten Richtervorbehalt gebe es eine engere Kontrolle, die für mehr Akzeptanz sorgen werde. Dirk Peglow vom Bund Deutscher Kriminalbeamter Landesverband Hessen plädierte ganz allgemein dafür, „dringend" den Verfassungsschutz „mit den notwendigen Instrumentarien" auszustatten, damit er auf Bedrohungen reagieren könne.

Parlamentarische Kontrolle

Bedenken vieler Sachverständiger zogen überdies die Regelungen zur Geheimdienstkontrolle auf sich. Ein einhellig geäußerter Kritikpunkt an den parlamentarischen Kontrollbefugnissen waren die begrenzten Möglichkeiten der Oppositionsfraktionen, denn in der hessischen Kontrollkommission sind nicht einmal alle fünf Parteien des Landtags vertreten. Mehrere Sachverständige forderten daher, die Opposition in jedem Fall an dem Kontrollgremium zu beteiligen. „Regierungstragende Fraktionen werden immer dazu tendieren, die Regierung nicht besonders scharf zu kontrollieren", so Hornung.

Weitere Vorschläge aus den Reihen der Sachkundigen bestanden darin, Sondervoten zuzulassen, um auch einer parlamentarischen Minderheit eine Stimme zu geben. Zudem sei es wichtig, den Verfassungsschutz zur Aktenherausgabe zu verpflichten und es nicht beim Recht auf Akteneinsicht zu belassen.

Es sei außerdem nötig, dass Geheimdienst-Beschäftigte direkt mit den Kontrollgremiumsmitgliedern sprechen können, sowohl aus eigener Initiative als auch wenn Abgeordnete Fragen an sie hätten, so Hornung. Kilian Vieth von der Stiftung Neue Verantwortung[6] bekräftigte dies, es müsse auch außerhalb des offiziellen Dienstwegs möglich sein, sich an die Kontrollgremien zu wenden. Er brachte außerdem den Mangel an technischer Kompetenz und Ressourcen in Kontrollgremien an, die besser ausgestattet werden sollten. Denn, so Vieth, „Kontrolle ist kein Selbstzweck", sie trage dazu bei, „dass der Verfassungsschutz effektiv und so fehlerfrei wie möglich operiert".

Die Sachverständigen stießen sich noch an einer weiteren Regelung im Gesetzesentwurf, die mit der Kontrolle der Geheimdienste und der Polizeien in Zusammenhang steht: Was sollen V-Leute und verdeckte Ermittler künftig dürfen?

Straffreie Räume bei V-Leuten

Die Diskussion um den Einsatz von V-Personen ist eng geknüpft an die Rolle Hessens im NSU-Komplex und die Mitwirkung hessischer V-Leute und V-Leute-Führer am Mord an Halit Yozgat[7] im Jahr 2006. Alexander Kienzle, Anwalt der Familie von Halit

Anna Biselli

Anna Biselli kommt aus der Informatik und hat gemerkt, dass sie der politische Kontext nicht loslässt. Deshalb hat sie erst einmal bei netzpolitik.org Praktikum gemacht, um dann dabeizubleiben. Am liebsten beschäftigt sie sich mit Datenschutz und spielt den Technik-Erklärbär. Man erreicht Anna per Telefon unter *+49-30-92105-984* oder unter *anna@netzpolitik.org* – am liebsten *verschlüsselt* [325C 6992 DCD3 1167 D9FA 9A57 1873 5033 A249 AE26]

Yozgat, attestierte dem hessischen Gesetzgeber: Es gebe keine wirksame Beschränkung bekannter Probleme durch den Gesetzesentwurf. Stattdessen normiere er „hochproblematische Dinge". Die Einflussnahme auf V-Leute sei nicht nur weiterhin zulässig, sie dürften sich auch an Straftaten beteiligen. Anstatt „straffreie Räume" im Umfeld des Verfassungsschutzes zu beseitigen, schaffe der Gesetzesentwurf genau das Gegenteil, so Kienzle. Der Gutachter Rolf Gössner von der Internationalen Liga für Menschenrechte pflichtete ihm bei und fügte in Bezug auf den NSU hinzu, damit werde „praktisch der Skandal verrechtlicht".

Ralf Poscher von der Universität Freiburg formulierte seine Bedenken bei der Straffreiheit elegant als „große Zweifel an der Weisheit der Pauschalität bei der Straffreistellung" und zählte einige Beispiele auf. Zu den straffreien Taten von V-Leuten würden nach dem Gesetzesentwurf sowohl Meineid als auch Urkundenfälschung und – ganz drastisch – der Handel mit Massenvernichtungswaffen zählen.

Dirk Peglow vom Bund Deutscher Kriminalbeamter Landesverband Hessen entgegnete, es sei einfach „illusorisch", dass man in diesem Bereich Menschen finde, „die aus dem Mädchenpensionat kommen". Man brauche eben Personen, die im kriminellen und auch im terroristischen Bereich unterwegs seien. Die Kollegen würden aber auf den Umgang mit diesen Menschen hin geschult.

Ein „Gesetzentwurf vieler verpasster Chancen", lautete hingegen Kienzles ernüchterndes Resümee. „Aus rechtsstaatlicher Sicht völlig unerträglich", nannte Till Müller-Heidelberg von der Humanistischen Union die Strafbarkeitslücke bei der V-Personen-Regelung.

Eine neue Extremismusklausel?

Unerträglich fanden den Gesetzesentwurf auch die geladenen sachverständigen Vertreter von Organisationen, die sich in Hessen für Demokratieförderung und gegen Fremdenhass einsetzen. Sämtliche Gutachter störte vor allem eine Art Gesinnungsklausel, die mit faktischen Berufsverboten einhergehe und für manche der Organisationen existenzbedrohend ist.

Vertreterinnen und Vertreter der verschiedenen zivilgesellschaftlichen Organisationen, etwa der Bildungsstätte Anne Frank oder dem Mobilen Beratungsteam gegen Rechtsextremismus und Rassismus (MTB), sprachen sich gegen Überprüfungen von Personen aus, die bei mit Landesmitteln geförderten Beratungsstellen und Projekten arbeiten. Dies sei, auch wenn es auf Einzelfälle beschränkt würde, ein „schwerer Eingriff in die Autonomie der Träger", so Kirsten Neumann vom MTB. Eine neue Extremismusklausel[8] sei abzulehnen, sagte Benedikt Widmaier vom Haus am Maiberg. Auch Reiner Jäkel vom Hessischen Jugendring sah das so.

Meron Mendel von der Bildungsstätte Anne Frank hatte bei seinen Sorgen die AfD im Hinterkopf. Ein solches Gesetz könne von Rechtspopulisten und Antisemiten als Einladung missverstanden werden und Träger durch Denunziation in ständigen Rechtfertigungszwang bringen. Er berichtete von einem Fall in seiner Bildungsstätte, bei dem eine Mitarbeiterin unter Verdacht geriet, weil sie auf einem Podium saß, auf dem auch eine vom Verfassungsschutz beobachtete Person saß. Ein anderes Beispiel betraf Mitarbeiter einer Salafismus-Beratungsstelle[9], die der Verfassungsschutz als potentielle Mitglieder der islamistischen Szene beobachtete. Das hessische Innenministerium wies zunächst an, sie zu suspendieren – erst zehn Monate später verkündete das Ministerium, es hätten sich doch „keine tatsächlichen Anhaltspunkte für extremistische Bestrebungen" ergeben.

Quo vadis?

Das Obige ist nur ein kleiner Ausschnitt der Kritik und Kommentare, die Vertreter unterschiedlicher Organisationen und Universitäten in der mehr als fünfstündigen Sitzung vortrugen. Wenn die Parlamentarier die Anhörung ernstnehmen, müssen sie nun an zahlreichen Punkten und in so gut wie allen Paragraphen des Entwurfs und weiterer damit verbundener Gesetze nachbessern.

Konflikte muss dabei vor allem die Grünen-Fraktion lösen, die den Spagat zwischen der mitregierenden CDU und der eigenen Parteibasis bewältigen muss, gerade in Anbetracht der bevorstehenden Landtagswahl im Oktober. Von Grünen-Mitgliedern gab es vor allem zu den Staatstrojanerplänen harsche Kritik – immerhin versprachen sie den Wählern vor der letzten Wahl noch, keine Staatstrojaner bei der Gefahrenabwehr zuzulassen.

NETZPOLITIK.ORG

Der Beitrag erschien zunächst bei netzpolitik.org (https://netzpolitik.org/2018/25-experten-lassen-kaum-ein-gutes-haar-an-hessischem-geheimdienstgesetz/). Wir danken für die freundliche Genehmigung zum Wiederabdruck.

Referenzen

1 *https://netzpolitik.org/2017/schwarz-gruen-in-hessen-will-staatstrojaner-fuer-verfassungsschutz/*
2 *https://netzpolitik.org/2017/streit-um-geplantes-hessentrojaner-gesetz-bei-den-gruenen/*
3 *https://netzpolitik.org/2017/spagat-fuer-die-gruene-landtagsfraktion-parteibasis-lehnt-hessentrojaner-ab/*
4 *https://netzpolitik.org/2018/breitseite-gegen-staatstrojaner-in-hessen-verfassungswidrig-und-gefaehrlich/*
5 *https://netzpolitik.org/2017/schattenmakler-hacking-werkzeuge-der-nsa-in-freier-wildbahn/*
6 *https://www.stiftung-nv.de/de/publikation/stellungnahme-zum-gesetzentwurf-zur-neuausrichtung-des-verfassungsschutzes-hessen*
7 *http://www.fr.de/politik/rechtsextremismus/hessen-rolle-des-v-manns-ungeklaert-a-1246546*
8 *http://www.fr.de/rhein-main/landespolitik/verfassungsschutz-in-hessen-protest-gegen-extremismusklausel-a-1401897,0*
9 *http://www.hessenschau.de/gesellschaft/mitarbeiter-von-salafismus-beratungsstelle-entlastet,beratungsstelle-vpn-100.html*

Jürgen Altmann und Dietrich Meyer-Ebrecht

Angriff und Verteidigung in der *Ära des Cyberkriegs*

Abendveranstaltung von W&F und BICC, 26. Januar 2018, Bonn

Die zunehmende Bedeutung des Cyberraums als *fünftem Kriegsschauplatz* war das Thema einer öffentlichen Diskussionsveranstaltung, die die Zeitschrift *Wissenschaft und Frieden* auf ihrer Jahrestagung in Zusammenarbeit mit dem Internationalen Konversionszentrum Bonn (BICC) am 26. Januar 2018 in Bonn ausrichtete. Der etwas sperrige Titel des Abends: *Ambivalenzen zwischen Angriff und Verteidigung in der ‚Ära des Cyberkriegs' – Theorie und Praxis der digitalen Strategie der Bundeswehr*. Der Anlass, dieses Thema zu wählen, war die Brisanz einer nun schon etwas zurückliegenden Nachricht, dass die Bundeswehr (Bw) eine eigenständige Einheit für Operationen im digitalen Raum, dem Cyber- und Informationsraum, in der Bundeswehrsprache kurz CIR, aufbaut. Auf dem Podium diskutierten Prof. Dr. Hans-Jörg Kreowski, Informatiker, Universität Bremen, Vorstandsmitglied des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF), Generalmajor Michael Vetter, Erster Stellvertretender Inspekteur und Chef des Stabes des Kommandos Cyber- und Informationsraum (CIR) in Bonn, und Prof. Dr. Matthew Smith, Informatiker, Universität Bonn und Fraunhofer Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKI), Wachtberg. Die Podiums- und anschließende Plenumsdiskussion moderierte Prof. Dr. Hartwig Hummel, Universität Düsseldorf, Vorstandsmitglied des Arbeitskreises Friedens- und Konfliktforschung (AFK) und von W&F. Das Podium widmete sich verschiedenen Aspekten des militärischen Engagements im Cyber- und Informationsraum und seinen Auswirkungen.

Prof. Kreowski stellte zunächst einige Fakten zusammen. Der neue Organisationsbereich *Cyber- und Informationsraum* (CIR) der Bundeswehr befindet sich mit rund 13.500 Dienstposten seit 2016 im Aufbau, die offizielle Indienststellung war im April 2017. Überwiegend werden vorhandene Abteilungen unter einem Dach zusammengeführt, die neben Heer, Marine und Luftwaffe eine neue Teilstreitkraft bilden. Unterstützt wird dieser Prozess durch massive Nachwuchswerbung und mit der Einrichtung eines Master-Studiengangs IT-Sicherheit an der Bundeswehr-Universität München.

Neben defensiven Aufgaben wird die neue Teilstreitkraft auch offensive Aufgaben haben und sich am weltweiten Cyberkriegswettrüsten (bei dem es vorwiegend um eine Stärkung der offensiven Fähigkeiten geht) beteiligen. Kreowski stellt die Frage, wie sich das mit dem Verteidigungsauftrag der Bundeswehr verträgt. Ebenso sei fraglich, ob die Vermischung militärischer Cyberverteidigung mit ziviler Cyberabwehr verfassungsgemäß ist. Denn Cyberangriffe, die geheim gehaltene Sicherheitslücken und Schwachstellen nutzen, erfordern ganz andere Kompetenzen als eine Cyberverteidigung, bei der es darum geht, vor allem zum Schutz der Zivilgesellschaft Sicherheitslücken zu schließen und Schwachstellen zu beheben. Um im *Darknet* Know-how über Eingriffsmöglichkeiten, wie z. B. *Zero-Day-Exploits*, anzukaufen, erhielte die neue Teilstreitkraft ein dreistelliges Millionenbudget (was vom nachfolgenden Redner bestritten wurde). In kontraproduktiver Weise würde dieses Wissen der zivilen Datenverarbeitung vorenthalten.

Kreowski sieht im Aufbau eines Cyberwaffenarsenals eine erhöhte Kriegsgefahr, denn angreifen ist einfacher als verteidigen, die Mittel sind vergleichsweise billig (und wiederverwendbar!). So schwinden die Hemmschwellen, und die Eskalation durch konventionelle Vergeltungsschläge auf Cyberangriffe macht deren Folgen unkalkulierbar. Die vorhersehbare Ausweitung von Kriegen in den digitalen Raum, stellte Kreowski fest, ist völkerrechtswidrig, denn aufgrund der hohen Verletzlichkeit ziviler Infrastrukturen stellt sie in erster Linie eine Bedrohung der Zivilgesellschaft dar.

Dies alles sind Gründe, warum das FIfF mit seiner Kampagne *Cyberpeace statt Cyberwar* die Ächtung jeglicher Form von Cyberwaffen, zumindest jedoch der offensiven, fordert. Das Internet müsse entmilitarisiert werden und allein dem Frieden dienen, anstatt für Ausspähung und militärische Operationen missbraucht zu werden. Konsequent wäre es, eine *Digitale Genfer Konvention* zu schaffen, die Cyberangriffe auf lebenswichtige zivile Infrastrukturen verbietet. Weitere Forderungen der Kampagne sind ein Verbot des Einsatzes konventioneller Waffen als Antwort auf Cyberattacken, international transparente forensische Untersuchungen angeblicher Cyberkriegsangriffe, die Offenlegung und Beseitigung aller Schwachstellen (statt sie für eigene Angriffe zu nutzen) sowie die Sicherung kritischer Infrastrukturen (z. B. durch Entnetzung und Dezentralisierung).

Kreowskis provozierende Fragen stehen im Raum – sie bleiben auch unbeantwortet im Raum stehen, als Generalmajor Vetter das Podium übernimmt und die Perspektive der Bundeswehr einbringt. Vetter spricht über die Digitalisierung im Bereich der Streitkräfte, über die neuen Optionen und auch über die neuen Verwundbarkeiten. Er berichtet über den Aufbau der Cyberstreitkräfte als Segment der nationalen Cybersicherheitsstrategie 2016 der Bundesregierung. Federführend für letztere ist der Bundesminister für Inneres, während die Umsetzung schwerpunktmäßig in den Händen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), des Bundeskriminalamtes (BKA) und des Bundesamtes für Verfassungsschutz (BfV) liegt. Die Cyber-Verteidigung obliegt dagegen der Bundeswehr. Geht es um mandatierte Einsätze, ist Cyber-Außenpolitik gefordert. Entsprechend liegt die Verantwortung beim Auswärtigen Amt. Eine völlig neue Herausforderung sei die fehlende Symmetrie zwischen digitaler und materieller Welt. Denn mit vergleichsweise wenig (Software-) Aufwand kann ein immenser materieller Schaden verursacht werden. Abzusehen ist, dass es den „klassischen" Krieg nicht mehr geben wird. Ob ein Krieg als physikalischer beginnt oder als digitaler, in beiden Fällen wird die jeweils andere Komponente alsbald dazukommen und den Krieg zu einem hybriden machen.

Hierauf muss die Bundeswehr vorbereitet sein, betont Vetter. Sie hat jetzt alle diesbezüglichen Aktivitäten in einer Abteilung, dem Kommando CIR mit derzeit 13.500 SoldatInnen und zivilen Angestellten, gebündelt. Das Kommando soll auf knapp 15.000 Personen wachsen. Zuständig ist das Kommando für den Schutz

der bundeswehreigenen IT-Systeme sowie der Satelliten-, Richtfunk- und terrestrischen Kommunikations-Infrastrukturen. Dazu betreibt es ein *Cyber Security Operations Center*, ähnlich wie die Telekom; es stellt mobile Einsatzgruppen (CERT) und beschäftigt Cyber-Forensiker. Weiterhin ist das CIR zuständig für das militärische Nachrichtenwesen. Dazu gehören die Aufklärung über Aktivitäten der Streitkräfte anderer Staaten, eine Krisenfrüherkennung, die Bereitstellung von 3D-Geo-Information sowie von Wetter- und Klimadaten. Viele dieser Aufgaben sind die bisherigen, neu ist jedoch, dass alle diese Aktivitäten – auf Anforderung verschiedener ziviler Behörden – in den Rahmen einer gesamtstaatlichen Cybersicherheit eingeordnet sind.

So werden mit Tornados und über Satelliten, kommerziellen wie militärischen, schon seit Längerem Funknetze überwacht. Zuständig dafür war und ist die Truppe für Elektronische Kampfführung (EloKa), jetzt Teil des Kommandos CIR. Zu ihren Aufgaben gehören auch Maßnahmen des Informationskrieges, wie die Beeinflussung der Zivilbevölkerung durch aufbereitete Nachrichten, unterstützt mit Narrativen, die Gegenpositionen beispielsweise zu Taliban- und IS-Narrativen vermitteln. Neu hinzu kommen Fähigkeiten, in gegnerische Netze eindringen zu können, nicht nur zur Aufklärung, sondern auch, um für operative Maßnahmen manipulierend eingreifen zu können. Vetter nennt Beispiele wie die Verhinderung des Auslösens von Sprengfallen per Mobilfunk durch mitgeführte Störsender oder durch gezielte Lahmlegung lokaler Mobilfunknetze. Dies entspräche dem klassischen Kriegsziel, die Luftabwehr auszuschalten (so geschehen z. B. in Serbien), indem Führungs- und Gefechtssysteme gehackt werden.

Solche Angriffe, so betont Vetter (um wenigstens diesen Punkt des Vorredners aufzugreifen), würden streng regelbasiert erfolgen. Für offensive Cyber-Einsätze würden dieselben rechtlichen Voraussetzungen gelten wie für kinetische Angriffe. Für Cyber-Einsätze zur Unterstützung konventioneller Verteidigung und Angriffe (wie z. B. in Afghanistan) werde grundsätzlich ein Mandat des Bundestages vorausgesetzt. Das Grundgesetz sei die eherne Grundlage. Auch würden bei derartigen Einsätzen, wie z. B. dem Blockieren eines Funknetzes, immer Rechtsberater hinzugezogen. Wegen möglicher weitreichender Kollateralschäden würde die rechtliche Prüfung sogar rigoroser ausfallen als bei kinetischen Angriffen. Ein grundsätzliches Problem dabei sei, dass bei Cyberangriffen extrem schnell gehandelt werden muss. Zu diesem Zweck laufen aus allen beteiligten Organisationen – BSI, BKA, BfV und Bw – Informationen über Angriffe in einem 2011 gegründeten Nationalen Cyberabwehrzentrum zusammen. Angestrebt wird, einen gemeinsamen Gefechtsstand für alle diese Organisationen zu schaffen. Die Bundeswehr würde auch im zivilen Bereich tätig werden, zwar nicht initiativ, aber auf Anforderung, wenn beispielsweise Kraftwerke nach einem großflächigen Ausfall wieder ans Netz angeschaltet werden müssen und die zivilen Kräfte dafür nicht ausreichen würden.

Zum besseren Verständnis der Materie liefert Prof. Smith in groben Zügen die technischen Fakten nach, die offensiven Cyberoperationen zugrunde liegen. Ausschlaggebend ist, dass zivile und militärische Informationssysteme unterschiedslos dieselben Hardware- und Softwarekonzepte und teils sogar dieselben Programmsysteme nutzen. Insofern sei eine Grenzziehung zwischen zivilen und militärischen Fragestellungen kaum möglich. Der Weg, nichtautorisiert in fremde Computer und IT-Netze einzudringen, führt über das Ausnutzen von Schwachstellen. Entstehen können sie durch Fehler in Soft- oder Hardware, durch Fehlkonfiguration von Programmen oder unbedacht im Zusammenspiel von Programmbausteinen – unvermeidbar bei der Komplexität heutiger Hardware und Software und der Vielzahl der beteiligten Entwickler. Schwachstellen und geheime Hintertüren können sogar absichtlich eingebaut oder nachträglich eingeschleust werden.

Smith erläutert, was ein so genannter *Exploit* ist – ein Softwarewerkzeug zur Ausnutzung einer Schwachstelle – und insbesondere ein *Zero-Day-Exploit*. Das ist ein Exploit, der eingesetzt wird, bevor die Schwachstelle aufgedeckt wird und damit erst die Chance zur Entwicklung eines Sicherheits-Updates geboten wird. Der Angreifer kann sich in der Zwischenzeit bereits unentdeckbar eingenistet haben und seine Herrschaft über das System weiter ausbauen. An Exploits arbeiten außer professionellen Entwicklern in militärischer oder geheimdienstlicher Mission unzählige Hacker, die ihr Wissen und ihre Entwicklungen auf einem florierenden Schwarzmarkt anbieten. Dort kann ein Zero-Day-Exploit, zugeschnitten beispielsweise auf Apples iOS, gut und gerne eine Million Euro kosten, und Entwicklungen gegen militärische Systeme können sogar noch sehr viel teurer sein. Solche hochkomplexen Cyberwaffen werfen jedoch noch ein besonderes Problem auf: Sie sind wiederverwendbar, dürfen also keinesfalls Gegnern in die Hände fallen. Sie müssen deshalb einen Selbstzerstörungsmechanismus eingebaut haben (dieser hat bei der bekannt gewordenen Schadsoftware *Stuxnet* offensichtlich nicht funktioniert). Ein eminentes Problem ist die Attribuierung, d. h. die faktische Unmöglichkeit, schnell und zuverlässig den Urheber einer Cyberattacke zu ermitteln. Ein voreiliger Gegenschlag, ausgeführt möglicherweise sogar unter Einsatz konventioneller Waffen, könnte deshalb schnell zu einer Eskalation führen oder, wenn er den Falschen träfe, ungewollt einen neuen Konflikt auslösen. Smith betont zum Abschluss noch einmal, wie vor ihm schon Kreowski, dass militärische und geheimdienstliche Aktivitäten im Cyberraum die Sicherheit ziviler Systeme schwächen, die Gesellschaft gefährden, statt zu schützen, und damit kontraproduktiv im Sinne des Auftrages unserer Bundeswehr sind. Wir müssten auch damit rechnen, dass Cyberangriffe eher zivile Systeme zum Ziel haben könnten als militärische, da letztere vermutlich aufwändiger geschützt werden. Terroristen und Kriminelle würden diese „weiche Flanke“ ohne Skrupel nutzen, wo sich Militärs aus humanitären Gründen noch zurückhalten müssten. Selbst wenn jedoch das primäre Ziel eine militärische Einrichtung wäre, wird ihr Angriff unkalkulierbare Kollateralschäden verursachen, denen wieder vorwiegend zivile Einrichtungen zum Opfer fallen würden.

Die abschließende Diskussion ist engagiert, aber wenig ergiebig hinsichtlich der Klärung der offensichtlich kontroversen Positionen. Zu offensiven Cyberwaffen der Bundeswehr will sich Vetter erwartungsgemäß nicht äußern. Er verweist darauf, dass die empfindlichste Schwachstelle der Mensch sei und deshalb eine Cyber-Awareness entwickelt werden müsse. Dass die Probleme, die militärische Aktivitäten im Cyberraum für die Zivilgesellschaft bringen, damit gelöst werden können, bezweifelt Smith. Bezüglich des Entwurfs von Völkerrechtsregeln im Cyberraum wird das Tallinn-Manual erwähnt (das Richtlinien für den Krieg aufstellt, aber keine Rüstungsbegrenzung behandelt). Vertrauensbildende Maßnahmen seien nötig und z. T. schon in Arbeit. Kreowski weist auf die wichtige Rolle der Prävention mit-

tels Technikfolgenabschätzung hin – mehr Geld sei hierfür nötig, ebenso auch für eine Rüstungskontrollforschung. Ein grundlegendes Problem sei, so Smith, dass Informationstechnologie und informatische Methoden fast unvermeidlich Dual-use-Charakter haben und dass dies zur Bildung einer ausgedehnten Grauzone in Forschung und Industrie führt.

Zu optimistisch wäre die Erwartung gewesen, dass sich die Podiumsteilnehmer in der Diskussion näher gekommen wären. Deutlich wird vielmehr, wie groß die Kluft zwischen den Positionen von Militärs und Zivilgesellschaft ist und wie wichtig es ist, dass die Zivilgesellschaft Gegenmodelle entwickelt – wie Kreowski abschließend noch einmal unterstreicht – und sich für ihre politische Durchsetzung einsetzt.

Eine Audiodatei der Veranstaltung ist verfügbar unter *https://nc.bicc.de/index.php/s/W4JfTsjDnQ4nFiv.*

Der Beitrag erschien zunächst in Wissenschaft & Frieden 1/2018. Wir danken für die freundliche Genehmigung zum Wiederabdruck.

Wissenschaft & Frieden 1/2018 „USA – eine Inventur“

Ein Jahr nach dem Amtsantritt von US-Präsident Donald Trump konzentrierte sich die Berichterstattung stark auf seine Person, seine Kapriolen, seine Tweets und seinen Gesichtsausdruck. Selbst seine geistige Zurechnungsfähigkeit wurde angezweifelt. Diese Art der Wahrnehmung seiner Präsidentschaft ist unangemessen: Sie lenkt den Blick der Öffentlichkeit noch mehr auf seine Person und lenkt damit ab von Trumps Politik und den Fakten, die er damit schafft. Gleichzeitig unterstellt sie, mit seinem Amtsantritt habe sich in den USA alles geändert.

W&F 1/2018 zeigt Kontinuitäten der US-Politik auf, u. a. in der Innen-, Außen-, Militär- und Rüstungspolitik, aber auch die Folgen der Politik unter Trump: Mehr für Rüstung und weniger für Entwicklungshilfe und Vereinte Nationen, Abschottung gegen die Migration aus dem Süden, wachsender rechter Populismus und Rassismus im Inneren der USA.

Im Einzelnen schreiben:

- *Andrew Lichterman*: Der militärisch-industrielle Komplex
- *William D. Hartung*: Mehr als eine Billion Dollar. Das Budget der USA für Militär, Rüstung und Verteidigung
- *Otfried Nassauer*: „Tailored Deterrence“. Eine Nuklearpolitik für Donald Trump
- *Simon Schulze*: Ein Jahr Präsident Trump. Mehr Rüstung, weniger Vereinte Nationen
- *Christine Ahn* und *Tae Lim*: Korea, Nordostasien und Trump
- *Joachim Guilliard*: Washingtons Nahost-Politik
- *Jürgen Wagner*: Trump oder Brexit? Ursachen und Ausprägungen des EU-Rüstungsschubs
- *Bill Fletcher jr.*: „America First“ und der rechte Populismus
- *Olaf Miemiec*: Rechter Populismus. Die Mär von der „autoritären Internationale“
- *Meztli Yoalli Rodríguez Aguilera* und *Mirna Yazmín Estrella Vega*: US-Grenzregime und Rassismus. Migration aus und durch Mexiko
- *Svenja Boberg*, *Tim Schatto-Eckrodt* und *Lena Frischlich*: Fabricated News. Der Einfluss von Fake News auf die politische Einstellung

Außerhalb des Schwerpunktes geht es um

- das Völkerrecht versus Atomwaffen (*Bernd Hahnfeld*)
- Martin Luther King als Gegner des Vietnamkrieges (*Karlheinz Lipp*)
- den Weg der badischen Kirche zur Kirche des Gerechten Friedens (*Theodor Ziegler*) sowie
- Putins Wiederwahl und die Verantwortung des Westens (*August Pradetto*)

Unter dem Titel *Deutsche Waffen, deutsches Geld – morden mit in aller Welt*, beleuchtet die kommentierte Presseschau den Einsatz deutscher Panzer im Krieg der Türkei gegen die Kurden und Syrien.

Wissenschaft & Frieden, 1/2018: „USA – Eine Inventur“, 9,00 € Inland, EU plus 3,00 € Porto.

W&F erscheint vierteljährlich. Jahresabo 35 €, ermäßigt 25 €, Ausland 45 €, ermäßigt 35 €, 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.

Bitte um Vorkasse: Sparkasse KölnBonn
DE86 3705 0198 0048 0007 72, SWIFT-BIC: COLSDE33XXX

Bezug: W&F c/o BdWi-Service, Gisselberger Str. 7, 35037 Marburg,
E-Mail: *vertrieb@wissenschaft-und-frieden.de*,
www.wissenschaft-und-frieden.de

Aufruf

Abrüsten statt Aufrüsten

Die Bundesregierung plant, die Rüstungsausgaben nahezu zu verdoppeln, auf zwei Prozent der deutschen Wirtschaftsleistung (BIP). So wurde es in der NATO vereinbart.

Zwei Prozent, das sind mindestens weitere 30 Milliarden Euro, die im zivilen Bereich fehlen, so bei Schulen und Kitas, sozialem Wohnungsbau, Krankenhäusern, öffentlichem Nahverkehr, Kommunaler Infrastruktur, Alterssicherung, ökologischem Umbau, Klimagerechtigkeit und internationaler Hilfe zur Selbsthilfe.

Auch sicherheitspolitisch bringt eine Debatte nichts, die zusätzlich Unsummen für die militärische Aufrüstung fordert. Stattdessen brauchen wir mehr Mittel für Konfliktprävention als Hauptziel der Außen- und Entwicklungspolitik.

Militär löst keine Probleme. Schluss damit. Eine andere Politik muss her.

Damit wollen wir anfangen: Militärische Aufrüstung stoppen, Spannungen abbauen, gegenseitiges Vertrauen aufbauen, Perspektiven für Entwicklung und soziale Sicherheit schaffen, Entspannungspolitik auch mit Russland, verhandeln und abrüsten.

Diese Einsichten werden wir überall in unserer Gesellschaft verbreiten. Damit wollen wir helfen, einen neuen Kalten Krieg abzuwenden.

Keine Erhöhung der Rüstungsausgaben – Abrüsten ist das Gebot der Stunde.

Erstunterzeichner*innen

Franz Alt, Schriftsteller | **Dr. Wolfgang Biermann**, Politikwissenschaftler, Initiative neue Entspannungspolitik JETZT! | **Dieter Maschine Birr**, (Ex Puhdys), Musiker | **Roland Blach**, DFG-VK, Kampagne „Büchel ist überall! atomwaffenfrei.jetzt“ | **Prof. Dr. Ulrich Brand**, Politikwissenschaftler, Institut Solidarische Moderne | **Prof. Dr. Peter Brandt**, Historiker, Initiative Neue Entspannungspolitik JETZT! | **Reiner Braun**, Präsident International Peace Bureau (IPB) | **Frank Bsirske**, Vorsitzender von ver.di | **Christine Buchholz**, MdB DIE LINKE. | **Marco Bülow**, MdB SPD | **Annelie Buntenbach**, Mitglied des Geschäftsführenden Bundesvorstandes des DGB | **Prof. Dr. Paul J. Crutzen**, Atmospheric Chemistry and Climate Research, Nobel Laureate 1995 | **Daniela Dahn**, Schriftstellerin | **Das Rilke Projekt (Schönherz & Fleer)**, Erfolgreichstes Deutsches Lyrikprojekt | **Renan Demirkan**, Schauspielerin, Autorin | **Prof. Dr. Klaus Dörre**, Soziologe | **Michael Erhardt**, Erster Bevollmächtigter der IG Metall Frankfurt | **Ute Finckh-Krämer**, MdB (2013-2017) SPD | **Peter Freudenthaler, Volker Hinkel**, von Fools Garden | **Ulrich Frey**, Initiative Neue Entspannungspolitik Jetzt! | **Thomas Gebauer**, Geschäftsführer von medico international | **Wolfgang Gehrcke**, DIE LINKE. | **Stephan Gorol**, Kulturmanagement | **Dr. Rolf Gössner**, Vorstandsmitglied internationale Liga für Menschenrechte | **Prof. Dr. Ulrich Gottstein**, IPPNW Gründungs-und Ehrenvorstandsmitglied | **Susanne Grabenhorst**, stellv. Vorsitzende IPPNW Deutschland | **Jürgen Grässlin**, Bundessprecher der DFG-VK | **Hermann Josef Hack**, Bildender Künstler | **Uwe Hassbecker**, Musiker (Silly) | **Prof. Dr. Frigga Haug**, Soziologin | **Uwe Hiksch**, Bundesvorstand NaturFreunde Deutschlands | **Reiner Hoffmann**, DGB-Vorsitzender | **Philipp Ingenleuf**, Netzwerk Friedenskooperative | **Otto Jäckel**, Vorsitzender IALANA Deutschland, Vereinigung für Friedensrecht | **Kristine Karch**, Co-Chair International Network No to War – No to NATO | **Margot Käßmann**, Theologin | **Katja Keul**, MdB Bündnis90/die Grünen | **Katja Kipping**, MdB, Vorsitzende DIE LINKE. | **Toni Krahl**, Musiker (CITY) | **Sabine Leidig**, MdB DIE LINKE. | **Wolfgang Lemb**, Geschäftsführendes Vorstandsmitglied IG Metall | **Sarah Lesch**, Liedermacherin | **Udo Lindenberg**, Musiker | **Anna Loos**, Schauspielerin, Sängerin (Silly) | **Pascal Luig**, Co-Sprecher „Kooperation für den Frieden“ | **Jürgen Maier**, Forum Umwelt und Entwicklung | **Prof. Dr. Mohssen Massarrat**, Politikwissenschaftler, Friedensforscher | **Hilde Mattheis**, MdB SPD | **Birgitta Meier**, Friedensmuseum Nürnberg | **Prof. Dr. Thomas Meyer**, stellv. Vorsitzender der SPD-Grundwertekommission | **Matthias Miersch**, MdB, Sprecher der Parlamentarischen Linken in der SPD-Bundestagsfraktion | **Prof. Dr. Maria Mies**, Soziologin, Öko-Feministin | **Michael Müller**, Vorsitzender NaturFreunde Deutschlands, ehem. Staatssekretär im Umweltministerium | **Julia Neigel**, Sängerin, Songwriterin | **Prof. Dr. Kai Niebert**, Präsident des Deutschen Naturschutzringes (DNR) | **Wolfgang Niedecken**, Musiker, Sänger (BAP), Maler, Autor | **Prof. Dr. Norman Paech**, Völkerrechtler | **Alexis Passadakis**, aktiv bei Attac Deutschland | **Anne Rieger**, Bundesausschuss Friedensratschlag | **Clemens Ronnefeldt**, Referent für Friedensfragen beim deutschen Zweig des Internationalen Versöhnungsbundes | **Alex Rosen**, Vorsitzender IPPNW Deutschland | **Michaela Rosenberger**, Vorsitzende der Gewerkschaft Nahrung Genuss Gaststätten (NGG) | **Rene Röspel**, MdB SPD | **Prof. Dr. Werner Ruf**, Politikwissenschaftler, Friedensforscher | **Prof. Dr. Jürgen Scheffran**, Physiker, Vorsitzender International Network of Engineers and Scientists for Global Responsibility (INES) | **Dr. Ute Scheub**, Autorin | **Heide Schütz**, Vorsitzende Frauennetzwerk für Frieden | **Prof. Dr. Gesine Schwan**, Vorsitzende der SPD-Grundwertekommission | **Prof. Dr. Johano Strasser**, ehem. Präsident des deutschen PEN | **Wolfgang Strengmann-Kuhn**, MdB Bündnis90/die Grünen | **Prof. Dr. Michael Succow**, Alternativer Nobelpreisträger, Michael Succow Stiftung | **Marlis Tepe**, Vorsitzende der Gewerkschaft Erziehung und Wissenschaft (GEW) | **Horst Trapp**, Friedens- und Zukunftswerkstatt | **Barbara Unmüßig**, Vorstand der Heinrich Böll Stiftung | **Hans-Jürgen Urban**, Geschäftsführendes Vorstandsmitglied IG-Metall | **Willi van Ooyen**, Bundesausschuss Friedensratschlag | **Kathrin Vogler**, MdB DIE LINKE. | **Antje Vollmer**, Vizepräsidentin des Deutschen Bundestages a.D. | **Dr. Christine von Weizsäcker**, Biologin, Präsidentin von Ecoropa | **Prof. Dr. Ernst-Ulrich von Weizsäcker**, ehem. Präsident des Wuppertal Instituts für Klima, Umwelt und Energie | **PD Dr. Uta von Winterfeld**, Politikwissenschaftlerin | **Peter Wahl**, Wissenschaftlicher Beirat von Attac | **Renate Wanie,** Vorstandsmitglied Bund für Soziale Verteidigung (BSV) | **Konstantin Wecker**, Musiker, Komponist | **Prof. Dr. Hubert Weiger**, Vorsitzender des BUND | **Dr. Christa Wichterich**, Soziologin, Publizistin | **Heidemarie Wieczorek Zeul**, Bundesministerin a.D. | **Lucas Wirl**, Geschäftsführer IALANA & NaturwissenschaftlerInnen-Initiative Verantwortung für Frieden und Zukunftsfähigkeit (NatWiss) | **Burkhard Zimmermann**, Initiative Neue Entspannungspolitik JETZT!

Angaben zur Person dienen der persönlichen Information

Malte Rehbein

Die „Asilomar AI Principles“ zu Künstlicher Intelligenz

Die im vergangenen Jahr veröffentlichten und von zahlreichen Wissenschaftlerinnen und Wissenschaftlern sowie weiteren Shareholdern aus Wirtschaft und Technik unterzeichneten Asilomar AI Principles[1] *sind ein Vorschlag für ein Regelwerk zum Umgang mit Künstlicher Intelligenz (KI). Sie umfassen 23 Imperative „ranging from research strategies to data rights to future issues including potential super-intelligence“[2] und können als eine Reaktion auf die beschleunigte technologische Entwicklung in diesem Bereich verstanden werden. Die Folgen dieser Entwicklung bezeichnet das organisierende* Future-of-Life-Institute *zu Recht als „major change […] across every segment of society“[3]. Jahrzehntelange Verheißungen der KI scheinen kurz vor dem Durchbruch zu stehen.*

Eine ethische Bewertung, rechtliche Regelung und konsequente politische Regulierung, die sowohl den Einsatz als auch bereits die Entwicklung von KI umfassen, sind dringend geboten. Diese Notwendigkeit ist in Deutschland inzwischen auch in der breiten Öffentlichkeit angekommen, wie etwa die Gründung des *Weizenbaum-Instituts* in Berlin und die Aufnahme der KI als *Schlüsseltechnologie* im Koalitionsvertrag von Union und SPD zeigen. Es ist zu begrüßen, dass sich mit Asilomar auch die wissenschaftlich-wirtschaftliche Prominenz diesem Thema widmet. Die vorgeschlagenen Prinzipien sind jedoch von ihrer grundsätzlichen Anlage und im Detail zu kritisieren.

Die 23 Imperative entstanden aus einer im Januar 2017 im kalifornischen Asilomar veranstalteten interdisziplinären Tagung *„Beneficial AI“* heraus. Nützlichkeit als Tagungsmotto gab dabei Tenor und Stoßrichtung der Prinzipien bereits vor:

> *„Artificial intelligence has already provided beneficial tools that are used every day by people around the world. Its continued development, guided by the following principles, will offer amazing opportunities to help and empower people in the decades and centuries ahead.“*[4]

Mit dieser technikdeterministischen und rein utilitaristischen Sichtweise auf den Einsatz von KI-Technologien bleiben viele Fragen offen. Denn den „amazing opportunities“ stehen auch zahlreiche Warnungen vor den Folgen eines (unregulierten) Ausbaus von KI-Technologien gegenüber. Führende Wissenschaftler wie *Stephen Hawking* halten ein exponentielles Wachstum von KI für möglich, bis hin zu einer verselbstständigten „Super-Intelligenz“, die den Menschen letztlich überflüssig mache. Bedrohungen werden auch aus der Zivilgesellschaft heraus aufgezeigt: „Slaughterbots“ am Beispiel autonomer Waffensysteme,[5] die britische Serie „Black Mirror“ und zahlreiche kulturkritische Literatur illustrieren in ihren Szenarien künftige Welten, die in ihren Dystopien erschrecken, zugleich aber äußerst realistisch wirken.

Zwischen profitabel und brandgefährlich

Der Einsatz von KI bietet ein riesiges Geschäftspotenzial. Es ist eine Technologie, die hohe finanzielle Profite ermöglicht; es ist ebenfalls eine Technologie, mit der Macht akkumuliert werden kann. Für wirtschaftliche wie politische Prozesse sind Daten und Informationen die Leitwährung,[6] für KI-Systeme sind sie ihr Futter, ohne die Maschinen nicht lernen und KI-Systeme nicht existieren könnten. Wer Daten *und* KI-Systeme kontrolliert, wird Macht ausüben können. Die Entwicklungen in China in Richtung einer *Big-Data-Diktatur* sind da sicherlich nur der Anfang.[7]

Bezeichnend für die Pole zwischen profitabel und brandgefährlich stehen die Aussagen von *Tesla*-Chef *Elon Musk,* der KI, vor allem in ihrer *starken* Form als *Artificial General Intelligence (AGI)* charakterisiert als „the most serious threat to the survival of the human race“.[8] Tritt eine solche „Fernwirkung“ (Jonas, s. u.) der Technologie ein, wäre es in der Tat ein „profound change in the history of life on Earth“ (Principle No. 20) – die radikalste Form der von der Gesellschaft geduldeten technologischen Folgen, nämlich das Ende menschlichen Lebens. Wer hier argumentiert, das Aufzeigen von Drohkulissen sei als Kulturkritik Teil der menschlichen Geschichte, habe sich aber nie bewahrheitet, möge sich vergegenwärtigen, dass in der Geschichte der Menschheit sehr wohl ganze Gesellschaften untergegangen sind, auch selbstverschuldet![9]

Musk, einer der „Endorser“ der Prinzipien, steht damit für das Dilemma, das typisch für komplexe ethische Fragen zu sein scheint. Offensichtlich verdient er durch sein Unternehmen Tesla, das für sehr fortschrittliche Technologien eben unter Nutzung von KI steht, nicht gerade wenig Geld. Es nimmt also kaum Wunder, wenn die Unterzeichner der Prinzipien Entwicklung und Einsatz von KI grundsätzlich bejahen und nicht grundsätzlich in Frage stellen. Dass erhebliche wirtschaftliche Interessen im Spiel sind, mag dafür ein Grund sein und ist bei einer Weiterentwicklung ethischer Grundsätze unbedingt mitzudenken.

Spricht Asilomar nun von „beneficial intelligence“ (Principle No. 1), so schließt sich unmittelbar die Frage an, wie *nützlich* zu definieren ist und wer bestimmt, was für wen als nützlich gilt – falls das überhaupt bestimmbar ist. Die grundlegende Prämisse des Utilitarismus ist zu diskutieren und kritisch zu hinterfragen, denn der Zweck heiligt nicht immer die Mittel. Schon gar nicht, wenn über den Zweck kein Konsens besteht, sondern die Zweckbestimmung von wenigen beherrscht wird. So ist aus Sicht der Rüstungsindustrie ein autonomes, KI-basiertes Waffensystem sicherlich sehr nützlich, wenn sich damit Geld verdienen lässt. Ebenso ist es einem totalitären Regime nützlich, wenn sich damit gezielt Dissidenten töten lassen. Potenzielle Opfer und demokratisch Gesinnte werden die Nützlichkeit anders bewerten.

Meine Überlegungen sind angeregt von der Verantwortungsethik, die Hans Jonas vor fast 40 Jahren formuliert hat. Nach Jonas' Ansatz der „Heuristik der Furcht“ ist bei menschlichen Entscheidungen zunächst von den potenziellen Folgen für die Zukunft auszugehen, die diese Entscheidung nach sich ziehen könnte. Jonas' Motiv, „die Unversehrtheit seiner [des Menschen] Welt und seines Wesens gegen die Übergriffe seiner Macht zu bewahren“,[10] und sein Imperativ „Handle so, daß die Wirkungen deiner Handlung verträglich sind mit der Per-

manenz echten menschlichen Lebens auf Erden“[11] können hilfreiche Leitbilder für den Umgang mit KI bilden. Es sollten aber nicht die einzigen bleiben, denn mit Jonas lässt sich zwar die Frage, wie eine zukünftige Welt *nicht aussehen darf,* recht gut beantworten, nicht aber die für mich wichtige Frage, wie sie *gestaltet sein soll.*

Um ethische und rechtliche Prinzipien für KI herzuleiten, sind also zwei Sichtweisen zu kombinieren: die dystopische (Jonas Ansatz der Heuristik der Furcht) und die utopische Zukunftsvorstellung. Bei letzterer stellt sich allerdings die Frage, wer die *schöne neue Welt* definiert. Wer sagt, was *gut* und *beneficial* ist und erklärt, warum das für alle gilt? Wie sieht also die Welt aus, in der wir zukünftig leben wollen? Diese Frage beantworten die Asilomar-Prinzipien nicht, und das ist problematisch. Sie unterstellen die Existenz einer allgemeingültigen und breit akzeptierten Zustimmung zu einer Zukunftskonzeption, die einem Technologiedeterminismus unterliegt, zugleich aber unbestimmt bleibt. Nehmen wir dies unkritisch hin, so laufen wir Gefahr, dass nur eine Silicon-Valley-Avantgarde bestimmt, wie wir künftig leben werden. Daraus wiederum erwächst unter anderem die Gefahr eines Totalitarismus durch eben diese Avantgarde.

Wer bestimmt also, was *gut* ist, wenn gleichzeitig die Technologie allumfassend ist, *alle* betrifft, nicht nur die, die ein bestimmtes KI-basiertes Produkt kaufen oder nutzen? Gibt es darüber Konsens? Wie findet man einen solchen Konsens auf einer globalen Ebene? Und wird es auch in der Zukunft Konsens sein, wenn Dinge nicht mehr rückgängig zu machen sind, die in der heutigen Gegenwart Konsens waren?

Wie bindend können Regeln sein?

Selbst wenn man sich jetzt auf ein Regelwerk festlegt, welches KI beispielsweise durch *Einbau* ethischer Prinzipien kontrollieren soll: Wer sagt, dass die KI selbst sich nicht über dieses Regelwerk hinwegsetzen und beginnen wird, eigenen Maßstäben, auch ethischen, zu folgen? Als Analogie mag Nordkorea dienen, ein Staat, der sich selbst aus der Weltgemeinschaft ausschließt und damit bestehenden Regelwerken entzieht und trotz der Regelwerke, Sanktionen und internationaler Ächtung Massenvernichtungswaffen entwickelt. Man könnte auch anders fragen: Wenn mit einem KI-System einem *Wesen* Intelligenz zugeschrieben und letztlich eine eigene Urteilsfähigkeit zugesprochen wird, warum sollte sich dieses Wesen dann den Regeln von Menschen unterwerfen, die ihm unterlegen erscheinen müssen? So sind auch militärisch höchst potente Staaten wie die USA und Russland von der Völkergemeinschaft nur schwer zu kontrollieren und dies auf Grund ihrer militärischen Überlegenheit. Bei KI ist zusätzlich zu bedenken, dass sie sich einer Kontrolle mit einer Aktionsgeschwindigkeit entziehen könnte, die eine menschliche (Gegen-) Reaktion unmöglich macht.

Ich habe auch keine Antwort auf diese Fragen, plädiere aber dafür, dass die Diskussion darüber geführt werden muss, und zwar von allen Betroffenen, nicht nur von profitierenden Technologen und Unternehmern. Dringend! Ethische Prinzipien für KI, bzw. Technik und Gesellschaftsentwicklung im Allgemeinen, brauchen dabei zwei klar illustrierte Szenarien als Orientierung: „die vorausgedachte Gefahr“[12] und eine Zukunftsvorstellung. Diese Zukunftsvorstellung müsste ausgehandelt werden.[13] Weniger ist hierbei an eine Utopie zu denken, sondern eher ist eine Charta der künftigen *conditio humana* zu zeichnen, die selbst nicht statisch, sondern wandelbar zu sehen ist: Was bedeutet (uns) das Menschsein, und was von dem technisch Machbaren kann noch als menschlich zugelassen werden? Denn es geht mit den Worten von Hans Jonas „nicht nur um physisches Überleben, sondern auch um Unversehrtheit des [menschlichen] Wesens.“[14]

Versuche ethischer und rechtlicher Regelungen für KI laufen ins Leere

Noch ist die dystopische Sicht nicht jedem klar, die nach Jonas' Konzeption der „Fernwirkung der Technik“ Kollateralschäden sowie Auswirkungen auf die Zukunft berücksichtigen muss. Auch der utopische Zukunftsentwurf, die Charta, ist nicht verhandelt. Das zeigt der in Asilomar angeregte Grundsatz deutlich:

> *„Teams developing AI systems should actively cooperate to avoid corner-cutting on safety standards“ (Principle No. 5).*

Die „safety standards“ oder allgemeiner, gesetzliche Regelungen und Limitierungen, gibt es noch nicht, und es wird schwer sein sie zu finden, insbesondere solange die technologische Entwicklung so viel schneller voranschreitet als eine Gesetzgebung reagieren und Rahmen setzen kann. Dieses von Soziologen in Bezug auf gesellschaftliche Anpassungs- und Veränderungsprozesse als „cultural lag“ bezeichnete Phänomen müsste eigentlich zu einem *Moratorium* führen, d. h. Entwicklungen so lange zu stoppen, bis die dringenden Fragen geklärt und auf breiter und globaler gesellschaftlicher Basis ausgehandelt sind. Das ist aber auf Grund der Dynamik technologischer Entwicklung und

Malte Rehbein

Prof. Dr. **Malte Rehbein** erforscht und lehrt formale und computergestützte Methoden und ihre Anwendungsmöglichkeiten für geistes- und kulturwissenschaftliche Fragestellungen (Digital Humanities) an der Universität Passau. Seine wissenschafts- und gesellschaftskritischen Äußerungen entstammen einer gewachsenen Sorge um die Gestaltung unserer Zukunft.
Website: *http://www.phil.uni-passau.de/dh/lehrstuhlteam/prof-dr-malte-rehbein/*

ihrer engen Verzahnung mit ökonomischen und machtpolitischen Interessen kaum vorstellbar.

Daher wirft Asilomar mehr Fragen auf als beantwortet werden. Ein Beispiel: Wir wollen keine autonom handelnden Waffensysteme. Ich zumindest nicht. Die Unterzeichner der Asilomar-Prinzipien hingegen haben offenbar nichts gegen solche Waffen. Das Einzige, das sie problematisieren, ist ein Wettrüsten mit diesen Systemen (Principle No. 18). An diesem Beispiel lässt sich gut illustrieren, wie schwierig es ist und weiterhin sein wird, so etwas wie einen gesellschaftlichen Konsens zu erwirken, wenn die Diskussion von ökonomischen und machtpolitischen Interessen dominiert wird.

Die Utopie-Prämisse

Asilomar versuchte, dies für sich im Kleinen so zu lösen:

> *„This consensus allowed us to set a high bar for inclusion in the final list [of principles]: we only retained principles if at least 90 % of the attendees [of the conference] agreed on them".*

Diese „high bar" der Inklusion gilt damit aber auch für kritische Stimmen und Minderheiten, die folglich ausgeschlossen werden! Da ist es kaum verwunderlich, dass „An arms race in lethal autonomous weapons should be avoided" (Principle No. 18) aufgenommen, aber kein grundsätzlicher Bann von autonomen Waffen ausgesprochen wurde. Hier zeigt sich das Problem der exklusiven Utopie-Prämisse, die Asilomar angewandt hat: Es erfordert 90 % Zustimmung, um einen Technologieeinsatz zu verbieten. Eine Prämisse, die dem europäischen, leider zunehmend ausgehöhlten Vorsorgeprinzip entspräche, würde hingegen 90 % Zustimmung erfordern, um einen solchen Einsatz zu erlauben. Die Frage müsste nach meiner Auffassung also lauten: Sind 90 % der Menschen für autonome Waffensysteme? Dann könnte man sie erlauben. Aber sie sollte eben nicht heißen: Findet sich eine Minderheit von 10 %, die einen Bann verhindert?

Die Schärfe der Problematik steckt weiterhin oft im Detail. So ist die Formulierung von „The application of AI to personal data must not unreasonably curtail people's real or perceived liberty" (Principle No. 13) äußerst subtil: Der Einsatz von KI darf gemäß den Unterzeichnern von Asilomar also durchaus menschliche Rechte beschneiden. Er solle es nur nicht in einer Weise tun, die als „unreasonably" (wahlweise zu übersetzen mit unvernünftig, unangemessen oder übertrieben)[15] charakterisiert wird. Nach meinem Verständnis einer demokratischen Gesellschaft sind Freiheitsrechte ein hohes Gut und gesetzlich geregelt. Eine Einschränkung ist den Gerichten vorbehalten – unter hohen Auflagen. Eine Abweichung davon ist Notstand und dessen Dauerzustand Totalitarismus.

Der Einsatz von KI, auch in ihrer schwachen Form, kann globale Auswirkungen haben, insbesondere wenn man die KI mit exekutiven Mitteln wie Waffen ausstattet oder ihr Zugriff auf kritische Infrastruktur erlaubt. Jonas spricht davon, dass die Reichweite menschlichen Handelns und daher menschlicher Verantwortung nicht mehr eng umschrieben werden kann.[16] Daher bedarf es globaler Regulierung und Mitspracherecht auch derer, die nicht unmittelbar zu den Profiteuren zählen. Der bereits herausgebildete *digital divide* innerhalb von Gesellschaften und zwischen Gesellschaften darf nicht weiter dazu führen, dass eine Gruppe über die Zukunft einer anderen bestimmt. Zudem muss die Bereitschaft da sein, nicht nur den Einsatz von KI in bestimmten Szenarien zu ächten, sondern gegebenenfalls schon die Entwicklung solcher Technologieformen zu unterbinden, wenn das Technologierisiko zu groß ist, was vor allem bei starker KI der Fall zu sein scheint. Eine zentrale Frage wird weiterhin sein, wie unsere gegenwärtigen Wirtschafts- und Gesellschaftssysteme umzugestalten sind, damit sie eine globale und auch langfristige, nachhaltige Perspektive begünstigen und nicht von den kurzfristigen technologischen und ökonomischen Interessen weniger dominiert werden.

Anmerkungen und Referenzen

1 *https://futureoflife.org/ai-principles/*
2 *https://futureoflife.org/bai-2017/*
3 *https://futureoflife.org/2017/01/17/principled-ai-discussion-asilomar/*
4 *https://futureoflife.org/ai-principles/*
5 *Stop Autonomous Weapons (2017) Slaughterbots. https://www.youtube.com/watch?v=9CO6M2HsoIA&t=.*
6 *Neben den Daten, die Menschen von sich direkt oder indirekt preisgeben (etwa durch soziale Medien, Nutzung von Suchmaschinen, Internet of Things) ist die Bedeutung einer Sammlung von Daten durch Sensoren (angefangen mit Überwachungskameras) nicht zu unterschätzen. Auch aktuelle Entwicklungen in Richtung „Neuro-Daten" sind zu beobachten: Schnabel U (2017) Attacke aufs Gedankenstübchen; Forscher fordern, Neurotechniken besser zu regulieren. Die Zeit 30.11.2017, S. 37.*
7 *Assheuer T (30.11.2017) Die Big-Data-Diktatur. Die Zeit 30.11.2017, S. 47.*
8 *Gibbs S (2014) Elon Musk: artificial intelligence is our biggest existential threat. The Guardian 27.10.2014, https://www.theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat.*
9 *Diamond J (2010) Kollaps; Warum Gesellschaften überleben oder untergehen. 4. Aufl. Fischer-Taschenbuch-Verlag, Frankfurt am Main.*
10 *Jonas H (1979) Das Prinzip Verantwortung; Versuch einer Ethik für die technologische Zivilisation. Insel-Verlag, Frankfurt am Main, S. 9.*
11 *Ebd., S. 35.*
12 *Ebd., S. 7.*
13 *Vgl. etwa die Leitfrage „Welche digitale Gesellschaft wollen wir werden?" der Bonner Gespräche zur politischen Bildung im März 2018 „Künstliche Intelligenz, Big Data und digitale Gesellschaft – Herausforderungen für die politische Bildung" (http://www.bpb.de/veranstaltungen/format/kongress-tagung/242756/kuenstliche-intelligenz-big-data-und-digitale-gesellschaft-herausforderungen-fuer-die-politische-bildung).*
14 *Jonas, Prinzip Verantwortung, S. 8.*
15 *In der nachträglich veröffentlichten Übersetzung der Prinzipien ins Deutsche wurde „unangemessen" gewählt.*
16 *Jonas, Prinzip Verantwortung, S. 15.*

Hans-Jörg Kreowski und Eberhard Zehendner

Editorial zum Schwerpunkt „FIfFKon 2017 – TRUST“

Im Anfang war das Wort. TRUST. Alles begann mit einer Idee: Wem kann ich trauen im Netz und warum? Um die genaue Formulierung und Formatierung des Titels wurde im Programm-Komitee einige Zeit gerungen. Dann stand er, der Titel der FIfFKon 2017. Was sollte nun daraus werden? Dazu gab es schon lange vorher konkrete Vorstellungen: Provokant und zu streitbarer Diskussion einladend, mit einer Mischung aus bewährten FIfF-Themen und ungewöhnlichen Perspektiven – und vor allem: bunt!

Laut ARD-DeutschlandTrend vom 5. April 2018 haben null Prozent der Befragten sehr großes Vertrauen in den verantwortungsbewussten Umgang von Facebook mit persönlichen Daten und nur zehn Prozent votierten für großes Vertrauen; dagegen sind fast neun von zehn Befragten misstrauisch. Konsequenzen wollen allerdings nur wenige ziehen. Beim aktuellen Facebook-Skandal ist die Meldung fast untergegangen, dass CDU und FDP in ihrem Bundestagswahlkampf Daten von Kundinnen und Kunden der Deutschen Post für ihre Wahlkampfzwecke genutzt haben – völlig legal. Aber genau das ist doch so skandalös, dass alle, die für das Erbringen bestimmter Leistungen personenbezogene Daten sammeln, diese für beliebige ominöse Zwecke verscherbeln dürfen. Wen wundert es da, dass Vertrauen fehlt: Misstrauen ist das Gebot der Stunde. Und es bleibt abzuwarten, ob die am 25. Mai in Kraft tretende Europäische Datenschutz-Grundverordnung den Missbrauch von personenbezogenen Daten eindämmen kann oder ihn wenigstens nicht länger legalisiert.

Diese beiden und viele weitere Beispiele zeigen, dass das Thema *TRUST – Wem kann ich trauen im Netz und warum?* der FIfF-Konferenz 2017 vom 20. bis zum 22. Oktober 2017 in Jena ins Schwarze getroffen hat. Der vorliegende Schwerpunkt reflektiert das weitgefächerte Programm der Tagung in einer Art bebildertem Kaleidoskop. Einige Vorträge sind ausführlich schriftlich ausgearbeitet, zu anderen finden sich kurze Zusammenfassungen mit ergänzenden Informationen, manche blieben aus den verschiedensten Gründen unberücksichtigt. Zu den Beiträgen gehören Hannes Mehnerts *Wem müssen wir beim Benutzen von Software vertrauen?*, Lutz Hasses *Vertrauen – Fortschritt – Kontrolle*, Thomas Grubers *Die Marschrichtung im Cyber- und Informationsraum,* Frank Geyers *Nutzung von Daten aus sozialen Netzwerken im Umfeld der zivilen Sicherheit*, Tobias Kraffts *Qualitätsmaße algorithmischer Entscheidungssysteme in der Kriminalprognostik* und Sylvia Johnigks *Herausforderungen an das Identitätsmanagement, allen Rollen gerecht zu werden.* Der Beitrag *Tihange–Doel Radiation Monitoring* eines TDRM-Autorenkollektivs, beginnend auf Seite 6, gehört eigentlich ebenfalls in den Schwerpunkt, wurde aber wegen seiner übergreifenden Wichtigkeit für das FIfF in das *Forum* eingeordnet.

Darüber hinaus haben Benjamin Kees, Rainer Rehak und Stefan Hügel ein Leporello erstellt: *FIfF wirkt – ein langer Blick zurück,* zu den wichtigsten Aktivitäten des FIfF von Ende 2016 bis zur FIfFKon 2017. Außerdem kommentieren Hans-Jörg Kreowski *Die Cyberpeace-Kampagne des FIfF* und Kai Nothdurft *Attribution von „Cyber“-Angriffen durch Politik und Medien.* Ergänzend arbeitet Carlo Schäfer in *Spam und Cybercrime im Jahre 2017* seine Anti-Spam-Demonstration im Foyer des Tagungsgebäudes auf, es gibt eine Zusammenfassung der Konferenz-Eröffnung sowie Berichte zu den Workshops *Algorithmen: schuldig oder unschuldig?* von Britta Schinzel, *ZensusVorbereitungsgesetz 2021* von Jens Rinne, *Handys – aber sicher!* sowie *IT-Sicherheit barrierefrei* von Eberhard Zehendner. Zwecks Auflockerung wurden einige Stimmen zur Konferenz eingefangen, insbesondere aus dem Technik- und dem Catering-Team.

Der Schwerpunkt endet – vermeintlich – mit dem Beitrag *Das war die FIfFKon 2017 – Nachbetrachtungen und Danksagungen*. Dort wird u.a. aufgeklärt, warum der Beitrag *Informationelle Selbstbestimmung und Datenautonomie mit Hubzilla* von Gustav Wall mit vollem Recht noch innerhalb des Schwerpunkts steht und was der kürzlich verstorbene, auf Seite 70 gewürdigte Visionär, Rebell und Lyriker *John Perry Barlow* mit unserem Konferenzthema zu tun hatte. Aufmerksamen Leserinnen und Lesern dürfte auch nicht entgehen, dass der von Dietrich Meyer-Ebrecht ab Seite 72 besprochene Film *Zero Days* auf der FIfFKon 2017 gezeigt wurde und im Übrigen das ganze Heft in Cover und SchlussFIfF eingepackt ist, die ebenfalls der Konferenz gewidmet sind.

Hans-Jörg Kreowski

Zur Eröffnung der FIfFKon 2017

Die FIfF-Konferenz 2017 an der Friedrich-Schiller-Universität in Jena wurde eröffnet vom Gastgeber Eberhard Zehendner, dem FIfF-Vorsitzenden Stefan Hügel und vom Prodekan der Fakultät für Mathematik und Informatik, Prof. Dr. Clemens Beckstein.

Während Eberhard Zehendner vor allem auf den Eröffnungsvortrag von Hannes Mehnert hinweist, geht Stefan Hügel in seiner Begrüßung auf das Thema der Konferenz ein, indem er zu Vertrauen im Netz und den vielen Gründen für Misstrauen ausführt:

FIfF-Vorsitzender Stefan Hügel, Fotos: Kai Nothdurft

> *„TRUST – Vertrauen – ist die Basis, auf der unsere Gesellschaft aufgebaut ist. Wenn wir einander nicht mehr vertrauen können, funktioniert unser Zusammenleben nicht – das gilt selbstverständlich auch im Netz. […] Doch das Vertrauen wird heute im Netz täglich verletzt, sowohl illegal als auch legal. Wir müssen uns vor kriminellen Menschen schützen, die unser Vertrauen missbrauchen. Seit den Veröffentlichungen des Whistleblowers Edward Snowden wissen wir aber auch, dass Behörden unsere Kommunikation umfassend ausspähen. […] Dazu kommt der Datenhunger der Diensteanbieter, die ihre Geschäftsmodelle auf der Nutzung der Daten aufbauen und dies zum Beispiel durch für den Laien unverständliche Nutzungsbedingungen formaljuristisch legalisieren. Dem soll mit dem neuen europäischen Datenschutzrecht gegengesteuert werden – doch inzwischen wissen wir, dass gerade die deutsche Bundesregierung massiv versucht, dieses Recht aufzuweichen und zu bremsen. Auch damit wird Vertrauen zerstört."*

Er vergisst aber auch nicht, dass Vertrauen und Vertrauensverlust nicht auf das Internet beschränkt sind, sondern auch die aktuelle politisch-gesellschaftliche Situation von einer massiven Vertrauenskrise geprägt ist.

> *„Unsere diesjährige Konferenz findet in politisch bewegten Zeiten statt. Gestattet mir ein paar Worte dazu: Gerade wurde bei der Wahl zum Deutschen Bundestag eine Partei gewählt, die offen rechtsradikale Inhalte vertritt; mindestens aber solche Mitglieder in ihren Reihen hat. Es ist also davon auszugehen, dass solche Positionen damit auch wieder in den Bundestag Einzug halten werden. Aus Umfragen wissen wir, dass ein großer Anteil der Wählerinnen und Wähler dieser Partei seine Wahlentscheidung aus Enttäuschung über die Politik der etablierten Parteien getroffen hat. Auch hier scheint demnach der Verlust an Vertrauen eine wichtige Rolle zu spielen. Den Parteien, die nun in Berlin die Regierung übernehmen […], aber auch den Mitgliedern der künftigen Opposition, die demokratische, freiheitliche Positionen vertreten und allen Menschen Respekt entgegenbringen, kommt dabei eine große Verantwortung zu. Meine Damen und Herren im Deutschen Bundestag und in der künftigen Bundesregierung: Bitte werden Sie dem Vertrauen Ihrer Wählerinnen und Wähler, werden Sie dieser Verantwortung gerecht!"*

Als Leiter der Arbeitsgruppe Künstliche Intelligenz, die neben technischen Themenkomplexen auch wissenschaftstheoretische und philosophische Aspekte der KI in ihrer Arbeit berücksichtigt, stellt Clemens Beckstein in seiner Grußbotschaft insbesondere die Verbindung seines eigenen Fachgebiets zur FIfF-Konferenz her. Er ordnet dem Thema TRUST drei Gegenstandsbereiche zu: die Handelnden, ihre Handlungen und die Regeln, denen sie dabei folgen. Vertrauensbruch ist dann einfach ein Regelverstoß. Da an der altehrwürdigen Universität Jena sich immer ein Verweis auf Zeiss, Abbe, Goethe, Schiller, Frege oder Marx anbietet, erläutert er Ablauf und Folgen eines Vertrauensbruchs am Beispiel des Zauberlehrlings von Goethe. Und er schließt mit einer Betrachtung des Vertrauensproblems bei der Digitalisierung heute: Die Rollen von Lehrling und Meister seien nicht eindeutig zuzuordnen, weil die handelnden Personen mal das eine, mal das andere seien, und im Gegensatz zu der berühmten Ballade, bei der am Ende der Meister die alte Ordnung wiederherstellt, sei sie bei der Digitalisierung unwiederbringlich verloren.

Prodekan Prof. Dr. Clemens Beckstein

Die komplette Rede von Stefan Hügel liegt unter *fiff.de/r/181000*. Videos der Reden finden sich unter *fiff.de/r/181001* (Zehendner), *fiff.de/r/181002* (Hügel), *fiff.de/r/181003* (Vorstellung Beckstein), *fiff.de/r/181004* (Beckstein).

Hannes Mehnert

Wem müssen wir beim Benutzen von Software vertrauen?

Möglichkeiten zur radikalen Verkleinerung der *Trusted Computing Base*

Das Thema der FIfF-Konferenz 2017 war „TRUST – Wem kann ich trauen im Netz und warum". Ich beschäftige mich mit Vertrauenswürdigkeit von Software und war deshalb als Vortragender[1] eingeladen. Das Vertrauen in Software spielt eine wichtige Rolle, um von Vertrauen im Netz reden zu können. Seit mehreren Jahren forsche ich an einer Alternative zu existierenden Betriebssystemen, die ich in diesem Artikel vorstellen werde.

Heutzutage sind Computer aus der westlichen Welt nicht mehr wegzudenken. Viele schützenswerte persönliche Daten werden mit Hilfe von Computern elektronisch verarbeitet, seien es die Kreditkartendaten, die bei einer Online-Flugbuchung übermittelt werden, Ausweisdaten bei einer Grenzkontrolle, Zugangsdaten beim Online-Banking, oder persönliche Daten in sozialen Netzwerken wie Facebook, Instagram, Twitter oder GitHub. All den bei diesen Diensten verwendeten EDV-Systemen muss vertraut werden, die Datensicherheit der persönlichen Daten sicherzustellen. Dieses Vertrauen muss von der Eingabe an der Tastatur, die auch wieder eine Firmware hat, über die installierte Software (Webbrowser, Betriebssystem etc.), den Übertragungsweg (beispielsweise TLS als sicheres Protokoll, sowohl hinsichtlich der Spezifikation als auch der Implementierung), bis hin zum Server des Diensteanbieters (Software, Administrierende, physikalische Sicherheit im Rechenzentrum) reichen. Auf die Hardware (CPU, deren Mikrocode, und andere Peripherie wie Tastatur, Bildschirm, Netzwerkkarte) und die Umgebung (berechtigte Administrierende, Zugangskontrolle zum Rechenzentrum) gehe ich in diesem Artikel nicht ein. Betrachten wir lediglich die Software, sind dies heutzutage Millionen Zeilen Code, die beispielsweise bei einer Kreditkartenbuchung ausgeführt werden.

Wie können wir Software vertrauen?

Um Software Vertrauen entgegenzubringen, gibt es mehrere Möglichkeiten: Wenn den Entwickelnden vollständig vertraut wird, keine Fehler bei der Programmierung zu machen, heißt dies aber nicht, dass die Software fehlerfrei ist. Umso mehr Quellcode involviert ist, desto mehr Fehler schleichen sich ein. Die Menge an Quellcode ist also entscheidend: je weniger, desto einfacher ist es, diesen nachzuvollziehen und dessen Korrektheit zu überprüfen, und ihm somit zu vertrauen. Auch die verwendete Programmiersprache spielt eine große Rolle, da Programmiersprachen unterschiedliche Fehlerquellen zulassen: Wenn beispielsweise der Speicher von einer Laufzeitumgebung automatisch (durch einen Algorithmus) verwaltet wird, können Entwickelnde keine Fehler in der Speicherverwaltung machen. Natürlich muss dem implementierten Algorithmus vertraut werden, aber wenn dieser mathematisch korrekt bewiesen wurde, oder schon allein, wenn die Laufzeitumgebung auf vielen Computern verwendet wird, ist die Wahrscheinlichkeit gering, dass noch Fehler gefunden werden. Die Möglichkeit besteht immer, auch bei einem Beweis kann es sein, dass die Annahmen nicht korrekt sind (zum Beispiel Annahmen über das Zahlensystem; Computer verwenden meist Datentypen mit endlichen Wertebereichen, nicht unendliche Zahlenmengen wie in der Mathematik). Wenn der Quellcode von Software nicht vorliegt, kann nur durch Beobachtung des Laufzeitverhaltens oder durch *Reverse Engineering* Vertrauen hergestellt werden – hierauf möchte ich nicht näher eingehen.

Die *Trusted Computing Base (TCB)* eines Systems ist die Hardware und Software, die sicherheitsrelevant ist: ein Fehler in einem Bestandteil der TCB korrumpiert die Sicherheit des Gesamtsystems. Die TCB eines Webbrowsers umfasst

- neben eigenem Quellcode, der die grafische Benutzeroberfläche realisiert,
- mindestens ein Rendering-Modul mit HTML- und CSS-Parser sowie Regeln, um die angeforderten Inhalte als Webseite auf dem Bildschirm darzustellen,
- meist auch einen JavaScript-Interpreter, zum Parsen und Ausführen von JavaScript-Code,
- diverse Programmteile, die Fonts, Bilder, Videos etc. parsen und darstellen können – häufig werden hierzu externe Bibliotheken (libpng, libjpeg etc.) verwendet,
- weitere Bibliotheken, die benutzt werden, um TLS-Verbindungen aufzubauen oder Basisfunktionalität bereitzuhalten (die Standard Library),
- und das Betriebssystem selbst, welches Funktionalität für Netzwerkverbindungen, Dateizugriffe, Grafikkartentreiber etc. bereitstellt.

Der gesamte Programmcode wird von einem Compiler zu Maschinencode übersetzt, wobei der Compiler wiederum auch Teil der TCB ist.

Um Vertrauen in ein Programm herzustellen, muss jede/r sich vorstellen können, wie sich das Programm zur Laufzeit verhält. Für einfache Programme, wie mathematische Funktionen, ist dies nicht schwer. Bei komplexeren Programmen, die Netzwerkverbindungen aufbauen und abbauen sowie Daten auf der Festplatte lesen und schreiben, ist eine Intuition über das Laufzeitverhalten der Programmiersprache – der formalen Semantik – hilfreich. Jede Funktion eines Programms muss begutachtet werden, und diese ist einfacher zu verstehen, wenn sie wenig Code beinhaltet, und dieser nur sehr begrenzt auf Daten zugreifen kann (beispielsweise durch Isolation und Kapselung in einer Programmiersprache).

Programmiersprachen unterscheiden sich durch die bereitgestellten Abstraktionen, und wie diese verwendet werden. Einfache Abstraktionen, wie Variablen und Funktionen, sind nahezu allgegenwärtig. Objektorientierte Sprachen bringen ein Objektsystem mit, das Abstraktionen erlaubt (Interfaces, Vererbung, …). Typen enthalten zur Compile-Zeit Information über die Form der Werte zur Laufzeit. Mit Hilfe von statischen Typsystemen können schon zur Compile-Zeit Fehler verhindert werden (das Programm lässt sich dann nicht kom-

pilieren), die in anderen Sprachen erst zur Laufzeit als Fehler auftreten. Bei imperativen Programmen werden Berechnungsabläufe beschrieben, wohingegen bei deklarativen Programmen die Beschreibung des Problems im Vordergrund steht. Funktionale Sprachen wie *Haskell* oder *OCaml* unterstützen die Entwicklung von deklarativen Programmen, und dank ihres ausdrucksstarken Typsystems können viele komplexe Invarianten durch das Typsystem sichergestellt werden. Proof-Assistenten, wie Coq, Isabelle und HOL4, oder abhängig typisierte Sprachen wie *Agda* und *Idris*, erlauben mathematische Spezifikationen als Typ zu formulieren, der sichergestellt wird. Ein einfaches Beispiel: die Länge einer Liste erhöht sich nach dem Hinzufügen eines Listenelements um eins,

```
add : n a list -> a -> (n + 1) a list
```

Bestehende Betriebssysteme sind sehr umfangreich (Millionen von Zeilen von Code) und zum Großteil in der imperativen und maschinennahen Sprache C vor Ewigkeiten (faktisch: Jahrzehnten, was aber bei der Entwicklungsgeschwindigkeit von Computern Ewigkeiten gleichkommt) entwickelt worden. Und sie werden weiterentwickelt, dabei wird häufig Abwärtskompatibilität angestrebt, somit wächst die Codemenge stetig.

MirageOS

Unser Ansatz, den ich im Folgenden vorstelle, basiert darauf, ein Betriebssystem von Grund auf neu zu entwickeln, statt mit bestehendem Code zu arbeiten. Vor rund 10 Jahren wurde *MirageOS* an der University of Cambridge gestartet. Beim Design von MirageOS fließen Erfahrungen aus bestehenden Betriebssystemen ein. Das Design umfasst neben Performance, Skalierbarkeit, Sicherheit (*Defense in Depth*) auch Lesbarkeit und Modularisierung. Als Programmiersprache wird OCaml eingesetzt, eine Multiparadigmen-Sprache mit funktionalen und objektorientierten Merkmalen sowie automatischer Speicherverwaltung und programmierbarem Modulsystem, eine formale Semantik des Sprachkerns. Einige Bestandteile, wie die Laufzeitumgebung von OCaml, sind nach wie vor in C entwickelt, aber nur in der Größenordnung von Tausenden Zeilen, statt Millionen wie in anderen Betriebssystemen.

Heutzutage benutzen viele Dienste Virtualisierungstechnologien wie Hypervisoren, um die einzelnen Dienste stark voneinander zu isolieren, damit der Schaden bei einer Kompromittierung gering ist. Die Aufgabe eines Hypervisors auf einem physikalischen Computer ist, die Ressourcen wie Arbeitsspeicher, Festplatte, Netzwerkkarten zu verwalten und den einzelnen virtuellen Maschinen zuzuweisen. Auch der Scheduler, der entscheidet, welche virtuellen Maschinen auf welchen Prozessoren ausgeführt werden, ist Teil des Hypervisors. Ein herkömmliches Unix-System enthält mehrere Prozesse, die voneinander isoliert auf den verfügbaren Prozessoren ausgeführt werden. Zur Isolation gibt es virtuellen Speicher, ein Prozess kann nicht auf den Speicher eines anderen zugreifen.

MirageOS ist ein Unikernel[2], der als virtuelle Maschine auf herkömmlichen Hypervisoren (*Xen*, *KVM*, *Bhyve*, *VMM*) ausgeführt wird. MirageOS beinhaltet allerdings nur einen einzigen Prozess, braucht somit keinen Scheduler und auch keinen virtuellen Speicher. Jeder MirageOS-Unikernel ist ein maßgeschneidertes System mit einer Aufgabe. Zur Compile-Zeit wird die Funktionalität durch die Auswahl der Bibliotheken zusammengestellt. Danach werden die Zielplattform gewählt und die plattformabhängigen Treiber (Netzwerkkarte, persistenter Speicher) benutzt. Grundlegende Netzwerkdienste wie DHCP, DNS, Firewall, Webserver sind für MirageOS bereits in OCaml als Bibliotheken implementiert und können nahezu beliebig zusammengestellt werden. Das virtuelle Maschinen-Image eines DNS-Servers ist beispielsweise etwa 3 MB groß, enthält neben dem Boot-Code und der OCaml-Laufzeitumgebung einen Netzwerkkartentreiber sowie einen TCP/IP-Stack und benutzt die DNS-Bibliothek. Ein Dateisystem, Prozessverwaltung, Nutzerverwaltung, interaktive Shell sind hier nicht notwendig und daher gar nicht erst im Unikernel enthalten. Die Angriffsfläche wird dadurch enorm reduziert (locker um zwei Größenordnungen), und durch die Benutzung von OCaml sind diverse Angriffsvektoren (Pufferüberläufe etc.) bereits eliminiert.

MirageOS (Abbildung 1 a) führt auf dem Hypervisor direkt die OCaml-Laufzeitumgebung aus und spart somit im Vergleich zu einem herkömmlichen System (Abbildung 1 b) viele Layer ein, die zur Komplexität beitragen.

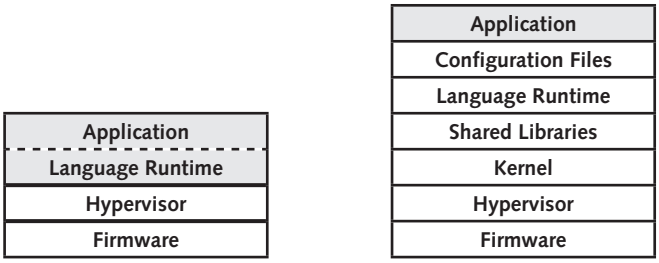


Abbildung 1: Software-Layer, (a) MirageOS, (b) herkömmlich. Thomas Gazagnaire, CC-BY-SA-4.0

Die Basis von MirageOS bilden hunderte Bibliotheken, die möglichst modular und deklarativ entwickelt wurden und werden. Durch das Modulsystem in OCaml abstrahieren wir zum Beispiel die Zielplattform: ein Unikernel kann sowohl zum Testen und Debuggen zu einem normalen Unix-Binary kompiliert werden, als auch zu einer virtuellen Maschine. Die einzelnen Betriebssystemkomponenten sind als Interfaces spezifiziert, und enthalten erweiterbare Fehlerdefinitionen. Eine konkrete Implementierung muss diesem Interface genügen (die entsprechende Funktionalität zur Verfügung stellen), kann aber neue Fehlerfälle hinzufügen. Konsumenten der Interfaces können auf Fehler programmatisch reagieren. Das erlaubt es beispielsweise, ein Dateisystem zu implementieren, das Daten via Netzwerk liest und schreibt – wo somit Kommunikationsfehler auftreten können. Jedes dieser Interfaces ist versioniert, eine neue Version muss nicht die identische Funktionalität wie die vorherige bereitstellen.

Die von uns entwickelten Bibliotheken, die Protokolle implementieren, wie TLS, TCP/IP, DNS, DHCP oder Git, haben meist einen Encoder und einen Decoder, um Binärdaten in typisierte Datenstrukturen zu wandeln oder einen Fehler zurückzugeben. Das zentrale Protokoll-Handling ist rein funktional und führt selbst keine Kommunikation aus. Die Funktion bekommt einen Zustand und ein Paket, und liefert einen neuen Zustand und möglicherweise Pakete zum Ausgeben zurück. Ein dediziertes Modul kümmert sich darum, Pakete zu empfangen, diese dem rein funktionalen Protokollhandling weiterzugeben und Pakete zu versenden. Der Vorteil ist, dass das Protokollhandling, meist eine State Machine, ohne reale Eingabe und Ausgabe getestet werden und mit nur lokalem Verständnis nachvollzogen werden kann.

Da ein Unikernel nur die unbedingt notwendige Funktionalität umfasst, ist dessen Konfiguration und Administration weniger komplex als ein General-Purpose-System. Daher sind Unikernels einfacher zu betreiben, und können auch von Nicht-ExpertInnen betrieben werden. Daher muss nicht mehr der IT-SpezialistIn im Freundeskreis vertraut werden, sondern der Betrieb kann von jeder Person selbst gemacht werden. Aktuell werden MirageOS-Unikernels nur als Quellcode verteilt, in Zukunft sind aber auch plattformspezifische Binärpakete denkbar. Sollte in einer benutzten OCaml-Bibliothek eine Sicherheitsschwachstelle gefunden werden, müssen alle Unikernels, die diese Bibliothek benutzen, neu kompiliert und deployed werden.

Als Beispiel soll hier *Canopy* dienen, ein MirageOS-Unikernel, der zum Großteil im Frühling 2014 in kurzer Zeit (eine Woche) entstanden ist. Canopy ist ein Content-Management-System, es stellt Content – in Form von Markdown-Dateien in einem Git-Repository – als Webserver zur Verfügung. Der Unikernel beinhaltet neben einem Webserver, sprich einem kompletten TCP/IP-Stack, einer HTTP-Implementierung und einer TLS-Bibliothek auch eine Git-Implementierung, die dazu benutzt wird, das über Boot-Parameter angegebene Repository in den Speicher zu klonen. Das Git-Repository enthält auch Konfigurationsinformationen (Name des Blogs, UUID, Startseite, Stylesheet). Um einen neuen Artikel einzupflegen, wird dieser in das Git-Repository *committed* und Canopy erhält eine spezielle HTTP-Anfrage, bei der Canopy das in den Speicher geklonte Git-Repository vom Server updatet. Berechtigungen, wer neue Artikel hinzufügen oder modifizieren darf, sind durch den Git-Server geregelt und nicht Teil von Canopy. Web-Feeds (Atom und RSS) werden von Canopy automatisch erzeugt und benutzen die Zeitstempel (*erstellt* und *letzte Änderung*) und Informationen zum Autor aus dem Git-Repository. Das Image der virtuellen Maschine ist 8 MB groß, beinhaltet die oben genannten Protokolle und kann auf verschiedenen Hypervisoren ausgeführt werden. Canopy benutzt keinen persistenten Speicher, sondern nur Arbeitsspeicher (etwa 20 MB plus die Größe des Git-Repositories). Canopy braucht sonst an Systemressourcen nur eine virtuelle Netzwerkkarte. Kein USB, keine Tastatur, keinen Bildschirm. Logs können bei Bedarf via syslog an einen anderen Rechner gesendet werden. Mein Blog (*https://hannes.nqsb.io*) benutzt Canopy, aber auch andere Seiten benutzen Canopy (*http://canopy.mirage.io*, *http://robur.io*).

Andere Beispiele sind ein autoritativer DNS-Server, ein DNS-Resolver, DHCP-Server, verschiedenste Webseiten, eine Firewall für QubesOS, ein Pong-Spiel im Qubes oder SDL-Framebuffer, und weitere, die gerade aktiv entwickelt werden.

Schlussfolgerung

Unikernels – neben MirageOS gibt es andere in anderen Programmiersprachen – sind schlanker als traditionelle Unix-Betriebssysteme. Durch die Reduktion der Trusted Code Base und durch die Verwendung einer Hochsprache sind sowohl die Angriffsfläche als auch die Menge der Angriffsvektoren minimiert. Da schon zur Compile-Zeit die benötigten Bibliotheken ausgewählt werden, ist die Komplexität eines Unikernels geringer als die traditioneller Multifunktionsbetriebssysteme. Daher ist der Betrieb eines Unikernels einfacher und robuster. Die Performance ist gleichauf mit anderen Implementierungen: unsere TLS-Implementierung erreicht bis zu 85 % der Geschwindigkeit von OpenSSL.[3]

Die Community um MirageOS wächst stetig, ist offen und hilfsbereit gegenüber Neueinsteigenden. Die Anwendungsfälle für Unikernels sind vielfältig, von Desktop-Anwendungen über digitale Infrastruktur und Webservices, bis hin zu robusten Services als Internet der Dinge. Mein Ziel mit MirageOS ist es, mehr Menschen zu ermöglichen, ihre eigene digitale Infrastruktur zu betreiben und damit Kontrolle über die eigenen persönlichen Daten zu bekommen. Es ist noch ein langer Weg. Viele Grundlagen sind bereits vorhanden, aber andere Bibliotheken fehlen noch – wie automatisierte verschlüsselte Backups, verteilt auf mehrere Computer.

Falls MirageOS Interesse geweckt hat, gibt es mehr Information auf *https://mirage.io*, auch dazu, welche Kommunikationskanäle die Community verwendet.

Anmerkungen und Referenzen

1 *Vortragsaufzeichnung unter fiff.de/r/181024, Folien fiff.de/r/181030*

2 *Siehe Madhavapeddy A, Scott DJ (2013) Unikernels; Rise of the virtual library operating system. CACM 57(1):61–69, doi:10.1145/2541883.2541895, sowie ACM Queue 11(11). http://queue.acm.org/detail.cfm?id=2566628*

3 *Siehe Kaloper-Meršinjak D, Mehnert H, Madhavapeddy A, Sewell P (2015) Not-quite-so-broken TLS; Lessons in re-engineering a security protocol specification and implementation. 24th USENIX Security Symposium (USENIX Security '15). USENIX Association, Washington, D.C., S 223–238. https://usenix15.nqsb.io/*

4 *Mehnert H, Ohlig J, Schirmer S (2013) Das Curry-Buch; Funktional programmieren lernen mit JavaScript. O'Reilly, Beijing*

Hannes Mehnert

Hannes Mehnert, PhD, forscht in mehreren Richtungen, von Programmiersprachen (Typsysteme, Visualisierungen von Compiler-Optimierungen) über funktionale Korrektheitsbeweise von objektorientierten Programmen, IDEs für abhängig typisierte Sprachen bis hin zu Netzwerk- und Sicherheitsprotokollen (TCP/IP, TLS, OTR). Er ist Co-Autor eines Buches über indische Küche und funktionale Programmierung in JavaScript.[4] Seit 2014 arbeitet er an MirageOS mit, von 2014 bis 2017 als PostDoc an der University of Cambridge, UK, seit 2018 bei einer gemeinnützigen GmbH in Berlin (*http://robur.io*). In seiner Freizeit ist Hannes nicht nur ein Hacker, sondern auch Barista. Er reist gern mit seinem Liegerad und repariert es auch selbst.

Lutz Hasse

Vertrauen – Fortschritt – Kontrolle[1]

Ein funktionierendes rechtliches System zum faktischen Garantieren des Datenschutzes für die Bürger eines Staats kann einen Zuwachs an Vertrauen gegenüber staatlichen Autoritäten bewirken. Versagt das System jedoch, verkehrt sich dieser Effekt ins Negative. Wie steht die Bundesrepublik Deutschland diesbezüglich derzeit da? Was wurde bereits erreicht? Was ist noch zu tun? Welche prinzipiellen Gefahren drohen dem Grundrecht auf informationelle Selbstbestimmung?

Was schafft Vertrauen bei Bürgern?

Lassen Sie mich zunächst mit einigen problematischen Beispielen beginnen, die veranschaulichen, wie es nicht gemacht werden sollte: Die zwischenstaatlichen Abkommen zum grenzüberschreitenden Datentransfer *Safe Harbor* und *Privacy Shield* tragen vielversprechende Namen, schaffen aber nur scheinbar Vertrauen. Denn diese Verträge leisten datenschutzrechtlich nicht, was die Bürger von ihnen erwarten, und sind überdies mit geltendem europäischem Recht nicht vereinbar. *Safe Harbor*, ein Abkommen zum sicheren Datentransfer zwischen EU und USA nach Art. 25 Abs. 6 der EU Datenschutzrichtlinie, wurde deshalb am 6. Oktober 2015 vom EuGH wieder aufgehoben. Und auch gegen das Nachfolge-Abkommen *Privacy Shield* wird bereits gerichtlich vorgegangen, das wird nach meinem Dafürhalten höchstens noch zwei Jahre halten. Zwar fordert die Wirtschaft derartige Instrumentarien, damit der Eindruck erweckt wird, Daten könnten rechtskonform in die USA übermittelt werden. Auf lange Sicht sind solche Systeme aber kontraproduktiv, weil ihr Zusammenbruch voraussehbar ist und dann zu einem tiefsitzenden Vertrauensverlust bei den Bürgern führt.[2]

Kurz noch ein anderes zwiespältiges Szenario: Viele Online-Handelsplattformen stellen Bewertungssysteme zur Verfügung, die Vertrauen bei zukünftigen Käufern schaffen sollen. Die Anzahl der *Sternchen* misst angeblich die Zufriedenheit anderer Käufer des Produkts und soll so eine schnelle Kaufentscheidung begünstigen. Aber kann man sich auf ein derartiges System auch verlassen?

Was schafft nun wirklich nachhaltig Vertrauen? Dies sind zunächst einmal tragfähige und für den Bürger verständliche Rechtsgrundlagen. Zu nennen ist hier vor allem das *Grundrecht auf informationelle Selbstbestimmung,* das ich seit meiner Wahl vor mehr als sechs Jahren täglich gegen seine immer schneller voranschreitende Entwertung verteidige.

Der Durchsetzung dieses Grundrechts dienen sollen u. a. das *Bundesdatenschutzgesetz* (in neuer Fassung) und die (teilweise noch zu novellierenden) *Datenschutzgesetze der Länder* sowie die ab dem 25. Mai 2018 unmittelbar und EU-weit geltende *Datenschutz-Grundverordnung (DS-GVO),* die nach Meinung des EuGH auch Anwendungsvorrang vor den entsprechenden nationalen Normen besitzt. Der *Verständlichkeit* der DS-GVO abträglich sind jedoch von ihr verwendete *unbestimmte Rechtsbegriffe,* die zunächst von den Aufsichtsbehörden, und mit ziemlicher Sicherheit dann auch von Gerichten, konkret auszulegen sind. Dies ist nicht ungewöhnlich für neue rechtliche Normen, aber es wird Jahre bis Jahrzehnte dauern, hier einigermaßen Klarheit zu schaffen.[3]

Noch problematischer sind zahlreiche Öffnungsklauseln in der Datenschutz-Grundverordnung; das sind quasi bewusste Gesetzeslücken, die es dem nationalen Gesetzgeber ermöglichen, eigene Regelungen zu treffen.[4]

Eine prinzipiell vertrauensbildende Maßnahme im elektronischen Geschäftsverkehr sind *Datenschutzerklärungen.* Doch während die DS-GVO für das Ersuchen um Einwilligung ausdrücklich eine verständliche und leicht zugängliche Form in einer klaren und einfachen Sprache vorschreibt, trifft auf die Belehrungen gerade durch große bekannte Unternehmen eher das Gegenteil zu. Derartige Intransparenz, gleichfalls durch lange AGB mit schwammigen Formulierungen, die mitunter wöchentlich geändert werden, ist keinesfalls Ungeschicklichkeit, sondern beabsichtigt: Wir sollen gar nicht genau verstehen, was wir da unterschreiben und welche Verwendung unserer Daten wir damit erlauben!

Für aussichtsreich, um Vertrauen zu gewinnen, halte ich dagegen u. a. folgende Ansätze:[5] Gütesiegel durch unabhängige (!) Prüfer, zuverlässige Verschlüsselung im Browser und in mobilen Netzen, ISO-Normen und nicht zuletzt ein leistungsfähiges Transparenzgesetz, wie es in Thüringen demnächst verabschiedet werden soll.[6]

Fortschritt

Ohne Quellenrecherche, belastbare Aussagen etc. ist die fundierte Beurteilung einer Aussage (und damit das Vertrauen in diese) nicht möglich. Was fehlt also? Das Wissen um Fakten … im Zeitalter der sozialen Medien nicht einfach zu erlangen. Bildung ist also eine zentrale Vertrauenskomponente, und die gute Nachricht ist: Schon ein bisschen Bildung hilft! Grundlagen können in der Bildung einfach vermittelt werden, durch ein Grundverständnis wächst auch Vertrauen.

Medienbildung und Informatikunterricht könnten das notwendige Wissen vermitteln.[7] Laut der ICILS-Studie 2013[8] hat Deutschland im Bereich der computer- und informationsbezogenen Kompetenzen international aber einen erheblichen Rückstand aufzuholen.[9] Die Strategie der Kultusministerkonferenz (KMK) *Bildung in der digitalen Welt* vom Dezember 2016 thematisiert das[10] und setzt dabei auf einen integrativen Ansatz zum Erreichen digitaler Medienkompetenz: Statt in einem neuen, eigenen Fach werden entsprechende Inhalte in jedem der vorhandenen Fächer geeignet gelehrt.[11]

Ohne Prüfungsrelevanz, mit teilweise sehr abstrakten Kompetenzbeschreibungen im Kursplan und inhaltlich wie auch vom Umfang her stark abhängig von schulinterner Planung, bleibt

die Wirkung bisher jedoch beschränkt. Zudem werden Fachlehrer nicht grundständig auf diese Aufgabe vorbereitet und generell fehlen Lehrkräfte für das Schulfach Informatik. Immerhin bekennt sich die KMK in Übereinstimmung mit der ICILS-Studie zur Herausforderung, die Schulen anforderungsgerecht auszustatten und die Lehrerausbildung im Bereich des Studiums, des Referendariats und der Fortbildung anzupassen. Richtungsweisend verfolgt die Medienbildung in der Thüringer Schule einen bildungsgangübergreifenden Ansatz, inhaltlich werden auch Recht, Datensicherheit und Jugendmedienschutz berührt.[12]

Die Auswirkungen fehlender Bildung und dadurch bedingten unberechtigten Vertrauens sind vielfältig und gerade für die digitale Lebenswelt von Kindern und Jugendlichen gravierend.[13] Dazu gehören Cybermobbing, Umgehung der Altersverifikation für Medieninhalte, Verstöße gegen das Urheberrecht, unbedarfte Preisgabe persönlicher Daten bis hin zu freizügigen Fotos. Nicht alles ist da vermeidbar, aber Aufklärung zu richtigem Umgang auf jeden Fall dringend geboten. Die Landesdatenschutzbehörden stellen hierfür umfangreiches Material kostenlos zur Verfügung.[14]

Kontrolle – Die Möglichkeiten der Aufsichtsbehörden

Das Grundrecht auf informationelle Selbstbestimmung gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Und unter den Bedingungen der automatischen Datenverarbeitung gibt es kein belangloses Datum mehr, sagt das Bundesverfassungsgericht. Auch, dass dieses Grundrecht in der Menschenwürde wurzelt. Die Menschenwürde zu schützen, ist Aufgabe aller staatlichen Gewalt, so steht es im Grundgesetz. Leider kann ich nicht erkennen, dass unser Staat bemüht ist, einen tatsächlichen, einen wirksamen Schutz dieses Grundrechts zu garantieren. Stattdessen sagt (nicht nur) unsere Bundeskanzlerin, Daten seien der Rohstoff der Zukunft, und verklärt dazu passend in zeitgemäßem Neusprech die Aushöhlung effektiven Datenschutzes als „Datenreichtum".

Wie das beispielsweise praktisch gehandhabt werden soll, zeigt der Vorschlag[15] des Bundesministeriums für Verkehr und digitale Infrastruktur. In einem „Datengesetz" soll geregelt werden, dass derjenige, als dessen „Verdienst" die Generierung von Daten anzusehen ist (im Automobil wäre das beispielsweise der Hersteller des Fahrzeugs), die Verfügungsgewalt über diese Daten erhält. Er (!) ist der „Dateneigentümer". Und wenn das so klappt, sollen als nächstes sogar Gesundheitsdaten an die Reihe kommen.[16] Deutlich wird hier, dass die Politik den Weg frei machen soll für eine ungehinderte Datenverwertung durch die Wirtschaft.

Trotz der beschriebenen Unzulänglichkeiten stellen die Datenschutz-Grundverordnung und die nachrangige nationale Gesetzgebung eine Reihe von Kontrollrechten für die Betroffenen zur Verfügung, die auch mittels der Aufsichtsbehörden ausgeübt werden können. Es kommt nun darauf an, noch bestehende nationale Freiräume klug für den Datenschutz zu nutzen und ggf. Fehlentscheidungen der Vergangenheit rückgängig zu machen. Landes- und Bundesdatenschützer sind auch in dieser Hinsicht verlässliche Partner der Bürgerinnen und Bürger und bürgerrechtlich orientierter Organisationen und Bewegungen.

Fazit

Die Politik sollte sich rasch von dem Konstrukt des „Datenreichtums" verabschieden und wieder zu einem nachhaltigen Schutz des Grundrechts auf informationelle Selbstbestimmung zurückkehren. Andernfalls riskiert sie, bei den Bürgern weiteres Vertrauen zu verspielen.

Anmerkungen und Referenzen

1 *Siehe vertiefend den gleichnamigen Vortrag auf der FIfF-Konferenz 2017, Video unter fiff.de/r/181007, Vortragsfolien fiff.de/r/181008*
2 *Vertiefung: Vortragsfolien fiff.de/r/181010, Vortragsvideo fiff.de/r/181009*
3 *Vertiefung: Vortragsvideo fiff.de/r/181011*
4 *Vertiefung: Vortragsfolien fiff.de/r/181012, Vortragsvideo fiff.de/r/181013*
5 *Vertiefung: Vortragsfolien fiff.de/r/181014*
6 *Vertiefung: Vortragsfolien fiff.de/r/181016, Vortragsvideo fiff.de/r/181015*
7 *Vertiefung: Vortragsfolien fiff.de/r/181017, Vortragsvideo fiff.de/r/181018*
8 *International Computer and Information Literacy Study, 2013, https://www.waxmann.com/fileadmin/media/zusatztexte/ICILS_2013_Berichtsband.pdf*
9 *Vertiefung: Vortragsfolien fiff.de/r/181019*
10 *Strategie der Kultusministerkonferenz Bildung in der digitalen Welt, Dezember 2016, https://www.kmk.org/fileadmin/Dateien/pdf/PresseUndAktuelles/2016/Bildung_digitale_Welt_Webversion.pdf*
11 *Vertiefung: Vortragsfolien fiff.de/r/181020*

Lutz Hasse

Dr. **Lutz Hasse** legte die Juristischen Staatsexamina in Niedersachsen ab. Es folgten Assistenzen an der Universität Osnabrück und ab 1992 an der Friedrich-Schiller-Universität Jena. Die Promotion erfolgte während der „Jenenser Phase" an der Universität Osnabrück. Anschließend erfolgte der Wechsel zur Thüringer Verwaltungsfachhochschule – Fachbereich Polizei; dort wurde er Leiter der Rechtsausbildung. Nach Tätigkeiten als Referatsleiter im Thüringer Innenministerium, beim Thüringer Landesbeauftragten für den Datenschutz und im Thüringer Sozialministerium wurde er 2012 und 2018 vom Thüringer Landtag zum Landesbeauftragten für den Datenschutz und die Informationsfreiheit gewählt.

12 *Vertiefung: Vortragsfolien fiff.de/r/181021*

13 *Vertiefung: Vortragsfolien fiff.de/r/181022*

14 *Beispielsweise die Broschüre Digitale Selbstverteidigung des TLfDI, https://www.tlfdi.de/mam/tlfdi/wir-ueber-uns/digitale_selbstverteidigung_broschuere_4web2018.pdf. Vgl. auch die Übersichten auf den Vortragsfolien fiff.de/r/181023. Besonders empfohlen sei das Jugendportal youngdata der unabhängigen Datenschutzbehörden des Bundes und der Länder, sowie des Kantons Zürich, https://www.youngdata.de/.*

15 *Studie „Eigentumsordnung" für Mobilitätsdaten?, http://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile*

16 *Vgl. a. a. O., S. 119f.*

Thomas Gruber

Die Marschrichtung im Cyber- und Informationsraum

Im April 2017 wurde das neue Kommando Cyber- und Informationsraum (CIR) *am Standort Bonn aufgestellt. Mit ihm existiert nun die Führungsstruktur für den militärischen Bereich Cyber- und Informationsraum, der voraussichtlich 2021 personell vervollständigt wird. Knapp 14.000 SoldatInnen sollen dann an verschiedenen deutschen Standorten arbeiten, bisher sind es etwa 12.500. Die Bundeswehr muss sich innerhalb kurzer Zeit um mehr als 1.000 IT-Fachkräfte, bevorzugt mit militärischer Ausbildung, bemühen – keine leichte Aufgabe.*

Doch auch ohne die volle Truppenstärke ist der neue Organisationsbereich bereits einsatzfähig: Zum Großteil wurden bereits bestehende Kommandos und deren untergeordnete Bataillone dem Kommando CIR unterstellt. In den Arbeitsbereich CIR fallen nun beispielsweise die psychologische Kriegsführung *(Zentrum Operative Kommunikation der Bundeswehr)*, die Störung feindlicher und Sicherung eigener Kommunikationsnetze *(Bataillone Elektronische Kampfführung)*, die Vernetzung und technische Ausstattung der Kriegseinheiten *(Kommando Informationstechnik der Bundeswehr)* sowie Angriff und Verteidigung im Cyberraum (*Computer Netzwerk Operationen*, bald: *Zentrum Cyberoperationen*).

Die genaue Struktur des neuen Organisationsbereichs und die Zielsetzung der Bundeswehr im Cyber- und Informationsraum sind unter anderem dem Abschlussbericht *Aufbaustab Cyber- und Informationsraum*[1], der *Strategischen Leitlinie Cyber-Verteidigung* des Bundesministeriums der Verteidigung (BMVg)[2] und dem *Weißbuch der Bundeswehr 2016*[3] zu entnehmen. Einen kurzen Überblick geben beispielsweise die Artikel *Es cybert bei der Bundeswehr*[4] und *Onlineoffensive*[5]. Jene thematischen Umrisse sollen im Folgenden um einige Gedanken zur deutschen Strategie im Cyber- und Informationsraum ergänzt werden, die während der FIfFKon 2017 angeregt wurden.[6]

Werbung, Wirkung, Widerstand

Die Aussetzung der Wehrpflicht ab dem Jahr 2011 beschränkt die Bundeswehr in ihrer wichtigsten Ressource: SoldatInnen. Gleichzeitig steigt die Zahl der deutschen Kriegseinsätze und damit auch der benötigten Truppenkontingente. In diese Zeit fällt nun noch der Aufbau des neuen Cyberkommandos – der Personalmangel ist programmiert. Das Gegenmittel der Wahl ist für das BMVg großflächige, bundesweite, zielgruppenorientierte Werbung. Von der Plakatkampagne „Mach, was wirklich zählt" über Werbeveranstaltungen in Schulen, auf Jobmessen und in Arbeitsagenturen bis zu YouTube-Serien („Die Rekruten", „Mali") – die Bundeswehr ist inzwischen omnipräsent. Zunehmend versucht sie dabei auch „Erstkontakt" zu jungen Menschen noch weit jenseits des Rekrutierungsalters aufzunehmen: Eigene Websites für Jugendliche, Werbung in Jugendmagazinen, gezielte Postsendungen, Abenteuercamps und vieles, vieles mehr. Etwa 35 Millionen Euro kostet die Nachwuchswerbung für das deutsche Militär jährlich. Immer dabei: Ein starker Fokus auf den neuen Organisationsbereich CIR. So macht beispielsweise das *Projekt Digitale Kräfte* zur Gewinnung von IT-Fachpersonal gut ein Viertel der Kosten der gesamten „Mach, was wirklich zählt"-Kampagne aus; in den vergangenen Jahren war die Bundeswehr wiederholt auf der Computerspiele-Messe *gamescom* mit einem Stand vertreten, 2017 sogar mit einer eigenen *Challenge-App* für Mobilgeräte; und im Rahmen der sogenannten *Cyber-Days* und eines *IT-Camps* gab es neben einer möglichst spannenden Übung und Lagerleben auch noch eine abschließende LAN-Party für die TeilnehmerInnen.

Die Werbeoffensive der Bundeswehr hat in den letzten Jahren durchaus Wirkung erzielt. 2017 vermeldete das Verteidigungsministerium begeistert, dass es „im Sendezeitraum der Serie *Die Rekruten* […] 40 Prozent mehr Zugriffe auf die Karriere-Website, ein Viertel mehr Anrufe bei der Karriere-Hotline und 21 Prozent mehr Bewerbungen bei Mannschaften und Unteroffizieren"[7]gab. Auch danach stieg das Interesse am SoldatInnenberuf weiter: Im ersten Halbjahr 2017 gab es beim deutschen Militär fast so viele Einstellungen wie im ganzen Jahr 2016.[8] Die *Castenow*-Werbeagentur, welche den Auftrag des Verteidigungsministeriums bekommen hat, erhält seitdem einen Preis der Werbebranche nach dem anderen.[9]

Die Sprüche (wie „Deutschlands Freiheit wird auch im Cyberraum verteidigt" und „Wir kämpfen auch dafür, dass du gegen uns sein kannst") und die Maßnahmen der Nachwuchswerbung sind oftmals sehr forsch bis provokativ – und das ist ohne Frage auch Kal-

Abbildung 1: Kind mit Waffe am Tag der Bundeswehr 2016 in Stetten am kalten Markt (Quelle: DFG-VK)[10,11]

kül, um die Bundeswehr wieder mehr zum öffentlichen Gesprächsthema zu machen. Allerdings hat dies in den letzten Jahren auch vermehrt zu Diskurs und Widerstand geführt, den sich das Verteidigungsministerium keineswegs so gewünscht haben dürfte. Nach dem *Tag der Bundeswehr 2016* gingen Fotos durch die Presse, auf denen Kinder – teilweise vermutlich noch im Grundschulalter – mit Handfeuerwaffen (siehe Abbildung 1) und auf Panzern zu sehen sind; die Kampagne *Schulfrei für die Bundeswehr* begleitet seit 2010 den Einsatz von Jugendoffizieren an deutschen Schulen mit vielfältigem Protest; Bundeswehrplakate werden regelmäßig zerstört oder kreativ umgestaltet (siehe Abbildung 2); wiederholt brandet die Diskussion darüber auf, ob die Bundeswehr mit jährlich über 1.000 rekrutierten Minderjährigen gegen die UN-Kinderrechtskonvention verstoße; und vieles mehr. Gerade der Anschein von Spiel und Spaß, den die Bundeswehr auch bei der Anwerbung von IT-Fachkräften für den CIR vermitteln will, und der krasse Gegensatz des tatsächlichen militärischen Wirkens heizen die öffentliche Diskussion derzeit immer wieder an.

Vom Besetzen des zivilen virtuellen Raumes zum Einsatz im Inneren

Der Angriff auf feindliche Computernetzwerke und die Verteidigung der eigenen im Auslandseinsatz ist eine Aufgabe des Organisationsbereichs CIR, viele weitere Arbeitsgebiete liegen allerdings im zivilen virtuellen Raum – vornehmlich auch im Inland. Zu Beginn der Diskussion um eine deutsche Cybertruppe dienten Wirtschaftskriminalität und zwischenstaatliche Spionage als häufig bemühte Motivationsquellen für eine militärische Aufrüstung des virtuellen Raumes. Zunächst konnten jene Ideen noch mit PR-Taktik verwechselt werden – die Bundeswehr als Retterin und Beschützerin der BürgerInnen und der deutschen Wirtschaft. Doch inzwischen wird immer klarer sichtbar, dass das Bedrohungsszenario *Cyberkrieg* auch hervorragend geeignet ist, das heftig umstrittene Konzept eines Inlandseinsatzes der Bundeswehr salonfähiger zu machen. Zumindest zeigen die verschiedenen Strategiedokumente zum CIR, dass der zivile virtuelle Raum zukünftig stärker militärisch durchdrungen und besetzt werden soll[12]: Das BMVg warnt vor „Bedrohungen im Cyber- und Informationsraum", wie etwa dem „Diebstahl und Missbrauch persönlicher Daten oder […] der Wirtschaftsspionage". „Eine besondere Herausforderung" ist weiter die feindliche „Nutzung der digitalen Kommunikation zur Beeinflussung der öffentlichen Meinung", beispielsweise „in sozialen Netzwerken" oder „auf Nachrichtenportalen". In der logischen Konsequenz erklärt das Verteidigungsministerium den Cyber- und Informationsraum neben „Land, Luft, See und Weltraum" zu einem neuen militärischen „Operationsraum"[13]. Die somit beschworene Bedrohungslage, gepaart mit der Definition eines fünften Schlachtfeldes, führt zu einem breiten Aufgabenspektrum für die junge Cybereinheit[14]: Neben dem Schutz der eigenen IT-Systeme und Angriffen auf feindliche Computer- und Kommunikationsnetzwerke soll die Bundeswehr in Zukunft auch zivile kritische IT-Infrastruktur schützen, mit den eigenen Informationen zu einem „gesamtstaatlichen Lagebild" beitragen und „an der Meinungsbildung im Informationsumfeld der Interessensgebiete der Bundeswehr" teilhaben. Das Wort *gesamtstaatlich* scheint sich beim BMVg größter Beliebtheit zu erfreuen. Es ermöglicht, die Bundeswehr in Fragen der zivilen Sicherheit neben Polizeien und Geheimdienste zu stellen und künftige Einsätze bei innerstaatlichen Gefahrenlagen zu rechtfertigen.

Abbildung 2: Beispiel für Adbusting, Bild aus „Was ist Adbusting?" https://sozialrevolutionaere-aktion.com/2018/02/22/was-ist-adbusting

Parlamentsvorbehalt, Solidaritätsklausel, Bündnisfall

Ein weiteres Hauptaugenmerk in Militärstrategien zum Cyber- und Informationsraum liegt auf der Einordnung militärischer Aktionen in die aktuelle Rechts- und Bündnislage. Denn zumindest auf dem Papier gibt es mehr oder minder strikte Voraussetzungen für den Einsatz militärischer Gewalt – so auch bei Angriffen auf Computer- und Kommunikationsnetzwerke. Auf bundesdeutscher Ebene gilt bei Auslandseinsätzen der Bundeswehr der Parlamentsvorbehalt, das heißt, ein deutscher Kriegseinsatz ist nur zulässig[15], wenn der Bundestag dem zustimmt. Nun sollte dies, wenn der Cyber- und Informationsraum schon als neues Schlachtfeld deklariert wird, selbstverständlich auch für den Bundeswehreinsatz im virtuellen Raum gelten. Und in der Tat spricht Katrin Suder, Staatssekretärin des BMVg, davon, dass ein Militäreinsatz im CIR ebenso wie jeder andere vom Bundestag abgesegnet werden müsse.[16] Das ist geschickt formuliert, denn für die zwei derzeit wahrscheinlichsten Angriffsszenarien wird es eben keine gesonderte parlamentarische Entscheidung geben: Entweder werden offensive Aktionen im CIR (so wie es auch aktuell der Fall ist) als Teil eines Auslandseinsatzes deklariert – die Entscheidung des Bundestages über den Gesamteinsatz rechtfertigt damit die militärischen Aktionen im virtuellen Raum. Oder die Bundesregierung ordnet mit der Begründung der Selbstverteidigung oder sonstiger Schutzmaßnahmen einen Cyberangriff an, mit dem Hinweis, dass „Gefahr im Verzug"[17] – für eine Abstimmung im Parlament also keine Zeit – sei.

Eine äußerst wichtige Rolle spielt die Idee des Cyberkrieges auch in westlichen Bündnisstrukturen wie der EU und der NATO. Denn zum einen kann innerhalb der Bündnisse eine allgegenwärtige Bedrohungslage durch angebliche Cyberangriffe aus Russland, China oder durch terroristische Gruppen heraufbeschworen werden, zum anderen hilft das Konzept der Cyberabwehr auch dabei, die rechtliche Schwelle zum Kriegseinsatz zu senken. Besonders deutlich wird dies beispielsweise in der Diskussion um das Vorgehen zur Bündnisverteidigung. Im Falle der NATO betrifft dies den *Bündnisfall* (Art. 5 des Nordatlantikvertrages), in der EU die *Beistandsklausel* (in Art. 42.7 des EU-Vertrages) sowie die *Solidaritätsklausel* (Art. 222 AEUV). Sie alle legitimieren den Einsatz militärischer Mittel von Einzelstaaten zum Zwecke der Verteidigung eines militärisch angegriffenen oder schwer bedrohten

Bündnispartners. Und was vor dem Konzept des Cyberkrieges noch eine vergleichsweise hohe Hürde war, könnte in Zukunft bei Bedarf sehr viel leichter werden. Denn sowohl in Stellungnahmen des EU-Parlaments als auch aus NATO-Kreisen wird immer wieder vernommen, dass die Beistandsverpflichtungen auch im Falle von Cyberangriffen zur Anwendung kommen sollen.[18] Im Extremfall könnte eine Hacking-Attacke damit einen bündnisweiten Kriegseinsatz (auch mit *konventionellen* Waffen) rechtfertigen. Angesichts der Tatsache, dass Polizeien, Sicherheitsfirmen und Militär jährlich zahlreiche Cyberangriffe auf westliche Verwaltungs-, Regierungs- und Sicherheitseinrichtungen verzeichnen, bergen solche Aussagen enormes Eskalationspotential.

Anmerkungen und Referenzen

1 *Abschlussbericht Aufbaustab Cyber- und Informationsraum, http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf, 3.1.2018.*
2 *Geheime Cyber-Leitlinie: Verteidigungsministerium erlaubt Bundeswehr „Cyberwar" und offensive digitale Angriffe, https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/, 3.1.2018.*
3 *Weißbuch der Bundeswehr 2016, https://www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf, 3.1.2018.*
4 *Es cybert bei der Bundeswehr: Digitales Aufrüsten um jeden Preis mit Gamern und Nerds, https://netzpolitik.org/2016/es-cybert-bei-der-bundeswehr-digitales-aufruesten-um-jeden-preis-mit-gamern-und-nerds/, 3.1.2018.*
5 *Onlineoffensive: Die Bundeswehr im Cyber- und Informationsraum, FIfF-Kommunikation 2/2017, S. 69–71. Abrufbar auch unter: http://www.imi-online.de/2017/04/03/onlineoffensive-die-bundeswehr-im-cyber-und-informationsraum/, 4.1.2018.*
6 *Vortrag „Die Bundeswehr im Cyber- und Informationsraum", FIfFKon 2017, Video fiff.de/r/181031, Vortragsfolien fiff.de/r/181032.*
7 *Werde Soldat, yo!, http://www.zeit.de/politik/deutschland/2017-10/bundeswehr-exclusive-mali-youtube-serie-die-rekruten, 4.1.2018.*
8 *Bewerber-Boom bei der Bundeswehr, http://www.rp-online.de/politik/deutschland/nach-rekruten-werbung-bewerber-boom-bei-der-bundeswehr-aid-1.7034502, 4.1.2018.*
9 *Castenow News, https://www.castenow.de/news/, 4.1.2018.*
10 *Grenze überschritten: Bundeswehr ließ Kinder an Handfeuerwaffen, PM DFG-VK und Netzwerk Friedenskooperative, Stuttgart, 13. Juni 2016, https://www.dfg-vk.de/unsere-themen/anti-militarisierung/grenze-ueberschritten-bundeswehr-liess-kinder-an-handfeuerwaffen.*
11 *Foto: https://www.dropbox.com/sh/nehz7aa5nim25t5/AADmEbzMW4wwP4tqN-5Kk2ita?dl=0*
12 *Weißbuch der Bundeswehr 2016, S. 36–38.*
13 *Geheime Cyber-Leitlinie: Verteidigungsministerium erlaubt Bundeswehr „Cyberwar" und offensive digitale Angriffe.*
14 *Abschlussbericht Aufbaustab Cyber- und Informationsraum, S. 13.*
15 *„Zulässig" nach Auffassung der deutschen Regierungen der letzten knapp 20 Jahre. Mithilfe der dabei hartnäckig ignorierten Regelungen im Zwei-plus-Vier-Vertrag (dass von deutschem Boden nur noch Frieden ausgehen darf), der Präambel des Grundgesetzes (Verpflichtung der BRD, dem Frieden der Welt zu dienen) und dem internationalen Völkerrecht (Verbrechen der Aggression) ließe sich durchaus eine grundsätzliche Unzulässigkeit deutscher Auslandseinsätze rechtfertigen.*
16 *Mandatierung, Attribution und offensive Fähigkeiten? Anhörung zur Bundeswehr im „Cyberraum", https://netzpolitik.org/2016/mandatierung-attribution-und-offensive-faehigkeiten-der-verteidigungsausschuss-zur-bundeswehr-im-cyberraum/, 5.2.2018.*
17 *Zur Reichweite des Parlamentsvorbehalts für Streitkräfteeinsätze bei Gefahr im Verzug, https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2015/bvg15-071.html, 5.2.2018.*
18 *Entschließung des Europäischen Parlaments vom 22. November 2012 zu den EU-Klauseln über die gegenseitige Verteidigung und Solidarität: politische und operationelle Dimensionen, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0456&language=DE&ring=A7-2012-0356, 5.2.2018; „Cyberangriffe können Bündnisfall nach Artikel 5 auslösen", https://www.welt.de/politik/article161307855/Cyberangriffe-koennen-Buendnisfall-nach-Artikel-5-ausloesen.html, 5.2.2018.*

Informationsstelle Militarisierung auf der FIfFKon 2017

Die Informationsstelle Militarisierung (IMI) arbeitet seit über 20 Jahren in einem breiten Spektrum friedenspolitischer und antimilitaristischer Themen mit einem starken Fokus auf Deutschland, die EU und die NATO. Wir veröffentlichen Analysen und Studien, stellen RednerInnen auf Demonstrationen, ReferentInnen für Konferenzen und veranstalten jährlich einen Kongress in Tübingen.

In den letzten Jahren haben sich dabei wiederholt Kooperationsmöglichkeiten mit dem FIfF ergeben, die unsere politische Arbeit sehr bereichert haben. Die zunehmende Automatisierung und Algorithmisierung der Kriegsführung sowie ein starkes Drängen militärischer AkteurInnen in den Cyber- und Informationsraum bieten derzeit viele gemeinsame Anknüpfungspunkte. Auch 2017 gab es wieder regen Austausch zwischen FIfF und IMI: etwa über gegenseitig abgedruckte Texte, einen Vortrag des FIfF-Vorstandes Hans-Jörg Kreowski auf dem IMI-Kongress 2017 und einen IMI-Vortrag auf der FIfFKon 2017. Auch war IMI dort Gast am Informationsstand des FIfF.

http://www.imi-online.de *Thomas Gruber, IMI-Beirat*

Thomas Gruber

Thomas Gruber ist Mathematiker und promoviert an der Universität Bremen zum Thema *Verquickung mathematischer und informationstechnologischer Forschung an deutschen Forschungseinrichtungen mit der modernen Kriegsführung*. Er ist Stipendiat der *Rosa-Luxemburg-Stiftung* und Mitglied der *Informationsstelle Militarisierung* (IMI) in Tübingen.

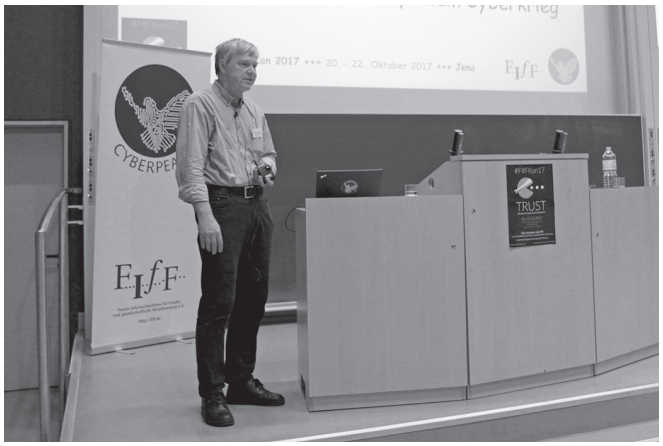
Hans-Jörg Kreowski

Die Cyberpeace-Kampagne des FIfF

Vergangenheit und Zukunft

Die Cyberpeace-Kampagne des FIfF ist recht gut dokumentiert, und es sind zahlreiche Publikationen entstanden, die einen guten Eindruck davon vermitteln, welche Ziele die Kampagne hat, welche Aktivitäten in ihrem Rahmen in den letzten fünf Jahren entfaltet worden sind. Der Rückblick auf die Kampagne, der im Vortrag auf der FIfFKon 2017 einen relativ breiten Raum einnahm, soll deshalb hier nicht noch einmal ausgeführt werden (Vortragsvideo unter fiff.de/r/181005, Vortragsfolien unter fiff.de/r/181006). Stattdessen will ich dafür werben und plädieren, dass sich viele besorgte Menschen an vielen Orten finden, um die Cyberpeace-Kampagne fortzuführen.

Auch wenn die Kampagne bisher schon als recht erfolgreich angesehen werden kann, was Veranstaltungen, Publikationen, Aktionen und die Verbreitung und Sichtbarkeit des Cyberpeace-Logos angeht, hat sie ihr eigentliches Ziel noch lange nicht erreicht. Einem Verbot von Cyberwaffen und einem friedlichen Internet sind wir nicht nähergekommen, und die Bedrohungen und Gefährdungen der zivilen Infrastrukturen sind enorm. Deshalb muss die Kampagne weitergehen. Und das heißt, mit allen verfügbaren Mitteln auf allen zugänglichen Ebenen für Cyberpeace einzutreten.



Hans-Jörg Kreowski erläutert die Cyberpeace-Kampagne des FIfF, Foto: Kai Nothdurft

In Bremen haben wir mit zwei Veranstaltungsformaten gute Erfahrungen gemacht, woran in diesem Jahr auch angeknüpft werden soll. Das kleine Format ist das Cyberpeace-Café – eine etwa zweistündige Veranstaltung mit einem längeren oder zwei kürzeren Vorträgen sowie möglichst viel Diskussion in einem passenden Ambiente, gern mit Kaffee und Kuchen o. ä. Das große Format ist das Cyberpeace-Forum – eine vier- bis sechsstündige Veranstaltung, z. B. verteilt auf Freitagabend und Samstagnachmittag oder ein Nachmittag und Abend, mit Podiumsdiskussion, kurzen Impulsvorträgen, Einführungsreferaten und auf jeden Fall Diskussionszeit. Thematisch bietet sich ein weites Spektrum von staatlicher Überwachung und der voranschreitenden Militarisierung der Gesellschaft über aktuelle Cyberattacken aller Art bis hin zu Cyberkrieg im engeren Sinne und der militärischen Nutzung von Informations- und Kommunikationstechnik überhaupt. Das Thema Cyberpeace als Gegenkonzept zum Cyberkrieg bietet die Chance, mit anderen Akteuren der Friedensbewegung zu kooperieren, ein großes Publikum weit über die Informatik hinaus anzusprechen und für möglichst viel öffentliche und mediale Aufmerksamkeit zu sorgen. Neben Vortragsveranstaltungen kann man natürlich auch Filmvorführungen, Infostände, Flashmobs oder Cyberpeace-Slams organisieren. Der Phantasie sind keine Grenzen gesetzt. Wenn vor allem zu Diskussion angeregt werden soll, bietet sich an, eingangs das fünfminütige Video *Cyberpeace statt Cyberwar* von Alexander Lehmann vorzuführen, das 2017 im Auftrag und mit Unterstützung des FIfF entstanden ist (*https://vimeo.com/216584485*, *https://www.youtube.com/watch?v=St955HBD-7k&feature=youtu.be*, *https://www.fiff.de/kurzfilm-cyberpeace-statt-cyberwar*).

Ausführliche Informationen zur Cyberpeace-Kampagne sind auf der Webseite *https://cyberpeace.fiff.de* zu finden. Und wer mehr zum Thema lesen möchte, wird u. a. hier fündig:

- Ute Bernhardt und Ingo Ruhmann (Hg.): Information Warfare und Informationsgesellschaft – Zivile und sicherheitspolitische Kosten des Informationskriegs, Dossier 74 als Beilage in Wissenschaft und Frieden 1/2014 und FIfF-Kommunikation 1/2014.

- Stefan Hügel, Hans-Jörg Kreowski und Dietrich Meyer-Ebrecht: Cyberwar and Cyberpeace. In: Handbook of Cyber-Democracy, Cyber-Development and Cyber-Defense, Springer, 2017, 25 Seiten.

- Sylvia Johnigk, Hans-Jörg Kreowski und Kai Nothdurft: Cyberwar – Schimäre oder reale Bedrohung? FIfF-Kommunikation 4/2014, S. 74–77.

- Dietrich Meyer-Ebrecht (Hg.): Kriegführung im Cyberspace, Dossier 79 als Beilage in Wissenschaft und Frieden 3/2015 und FIfF-Kommunikation 3/2015.

Hans-Jörg Kreowski

Hans-Jörg Kreowski ist Professor (i. R.) für *Theoretische Informatik* an der Universität Bremen und Vorstandsmitglied des *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung*. Neben seinen fachlichen Schwerpunkten hat er seit vielen Jahren auch immer wieder zur unheilvollen Verflechtung von Informatik und Rüstung in Wort und Schrift Stellung genommen.

FIfFKon-Splitter I

Was wäre eine Konferenz ohne Versorgung für das leibliche Wohl?! Die wurde für die FIfFKon 2017 rundum bestens gesichert vom Chileprojekt 2018 – Schülerinnen und Schüler der Klasse 10a des Christlichen Gymnasiums Jena, unterstützt von Eltern und der Spanisch-Lehrerin der Klasse. Jährlich reist eine Klasse, in der Spanisch unterrichtet wird, zu einer Partnerschule nach Chile, um die Situation dort hautnah kennen zu lernen – und natürlich auch, um sich einmal ausschließlich in Spanisch zu verständigen. Die nötigen Mittel für diese Reise verdienen die jungen Leute überwiegend durch Catering bei Veranstaltungen. Die FIfFKon 2017 lag da von der Zahl der Gäste zwar nur im Mittelfeld, stellte aber besondere Anforderungen an die Logistik, da sie über drei Tage lief.

Auch ohne Technik geht es schwerlich auf einem informatiklastigen Event. Glücklicherweise waren ein Absolvent und ein früherer wissenschaftlicher Mitarbeiter der Fakultät bereit, die Aufgaben eines „Technik-Managers" ohne Entlohnung zu übernehmen. Das FIfF führte nach Abschluss der FIfFKon 2017 mit einem der Technikverantwortlichen ein Interview, das nachfolgend gekürzt abgedruckt ist, und fragte beteiligte Schülerinnen und Schüler nach ihrem Eindruck – die Antworten sind in das Interview eingestreut.

FIfF: Herr Merker, Sie waren Technik-Manager auf der FIfFKon 2017 in Jena. Wie sehen Sie nachträglich die Dimension, die technische Herausforderung dieser Veranstaltung?

Rochus Merker: Ich habe schon größere Tagungen gemacht. Die Herausforderung hier war eher, Hardware an die Gegebenheiten der Uni anzupassen. Und es ging von Freitag bis Sonntag. Im Notfall hätten wir vielleicht Probleme bekommen, einen Techniker der Uni anzusprechen. Aber es war ja alles in Ordnung. Auch die Technik der Vortragenden hat gut funktioniert, und die meisten von denen wussten auch, was sie taten. Insofern war da nicht viel zu tun, am Anfang mal ein paar Kabel verlegen. Ich musste keine Unterstützung geben, einen zweiten Bildschirm aktivieren, oder so.

FIfF: Was sind denn die größten Ängste, die man als betreuender Techniker bei so einer Tagung hat?

Rochus Merker: Wo man in Sekundenschnelle Entscheidungen treffen, reagieren muss, sind Stromausfall oder Kabelbruch; egal, welches Kabel, ob Audio oder Video. Und Ausfälle des Internets. Dass mal ein Notebook abstürzt, ist nicht so schlimm, das ist man gewohnt. Neu starten, und alles geht wieder.

FIfF: Gibt es irgendeine Anekdote? Wo Sie sagen, das war jetzt aber unerwartet an irgendeiner Stelle, aber wir haben es trotzdem noch ganz prima hingekriegt?

Rochus Merker: Die Leute von T-Systems hatten anfangs Probleme, ihr Video zu starten. Wir haben das dann separat auf Ihrem Notebook gestartet.

Es war sehr angenehm. Die Leute waren freundlich und interessiert. Ich habe vielen erklärt, was wir in Chile machen wollen und viele positive Rückmeldungen bekommen. Das Essen hat auch allen geschmeckt und wir hatten gut zu tun alle satt zu bekommen. Das meiste hat gut geklappt und auch von der kaputten Kaffeemaschine ließen wir uns nicht unterkriegen. Alles in allem war das Catering sehr erfolgreich. (Else)

Das Catering in der Uni hat sehr viel Spaß gemacht. Die Stimmung war toll und wir haben viele neue Leute getroffen. Es war gut, dass schon Getränke da waren und wir eine Ansprechpartnerin vor Ort hatten. (Tabea und Alina)

FIfF: Ich selbst habe eine böse Überraschung erlebt. Hatte meinen Blu-Ray-Player im kleinen Hörsaal ausprobiert, wo alles prima ging, mit der simplen Technik aber bloß ein kleines Bild warf. Ich hätte den Film gerne auch im großen Hörsaal von Blu-Ray abgespielt, habe dort aber keinen Ton bekommen.

Rochus Merker: Stimmt. Aber von Ihrem Laptop konnten Sie den Film dann doch problemlos abspielen.

FIfF: Nach der FIfFKon ist immer vor der FIfFKon, es gibt ja jedes

Ich fand die Konferenz sehr schön, vor allem, dass wir mit den Menschen viel reden konnten und ihnen unser Projekt erklären konnten. Außerdem war es natürlich auch schön zu sehen, dass allen unser Essen geschmeckt hat. Ich fand es unglaublich gut, dass wir es stemmen konnten, trotz der anfänglichen Bedenken. (Juliane)

Jahr eine. Hätten Sie ein paar Tipps für Veranstalter, die wie ich keine Profis sind, an welche Dinge man bezüglich Technik da besonders denken sollte?

Rochus Merker: Immer mehr Kabel und Adapter dabeihaben als eigentlich benötigt. An Apple-Adapter denken, die fehlen oft. Probleme macht häufig DisplayPort auf HDMI, das ist ganz wichtig, auch bei neuen Notebooks. Wenn man die Ressourcen hat, vielleicht auch angewinkelte Stecker beschaffen. Ganz wichtig bei Audio, wird viel vergessen, ist XLR-Kabel, das hat keiner mehr standardmäßig. An der Uni wird das meist irgendwo verwahrt, sollte man sich vorher geben lassen. Um zum Beispiel ein Audiokabel zu verlängern oder noch eine Box anzuschließen.

Wir fanden das Catering gut. Doch war es während der Vorträge etwas langweilig. Und wir fanden es etwas seltsam, dass wir das Wasser für die Wiener von der Toilette holen mussten. Aber es hat Spaß gemacht, den Leuten von unserem Projekt zu erklären. (Shannon und Karolin)

FIfF: Während der Tagung waren Sie an sehr vielen Stellen und hatten da auch das akustische und optische Erlebnis. Würden Sie sagen, dass man überall gut hören, gut sehen konnte, dass die Videos anständig zu erkennen waren?

Rochus Merker: Jedenfalls ohne größere Probleme. Es gab kurz Beschwerden, hinten wäre es nicht laut genug, aber das betraf

Kulinarisches Zentrum der FIfFKon, Foto: Marianne Mauch

nicht viele, und die haben sich dann weiter nach vorne gesetzt. Darüber waren wir ganz froh, denn die Videoaufnahmen wurden ja auch hinten gemacht, und wir hätten uns sonst wegen der Nebengeräusche noch was einfallen lassen müssen.

FIfF: Haben Sie denn von den Vorträgen inhaltlich auch was mitbekommen, neben der Arbeit, die Sie gemacht haben?

Rochus Merker: Ich wusste nicht, was auf mich zukommt. Hatte zwar im Programm gelesen und bin ja aus der Branche, aber mir keine großen Gedanken gemacht. Insofern war ich positiv überrascht. Die Vortragenden haben die Leute mitgenommen, das lag sicher auch an dem sehr aktiven Publikum, sehr gemischt, total sympathisch. Dadurch wurden viele Sachen aufgeklärt, die ich nicht gleich verstanden hatte und vielleicht eine Viertelstunde später wieder vergessen hätte. Ich konnte nur am Freitag bei den Vorträgen sein und fand die durchweg super, wie auch den Workshop am Samstag (Anm. der Redaktion: Industrial Security). Der Vortrag des Datenschutzbeauftragten war für mich der abgefahrenste von allen, weil er alles so auf den Punkt brachte und ich nicht gedacht hätte, dass jemand so ehrlich ist.

FIfF: Würden Sie den Leserinnen und Lesern unserer Zeitschrift noch verraten, was Sie beruflich machen?

Rochus Merker: Administrator für die Schulen in Jena. Ich bin studierter Informatiker. Freiberuflich habe ich Kongresse technisch betreut.

FIfF: Vielen Dank fürs Interview, vielen Dank für die Unterstützung! Ich hoffe, wir haben wieder öfters miteinander zu tun. Ich muss dazu sagen, ich kenne Herrn Merker ganz gut aus dem Studium …

Die Konferenz war wirklich schön, es herrschte eine angenehme Atmosphäre. (Felix)

Es war sehr informierend und aufschlussreich. (Josie)

Carlo Schäfer

Spam und Cybercrime im Jahre 2017

Spam wird häufig mittels kompromittierter E-Mail-Konten erzeugt, auf die zu diesem Zweck Botnetze zugreifen. Auf der FIfF-Konferenz 2017 in Jena (#FIfFKon17) wurde im Rahmen einer Demonstration im Foyer des Veranstaltungsgebäudes die Dimension solcher illegalen Zugriffe sowie deren Abwehr gezeigt.

Botnetze – die Quelle des Cybercrime

Das weltweite Malware-Aufkommen der letzten zwölf Monate entwickelte sich, wie in Abbildung 1 gezeigt, sehr dynamisch und fiel im Januar 2018 auf ein Vorkommen von einer in 786 E-Mails. Dies ähnelte dem Aufkommen von Anfang 2017, als vorübergehend die Botnetz-Aktivität des weltgrößten Spam-Botnetzes *Necurs* eingeschränkt war.

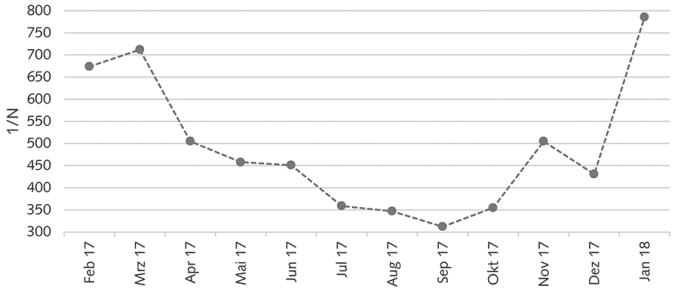


Abbildung 1: Weltweites Malware-Aufkommen 2017/2018 (Symantec 2018)

Das Aufkommen von Malware sank im Januar 2018, nachdem vermehrt Anti-Malware-Kampagnen durchgeführt wurden. Aktuell liegt die Anzahl an neuen Malware-Varianten pro Monat annähernd konstant bei 43 Millionen, das ist weniger als die Hälfte im Vergleich zu Februar 2017 mit 94 Millionen (Symantec 2018).

Im März 2017 wurde *Necurs* für Kampagnen zur Aktienmanipulation verwendet und somit weniger andere Malware wie zum Beispiel die Trojaner *Locky* und *Dridex* verbreitet. Ziel dieser Kampagnen war es, mittels *Pump-and-Dump-Nachrichten* – also Spam-Falschmeldungen – Aktienkurse künstlich in die Höhe zu treiben. Die Verantwortlichen der Kampagnen kauften zuvor Anteile dieser sogenannten Pennystocks billig auf, um sie nach dem künstlich gepushten Kursgewinn wieder zu veräußern (Baird et al. 2017).

Eingehender Spam

Im Januar 2018 waren 55 Prozent aller E-Mails Spam. Während der letzten zwölf Monate hat sich an diesem Wert nicht viel geändert. In den letzten fünf Jahren wurde auch die Anzahl der bei der Friedrich-Schiller-Universität (FSU) Jena eingehenden Spam-Nachrichten analysiert, das Ergebnis ist in Abbildung 2 zu sehen; der Trend entspricht der globalen Spam-Welle.

Ausgehender Spam

Dennoch kann man die Aktivität der einzelnen Botnetze deutlich erkennen. Bevor große Kampagnen gestartet werden, sind

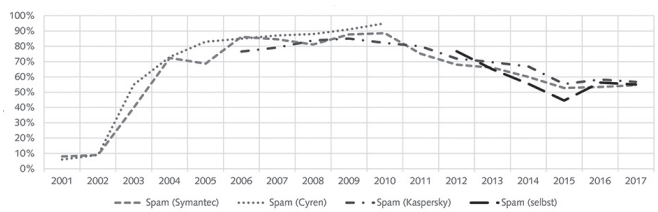


Abbildung 2: Weltweite Spam-Entwicklung der letzten 17 Jahre (Kaspersky 2018; Symantec 2017; Cyren 2018) und eigene Messungen an der FSU Jena

vermehrt Phishing-Nachrichten im Umlauf, die Zugangsdaten für E-Mail-Konten abgreifen sollen. Diese werden in den darauffolgenden Stunden beziehungsweise Wochen auf Funktionalität validiert und für die eigentlichen Kampagnen verwendet. Zugangsdaten, die einmal abgegriffen wurden, werden zyklisch – auch Jahre später – geprüft, um diese wieder zu verwenden. Deshalb sollten Passwörter niemals recycelt werden, da alte Zugangsdaten mit dazugehörigen Passwörtern nie in Vergessenheit geraten. Ein Botnetz verwendet anschließend diese kompromittierten Konten, um die eigentlichen Spam-Kampagnen durchzuführen. Im August 2017 wurde zum Beispiel das Botnetz *Onliner* identifiziert. Es verfügte zu diesem Zeitpunkt über 711 Millionen E-Mail-Adressen sowie rund 80 Millionen Zugangsdaten für E-Mail-Server, um über diese vertrauenswürdigen SMTP-Server Spam zu versenden (Westernhagen 2017). Dieser Missbrauch (Schäfer 2016b) und mögliche Gegenmaßnahmen (Schäfer 2014, 2015, 2017) wurden in der FIfF-Kommunikation 4/2015 im Beitrag *Die Rolle von Spam im Cybercrime* genauer betrachtet (Schäfer 2016a).

#FIfFKon17

Während der #FIfFKon17 wurde gezeigt, wie kompromittierte Konten missbraucht werden, um unerwünschte Nachrichten zu versenden. Um dem entgegenzuwirken, analysiert ein selbst entwickeltes System in Echtzeit automatisiert die entstehenden Metadaten, wodurch die missbrauchten Konten identifiziert werden können. Dieses Vorgehen sorgte für großes Interesse unter den Besuchern der Vorführung, vor allem, da sich lokal erzeugter ausgehender Spam komplett vermeiden lässt. Die eigene E-Mail-Reputation ist somit nicht mehr gefährdet, wodurch das Blacklisting der eigenen IP-Adressen verhindert werden kann. Erst das ermöglicht eine funktionierende Kommunikation mit den Empfängern – andernfalls gleicht dies einer sozialen Ausgrenzung.

Die *Necurs*-Bots, die gekaperte Konten nutzten, wurden für die Vorführung auf der #FIfFKon17 analysiert und geographisch zugeordnet. So war es möglich, während eines Zeitraums von 15

Stunden einen Missbrauch zu visualisieren. Während dieser Zeit wurden zwar alle unerwünschten Nachrichten entgegengenommen, um dem Botnetz funktionierende Konten vorzutäuschen. Diese E-Mails wurden jedoch nicht weitergeleitet, um die eigene Reputation nicht zu gefährden. Über 3.000 Bots des *Necurs*-Botnetzes versuchten, ein lokales Konto zu missbrauchen, und erzeugten in 15 Stunden mehr als 20 Millionen Spam-E-Mails.

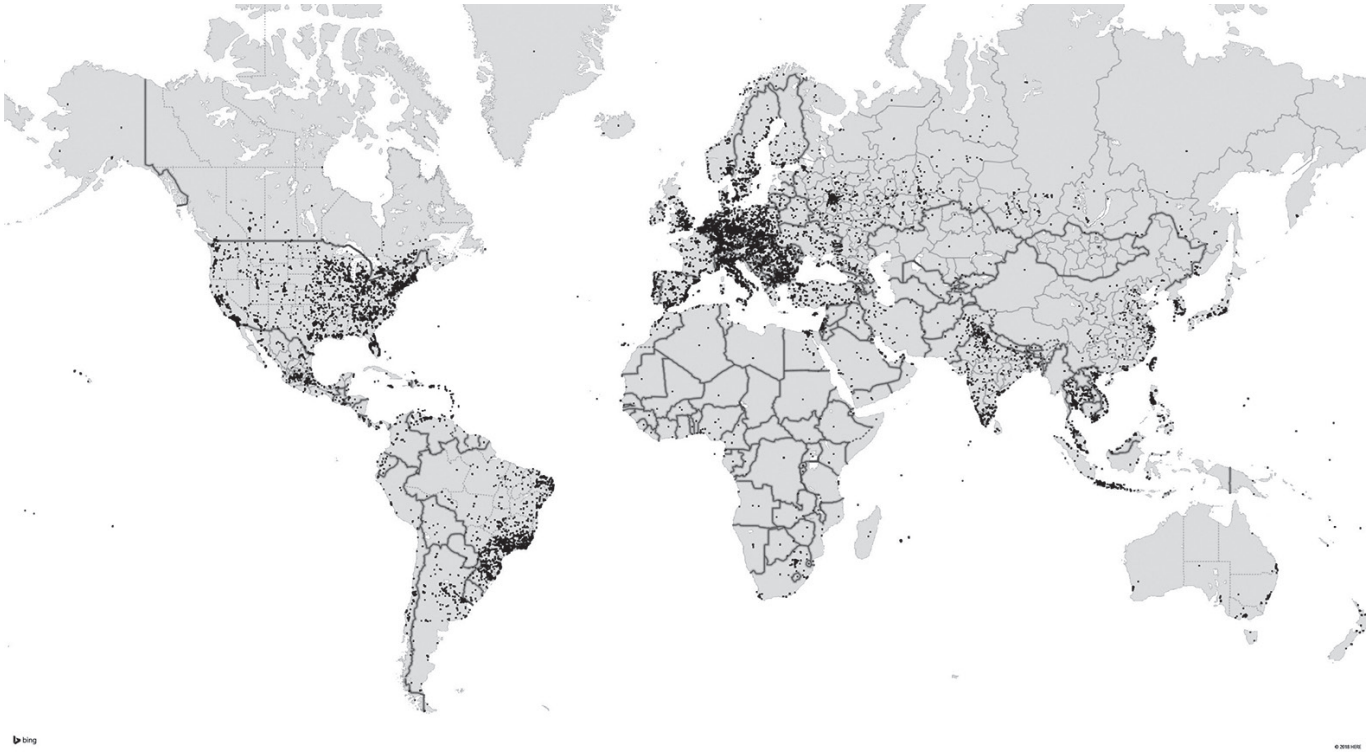


Abbildung 3: Geografische Herkunft von Angriffen des Necurs-Botnetzes innerhalb von 15 Stunden auf die E-Mail-Infrastruktur der FSU Jena

Ein solcher Missbrauch von Konten findet ständig statt und betrifft alle E-Mail-Anbieter. Des Öfteren werden auch große Provider von anderen geblockt, und deren Kunden finden einen gestörten E-Mail-Versand vor. Das lässt sich mit den richtigen Erkennungssystemen unterbinden, wie auf der #FIfFKon17 gezeigt wurde.

Referenzen

Baird S, Brumaghin E, Carter E, Schultz J (20. März 2017) Necurs diversifies its portfolio. http://blog.talosintelligence.com/2017/03/necurs-diversifies.html

Cyren Ltd. (2018) Resource center. https://www.cyren.com/resources

Kaspersky Lab (2018) Securelist Archive, Spam Statistics. https://securelist.com/all/?tag=126

Schäfer C (2014) Detection of compromised email accounts used by a spam botnet with country counting and theoretical geographical travelling speed extracted from metadata. 25th International Symposium on Software Reliability Engineering Workshops, IEEE, S 329–334. doi:10.1109/ISSREW.2014.32

Schäfer C (2015) Detection of compromised email accounts used for spamming in correlation with mail user agent access activities extracted from metadata. Symposium on Computational Intelligence for Security and Defense Applications (CISDA), IEEE. doi:10.1109/CISDA.2015.7208641

Schäfer C (2016a) Die Rolle von Spam im Cybercrime. FIfF-Kommunikation 32(4):27–29. http://www.fiff.de/publikationen/fiff-kommunikation/fk-2015/fk-2015-4/fk-2015-4-content/fk-2015-4-p27

Schäfer C (2016b) Mail Infrastructure Traffic Analyzer – Erkennung kompromittierter E-Mail-Accounts. Dissertation, Univ. Jena

Schäfer C (2017) Detection of compromised email accounts used for spamming in correlation with origin-destination delivery notification extracted from metadata. 5th International Symposium on Digital Forensic and Security (ISDFS), IEEE. doi:10.1109/ISDFS.2017.7916494

Symantec Corporation (2017) Security Center Archived Publications. https://www.symantec.com/security-center/archived-publications

Symantec Corporation (2018) Internet Security Monthly Threat Report, Januar 2018. https://www.symantec.com/security_response/publications/monthlythreatreport.jsp?id=2018-01

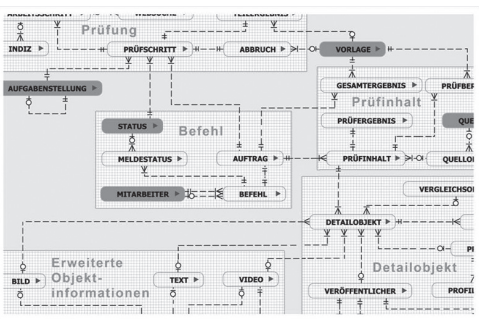
Westernhagen Ov (30. August 2017) Spambot nutzt 711 Millionen Mail-Adressen zur Malwareverbreitung. Heise Security. https://heise.de/-3817207

Carlo Schäfer

Dr. **Carlo Schäfer** ist promovierter 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 Freistaat Thüringen.

Frank Geyer

Nutzung von Daten aus sozialen Netzwerken im Umfeld der zivilen Sicherheit[1]



Social Media (SM)-Plattformen wie Facebook *und* Twitter *bieten für die Bewältigung von Großschadenslagen und Krisen interessante neue Möglichkeiten.*

So konnte etwa im Laufe des *Elbe-Hochwassers 2013* über bevölkerungsgenerierte Krisenkarten[2] oder die Gewinnung freiwilliger Kräfte im Netz praktisch gezeigt werden, dass vor allem durch die direkte Beteiligung der Betroffenen neue Potenziale entstehen.[3] Aktuell nutzen deutsche *Behörden und Organisationen mit Sicherheitsaufgaben (BOS)*[4] diese Potenziale nicht oder nur in einem sehr geringen Umfang, wie aktuelle Umfragen in dieser Zielgruppe zeigen.[5] Im Rahmen des Dissertationsvorhabens[6] *bridged* wurde ein Beitrag geleistet, diese Situation zu verbessern.

Dazu wurde zunächst eine Recherche zum aktuellen Stand von Forschung und Praxis durchgeführt, um Chancen und Risiken sowie aktuelle praktische Herausforderungen detailliert benennen zu können. Dabei zeigte sich, dass unter anderem für die exakte Erfassung der aktuellen Lage bei einem so weiträumigen Ereignis wie einem Hochwasser *SM-Plattformen* wertvolle Informationen bieten. Betroffene sind nahezu überall und nahezu jederzeit vor Ort und können auch zu Zeiten Informationen liefern, bei denen eine klassische Lagefeststellung zum Beispiel aus Personalmangel nur schwer oder gar nicht durchführbar ist. So wurden auch zum *Elbe-Hochwasser 2013* mit bis zu 35.000 Netz-Beiträgen pro Tag sehr viele Informationen öffentlich verbreitet, die einen wesentlichen Beitrag dazu leisten können, das Lagebild zu vervollständigen und damit leichter Entscheidungen für die Krisenbewältigung zu treffen.[7]

In der Praxis in Deutschland findet eine Nutzung dieses Informations-Pools bisher kaum statt

Neben der zu bewältigenden Informationsflut stellt die *Vertrauenswürdigkeit der Daten* das zentrale Problem dar: Unter den vielen wertvollen Informationen finden sich immer wieder Falschinformationen.[8] Die Gründe hierfür sind vielschichtig und reichen von fehlender Sachkenntnis bezüglich der Lagebeurteilung in der Bevölkerung bis zu mutwilliger Fehlinformation[9], etwa um selbst möglichst schnell Hilfe zu bekommen.

Damit stehen handelnde Personen in Krisenstäben vor der *Herausforderung, den Wahrheitsgehalt von Informationen in sozialen Medien überprüfen und bewerten* zu müssen, bevor diese zur Vervollständigung des Lagebilds und damit zur Entscheidungsunterstützung genutzt werden können. Aufgrund der Heterogenität und Anonymität des Internets ist das ein aufwändiger Schritt, der mit großer Sorgfalt und viel Sachverstand durchgeführt werden muss.[10]

Um die Mitarbeiterinnen und Mitarbeiter der *BOS* in diesem Prozess zu unterstützen,[11] erfolgten im Rahmen des Projekts Analyse, Entwurf und Implementierung des *Framework bridged,* welches eine IT-Unterstützung und Teilautomatisierung des Verifikationsprozesses ermöglicht. Diese Grundlagenarbeit ermöglicht eine Anwendung, die schrittweise durch die Überprüfung des Wahrheitsgehalts führt und alle hierfür benötigten Informationen weitgehend automatisiert zusammenstellt.

Eine strukturierte Erfassung der Ergebnisse der einzelnen Prüfschritte soll zudem im Anschluss eine fundierte Bewertung der Vertrauenswürdigkeit möglich machen. Hierfür müssen sowohl die speziellen Anforderungen der Arbeit von Krisenstäben in Deutschland (wie die geltende Rechtslage, wiederkehrende Prüfung von Inhalten bei neuer Faktenlage, interne und externe Freigabeprozesse) adressiert und bewältigt werden als auch technische Herausforderungen (etwa die Zusammenführung heterogener und unvollständiger Daten in einen integrierten Datenbestand).

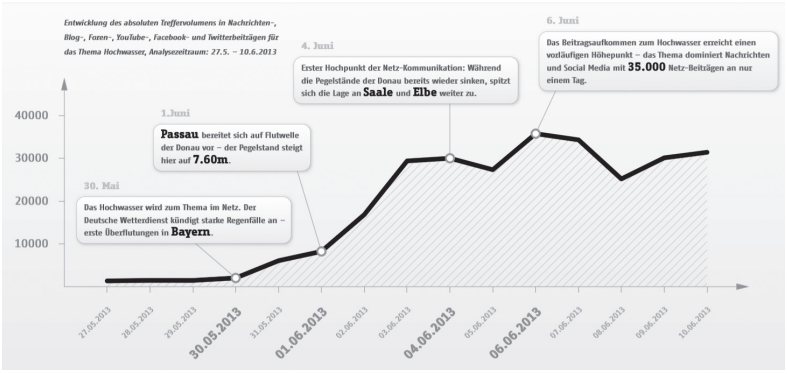
Als Ausgangspunkt für dieses Vorhaben wurde der Prozess der Verifikation und Freigabe von Inhalten innerhalb und zwischen *BOS* untersucht, um so die besonderen Anforderungen der Zielgruppe festhalten zu können. Außerdem wurde der Bereich des Online-Journalismus beleuchtet.

Im Anschluss an diesen Arbeitsschritt wurde mittels der Prozessmodellierungssprache *Business Process Model and Notation (BPMN)*[12] ein logisches Prozessmodell für den bisher unerforschten Verifikationsprozess erstellt. Nachfolgend wurde mittels konzeptuellem und logischem Datenmodell eine integrative Datenhaltung für das *Framework bridged* entworfen, die neben allen genutzten Informationen aus dem Web auch alle Prozessdaten rechtssicher speichert.

Prozessmodell und Datenmodell bilden die Basis zur Definition der Architektur, der Komponenten und der Schnittstellen für das *Framework bridged.* Auf Basis des Client-Server-Modells wurden

der Aufbau des Frameworks, seine Integration in die Stabsarbeit und die Schnittstellen zur Erfassung von Informationen von außen definiert. Zur Demonstration der Anwendung des Frameworks in der Stabsarbeit ist abschließend eine Web-Oberfläche auf Basis von *bridged* prototypisch implementiert worden.

Mit Abschluss der Arbeiten am Projekt *bridged* beendete der Autor die Arbeiten in der zivilen Sicherheitsforschung. Ihm sind keine weiterführenden Forschungen in diesem Bereich am Lehrstuhl für Softwaretechnik der Friedrich-Schiller-Universität Jena bekannt.



Die „Jahrhundertflut" im Web – Quelle:]init[, CC BY-NC 3.0

Anmerkungen und Referenzen

* Verwendetes Bildmaterial: Linkes Foto: „Members of the The Los Angeles County Fire Urban Search and Rescue Team, Task Force 2, who travelled with the 452nd Air Mobility Wing, March Air Reserve Base, Calif., to the earthquake and tsunami stricken areas of Japan just four days after the devastation, search through rubble with their Japanese counterparts." (U.S. Air Force photo/Technical Sgt. Daniel St. Pierre). Rechtes Foto: „Many notices were put up around the scene of the Grenfell Tower fire tragedy to help find missing persons from the tower. Bramley Road, London (near Latimer Road underground station). June 16, 2017." (CC BY 2.0, Text und Bild: Jonathan Miller).

1 *Siehe vertiefend den gleichnamigen Vortrag auf der FIfF-Konferenz 2017, Video unter fiff.de/r/181025, Vortragsfolien fiff.de/r/181026*

2 *Schön dokumentiert im Video* Lars und Isa: Zwei gegen die Flut*, Google-Kanal auf YouTube, 15. Oktober 2013. https://www.youtube.com/watch?v=AJtQIyiFtVM*

3 *Mildner S (2013) Bürgerbeteiligung beim Hochwasserkampf; Chancen und Risiken einer kollaborativen Internetplattform zur Koordination der Gefahrenabwehr. In: Köhler T, Kahnwald N (Hrsg) (2013) Gemeinschaften in Neuen Medien (GeNeMe '13). TUDpress, Dresden, S 13–21. http://nbn-resolving.de/urn:nbn:de:bsz:14-qucosa-125674*

4 *„Staatliche (polizeiliche und nichtpolizeiliche) sowie nichtstaatliche Akteure, die spezifische Aufgaben zur Bewahrung und/oder Wiedererlangung der öffentlichen Sicherheit und Ordnung wahrnehmen. Konkret sind dies z. B. die Polizei, die Feuerwehr, das THW, die Katastrophenschutzbehörden der Länder oder die privaten Hilfsorganisationen, sofern sie im Bevölkerungsschutz mitwirken." Nach: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Glossar, https://www.bbk.bund.de/DE/Servicefunktionen/Glossar/_function/glossar.html?lv2=4968152&lv3=1948880. Zugegriffen: 28. März 2018*

5 *Heine M (2014) Social Media im Krisen- und Katastrophenmanagement; Stand und Verbreitung. In: Gronau N, Heine M, Baban CP (Hrsg) (2014) Social Media im Krisen- und Katastrophenmanagement. Gito, Berlin*

6 *Geyer F (2017) Ein Framework für den teilautomatisierten Verifikations- und Integrationsprozess für Daten aus sozialen Netzwerken im Umfeld der zivilen Sicherheit. Dissertation, Fakultät für Mathematik und Informatik, Friedrich-Schiller-Universität Jena. urn:nbn:de:gbv:27-dbt-20170314-1118271*

7 *Marwan P (14. Juni 2013) Sommerhochwasser überflutet auch Soziale Netzwerke. ITespresso. http://www.itespresso.de/2013/06/14/sommerhochwasser-ueberflutet-auch-soziale-netzwerke/*

8 *Dass dies auch beim Informationsfluss in der anderen Richtung, also von Behörden in soziale Netzwerke, zu fatalen Folgen führen kann, wird in dem Film* The Thread *(2015, Regie: Greg Barker, http://www.imdb.com/title/tt4211516/) eindrucksvoll demonstriert: Nach dem Bombenanschlag auf den Boston Marathon 2013 werden durch die Behörden Bilder mutmaßlicher Täter verbreitet, was zu einer Menschenjagd auf Unschuldige führt.*

9 *Siehe z. B. die eigene Fallstudie zu den Vorgängen nach dem Anschlag am 19. Dezember 2016 auf den Berliner Weihnachtsmarkt am Breitscheidplatz, dargestellt auf den Vortragsfolien fiff.de/r/181028 und im Videomitschnitt fiff.de/r/181027.*

10 *Als Leitfaden empfohlen: Silverman C (Hrsg) (2014) Verification handbook; An ultimate guideline on digital age sourcing for emergency coverage. European Journalism Centre, Maastricht. http://verificationhandbook.com/*

11 *Dass das manuelle Sichten großer Mengen von Bildmaterial aus der Bevölkerung wenig erfolgversprechend ist, zeigt sehr anschaulich folgender Bericht über die Ermittlungen zur Kölner Silvesternacht 2015: Schmidt J-E (27. Juni 2016) Die Linsen der Vielen; Wie Handyvideos die Polizeiarbeit verändern. News auf heise.de. http://www.heise.de/newsticker/meldung/Die-Linsen-der-Vielen-Wie-Handyvideos-die-Polizeiarbeit-veraendern-3249138.html*

12 *Vgl. z. B. Object Management Group, Inc. (2018) Business Process Model and Notation. http://www.bpmn.org/. Zugegriffen: 28. März 2018*

Frank Geyer

Dr.-Ing. **Frank Geyer** ist seit 2017 Business Consultant bei der IBYKUS AG für Informationstechnologie Erfurt und beschäftigt sich aktuell mit der Konzeption von Softwarelösungen für die EU-konforme Fördermittelverwaltung (Haushaltsführung, Monitoring) durch Bundes- und Landesbehörden. Zuvor war er von 2013 bis 2016 wissenschaftlicher Mitarbeiter an der Friedrich-Schiller-Universität Jena. In seiner wissenschaftlichen Arbeit bis hin zur Promotion lag ein Schwerpunkt in der Entwicklung IT-gestützter Einsatzunterstützungssysteme.

Benjamin Kees, Rainer Rehak, Stefan Hügel

FIfF wirkt – ein langer Blick zurück

Jahresrückblick 2016/17

In unserem Jahresrückblick stellten wir die wichtigsten Aktivitäten des FIfF seit Ende 2016 dar. Einen Überblick dazu gibt die Zeitleiste, die unter dem Beitrag dargestellt ist. Mit Auszügen aus unseren Stellungnahmen, Pressemitteilungen und Beiträgen zur FIfF-Kommunikation illustrieren wir die Aktivitäten.

September 2016

FREIHEIT 2.0 wurde von dem Künstler Florian Mehnert in Weil am Rhein, Basel und Huningue im September und Oktober 2016 als partizipatives Kunstprojekt realisiert:

> *Die Installation FREIHEIT 2.0 bestand aus 4 Elementen: Der Self-Tracking-App, die mittels der GPS-Funktion von Smartphones die Bewegungsprofile der Nutzenden [visualisiert], zweitens den FREIHEIT-Umfirmierungen von Geschäften, drittens einem Leitsystem durch die Straßen der Stadt Weil am Rhein und schließlich den Big-Data-Kolloquien. Die letzteren werden in diesem Schwerpunkt verschriftlicht. Am Ende können auch aus der Self-Tracking-App erzeugte Bilder als Kunstwerke verkauft werden.*[1]

Das FIfF war durch Britta Schinzel und Benjamin Kees an den *Big-Data-Kolloquien* beteiligt und veröffentlichte einen umfassenden Schwerpunkt dazu in der *FIfF-Kommunikation*.[2]

November 2016

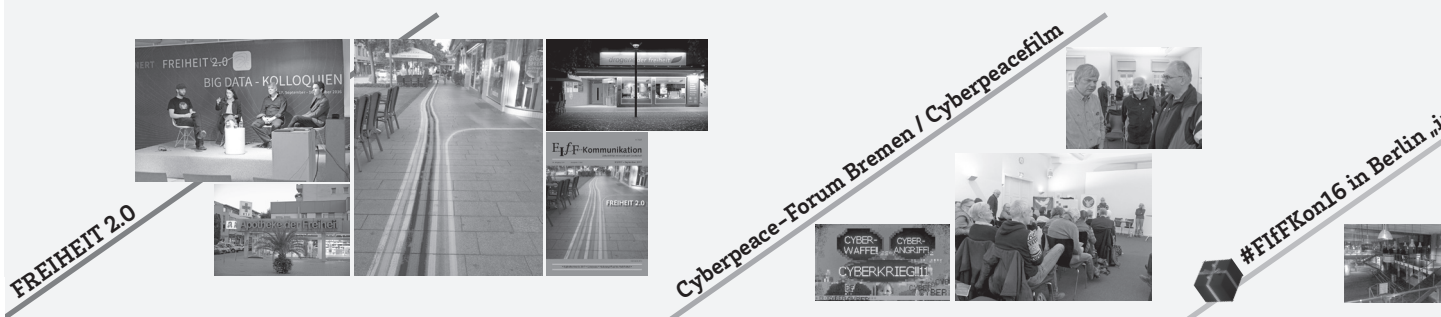
Am Freitag, dem 11. November 2016, von 18 bis 20 Uhr und am darauffolgenden Samstag von 14 bis 16 Uhr fand das **Cyberpeace-Forum** im Haus der Wissenschaft in der Bremer Innenstadt statt, das durch das FIfF organisiert wurde:

> *[Das Cyberpeace-Forum] war konzipiert als ein Bremer Beitrag zur Cyberpeace-Kampagne des FIfF zur Diskussion aktueller Entwicklungen zum Thema Cyberkrieg. Die Veranstaltung begann am Freitagabend mit einer Podiumsdiskussion anlässlich der Kooperation der Hochschule Bremen mit der Bundeswehr. Am Samstagnachmittag wurden aktuelle Entwicklungen und Gegenentwürfe zum Thema Cyber- und Drohnenkrieg vorgestellt und diskutiert. Beide Veranstaltungsteile waren mit je rund 80 Teilnehmenden passabel besucht. Das Publikum war gut gemischt: Jung und Alt, Frauen und Männer, viele Friedensbewegte, erstaunlich wenige mit direktem Informatikbezug.*[3]

Benjamin Kees, Rainer Rehak und Stefan Hügel bei der Präsentation des Jahresrückblicks, Foto: Kai Nothdurft

Ende November fand unsere **FIfF-Konferenz 2016** statt. Diesmal wieder in Berlin, unter dem Leitmotiv *in.visible systems*:

> *In einer digitalisierten Gesellschaft untergraben unsichtbare Systeme die individuelle Selbstbestimmung und die demokratische Mitbestimmung. Doch nicht nur das, die Manipulation des Denkens und Handelns ist zur treibenden Kraft der IT-Entwicklung geworden. Dies wurde vom 25. bis zum 27. November 2016 in Berlin auf der FIfF-Konferenz 2016 deutlich. […]*
>
> *Zweck von Informationstechnik ist immer auch Komplexitätsreduktion und -verschleierung. Die Zusammenhänge bleiben nicht nur unsichtbar, sondern sie werden*



ganz gezielt versteckt. Dies geschieht einerseits zur sinnvollen Komplexitätsreduktion, andererseits aber auch, um verdeckte Zwecke zu verfolgen. Die Möglichkeit, ein inzwischen durchdigitalisiertes Leben und die genutzte Infrastruktur mündig zu beurteilen oder gar zu gestalten, wird so zunehmend unmöglich gemacht.

in.visible systems – Versteckte Informationstechnik ist nicht diskutierbar. Unter diesem Leitmotiv stand die FIfF-Konferenz 2016, die vom 25. bis zum 27. November 2016 in Berlin stattfand Themen der Konferenz waren Geheimdienste und die Defizite ihrer (parlamentarischen) Kontrolle; Informationsfreiheit, ihre Verhinderung durch Amtsträger.innen und der Versuch, sie wieder durchzusetzen; Techniknutzung und Algorithmen in sozialen Kontexten; Ethik in Informatik und Wissenschaft; Theorien der Transparenz; kultivierte Unsichtbarkeit; das technisch Unbewusste. Mehrere Workshops ergänzten das Programm zu Themen wie Malware, globalen Friedensinitiativen, Menschenrechten, politischer Informatik und nachhaltiger Mobilität.[4]

Cryptoparties sind weltweit organisierte Veranstaltungen, offen für alle Interessierten, bei denen das notwendige Wissen für den Selbstschutz im digitalen Raum vermittelt wird. Dies umfasst verschlüsselte Kommunikation, Vermeidung von Tracking beim Surfen im Web und allgemeine Sicherheitsempfehlungen für die Nutzung von Computern und Smartphones.[5]

In München wurden mehrere Cryptoparties organisiert: im November 2016, Januar, März, Mai und September 2017. Partner des FIfF waren dabei der muCCC und das Medienzentrum München.

Dezember 2016

Der **Friedensratschlag**[6] in Kassel ist die jährlich stattfindende Zusammenkunft der Friedenbewegung, die am 3./4. Dezember 2016 stattfand. Das FIfF, das aus der Friedensbewegung hervorgegangen ist, will auch dort seine Themen platzieren. So veranstalteten Dietrich Meyer-Ebrecht und Stefan Hügel für das FIfF einen Workshop zum Thema Cyberpeace, bei dem wir die Problematik und unseren Gegenentwurf darstellten und diskutierten.[7]

Das Projekt **TDRM**[8] – Tihange Doel Radiation Monitoring – macht radioaktive Strahlung in Belgien, den Niederlanden und Deutschland sichtbar und schafft damit Transparenz für die Bedrohung durch die belgischen Reaktoren Tihange und Doel, deren Zustand inzwischen zu einer massiven Bedrohung für weite Gebiete in diesen Ländern führt:

Die Sicherheitsprobleme der belgischen Uralt-AKWs Tihange und Doel (65 bzw. 150 km westlich von Aachen) spitzen sich weiter zu. In Sorge um zuverlässige und auch rechtzeitig verfügbare Information hat sich eine Arbeitsgemeinschaft konstituiert, die mit Hilfe eines unabhängigen Netzes von Stationen für die Messung der atmosphärischen Radioaktivität in der Region Tihange-Doel-Aachen zur Aufklärung und Sicherheit der Bürgerinnen und Bürger beitragen will.

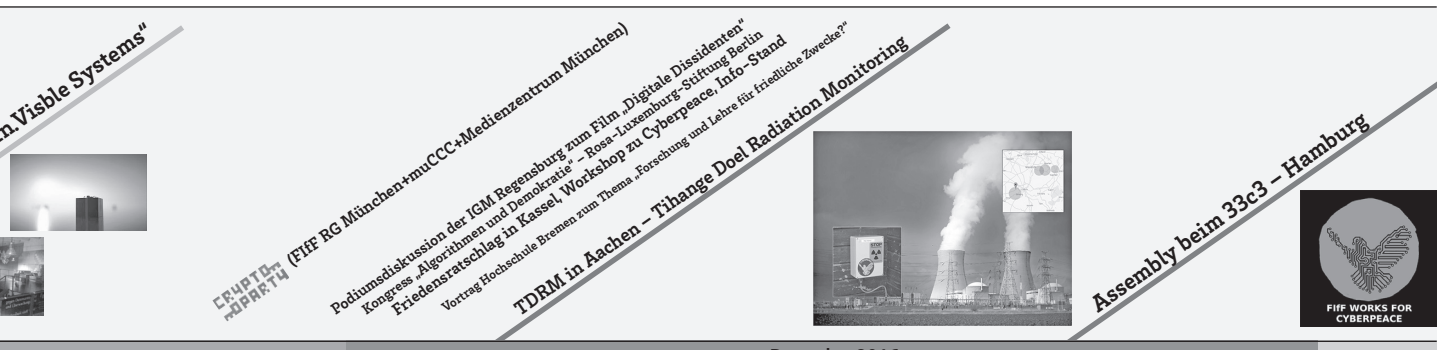
Das Netzwerk wird von einer Projektgruppe des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF) entwickelt, realisiert und betrieben. Sie kooperiert in einer Arbeitsgemeinschaft mit Aachener Mitgliedern der Internationalen Ärzte gegen den Atomkrieg, Ärzte in sozialer Verantwortung e. V. (IPPNW) und mit dem Aachener Aktionsbündnis gegen Atomenergie (AAA). Die Messdaten stehen allen Bürgern unbewertet im Internet zur Verfügung.[9]

Das Messnetz ging im Dezember 2016 in Betrieb, wächst seitdem stetig und soll weiter ausgebaut werden. Über den Start wurde in überregionalen Medien – u. a. in der *Tagesschau* – berichtet.

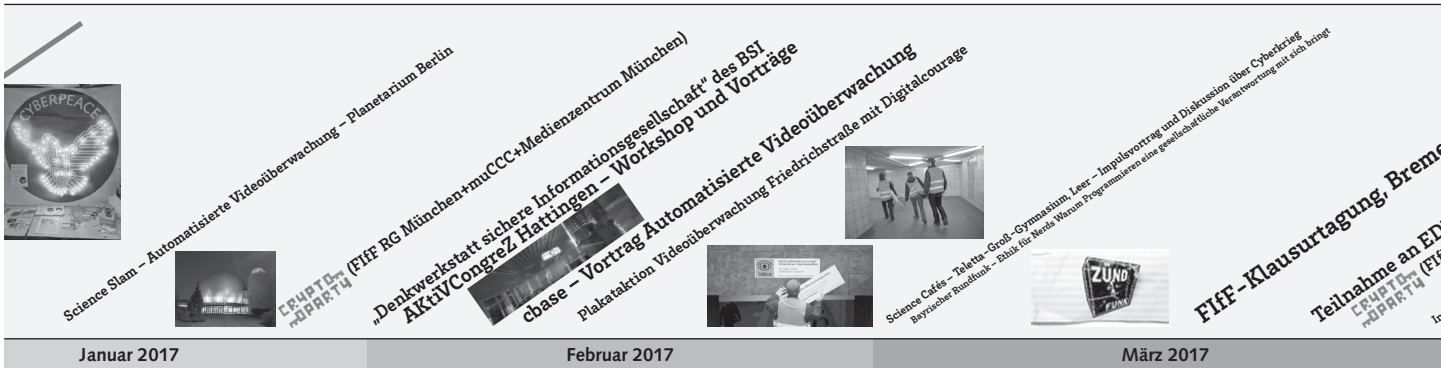
Mittlerweile eine feste Instanz beim **Chaos Communication Congress**, der als 33c3 Ende Dezember 2016 (vorläufig) zum letzten Mal in Hamburg stattfand, ist unsere **FIfF-Assembly**. Unter unserer beleuchteten Kyberfriedenstaube gab es Informationen über das FIfF, Diskussionen und Gespräche, oder einfach die Möglichkeit, sich von der Fülle der Congresseindrücke bei einer Tasse Tee zu erholen. Unser Partner bei der Assembly war erneut Amnesty International.[10]

Februar 2017

Im Februar war das FIfF gleich durch vier Aktive auf dem **AKtiV-CongreZ** in Hattingen vertreten, wo wir das FIfF vorstellten und uns aktiv an den Workshops beteiligten. Eine Folgeaktion, die dort beschlossen wurde, war die **Plakataktion zur Videoüberwachung** gemeinsam mit Digitalcourage am U-Bahnhof *Friedrichstraße* in Berlin.[11]



Dezember 2016



Mai 2017

Auf der Konferenz re:publica 2017 in Berlin stellten wir unseren Film **Cyberpeace statt Cyberwar**[12] vor:

> *Am ersten Tag der* re:publica 17 *fand eine besondere Premiere statt: Das FIfF stellte gemeinsam mit Animationsfilmduo* Motionensemble *unseren neuen Kurzfilm „Cyberpeace statt Cyberwar" vor. Der Film warnt eindringlich vor den Gefahren eines Cyberkriegs und erklärt, wie ein solcher Krieg ablaufen würde. Der Film ist unter https://youtu.be/St955HBD-7k abrufbar. […]*
>
> *Das FIfF fordert, dass Cyberwaffen auf rein defensive Zwecke beschränkt bleiben. Sie dürfen weder hergestellt, noch gehandelt, noch für offensive Zwecke eingesetzt werden. Deutschland muss auf eine offensive Cyberstrategie verzichten, sich verpflichten, keine Cyberwaffen zu entwickeln und zu verwenden und internationale Abkommen zu einem weltweiten Bann von Cyberwaffen müssen angestrebt und gefördert werden. Mit seiner Kampagne Cyberpeace setzt sich das FIfF für diese Forderungen ein.*[13]

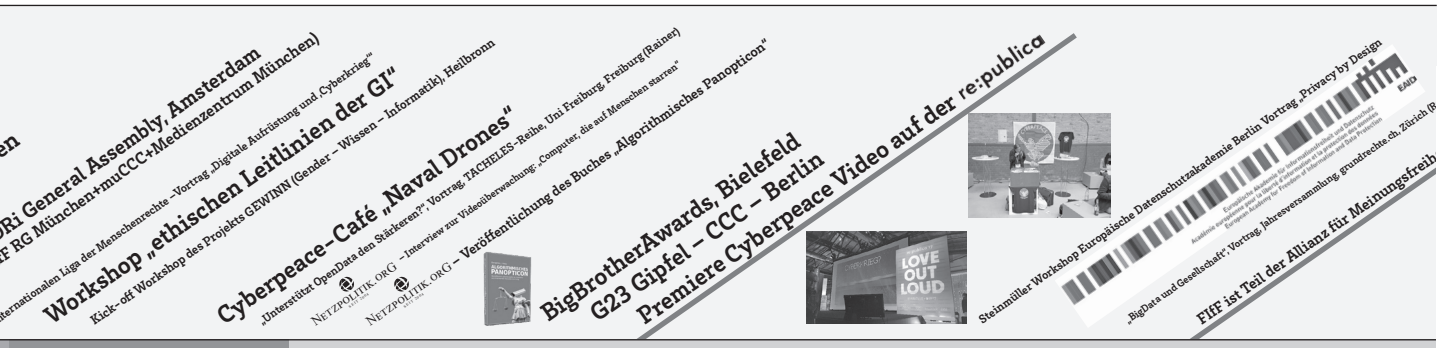
Mit dem **Netzwerkdurchsetzungsgesetz** (NetzDG) hat die Bundesregierung ein Gesetz gegen sogenannte *Hate-Speech* durchgesetzt, das nicht nur nutzlos, sondern sogar gefährlich ist. In der Allianz für Meinungsfreiheit hat sich ein breites Bündnis gegen dieses Gesetz zusammengefunden und eine Deklaration veröffentlicht, die auch das FIfF unterzeichnet hat:

> *In Reaktion auf die Verabschiedung des Netzwerkdurchsetzungsgesetzes (NetzDG) durch das Bundeskabinett am 5. April 2017 hat das FIfF zusammen mit anderen die **Deklaration für die Meinungsfreiheit** unterschrieben. Hier ein paar Auszüge:*
>
> 1. *Internetdiensteanbietern kommt bei der Bekämpfung rechtswidriger Inhalte eine wichtige Rolle zu, indem sie diese löschen bzw. sperren. Sie sollten jedoch nicht mit der staatlichen Aufgabe betraut werden, Entscheidungen über die Rechtmäßigkeit von Inhalten zu treffen.*
>
> 2. *Die Meinungsfreiheit ist ein kostbares Gut. Sie geht so weit, dass eine Gesellschaft auch Inhalte aushalten muss, die nur schwer erträglich sind, sich aber im Rahmen der gesetzlichen Regelungen bewegen. Die Demokratie nährt sich an einem pluralistischen Meinungsbild.*
>
> 3. *Gerade bei solchen Inhalten, bei denen die Rechtswidrigkeit nicht, nicht schnell oder nicht sicher festgestellt werden kann, sollte kein Motto „Im Zweifel löschen/sperren" bestehen.*
>
> *Wir erkennen an, dass Handlungsbedarf besteht, sind zugleich aber der Ansicht, dass der Gesetzentwurf nicht dem Anspruch genügt, die Meinungsfreiheit adäquat zu wahren. Im Gegenteil, er stellt die Grundsätze der Meinungsfreiheit in Frage.*[14]

Juni 2017

In Göteborg fand der **IS4SI Summit 2017 der International Society for Information Studies** statt. Das FIfF war durch Hans-Jörg Kreowski dort vertreten, der einen Workshop zum Transhumanismus organisierte und selbst einen Vortrag *Transhumanism and Nanotechnology – will old Myths come true?* hielt.

Wir nahmen mit einer Pressemitteilung Stellung zum **Staatstrojaner**, der durch die Große Koalition aus CDU/CSU und SPD im Bundestag verabschiedet worden war:



*Gestern haben CDU/CSU und SPD im Bundestag das **staatliche Hacking** zum Alltagsinstrument für Behörden erklärt. Es geht dabei nicht einmal um die Verhinderung des sonst so gern herangezogenen internationalen Terrorismus, sondern um die Aufklärung bereits erfolgter Taten wie etwa Steuerhinterziehung, Betäubungsmitteldelikte oder missbräuchlicher Asylantragstellung. Es werden also Maßnahmen, die das Bundesverfassungsgericht im Jahre 2008 gerade noch bei tatsächlichen Anhaltspunkten einer konkreten Gefahr für Leib, Leben oder den Bestand des Staates für verfassungsmäßig erachtet hat nun für die Verfolgung gewöhnlicher Delikte vorgesehen. **Anstatt also mit Softwarehaftung und allgemeinen Sicherheitslücken-Meldepflichten unsere IT-abhängige Gesellschaft wirklich sicherer zu machen, wird hier ein kurzfristiges Sicherheitsversprechen mit langfristiger brandgefährlicher IT-Unsicherheit erkauft.*[15]

Juli 2017

Zum **Handbook of Cyber-Development, Cyber-Democracy and Cyber-Defense** haben Stefan Hügel, Hans-Jörg Kreowski und Dietrich Meyer-Ebrecht einen Beitrag *Cyberpeace and Cyberwar* beigetragen. Der Beitrag wurde im Juli 2017 online veröffentlicht, eine Printveröffentlichung ist 2018 geplant. Die Zusammenfassung:

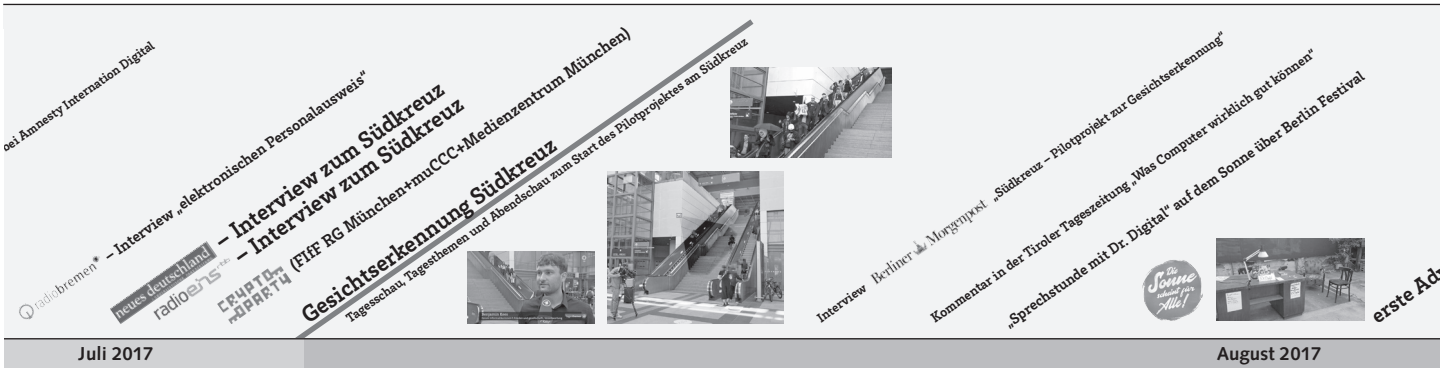
For a decade at least, a worldwide cyber armament race takes place; cyber attacks against all kinds of information and communication systems are a daily reality, and cyberwar becomes a growing threat. In this chapter, the military, political, and technological aspects of cyberwar are surveyed and discussed on one hand. On the other hand, the vision of cyberpeace is sketched as a counter-concept.[16]

August 2017

Am 1. August 2017 begann in Anwesenheit von Bundesinnenminister Thomas de Maizière das Pilotprojekt zur **Videoüberwachung mit Gesichtserkennung am Bahnhof Berlin-Südkreuz**. Die kritischen Aktionen und Stellungnahmen fanden überregionale Beachtung; Benjamin Kees erläuterte in der *Tagesschau*, warum wir dieses Projekt ablehnen. Dazu veröffentlichten wir eine umfassende Stellungnahme als Pressemitteilung:

Am Berliner Bahnhof Südkreuz testen die Deutsche Bahn, das Bundesministerium des Innern und die Bundespolizei in Kooperation mit dem Bundeskriminalamt ab heute, ob es möglich ist, mit biometrischer Gesichtserkennung im öffentlichen Raum nach Menschen zu fahnden. In einer späteren Phase des Projektes sollen zusätzlich Verhaltenserkennung und Verhaltensbewertung zum Einsatz kommen.

Beim aktuellen Test könne man die als beobachtet markierten Bereiche noch umgehen, kündigte die Bundespolizei an. Tatsächlich sind die Bereiche jedoch so gewählt, dass zum Beispiel diejenigen, die auf eine Rolltreppe angewiesen sind, dem Blick der Kameras nicht ausweichen können. Wenn es zu einem späteren Echt-Einsatz solcher Systeme kommt, wird es einen unüberwachten Ausweichbereich ohnehin nicht mehr geben. Alle, die am öffentlichen Leben teilnehmen, müssen dann damit umgehen, dass sie in ihrer täglichen Nutzung der öffentlichen Verkehrsmittel von Computern in Echtzeit vermessen, analysiert, bewertet und in allen möglichen privaten Momenten identifiziert werden können. Gleichzeitig können diejenigen, nach denen gefahndet wird, sich mit einfachsten Maßnahmen wie Sonnenbrillen, Mützen, Bärten, Make-up oder dem einfachen Blick nach unten aufs Smartphone der Identifizierung entziehen.[17]



Bereits im Vorjahr forderten wir per **Infomationsfreiheitsklage** Infomationen zum „Gefährdungsgebiet" in der Rigaer Straße in Berlin. Dieses Jahr ging es in Revision.

September 2017

Gegen die zunehmende Überwachung, für die die Vorratsdatenspeicherung nur noch ein Beispiel unter Vielen ist, gingen wir im September auf die Straße: *Freiheit ~~4.0~~ feiern – Rettet die Grundrechte* war das Leitmotiv der **Demonstration** in Berlin und in Karlsruhe. 50 Organisationen, darunter das FIfF, demonstrierten am 9. September 2017. Leider meinte es das Wetter nicht gut mit uns – es regnete in Strömen. Doch unsere Grundrechte sind wichtiger als ein paar Regentropfen!

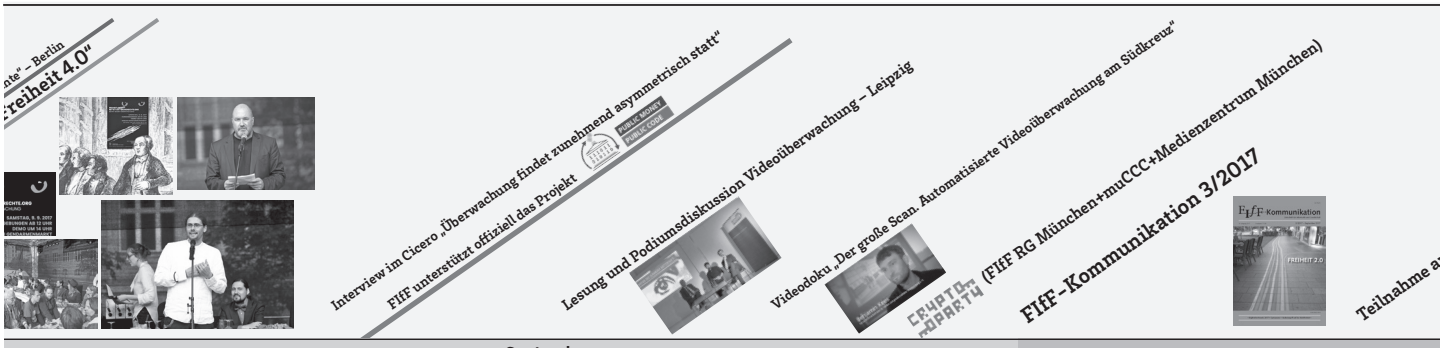
Das Bündnis versammelte sich hinter dem Aufruftext:

> *Wir haben genug von einer Regierung, die durch die Hintertür und über Nacht Gesetze für das Hacken unserer Rechner und Smartphones durchdrückt und uns Bürger nur als Datengeber für staatlichen und kommerziellen „Datenreichtum" sieht.*
>
> *Wir wollen uns für diejenigen starkmachen, denen die Freiheit genommen wurde, weil sie als Journalist.innen und Aktivist.innen ihren Beruf ausgeübt haben. Als Teil einer Gesellschaft, in der Überwachung immer mehr zum Normalzustand wird, setzen wir uns für diejenigen ein, die sich auf private Gespräche über Telefon und Internet verlassen müssen.*
>
> *Wir tanzen an gegen die politische Treibjagd von einem vermeintlichen Bedrohungszustand zum nächsten. Wir wollen eine breite Diskussion darüber, in welcher digitalen Gesellschaft wir leben wollen. Wir setzen uns für das Ende von immer neuen Überwachungsgesetzen ein und fordern stattdessen durchdachtes Handeln im Sinne der Freiheit.*
>
> *Wir stellen uns gegen grundrechtsfeindliche, aktionistische Symbolpolitik und wollen gemeinsam über eine freiheitliche Zukunft nachdenken, von der alle Menschen etwas haben. Wir wollen unsere Freiheit feiern und ein gutes Beispiel für alle sein, die sich kreativ gegen die Alarmisten in der Politik zur Wehr setzen wollen.*
>
> *Wir haben keine Angst und lassen uns auch keine einreden!*

Das FIfF war mit einem Informationsstand präsent und stellte mit Stefan Hügel einen der Redenden auf der Kundgebung. Zusätzlich organisierten wir ...

… die **Festtafel für die Freiheit**, zu der Juliane Krüger und Rainer Rehak als Festkomitee für das FIfF einluden. Inspiriert durch das Hambacher Fest 1832 wurden an der Tafel Brot und Wein gereicht und in Tischreden die Bedeutung der Freiheit herausgestellt:

> *Ohne Freiheit ist alles nichts! Die ist uns jedoch mit den jüngsten Gesetzesvorhaben immer mehr abhanden gekommen. Statt allerdings in Depressionen zu verfallen, lasst uns bei Wein und Kuchen gemeinsam über eine freiheitliche Zukunft nachdenken: In welcher digitalen Gesellschaft wollen wir leben? [...]*
>
> *An einer langen **„Festtafel der Freiheit"** wollen wir mitgebrachte Gedanken genauso teilen wie mitgebrachte Picknickkörbe. Damit erinnern wir zugleich an die Zeit,*



*in der Versammlungsfreiheit und von BürgerInnen organisierte Demonstrationen noch erkämpft und Forderungen nach Freiheit und Bürgerrechten noch als Bankett getarnt werden mussten: Das **Hambacher Fest** von 1832, eines der bedeutendsten Ereignisse der deutschen Demokratiegeschichte und zugleich Wiege der europäischen Einigung.*[18]

Die Kampagne **Public Money – Public Code** fordert, dass durch öffentliches Geld finanzierte Software auch der Öffentlichkeit zu Verfügung stehen und deswegen unter eine freie Lizenz gestellt werden muss:

Warum wird durch Steuergelder finanzierte Software nicht als Freie Software veröffentlicht?

Wir wollen rechtliche Grundlagen, die es erfordern, dass mit öffentlichen Geldern für öffentliche Verwaltungen entwickelte Software unter einer Freie-Software- und Open-Source Lizenz veröffentlicht wird. Wenn es sich um öffentliche Gelder handelt, sollte auch der Code öffentlich sein!

Von allen bezahlter Code sollte für alle verfügbar sein![19]

Das FIfF hat sich der Kampagne angeschlossen.

Referenzen

1 *Britta Schinzel (2017): FREIHEIT 2.0, ein Kunstprojekt von Florian Mehnert. Editorial zum Schwerpunkt. FIfF-Kommunikation 3/2017, S. 12–13*

2 *Britta Schinzel (Hg.) (2017): FREIHEIT 2.0. Schwerpunkt. FIfF-Kommunikation 3/2017, S. 12–41*

3 *Hans-Jörg Kreowski (2017): Cyberpeace-Forum. Einleitung zum Schwerpunkt. FIfF-Kommunikation 2/2017, S. 64–65*

4 *Benjamin Kees, Rainer Rehak, Stefan Hügel (2017): in.visible systemS. Editorial zum Schwerpunkt. FIfF-Kommunikation 1/2017, S. 12–13*

5 *https://www.cryptoparty.in*

6 *http://www.friedensratschlag.de*

7 *Stefan Hügel, Dietrich Meyer-Ebrecht (2017): Cyberwar – Cyberpeace: Wir brauchen einen Gegenentwurf. in: Lühr Henken (Hg.): Spannungen, Aufrüstung, Krieg – und kein Ende? Konfliktanalysen und Lösungsansätze aus der Friedensbewegung. Kassel: Verlag Winfried Jenior*

8 *https://tdrm.fiff.de*

9 *Dietrich Meyer-Ebrecht (2016): Tihange-Doel Radiation Monitoring – ein unabhängiges Messnetz. FIfF-Kommunikation 4/2016, S. 8*

10 *https://amnesty.de*

11 *FIfF/digitalcourage (2017): Erste U-Bahnhaltestelle mit ehrlichen Hinweisen zu Videoüberwachung. SchlussFIfF. FIfF-Kommunikation 1/2017, S. 92*

12 *https://vimeo.com/216584485*

13 *https://www.fiff.de/kurzfilm-cyberpeace-statt-cyberwar*

14 *https://deklaration-fuer-meinungsfreiheit.de, https://www.fiff.de/presse/pressemitteilungen/netzwerkdurchsetzungsgesetz-allianz-fuer-meinungsfreiheit-regt-runden-tisch-an*

15 *https://www.fiff.de/presse/pressemitteilungen/entfesselter-trojaner-grosse-koalition-verhoehnt-it-sicherheit-und-demokratie*

16 *Stefan Hügel, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht (2018): Cyberwar and Cyberpeace. in: Elias G. Carayannis, David F. J. Campbell, Marios P. Efthymiopoulos (Hg.): Handbook of Cyber-Development, Cyber-Democracy and Cyber-Defense. DOI 10.1007/978-3-319-06091-0_41-1. Cham, Switzerland: Springer International Publishing AG*

17 *https://www.fiff.de/verfaelschte-studie-zur-tauglichkeit-grundrechtswidriger-techniken*

18 *https://www.fiff.de/festtafelderfreiheit*

19 *https://publiccode.eu/de/*

FIfF-Studienpreis 2017
1. Preis

Tobias D. Krafft

Qualitätsmaße algorithmischer Entscheidungssysteme in der Kriminalprognostik

In meiner Masterarbeit vom Juni 2017 mit dem Titel Qualitätsmaße binärer Klassifikatoren im Bereich kriminalprognostischer Instrumente der vierten Generation *(Krafft 2017) setze ich mich kritisch mit der Integration von algorithmischen Entscheidungssystemen (ADM) in der Kriminalprognostik auseinander.*

1. Einleitung

In der heutigen digitalen Gesellschaft unterstützen algorithmische Entscheidungssysteme, ADM (*algorithmic decision making*) genannt, vgl. Zweig (2016), zunehmend die Entscheidungsfindung in den verschiedensten Bereichen (Lischka und Klingel 2017), auch in der Justiz. Verlässt sich nun eine Gesellschaft in einem derart relevanten Bereich wie der Justiz in der Urteilsfindung auf algorithmenbasierte Risikoprognosen, so muss deren Evaluation ein zentrales Anliegen sein.

Die Arbeit verfolgt daher das Ziel, den aktuellen Stand um die Beurteilung von ADM-Prozessen im kriminalprognostischen Bereich zu erfassen und kritisch zu hinterfragen. Wegweisend für mein Vorgehen sind die im *ADM-Manifest* (AlgorithmWatch 2016) der 2016 gegründeten Bürgerinitiative *AlgorithmWatch* differenzierten Aspekte als Bestandteil der algorithmischen Entscheidungsfindung.

Während in den USA schon seit längerem ADM-gesteuerte Kriminalprognosen eingeführt sind, nutzen deutsche Gerichte aufgrund des *Individualisierungsgebots* (Maschke 2008) in der deutschen Rechtsprechung individuelle kriminalprognostische Gutachten, die durch entsprechende Sachverständige erstellt und bei gewissen strafrechtlichen Entscheidungen miteinbezogen werden müssen[1]. Es ist jedoch zu vermuten, dass sich dies im Hinblick auf die Aufmerksamkeitsökonomie sowohl der Richter als auch der Sachverständigen in absehbarer Zeit ändern könnte, sollte die deutsche Justiz mit Argumenten der Effizienz und angeblicher Objektivität vom Einsatz ADM-gestützter Prognoseinstrumente überzeugt werden. Insofern war es ein zentrales Anliegen der Arbeit, eine weitere Diskussion über Chancen und Risiken beim Einsatz algorithmenbasierter Risikoprognosen auf wissenschaftlicher Grundlage zu ermöglichen; siehe auch Zweig et al. (2018).

Dazu wird im Folgenden das üblicherweise verwendete Qualitätsmaß zur Bewertung von Klassifikatoren, die sogenannte *Area under the Receiver Operating Characteristic (AUC)* kritisch hinterfragt und dem *Positive Predictive Value among the first k* (PPV_k) als weitere Bewertungsalternative, die zudem als Evaluationsmöglichkeit den richterlichen Entscheidungsprozess realistischer abbildet, gegenübergestellt. Die Überprüfung, ob es Klassifikatoren gibt, für die diese Qualitätsmaße zu unterschiedlichen Ergebnissen kommen können, kam zu frappierenden Ergebnissen, denn es ergaben sich mögliche Abweichungen von bis zu 0,75. Die Diskrepanz zwischen den beiden Qualitätsmaßen konnte an einem realen Datensatz aus den USA für das sogenannte COMPAS-Tool, ein kriminalprognostisches Instrument der vierten Generation, nachgewiesen werden.

Im abschließenden Fazit werden mögliche gesellschaftliche Folgen aufgezeigt und versucht, Handlungsempfehlungen und Lösungsvorschläge zu umreißen.

1.1 Die Integration von ADM-gestützten Risikoprognosen im US-amerikanischen Justizwesen

Das Justizsystem der USA ist im Begriff, zu kollabieren: Als Folge der etablierten Praxis, drakonische Strafen zur Abschreckung zu nutzen, sitzen derzeit in US-amerikanischen Gefängnissen knapp 2,15 Millionen Inhaftierte (Statista 2017) ein. Die hohe Zahl von Gefängnisinsassen beschert den USA explodierende Kosten im Strafvollzug, sodass die Suche nach einer effizienten Kostenreduzierung ein zentrales Anliegen der US-amerikanischen Justiz ist.

Die Erkenntnis, kostenintensive Haftstrafen auf Bewährung auszusetzen, ließ die Kriminalprognose zunehmend in den Fokus juristischer Überlegungen rücken, und man forderte bei der Urteilsfindung eine genauere Einschätzung des Kriminalitätsrisikos (Chettiar und Gupta 2011). Daher benutzt die Justiz aller US-Bundesstaaten seit Jahren Tools zur Risikobewertung in verschiedenen Bereichen der Rechtsprechung (EPIC 2017), wobei von einigen Behörden, wie zum Beispiel in Florida, hauptsächlich das von der US-Firma *Northpointe* Ende der 1990er-Jahre entwickelte *COMPAS Assessment Tool (Correctional Offender Management Profiling for Alternative Sanctions)* zum Einsatz kommt (Northpointe 2012b).

2. Problematik und Instrumente der Kriminalprognose

In früheren Zeiten oblag die Rechtsprechung allein dem Richter und etwaigen Beratern. Diese nur auf der subjektiven Entscheidung des Richters basierende Urteilsfindung war extrem anfällig für Fehlurteile, auch hinsichtlich der Höhe des verhängten Strafmaßes, sodass man seit der Aufklärung (Cesare 1764) versuchte, objektive Kriterien für die Urteilsfindung zu entwickeln. Doch trotz aller Bemühungen sieht sich auch heute noch jede Kriminalprognose mit dem Problem konfrontiert, dass eine hundertprozentige Vorhersage nicht garantiert werden kann. Das menschliche Verhalten resultiert eben nicht nur aus individuellen Persönlichkeitsmerkmalen, sondern wird dazu durch verschiedenste situative Faktoren beeinflusst (Danziger et al. 2011), die aufgrund ihrer Variabilität nur vage abschätzbar sind (Bliesener et al. 2014, S. 425f.).

Der Baxstrom-Fall aus dem Jahr 1966 sensibilisierte weltweit auch die Öffentlichkeit für diese Problematik. Bei dem unbeabsichtigten Experiment mussten aus formaljuristischen Gründen der Gewalttäter Johnnie Baxstrom sowie 967 weitere, als gefährlich eingeschätzte Straftäter im Bundesstaat New York freigelassen werden. Nach insgesamt vier Jahren in Freiheit waren aber lediglich 14,2 % der als gefährlich eingestuften Täter erneut straffällig geworden, darunter nur 2,5 % wegen schwerer

Gewaltstraftaten (Obergfell-Fuchs 2011, S. 17; US Supreme Court 1966).

2.1 Instrumente der Kriminalprognostik

Im Bestreben, die Kriminalprognose auf eine überprüfbare Basis zu stellen, wurden eine Vielzahl von Prognoseinstrumenten entwickelt (Guy 2008), sodass hier der in der Fachliteratur üblichen Einordnung in ‚Generationen' grob gefolgt wird (Döbele 2014, S. 20–26; Rettenberger und Franqué 2013, S. 21f.).

Anfang des 20. Jahrhunderts wurden erste Kriterienkataloge entwickelt, sogenannte Prognosetafeln, mit denen man potenzielle Straftäter zu identifizieren hoffte (Nedopil und Gross 2005, S. 43f.) und die den Grundstein zur statistischen Kriminalprognose legten. Sie basierten auf rückfallrelevanten Faktoren, die aus Akten entlassener Straftäter extrahiert wurden. Diese statischen Merkmale wurden von der zweiten Generation durch personen- und tatbezogene Faktoren ergänzt, dennoch blieben etwaige Wandlungen der Täterpersönlichkeit weiterhin unberücksichtigt, sodass der Straftäter hier „zum Gefangenen seiner Biographie" (Dittmann 2003) wurde. Folgerichtig führte die dritte Generation zu Instrumenten, welche die Datenbasis um dynamische Faktoren, wie „persönliche Einstellung der Straftäter, […], soziale Bindungen" usw. (Döbele 2014) erweiterten.

Die vierte Generation repräsentiert den aktuellsten Stand der Kriminalprognostik und sieht ein breites Band an Einsatzmöglichkeiten für verschiedenste Prognosebereiche vor. Zum einen fließen immer mehr variable Aspekte in den Beurteilungsprozess ein, zum anderen beschränken sich die Tools nicht mehr nur auf Risikoprognosen von Verhaltensweisen, sondern bieten Empfehlungen für Therapiepläne an oder werben sogar damit, dass sie Aussagen machen könnten, ob ein Straftäter vor Gericht erscheine oder nicht, vgl. z. B. Northpointe (2012b).

2.2 COMPAS als Instrument der vierten Generation

Ein bekanntes Vorhersageinstrument der vierten Generation ist die *Correctional Offender Management Profile for Alternative Sanctions,* kurz COMPAS genannte Web-Applikation, die vom *Northpointe Institute for Public Management Inc.* als automatisierte Entscheidungsunterstützung zur Bewertung von Straffälligen entwickelt wurde (Northpointe 2012a). Die Firma wirbt mit dem Angebot, mit Hilfe ihres Algorithmus ließe sich auf Basis von 137 Merkmalen eine genaue Prognose der Rückfallwahrscheinlichkeit (*predicted recidivism*) eines Angeklagten erstellen (Brennan et al. 2009b), so dass einige Staaten der USA diese bereits im juristischen Prozess einsetzen, um beispielsweise Richter bei Bewährungsfragen zu beraten.

Wie bei fast allen Instrumenten der vierten Generation ist jedoch auch dieser Algorithmus proprietär und folglich eine ‚Blackbox' (Diakopoulos 2014), sodass die geringe Transparenz der Algorithmen und die daraus resultierende fehlende Einsicht in den Bewertungsprozess auch beim COMPAS-Tool ein großes Problem darstellt. Mögliche Überprüfungsstrategien sind sogenannte Blackbox-Analysen, die eigentlich aus der Softwareentwicklung stammen, vgl. Beizer (1995), und bei denen ohne Kenntnis der inneren Funktionsweise der Algorithmen die tatsächlichen Ergebnisse mit den zu erwartenden überprüft werden.

ProPublica, eine durch Spenden finanzierte US-Rechercheorganisation, hat 2016 eine Studie veröffentlicht, die für das COMPAS-Tool eine dramatische Ungleichbehandlung von Schwarzen und Weißen nachgewiesen hat (Angwin et al. 2016). Die Antwort aus dem Hause Northpointe (Dieterich et al. 2016) begründete die festgestellten Ergebnisse mit der Nutzung eines anderen Fairnesskriteriums und zeigt so den sehr weiten Modellierungsrahmen auf, dem solche Instrumente unterliegen. An dieser Stelle sei noch angemerkt, dass die unter *Northpointe* bekannte und erfolgreiche Firma kurz nach der Debatte aus ungeklärten Gründen ihren Namen in *Equivant* geändert hat.

3. Abweichung zwischen *AUC* und PPV_k

Die Kontroverse von 2016 zeigt die dringende Notwendigkeit, den Bewertungsprozess dieser Algorithmen näher zu beleuchten. Anderenfalls ist keine realistische Einschätzung möglich, ob und wann ein solches ADM zur Beurteilung von Menschen in einem so essenziellen Bereich wie der Justiz eingesetzt werden sollte.

Die in der Justiz Anwendung findenden Instrumente münden in binäre Klassifikatoren[2], da die juristische Fragestellung nur duale Urteile zulässt: Schuldig oder nicht. Das bestehende Repertoire

Tobias D. Krafft

Tobias D. Krafft, M.Sc., ist Doktorand am Lehrstuhl *Algorithm Accountability* von Prof. Katharina A. Zweig an der TU Kaiserslautern. Als Preisträger des Studienpreises 2017 des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung reichen seine Forschungsinteressen von der (reinen) Analyse algorithmischer Entscheidungssysteme bis hin zum Diskurs um deren Einsatz im gesellschaftlichen Kontext. Im Rahmen seiner Promotion hat er das Datenspendeprojekt mitentwickelt und einen Teil der Datenanalyse durchgeführt. Er ist einer der Sprecher der Regionalgruppe Kaiserslautern der Gesellschaft für Informatik, die es sich zur Aufgabe gemacht hat, den interdisziplinären Studiengang der Sozioinformatik (TU Kaiserslautern) in die Gesellschaft zu tragen. Zuschriften an *krafft@cs.uni-kl.de*

zur Bewertung solcher Klassifikatoren ist zwar differenziert, jedoch wurden bereits 1977 die ersten Rückfälligkeitsvorhersage-Statistiken mit der *Area under the Receiver Operating Characteristic (AUC)* bewertet (Fergusson et al. 1977). Dieses im maschinellen Lernen häufig verwendete Qualitätsmaß hat sich in der Kriminalprognose als vorherrschend etabliert.

Obwohl es sich hierbei eigentlich um eine Betrachtung der Sensitivität und Falsch-Positiv-Rate handelt (Aggarwal 2015, S. 340f.; Bradley 1997, S. 2; Peterson et al. 1954), lässt sich die *AUC* bei der Bewertung binärer Klassifikatoren zusätzlich als die Wahrscheinlichkeit interpretieren, in einer zufälligen Stichprobe, bestehend aus je einem Element beider Klassen, dem Element der ersten Klasse eine höhere Wahrscheinlichkeit zuzuordnen, zu dieser zu gehören (Hanley und McNeil 1982, S. 2). Hat ein ADM-System also eine *AUC* von 0,72, so kann es, gegeben einen rückfällig werdenden Straftäter und einen, der es nicht wird, mit einer Wahrscheinlichkeit von 72 % korrekt entscheiden, welcher von beiden der rückfällig Werdende ist.

Dennoch ist ihr Ruf als bestes Qualitätsmaß der Kriminalprognose (Barnoski und Drake 2007) insgesamt nicht nachvollziehbar, auch die uneinheitliche Anwendung der *AUC* in verschiedenen Disziplinen erstaunt. So verwendet die Humanmedizin andere Schwellenwerte (Leushuis et al. 2009) als die Risikoprognose. Es ist nicht zu verstehen, warum diese Werte je nach Disziplin differieren (Leushuis et al. 2009; Endrass et al. 2008) und warum bei kriminalprognostischen Instrumenten ein deutlich niedrigerer Wert (0,65–0,75) (Lansing 2012, S. 22) als Garant für eine gute Klassifikation angesehen wird.

Aber selbst, wenn ein Klassifikator eine *AUC* von 1,00 erreicht, könnte er jedem Rückfälligen eine Rückfallwahrscheinlichkeit von 10 % und jedem nicht Rückfälligen eine von 9 % prognostizieren. Obwohl laut *AUC* diese Klassifizierung eine perfekte Trennschärfe aufweist, ließe sich einerseits sehr schwer zwischen den beiden Klassen separieren, andererseits ist eine solch niedrige Rückfallwahrscheinlichkeit in keiner Art hilfreich, wenn die Basisrate höher liegt als die Prognose.

Diese Diskrepanz würde sich zwar auch bei einer Nutzung des PPV_k widerspiegeln, jedoch bildet dieser, wie im Folgenden erläutert wird, den generellen Entscheidungsprozess eines Richters deutlich besser ab.

Der *Positive Predictive Value among the first k (PPV_k)* stellt eine andere, in der Kriminalprognostik allerdings kaum beachtete Möglichkeit dar, einen Klassifikator zu bewerten. Allein die Eigenschaft „ist unter den ersten k", also am höchsten gerankt, ist hier relevant, sodass der PPV_k eine Möglichkeit bietet, den Fokus auf die tatsächliche Anzahl korrekt klassifizierter Objekte im vorderen Bereich der Sortierung zu legen. Da er fast vollständig auf eine Betrachtung der genauen Sortierung der Elemente, vor allem im hinteren Teil, verzichtet, wird er dem richterlichen Entscheidungsprozess zudem deutlich gerechter, denn **auch Richter folgen wahrscheinlich einer inneren Skala,** um für einen Straftäter zu bestimmen, ob dieser rückfällig werden würde oder ab welchem Bereich Straftätern eine Bewährung gewährt wird oder nicht.

Sowohl aufgrund seiner Eignung zur Bewertung eines Klassifikators als auch seiner Nähe zum richterlichen Entscheidungsprozess wurde der PPV_k gewählt, um der *AUC* mathematisch gegenübergestellt zu werden. Das Ergebnis der Analyse zur Klärung, wie weit die beiden Werte für einen gegebenen Klassifikator voneinander abweichen können, ist besorgniserregend: Abweichungen von bis zu 0,75 sind nachweislich möglich.[3]

Die Abweichung dieser beiden Maße ist auch insofern von Relevanz, als Northpointe aktuell nur die hohe *AUC* (Northpointe 2012b) angibt, um ihre vermeintlich guten Klassifikatoren zu bewerben.

4. Überprüfung der Ergebnisse für das COMPAS Assessment Tool

Die aufgezeigten Ergebnisse geben zwar für eine binäre Klassifizierung Aufschlüsse über die Lage der jeweiligen maximal/minimal möglichen PPV_k-Werte bei fixierter *AUC* und vice versa, jedoch können mittels dieser Formeln noch keine Rückschlüsse darüber gezogen werden, wie sich die Verteilung zwischen diesen Werten darstellt. Um die gesellschaftliche Brisanz der möglicherweise fehlenden Korrelation anhand von anwendungsbezogenen Daten zu erörtern, wurden die von ProPublica öffentlich bereitgestellten Datensätze extrahiert und entsprechend analysiert. Da hierbei das momentan in Wisconsin, USA, auf jeder Stufe des Justizprozesses angewandte (Wisconsin Department of Correction 2018) COMPAS Assessment Tool anhand echter Datensätze evaluiert werden kann, lässt sich überprüfen, ob im Anwendungsbezug die Korrelation von *AUC* und PPV_k gewahrt bleibt oder sie deutlich voneinander abweichen. Es muss darauf hingewiesen werden, dass den folgenden Ergebnissen lediglich ein Algorithmus und ein lokal erfasster Datensatz zugrunde liegt.

4.1 Erläuterung zum COMPAS Assessment Tool

Das Tool wurde 1998 als „Breitband"-Bewertung konzipiert und kann anhand verschiedener Fragebögen in 22 verschiedenen Bedürfnis- und Risikobereichen Prognosen über Individuen erstellen (Northpointe 2012a), unter anderem die folgenden:

- *General Recidivism Risk Scale:* Generelles Rückfallrisiko *(GRRS)*
- *Violent Recidivism Risk Scale:* Gewaltbasiertes Rückfallrisiko *(VRRS)*

Die kontinuierliche Vorhersage der einzelnen Skalen wird im Justizwesen auf binäre Entscheidungen abgebildet, z. B. auf Fragen, ob der verurteilte Straftäter auf Bewährung das Gefängnis verlassen darf oder nicht. Somit bietet sich in der Evaluation das Spektrum eines binären Klassifikators an, weshalb Northpointe (2012b) selbst die hohe *AUC* seines Algorithmus lobt und mit der *AUC* in verschiedenen Studien wirbt, die den COMPAS GRRS mit den in Tabelle 1 aufgeführten *AUC*-Werten beurteilen (Northpointe 2012b).

Quelle	Jahr	Stichprobengröße	Betrachtungszeitraum der Rückfälligkeit	AUC
(Brennan et al. 2009a) (Brennan et al. 2009b)	2009	2.328	1 Jahr	0,68
(Farabee et al. 2010)	2010	25.009	2 Jahre	0,70
(Lansing 2012)	2012	11.289	2 Jahre	0,71

Tabelle 1: Auszug der von Northpointe (2012b) veröffentlichten Liste an Evaluationen des COMPAS-Assessment-Tools

4.2 Auswertung der ProPublica-Daten zum COMPAS Assessment Tool

Dem vorliegenden ProPublica-Datensatz konnten für 11.777 Personen alle notwendigen Informationen entnommen werden, um sowohl die *AUC* als auch den erreichten PPV_k zu bestimmen[4].

Wenn angenommen wird, dass ein Richter in seinem Distrikt den vorliegenden Datensatz zu bearbeiten hat, so hätte er bei der zufälligen Verurteilung eines Delinquenten entsprechend der im Datensatz vorherrschenden Basisrate eine Wahrscheinlichkeit von 36 %, dass dieser rückfällig wird. Nutzt er nun das vorgestellte COMPAS-Tool und kann auf Grund seiner Erfahrung mit dem Distrikt die Basisrate korrekt abschätzen, verurteilt also nur die Straftäter, die in den oberen 36 % der Datenpunkte liegen, so erreicht er, der Interpretation des PPV_k folgend, lediglich mit einer Wahrscheinlichkeit von ungefähr 53 % (siehe Abbildung 1) einen wirklich rückfällig Werdenden.

Viel drastischer stellt sich der Unterschied zwischen *AUC* und PPV_k für die *Violent Recidivism Risk Scale (VRRS)* dar. In Abbildung 2 ist durch den grünen Punkt zu erkennen, dass es Northpointe mit diesem Klassifikator deutlich in das untere Drittel des möglichen Wertebereichs für den PPV_k mit vorliegender *AUC* von 0,69 schafft. Es ist jedoch zu beachten, dass der Klassenunterschied mit geringer Basisrate von 8 % deutlich größer ist, sodass es wiederum schwieriger wird, eine Klassifizierung zu schaffen, welche die wenigen Rückfälligen von den vielen nicht Rückfälligen separiert. Ein Richter würde hier durch zufällige Urteile einen tatsächlich gewaltbasiert Rückfälligen lediglich mit einer der Basisrate entsprechenden Wahrscheinlichkeit von 8 % erfassen. Dieser Wert kann zwar durch die Anwendung des COMPAS-Tools um 11,6 Prozentpunkte erhöht werden, jedoch liegt die Trefferwahrscheinlichkeit innerhalb der ersten 1.085 Straffälligen immer noch bei nur 20 % und gibt dem Anwender keine wirklich stichhaltige Prognose, auf der sein Urteil aufgebaut werden könnte.

5. Fazit

Die hohe Nutzungsquote der *AUC* bei binären Klassifikatoren für Rückfälligkeitsvorhersagen erscheint willkürlich und nur durch die Verbreitung beim maschinellen Lernen begründet. Auch die Überprüfung der *AUC* hinsichtlich ihrer Eignung als

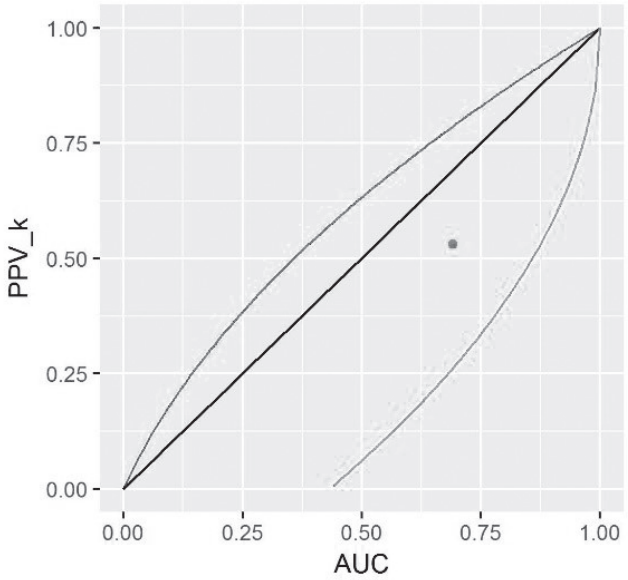


Abbildung 1: Auswertung des COMPAS-Scores (GRRS) auf den ProPublica-Daten (grüner Punkt) bei eingezeichnetem maximalen PPV_k (obere Kurve, blau) und minimalem PPV_k (untere Kurve, rot) für jeweils fixierte AUC auf der x-Achse, Abbildung aus (Krafft 2017).

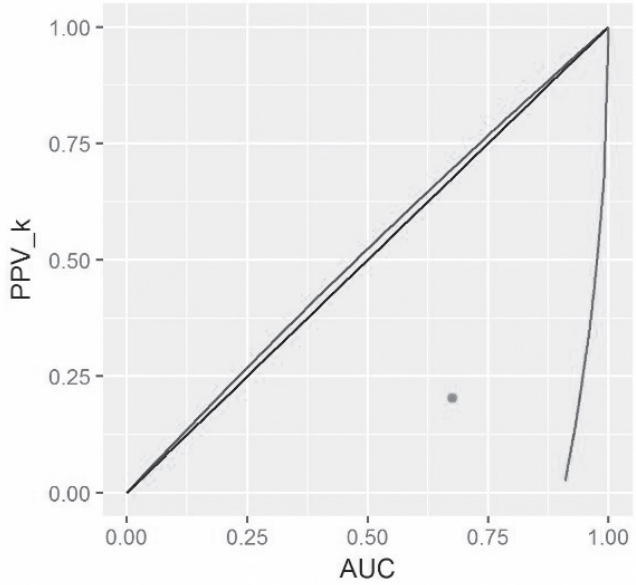


Abbildung 2: Auswertung des COMPAS-Scores (VRRS) auf den ProPublica-Daten (grüner Punkt) bei eingezeichnetem maximalen PPV_k (obere Kurve, blau) und minimalem PPV_k (untere Kurve, rot) für jeweils fixierte AUC auf der x-Achse, Abbildung aus (Krafft 2017).

Bewertungsmaßstab in der ADM-gestützten Kriminalprognose blieb deutlich hinter den Erwartungen zurück. Die Abweichung vom näher am richterlichen Entscheidungsprozess evaluierenden PPV_k kann inakzeptabel hoch sein, sodass eine zukünftige Heranziehung der *AUC* als ausschließliches Qualitätsmaß kritisch zu hinterfragen ist.

Sollte die *AUC* weiterhin in der Justiz Verwendung finden, müssten Gutachter wie Richter die Aussagekraft eines hohen *AUC*-Wertes richtig zu interpretieren wissen und dürften die Fähigkeit der Instrumente zur Rückfälligkeitsprognose aufgrund des Vorliegens hoher Validitätswerte nicht überschätzen (Eher et al. 2008). Hier bedarf es massiver Aufklärung, da die Tendenz besteht, dass Menschen softwarebasierte Prognosen als verlässlicher und objektiver empfinden, was die Gefahr einer unkritischen Übernahme dieser Prognosen birgt.

Die aufgeführten Probleme haben weiterhin gezeigt, dass es von immenser Bedeutung ist, das Anwendungsgebiet sowie die dort vorherrschende Datenlage und Qualität genauestens mit der Lernumgebung der Algorithmen abzugleichen, vgl. Burnham et al. (2002), denn „der beste Klassifikationsalgorithmus ist gerade so gut wie die ihm vorliegende Information" (Hengen et al. 2004).

Mögliche Konsequenzen und Forderungen

Sollte im deutschen Justizwesen die Einführung ADM-gesteuerter Prozesse zur Diskussion stehen, könnte Deutschland von den Erfahrungen und Fehlern anderer Länder profitieren. Es ist zu hoffen, dass dies ohne überstürzten politischen Aktionismus, sondern mit Bedacht nach einer ausführlichen Debatte erfolgt. Keinesfalls sollte es wie beim Jugendstrafrecht in den USA (Baird 2009, S. 2) zu einer voreiligen Nutzung von Algorithmen kommen. Bei der Risikoprognose steht ein Mensch im Mittelpunkt algorithmischer Betrachtung, sodass Auswahl, Überprüfung und Nutzung von algorithmischen Entscheidungshilfen größte wissenschaftliche und gesellschaftliche Aufmerksamkeit geschenkt werden muss. Es geht um existenzielle Urteile für die Betroffenen und Fehlurteile könnten fatale Auswirkungen auf deren Leben haben[5].

Damit aber eine weiterführende Forschung betrieben werden kann, müsste der Staat die notwendigen finanziellen Mittel zur Verfügung stellen. Es ist kein akzeptabler Status quo, wenn kritische Untersuchungen zu Risiken und gesellschaftlichen Folgen der ADM-Prozesse abhängig vom Interesse und verfügbaren Budget beliebiger Institutionen sind. So ist der Anstoß der Fairness-Debatte um das COMPAS-Tool nur dem Engagement des Recherchebüros ProPublica zu verdanken.

Schon normative Entscheidungen, z. B. über Fairness-Kriterien, müssten bei der Gestaltung eines ADM-Prozesses im Konsens mit der Gesellschaft gefällt werden. Sinnvolle Handlungsempfehlungen hierfür gibt das ADM-Manifest (AlgorithmWatch 2016) in den Punkten 3/4:

3. ADM-Prozesse müssen nachvollziehbar sein, damit sie demokratischer Kontrolle unterworfen werden können.
4. Demokratische Gesellschaften haben die Pflicht, diese Nachvollziehbarkeit herzustellen: durch eine Kombination aus Technologien, Regulierung und geeigneten Aufsichtsinstitutionen.

Demzufolge wären die Vertreiber gefordert, die Algorithmen ihrer angebotenen Tools so weit offenzulegen, „dass Erklärbarkeit, Nachvollziehbarkeit, unabhängige Überprüfbarkeit und die Möglichkeiten zur forensischen Datenanalyse gegeben sind" (Lischka und Klingel 2017). Sollte dies nicht geschehen, wäre es auch hier Aufgabe des Staates, durch geeignete Maßnahmen eine informierte Debatte zu ermöglichen.

Abschließend lässt sich konstatieren, dass die Gesellschaft bei der Integration eines Risikovorhersage-Instruments die Auswahl des Bewertungsmaßstabs als eine der wichtigsten Modellierungsentscheidungen verstehen muss, denn:

> *„We recognize that creation of valid, reliable, and robust risk assessment instruments is both a science and an art."*[6]

Referenzen

Aggarwal CC (2015) Data mining; The textbook. Springer, Cham

AlgorithmWatch (2016) Das ADM-Manifest | The ADM Manifesto. https://algorithmwatch.org/das-adm-manifest-the-adm-manifesto/. Zugegriffen: 22. Februar 2018

Angwin J, Larson J, Mattu S, Kirchner L (2016) Machine bias; There's software used across the country to predict future criminals. And it's biased against blacks. ProPublica, 23. Mai 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Zugegriffen: 22. Februar 2018

Azariadis C (1981) Self-fulfilling prophecies. J Econ Theory 25:380–396. doi:10.1016/0022-0531(81)90038-7

Baird C (2009) A question of evidence; A critique of risk assessment models used in the justice system. National Council on Crime and Delinquency, Madison, WI

Barnoski R, Drake EK (2007) Washington's Offender Accountability Act; Department of Corrections' static risk instrument. Washington State Institute for Public Policy, Olympia, WA. http://www.wsipp.wa.gov/ReportFile/977/Wsipp_Washingtons-Offender-Accountability-Act-Department-of-Corrections-Static-Risk-Instrument_Full-Report-Updated-October-2008.pdf

Beizer B (1995) Black-box testing; Techniques for functional testing of software and systems. Wiley, New York, NY

Bliesener T, Lösel F, Köhnken G (Hrsg) (2014) Lehrbuch der Rechtspsychologie. Huber, Bern

Bradley AP (1997) The use of the area under the ROC curve in the evaluation of machine learning algorithms. Pattern Recognit 30:1145–1159. doi:10.1016/S0031-3203(96)00142-2

Brennan T, Dieterich B, Breitenbach M, Mattson B (2009a) A Response to "Assessment of Evidence on the Quality of the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS)". Northpointe Institute for Public Management, Inc. http://www.northpointeinc.com/files/whitepapers/Response_to_Skeem_Louden_Final_071509.pdf

Brennan T, Dieterich W, Ehret B (2009b) Evaluating the predictive validity of the Compas risk and needs assessment system. "Crim Justice Behav 36:21–40. doi:10.1177/0093854808326545

Burnham BR, Thompson DF, Jackson WG (2002) Positive predictive value of a health history questionnaire. Mil Med 167:639–642. doi:10.1093/milmed/167.8.639

Cesare B (1764) Dei delitti e delle pene. In: Opera immortale del Marchese di Beccaria. R. Sammer, Wien, 1798

Chettiar IM, Gupta V (2011) Smart reform is possible; States reducing incarceration rates and costs while protecting communities. American Civil Liberty Union (ACLU). SSRN, 27. September 2011. doi:10.2139/ssrn.1934415

Danziger S, Levav J, Avnaim-Pesso L (2011) Extraneous factors in judicial decisions. PNAS USA 108:6889–6892. doi:10.1073/pnas.1018033108

Diakopoulos N (2014) Algorithmic accountability reporting; On the investigation of black boxes. Tow Center for Digital Journalism, Columbia University, Februar 2014. http://towcenter.org/wp-content/uploads/2014/02/78524_Tow-Center-Report-WEB-1.pdf

Dieterich W, Mendoza C, Brennan T (2016) COMPAS risk scales: Demonstrating accuracy equity and predictive parity. Northpointe. http://go.volarisgroup.com/rs/430-MBX-989/images/ProPublica_Commentary_Final_070616.pdf

Dittmann V (2003) Was kann die Kriminalprognose heute leisten? In: Häßler F, Rebernik E, Schnoor K, Schläfke D, Fegert JM (Hrsg) (2003) Forensische Kinder-, Jugend- und Erwachsenenpsychiatrie; Aspekte der forensischen Begutachtung. Schattauer, Stuttgart, S 173–187

Döbele A-L (2014) Standardisierte Prognoseinstrumente zur Vorhersage des Rückfallrisikos von Straftätern; Eine kritische Betrachtung des Einsatzes in der Strafrechtspflege aus juristischer Sicht. Kovač, Hamburg

Eher R, Rettenberger M, Schilling F, Pfäfflin F (2008) Validität oder praktischer Nutzen? Rückfallvorhersagen mittels Static-99 und SORAG. Eine prospektive Rückfallstudie an 275 Sexualstraftätern. Recht & Psychiatrie 26:79–88

Electronic Privacy Information Centre, EPIC (2017) Algorithms in the criminal justice system. https://epic.org/algorithmic-transparency/crim-justice/. Zugegriffen: 25. Januar 2018

Endrass J, Urbaniok F, Held L, Vetter S, Rossegger A (2008) Accuracy of the Static-99 in predicting recidivism in Switzerland. Int J Offender Ther Comp Criminol. doi:10.1177/0306624X07312952

Farabee D, Zhang S, Roberts REL, Yang J (2010) COMPAS validation study; Final report. UCLA Integrated Substance Abuse Programs (ISAP), 15. August 2010. https://www.cdcr.ca.gov/adult_research_branch/Research_Documents/COMPAS_Final_report_08-11-10.pdf

Fergusson DM, Fifield JK, Slater SW (1977) Signal detectability theory and the evaluation of prediction tables. J Res Crime Delinq 14:237–246. doi:10.1177/002242787701400209

Guy LS (2008) Performance indicators of the structured professional judgment approach for assessing risk for violence to others; A meta-analytic survey. Dissertation, Simon Fraser University

Hanley JA, McNeil BJ (1982) The meaning and use of the area under a receiver operating characteristic (ROC) curve. Radiology 143:29–36. doi:10.1148/radiology.143.1.7063747

Hengen H, Feid M, Pandit M (2004) Überwacht lernende Klassifikationsverfahren im Überblick, Teil 1 (Overview of Supervised learning Classification Methods, Part 1). Automatisierungstechnik/Methoden und Anwendungen der Steuerungs-, Regelungs- und Informationstechnik 52(3):A1–A8. doi:10.1524/auto.52.3.A1.34763

Krafft TD (2017) Qualitätsmaße binärer Klassifikatoren im Bereich kriminalprognostischer Instrumente der vierten Generation. Masterarbeit, Fachbereich Informatik, TU Kaiserslautern. arXiv:1804.01557

Lansing S (2012) New York State COMPAS-probation risk and need assessment study; Examining the recidivism scale's effectiveness and predictive accuracy. NCJ 247345. https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=269445.

Leushuis E, van der Steeg JW, Steures P, Bossuyt PMM, Eijkemans MJC, van der Veen F, Mol BWJ, Hompes PGA (2009) Prediction models in reproductive medicine; A critical appraisal. Hum Reprod Update 15:537–552. doi:10.1093/humupd/dmp013

Lischka K, Klingel A (2017) Wenn Maschinen Menschen bewerten. Bertelsmann Stiftung. doi:10.11586/2017025

Maschke W (2008) Die Kriminalprognose im Einzelfall. In: Dölling D (Hrsg) (2009) Gutachten im Jugendstrafverfahren. DVJJ, Heidelberg, S 85–102

Nedopil N, Groß G (2005) Prognosen in der Forensischen Psychiatrie; Ein Handbuch für die Praxis. Pabst, Lengerich, Westf.

Northpointe (2012a) COMPAS risk & need assessment system; Selected questions posed by inquiring agencies. http://www.northpointeinc.com/files/downloads/FAQ_Document.pdf. Zugegriffen: 22. Februar 2018

Northpointe (2012b) Practitioner's guide to COMPAS core. http://www.northpointeinc.com/downloads/compas/Practitioners-Guide-COMPAS-Core-_031915.pdf

Obergfell-Fuchs J (2011) Gefährliche Straftäter aus kriminologischer und psychologischer Sicht. In: Sicherungsverwahrung und Führungsaufsicht; Wie gehen wir mit gefährlichen Straftätern um? Evangelische Akademie, Bad Boll

Peterson W, Birdsall T, Fox W (1954) The theory of signal detectability. Trans IRE Prof Group Inf Theory 4(4):171–212. doi:10.1109/TIT.1954.1057460

Rettenberger M, von Franqué F (Hrsg) (2013) Handbuch kriminalprognostischer Verfahren. Hogrefe, Göttingen, Bern, Wien

Statista (2017) Länder mit der größten Anzahl an Inhaftierten (Februar 2017*). https://de.statista.com/statistik/daten/studie/3212/umfrage/laender-mit-den-meisten-gefangenen-im-jahr-2007/. Zugegriffen: 22. Februar 2018

US Supreme Court (1966) Baxstrom v. Herold, 383 U.S. 107 (1966). https://supreme.justia.com/cases/federal/us/383/107/case.html

Wisconsin Department of Correction (2018) COMPAS. https://doc.wi.gov/Pages/AboutDOC/COMPAS.aspx. Zugegriffen: 29. März 2018

Zweig KA (2016) 2. Arbeitspapier: Überprüfbarkeit von Algorithmen. AlgorithmWatch, 7. Juli 2016. http://algorithmwatch.org/zweites-arbeitspapier-ueberpruefbarkeit-algorithmen/. Zugegriffen: 22. Februar 2018

Zweig KA, Wenzelburger G, Krafft TD (2018) On chances and risks of security related algorithmic decision making systems. Erscheint in European Journal for Security Research

Anmerkungen

1 *Die Ausführungen zur Handhabung der Risikoprognostik im deutschen Justizwesen sind in Kapitel 1.2.2 meiner Masterarbeit (Krafft 2017) nachzulesen.*

2 *Eine genauere Erklärung der Terminologie ist im Kapitel 2 meiner Masterarbeit (Krafft 2017) nachzulesen.*

3 *Die mathematische Beweisführung kann bei Interesse in Kapitel 4 der Masterarbeit (Krafft 2017) nachgelesen werden.*

4 *Der Wert für die tatsächliche Rückfälligkeit eines Individuums bezieht sich in dem durch ProPublica offerierten Datensatz auf ein Zweijahresfenster, soweit es das Broward County Sheriff's Office in Florida erfassen konnte.*

5 *Als Beispiel sei der ‚Feedback Loop' genannt, nach dem ein ‚false positive' (fälschlicherweise Verurteilter) tatsächlich im Sinne der ‚self fulfilling prophecy' (Azariadis 1981) kriminell würde.*

6 *Wir stellen fest, dass die Erstellung eines fundierten, zuverlässigen und robusten Risikobeurteilungsinstruments sowohl eine Wissenschaft als auch eine Kunst ist. (Baird 2009, S. 10)*

FIfFKon-Splitter II

An dieser Stelle sollen nun Besucherinnen und Besucher der FIfF-Konferenz 2017 zu Wort kommen, die einerseits durch permanente unterstützende Tätigkeiten zum Gelingen der Tagung beigetragen haben, andererseits aber auch etliche der Vorträge inhaltlich konzentriert und im Detail verfolgen konnten.

Warum die Bedeutung des FIfF nicht groß genug sein kann und warum ich Mitglied wurde

Als Informatikstudent in Jena habe ich von der FIfFKon 2017 *TRUST – Wem kann ich trauen im Netz und warum?* erfahren. Ein unaufhebbares Thema, nicht nur dieses, finde ich.

Nicht erst seit den Snowden-Enthüllungen bin ich der Ansicht, dass die Informatik in Zukunft eine immer größere Bedeutung in der Gesellschaft haben wird und auch die Verflechtung wie auch die Beziehungen und gesellschaftlichen Zusammenhänge nicht wegzudenken sind. Dass flächendeckende Überwachung schon lange praktiziert wird, veranschaulicht, denke ich, sehr gut das Buch *Überwachtes Deutschland: Post- und Telefonüberwachung in der alten Bundesrepublik* von Josef Foschepoth.

Ganz bewusst habe ich mich mit der Aufnahme meines Studiums für Informatik entschieden, und das obwohl ich auch die Schriften und Vorlesungen von Michel Foucault sehr gut kenne und diese liebe, denn besonders er hat die Spaltungslinien der Gesellschaft(en) herausgearbeitet. Der Blick im Vorfeld des Studiums, in welchem ich mich besonders intensiv mit Philosophie sowie Soziologie beschäftigt habe, hat mir noch deutlicher die Bedeutung der Informatik für die Gesellschaft aufgezeigt, denn die öffentliche Gewalt, der Staat und somit die Politik kennen keine Grenzen. Damit war für mich klar, im Oktober (zum Studienbeginn), zur Konferenz: ich möchte ein Teil des FIfF sein.

Maximilian Hagner, FIfF-Neumitglied

Viel Licht, doch auch ein wenig Schatten …

In der Retrospektive kann ich aus dem Blickwinkel einer nicht mit der Thematik, sehr wohl aber organisatorisch mit der Konferenz befassten Beteiligten sagen:

Sehr viel Spaß hatte ich, aber auch reichlich Mühe bei der Organisation der unmittelbaren Versorgungsaufgaben – 48 Stunden Catering, Beschaffung eines ungeplanten Abendessens, Kaffee-„Tante", Müllfee – Ansprechpartnerin für die unterschiedlichsten Fragen – fehlendes Notebook, Ersatz für den verspäteten Kameramann u. a. – immer am Puls der Konferenzabläufe: so mein Selbstverständnis im Rahmen der Konferenz.

Aber da war vor allem das Leitthema der Konferenz, *Wem kann ich trauen im Netz und warum?,* das für mich – und streng besehen für jeden Bürger dieses Landes – von besonderer Relevanz war. Die breite Streuung der Themensetzung, die Dichte der Veranstaltungen, die unterschiedlichen Möglichkeiten, sich bei den Workshops persönlich einzubringen, das Mitdiskutieren nach den einzelnen Vorträgen: eine lebendige Veranstaltung, ein gelungenes Gesamtkonzept, für fast jeden Interessierten war etwas dabei. Ich bedauere, nicht immer und überall mit dabei gewesen zu sein.

Was habe ich aus welchen Vorträgen mitgenommen? Schwierig: der Beitrag von Hannes Mehnert, der sehr theoretisch auf technische Details einging und für mich als Außenstehende schwer verständlich war. Hochinteressant: das Thema des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit, Dr. Lutz Hasse. Trotz bitterernstem Hintergrund amüsant: der Animationsfilm *Cyberwar for Dummies,* der knapp und einprägsam Wirkmechanismen eines Cyberkriegs anschaulich machte.

Mein absoluter Favorit, mein persönliches Highlight war das Referat von Frau Professor Dr. Sabine Rehmer, *Vertrauen und IT-Sicherheit – zwei Gegenspieler?* Ein für mich überraschend neuer und nachhaltig wirkender Beitrag, untersetzt mit Beispielen aus ihrer Forschung: Psychologie und Informatik als Sinnzusammenhang. Beiträge dieser Art sollte es mehr geben! Aufrüttelnd der Beitrag *IT-Sicherheit im Gesundheitswesen* von Stefan Jäger, der auf erschreckende Sicherheitslücken hinwies.

Meine hohe Erwartungshaltung als Kommunikationswissenschaftlerin beim Thema *Glaubwürdigkeit der Medien: Wer kontrolliert wie den MDR? Kann ich den öffentlich-rechtlichen Angeboten im Netz trauen? Eine Rundfunkrätin berichtet.* wurde leider kaum erfüllt. Ich fühlte mich sehr an mein Grundstudium erinnert, als Frau Prof. Dr.-Ing. Gabriele Schade sehr ausführlich auf die Entstehung des MDR rekurrierte. Für die eigentliche, so spannende, Fragestellung blieb kaum Zeit. Sehr schade!

Erfrischend lebendig der Vortrag von Felix Baral-Weber, der die Abgründe, das Suchtpotenzial der vermeintlich kostenfreien Free-to-Play-Spiele skizzierte.

Besonders berührt hat mich die Verabschiedung von Prof. Dr.-Ing. Dietrich Meyer-Ebrecht aus seiner Funktion als stellvertretender Vorsitzender des FIfF: Mit einem Glas Sekt wurden wohl auch bei anderen FIfF-Mitgliedern die Emotionen hinuntergeschluckt. Danke Dietrich, möchte auch ich sagen, die um sein Wirken und seinen Einsatz für das FIfF weiß – und schön findet, dass er zumindest dem Vorstand des FIfF auch weiterhin angehören wird.

Ein wenig erschöpft war ich schon am Ende der Tagung, doch vor allem sehr zufrieden und persönlich bereichert.

Pia Geißler, Seminarleiterin in der beruflichen Rehabilitation

Kai Nothdurft

Attribution von „Cyber"-Angriffen durch Politik und Medien

In meinem Vortrag auf der FIfFKon 2017 in Jena habe ich zunächst eine Einführung in die Methoden der IT-Forensik gegeben. Ich habe kurz dargestellt, welche digitalen Spuren ForensikerInnen untersuchen und wie einfach solche Spuren verwischt und manipuliert werden können. Dies sollte veranschaulichen, warum die Attribution eines Hacker-Angriffs eine große Herausforderung und eine klare Identifikation der Angreifenden nur selten möglich ist. Am Beispiel des Bundestagshacks 2015 habe ich dargelegt, auf welcher Informationsbasis die Medien die Täteridentifizierung vornahmen und sich der Narrativ gebildet hat, dass die Angriffe aus Russland stammen würden.

Während ForensikerInnen zumeist professionell einen Vorfall untersuchen und bewerten und ihnen die oben geschilderten Unsicherheiten nur allzu bewusst sind, machen es sich sowohl Politik als auch Medien häufig mit der Zuordnung eines Angriffs zu einer bestimmten Gruppe einfacher. Wir haben es dabei mit einer Meinungs- und Stimmungsmache zu tun, die nur auf einer sehr eingeschränkten Faktenlage basiert. Es muss ein Schuldiger gefunden und der Öffentlichkeit präsentiert werden. Wenn es ins Weltbild passt, wird auch eine dünne Indizien-„Beweis"lage, die eh nur Experten verstehen, als ausreichend für eine Schuldzuweisung angesehen. Dies kann in einer gefährlichen Eskalation münden und muss friedenspolitisch thematisiert und kritisiert werden.

Erstaunlich selten fällt der Verdacht auf Geheimdienste verbündeter oder befreundeter Staaten, obwohl z. B. durch die Snowden Leaks sehr gut dokumentiert wurde, dass sich NSA und GCHQ auch beim Ausspionieren und Hacken von Verbündeten nicht zurückhalten. Das bedeutet nicht, dass Russland, China oder Nordkorea Waisenknaben sind, aber sie sind eben keineswegs die Einzigen, die über militärische Hackereinheiten verfügen. Die NSA dürfte die fortschrittlichste, mit dem größten Etat ausgestattete Einheit unterhalten. Im US-militärisch-wirtschaftlichen Komplex haben die US-Dienste außerdem privilegierten Zugang zu weltweit eingesetzten IT-Produkten inklusive zu deren Schwachstellen und möglicherweise auch Hintertüren. Eine Sicherheitslücke erlaubt dem Hersteller jedoch immer, die Absicht für den Einbau oder das Offenhalten einer Hintertür abzustreiten (plausible deniability).

Im Falle eines russischen Produkts, der Antimalware-Lösung von Kaspersky, wurde eine behauptete, aber nicht nachgewiesene Zugriffsmöglichkeit der russischen Regierung insbesondere in den USA als Risiko betrachtet und das Produkt vom Einsatz in Behörden ausgeschlossen.[1] Dem war ein bizarrer Sicherheitsvorfall vorangegangen. Ein externer Mitarbeiter der NSA hatte unter Verletzung mehrerer Sicherheitsvorschriften auf seinem Privat-PC „dienstliche" NSA-Malware gespeichert.[2] Der auf dem PC installierte Virenscanner von Kaspersky stufte diese Malware völlig korrekt als verdächtig ein und lud diese NSA-Cyberwaffen zur weiteren Analyse zu einem Kaspersky-Server hoch. Angeblich gelangten diese dann zu russischen Geheimdienstkreisen, wobei eine Mitschuld oder gar aktive Beteiligung von Kasperskys Produkt zwar in einem Wallstreet-Journal-Beitrag behauptet, aber nicht näher erläutert oder gar nachgewiesen und von Kaspersky vehement bestritten wurde.[3]

Pikanterweise machte der israelische Geheimdienst, der einen seiner Mitarbeiter bei Kaspersky eingeschleust hatte, die NSA erst auf das Sicherheitsproblem aufmerksam, dass sie die Kontrolle über mehrere ihrer Cyberwaffen verloren hatte.

Am 28.2.2018 meldete dpa einen Hackerangriff auf das Datennetz der Bundesverwaltung und beschuldigte APT28 als Tätergruppe, die auch als Schuldige in dem im Vortrag behandelten Bundestagshack gelten. Dies wurde bereits am Folgetag (1.3.2018) korrigiert, nun soll es die „russische Hackergruppe Snake"[4] gewesen sein. Vielleicht wird der forensische Bericht noch veröffentlicht, dann ließe sich möglicherweise eine fundierte Bewertung treffen, auf welchen Spuren die Behauptung fußt.

Referenzen

1 https://www.heise.de/newsticker/meldung/USA-verbieten-Behoerden-Nutzung-von-russischer-Kaspersky-Software-3831122.html
2 https://www.heise.de/newsticker/meldung/Russland-soll-dank-Kaspersky-Software-NSA-Dokumente-an-sich-gebracht-haben-3851108.html
3 https://www.heise.de/newsticker/meldung/Kaspersky-Keine-Weitergabe-von-NSA-Malware-an-russische-Hacker-3871326.html
4 https://www.heise.de/newsticker/meldung/Bundeshack-Russische-Hackergruppe-Snake-soll-hinter-Angriff-stecken-3984930.html

Kai Nothdurft

Kai Nothdurft arbeitet als *Information Security Officer* in einer großen deutschen Versicherung. Seit 2009 ist Kai Nothdurft im Vorstand des FIfF e. V. aktiv. Seit Jahren hält er Vorträge und schreibt Artikel, die sich kritisch mit seinem Fachgebiet IT-Sicherheit beschäftigen.

Sylvia Johnigk

Herausforderungen an das Identitätsmanagement, allen Rollen gerecht zu werden

Outsourcing hat in den letzten Jahren die Möglichkeiten, mittels Identitätsmanagement und Zugriffskontrolle den Zugriff auf Unternehmensdaten zu schützen, radikal verschlechtert. Der Vortrag hat sich diesem Thema gewidmet und zeigt auf, vor welchen Herausforderungen Unternehmen stehen, die im Rahmen der Digitalisierung jeden Prozess auslagern, der nicht im Fokus des Kerngeschäfts steht.

Das im Vortrag dargestellte fiktive Unternehmen steht exemplarisch für viele real existierende Unternehmen.

Ende des letzten Jahrtausends

Noch vor gut 20 Jahren hatte unser fiktiver Finanzdienstleister seine eigene IT-Abteilung. Die Hardware wie Server, Endgeräte wie Desktop-Rechner, Laptops und Mobiltelefone, und Software waren Eigentum des Unternehmens. Die Geräte wurden weitestgehend von angestelltem Personal betrieben und gewartet.

Das Personal arbeitete in Gebäuden, die Eigentum des Unternehmens waren. Zutritt zu den Gebäuden wurde anhand des Mitarbeiterausweises durch menschliche und/oder technische Einlasskontrolle überprüft. Zugriff auf die Daten bekam nur derjenige, der sich an einem Desktop-Rechner entweder mittels eindeutigen Profilen User/Passwort oder Mitarbeiterausweis/Passwort authentisieren konnte. Hinter jedem Profil waren die dedizierten erlaubten Zugriffsmöglichkeiten hinterlegt. So war mehr oder weniger gewährleistet, dass nur das Personal mit den Daten arbeiten konnte, für die es zuständig war. Hochsicherheitszonen wie das Rechenzentrum waren durch zusätzliche Schleusen besonders geschützt.

Ende des letzten Jahrtausends arbeiteten Anton, Anna, Anke, Andre und Andrea gemeinsam in einem Unternehmen. Anton, Anna und Andrea arbeiteten in der IT-Abteilung, während Anke und Andre in der Fachabteilung arbeiteten. Da das Unternehmen damals ein hohes Sicherheitsbewusstsein hatte, benutzten die Mitarbeiter für das Login Smartcards kombiniert mit einem Passwort.

Die Zeit des Auslagerns beginnt

Anfang des Jahrtausends begann das Unternehmen, seine IT auszulagern. Zu Anfang geschah dies nur, um Kosten besser skalieren zu können bzw. Einsparungspotential besser erkennen zu können. Als IT-Mitarbeiter arbeiteten Anton, Anne und Andrea nun in der neu gegründeten IT-Tochter des Unternehmens. Damit die IT-Tochter kostengünstig ihre Dienste anbieten konnte, wurden, obwohl Administratoren in besonders großem Umfang mit sensiblen Daten arbeiten, als erstes die Kosten für die Smartcards resp. den Smartcard-Leser am Endgerät eingespart. Fortan meldeten sich die Administratoren nur noch mit der unsicheren Login-Prozedur User/Passwort an. Dass dies das Sicherheitsniveau des Unternehmens senkte, interessierte das Management nur am Rande, da die Kostenersparnis im Vordergrund stand und es keine besonderen Gesetze gab, die die Anmeldung mit Smartcard forderten.

Ansonsten hatte sich wenig geändert, bei IT-Problemen konnten die Mitarbeiter des Kernunternehmens wie Anke und Andre einfach kurz anrufen, ihr Problem schildern und in der Regel konnten kleine Probleme sofort und ganz ohne formalen Prozess gelöst werden. Dies sollte sich in der folgenden Zeit ändern.

Um weitere Kosten zu sparen, wurde als nächstes versucht, die Kosten für die Endgeräte der Mitarbeiter zu reduzieren. Die Lösung war, dass neue Endgeräte (Desktop-Rechner bzw. Laptops) nicht gekauft, sondern geleast wurden. Zudem wurde der First Level Support an denselben IT-Dienstleister ausgelagert. Im Laufe der Zeit wurden immer mehr Service-Dienstleistungen rund um die Endgeräte ausgelagert. Arbeiteten die externen Service-Mitarbeiter anfangs noch in den Räumen des Unternehmens mit geleasten Endgeräten und verfügten wie interne Mitarbeiter über eine User/Passwort-Kombination zum Einloggen in das Firmennetzwerk, so benutzten sie zunehmend die Möglichkeit, sich via VPN und RSA Token in das Unternehmensnetzwerk einzuloggen. So wurden die Kosten für Arbeitsplätze und Endgeräte eingespart. Zusätzlich wurden interne Mitarbeiter, die bisher den Service geleistet hatten, entweder in vorzeitigen Ruhestand geschickt oder an den externen Dienstleister ausgelagert. Anna nahm das Angebot an und arbeitete fortan als externe Mitarbeiterin weiter im alten Unternehmen. Man konnte Anna zwar immer noch anrufen, aber Anna war nun nur noch gegenüber ihrem neuen Arbeitgeber weisungsgebunden. So konnten selbst kleine Probleme nur im Rahmen eines formalen Prozesses gelöst werden.

Obwohl keine (nennenswerten) Kosten eingespart wurden, wurden als nächstes die Server nicht mehr gekauft, sondern ebenfalls geleast. Weitere First- und Second-Level-Services wurden ebenfalls an den externen Server-Dienstleister ausgelagert. Wie schon zuvor wurden interne Mitarbeiter in den Vorruhestand geschickt, oder konnten fortan in dem externen Unternehmen arbeiten. Anton arbeitete nun bei dem externen Server-Dienstleister, wie Anne loggte er sich nun via VPN und RSA Token ein.

Obwohl weiterhin keine nennenswerten Kosten eingespart wurden, wurde als nächstes die Software (z. B. Betriebssysteme, Office, Virensoftware, Firewalls etc.) nicht mehr gekauft, sondern geleast, und wieder schieden Mitarbeiter aus dem Unternehmen aus, da auch die Services rund um die Installation und Wartung ausgelagert wurden. Mit der Zeit verlor das Unternehmen nicht nur immer mehr IT-Wissen, sondern auch den Überblick, da die Zahl der involvierten Firmen immer größer wurde.

Da die RSA Token vom Unternehmen herausgegeben und verwaltet wurden, konnten nur externe Mitarbeiter auf die Unternehmensdaten zugreifen, wenn die externen Mitarbeiter im Unternehmen bekannt waren. So war das Unternehmen bei-

spielsweise 2011 noch im Bilde, als es Sicherheitsprobleme mit den RSA Token gab. Damals war die Technologie der RSA Token gehackt worden, und RSA benötigte mehr als drei Monate, bis sie die Sicherheitslücke schließen konnten. Zu diesem Zeitpunkt war man sich zumindest des Risikos bewusst, da man den Umfang der RSA-Zugänge zahlenmäßig erfassen konnte und auch wusste, auf welche Daten die externen Mitarbeiter zugreifen durften. So war man in der Lage, Zugriffe auf besonders sensible Daten via RSA-Zugängen zu kappen und die Mitarbeiter wieder über die konservativen Zugänge arbeiten zu lassen, sprich, diese Mitarbeiter mussten wieder Arbeitsplätze im Unternehmen nutzen.

Das international agierende Unternehmen betreibt auch kein eigenes WAN (Netzwerk), um ihre einzelnen Lokationen miteinander zu verbinden, sondern setzt auf Telco-Provider, und auch vor Ort für das LAN wird auf ausgewiesene Provider zurückgegriffen. Diese Zugriffsmöglichkeiten auf Netzwerkebene erfolgen bereits unter dem Radar des Finanzdienstleisters. Aus dem verteilten Arbeiten in internationalen Teams ergibt sich die Herausforderung, wie man die Daten so speichert, dass Mitarbeiter kostengünstig rund um die Uhr darauf zugreifen können.

Ab in die Cloud

Hatte das Unternehmen bislang noch halbwegs einen Überblick über sein Identitätsmanagement und die Zugriffskontrolle und damit darüber, wer alles auf die Unternehmensdaten zugreifen kann, so geht dieser mit dem Zeitalter des Cloudcomputing völlig verloren.

Der wesentliche Unterschied ist vor allem, dass nun die Daten außer Haus gespeichert und verarbeitet werden in der Cloud. Selbst personenbezogene Daten, die „eigentlich" gemäß dem BDSG oder zukünftig gemäß der EU-Datenschutzgrundverordnung zumindest innerhalb der EU gespeichert und verarbeitet werden müssen, werden schlussendlich irgendwo verarbeitet.[1]

Das Unternehmen nimmt einen Clouddienstleister in Anspruch. Es muss sich bei Vertragsabschluss und in den folgenden Jahren davon überzeugen, dass der Clouddienstleister die in der EU geltenden Gesetze auch einhält.

Bezogen auf das Identitätsmanagement und Zugriffsmanagement heißt das, dass unser fiktiver Finanzdienstleister sich davon überzeugen muss, dass sein IT-Dienstleister sich davon überzeugt, dass der gewählte Cloudprovider hinsichtlich des Identitätsmanagements dasselbe Schutzniveau bietet, wie er selbst es nach EU-Recht erbringen muss. Der Cloudanbieter greift auf Subprovider zu, um einen 7*24-Stunden-Service anbieten zu können. In dem Outsourcing-Vertrag bzw. in dem Auftragsdatenschutzvertrag werden 20 weitere Subprovider vereinbart (deren Unternehmen in den USA, Kanada, Brasilien, Singapur, Indien, der Türkei etc. ansässig sind), die ebenfalls auf die Daten Zugriff haben. Zusätzlich lässt sich der Cloudanbieter vertraglich festschreiben, dass er jederzeit neue Subprovider beauftragen kann, solange sich das Subunternehmen vertraglich verpflichten lässt, sich an die EU-Gesetzgebung zu halten. Dies muss der Cloudanbieter dem Kunden zwar mitteilen, aber unser Finanzdienstleister kann de facto nicht widersprechen, sondern lediglich den Vertrag kündigen. Dass auch die Subprovider Verträge mit weiteren Subprovidern schließen, und diese ebenfalls mit Subprovidern arbeiten, und die wiederum ... macht dies nicht einfacher.

Konsequenzen aus dem Cloudcomputing

Fakt ist, dass unser fiktives Unternehmen nicht mehr weiß, wer auf die Daten zugreifen kann. Es weiß auch nicht mehr, mit welchen Verfahren (User/Passwort, RSA Token/Passwort etc.) zugegriffen wird. Anton arbeitet übrigens derzeit bei einem dieser Subprovider in Estland, seiner alten Heimat. Estland ist ein modernes EU-Land, deshalb gibt es Personalausweise mit Chip und digitaler Signatur. Damit meldet sich Anton jeden Morgen aus seinem Home-Office an und hat so als Superadmin Zugriff auf die Unternehmensdaten. Bis zum September 2017 war dieses Verfahren mindestens so sicher wie gefordert. Nach dem Hack[2] des estnischen Chipkartensystems im September wäre zumindest eine Überprüfung des Verfahrens notwendig. Der Finanzdienstleister hat dazu de facto keine Chance. Das Unternehmen muss sich darauf verlassen, dass die Prüf-Kette über alle Subprovider funktioniert. Die fehlende Möglichkeit der Kontrolle aller Dienstleister und Subdienstleister ist im Übrigen nicht nur beim Identitäts- und Zugriffskontrollmanagement ein Problem, sondern bei allen Sicherheitsthemen.

Anmerkungen

1 *Dies geht für den Cloudprovider deshalb, weil der Gesetzgeber die Möglichkeit gibt, dies über die EU Standard Clauses, Privacy Shield bzw. Binding Corporate Rules absichern. Diese Verfahren sind Nachfolger des Safe-Harbor-Abkommens, das im Oktober 2015 vom Europäischen Gerichtshof kassiert wurde. Jedes stellt einen Vertrag zwischen Unternehmen dar, wobei sich beteiligte Unternehmen in Drittstaaten verpflichten, die europäischen Gesetze einzuhalten., aber keines bietet einen besseren Schutz als das Safe-Harbor-Abkommen.*

2 *heise online, Estland: Sicherheitslücke in fast 750.000 ID-Cards, https://www.heise.de/newsticker/meldung/Estland-Sicherheitsluecke-in-fast-750-000-ID-Cards-3822597.html*

Sylvia Johnigk

Sylvia Johnigk forscht und arbeitet seit über 25 Jahren im Bereich IT-Sicherheit, seit 2009 ist sie selbständige Beraterin in Großkonzernen. Ebenfalls seit 2009 ist sie im Vorstand des FIfF e. V.

Britta Schinzel

Workshop „Algorithmen: schuldig oder unschuldig?“

Algorithmen versus Programme, Software, IT-Systeme

Mit der Popularisierung des Algorithmusbegriffs geht eine Erweiterung desselben auf beliebige Software-Systeme einher. Insbesondere werden Entscheidungssysteme, Lern- und sonstige KI-Programme immer öfter als Algorithmen bezeichnet. Solche Systeme können in der Tat aus unterschiedlichen Gründen Ergebnisse liefern, die Ungleichgewichte dar- und herstellen. Es sollte in diesem Workshop diskutiert werden, ob Algorithmen Entscheidungs- und Handlungsmacht zugebilligt, ihnen diskriminierende Eigenschaften zugeschrieben werden können und ob umgekehrt ethische, soziale oder gendersensible Forderungen an Algorithmen gestellt werden können. Nimmt man die engere mathematische und informatorische Definition weiterhin ernst; oder ist es sinnvoll, auch innerhalb der Informatik-Community die Unterscheidung zwischen Algorithmus und Programmsystem oder Maschinensystem nicht mehr zu treffen? Scheint doch die Welt sich dieses sexyer klingenden Namens bemächtigt zu haben.

Die formale Fassung des Algorithmusbegriffs geschah beginnend mit Kurt Gödel in den 1930er-Jahren als partiell rekursive Funktionen, rasch gefolgt von vielen anderen Formalisierungsversuchen, einschließlich der Turingmaschinen, welche sich alle als funktionell äquivalent erwiesen. Rasch erwiesen sich dabei auch alle Unentscheidbarkeitseigenschaften, die beispielsweise formale Verifikation von Algorithmen und viel mehr noch von Programmen im Allgemeinen unmöglich machen. Wichtige Eigenschaften von Algorithmen sind ihre Universalität für eine gegebene Eingabemenge, die prinzipielle Aufschreibbarkeit durch Menschen von Hand. Sie werden von Menschen entwickelt und man kann in definierbaren Grenzen Korrektheit formal verifizieren (wenn auch nicht für alle p.r.f. wegen der Unentscheidbarkeit der Äquivalenz von Algorithmen), während man komplexe Programmsysteme meist nur testen kann. Knuths Definition[1] hingegen, die finite Rechenzeiten für alle Eingaben verlangt – eine unentscheidbare Eigenschaft –, lässt sich, wie er auch selbst gesehen hat, nicht klar definieren. Wann soll die Maschine beispielsweise abbrechen, Werte liefern? Wieviel Speicherplatz muss man ihr verfügbar halten? Im Gegenteil kann finite Rechenzeit jeweils immer nur neu mittels Heuristiken und Constraints eingehalten werden, mehr noch müssen für erlebbare Ausführungszeiten Einschränkungen des Geltungsbereichs oder der Korrektheit in Kauf genommen werden. Es ist zu hinterfragen, ob die Kombination eines Algorithmus mit Heuristiken noch als ein geschlossener Algorithmus bezeichnet werden kann, denn er ist dann nicht mehr universell für alle Eingaben. Dann erhält man evtl. nur für zu eruierende Prozentsätze korrekte oder beste Ergebnisse. Doch anders kann man oft mit gegebenen Problemen nicht umgehen.

Es wurde über Suchmaschinenalgorithmen und machine-lernende KI-Systeme gesprochen und hier die Grenze zwischen dem mathematischen Such- oder Lern-Algorithmus und den Stellen, wo Kontingenz in das System einfällt, festzustellen versucht. Das geschieht bei Suchmaschinen bereits bei der Speicherung der Netze, die die wichtigen Ausgangspunkte auswählt und das „tracing“ von „trusted“ Knoten ausgehend aufbaut. Natürlich sind die Suchmaschinenalgorithmen viel komplexer kombiniert und werden zudem wöchentlich oder täglich verändert, um die Manipulation durch SEO-Agenturen[2] zu untergraben. In diesem Kontext wird von AlgorithmWatch darauf hingewiesen, dass Transparenz nicht immer gefordert werden sollte, denn die Offenlegung eines Systems von Suchmaschinenalgorithmen macht dieses im Gegenteil anfällig für die Beeinflussung der Ergebnisreihenfolgen durch Nutzende.

Bei lernenden Systemen wird in der Trainingsphase ein Modell gebildet, das die Lernstruktur zusammenfasst. Dies kann nicht mehr als der eigentliche Algorithmus betrachtet werden, er ist schon nicht mehr universell, nicht mehr reengineerbar und also gewissermaßen kontingent „verschmutzt“. Das so trainierte Netz ist nun bereit für die eigentliche Dateneingabe, ist aber im obigen Sinne kein Algorithmus mehr.

Dagegen stehen Initiativen wie die Tagung „Digitales Leben – Vernetzt. Vermessen. Verkauft? #Werte #Algorithmen #IoT“, über die Rechts- und Werteordnung in der digitalen Transformation, die am 3. Juli 2017 in Berlin durch das Bundesministerium der Justiz und für Verbraucherschutz veranstaltet wurde. Hier bedient sich beispielsweise der Themenblock „Algorithmen – Wie sie uns bewerten und steuern, wie wir sie kontrollieren können“ eines erweiterten Algorithmusbegriffs. Es wird gefragt, welche Rahmenbedingungen beim Einsatz von Algorithmen erforderlich sind. Wie steuern Algorithmen unser Verhalten? Welche Risiken sind mit dem Einsatz von Algorithmen verbunden? Wie können diskriminierende Effekte bei ihrem Einsatz verhindert werden? Ist Transparenz für die Verbraucherinnen und Verbraucher anzustreben und wie kann sie ggf. hergestellt werden? Ist eine Kontrolle durch eine Digitalagentur, einen Algorithmen-TÜV oder Algorithmiker erforderlich?

Britta Schinzel

Britta Schinzel promovierte in Mathematik, arbeitete in der Computerindustrie und habilitierte sich in der Informatik. Im Rahmen ihrer Professur für Theoretische Informatik an der RWTH Aachen arbeitete sie zunehmend interdisziplinär. Sie war von 1991 bis 2008 Professorin für Informatik und Gesellschaft und Gender Studies in Informatik und Naturwissenschaft an der Universität Freiburg.

Alle solchen Fragen sind, wenn auch unter den Begriffen Software-Systeme, Algorithmische Systeme, Maschinen dringend zu behandeln. Einfallstore für Kontingenzen sind bereits intentional eingeschränkte Programmiersprachen und -umgebungen. Das Requirements Engineering und die Spezifikation bzw. das Pflichtenheft sind zweckgerichtete Einengungen der Funktionalität, weiter eingeengt durch Entwurf und Architektur; und schließlich v. a. für KI- und Lernsysteme die immer beschränkten Dateneingaben.

Algorithmen jedoch werden mit Objektivität, fehlerfreiem Ablauf, Interesselosigkeit, Zweckfreiheit assoziiert, während Programme, die Algorithmen verwenden, zweck- und zielorientiert sind. Auch sogenannte Entscheidungsalgorithmen sind intentional gesteuerte Programme. Diese Sprachverwendung hat jedoch ethische Folgen: nämlich die Abweisbarkeit von Verantwortung, die so an scheinbar objektive Maschinen abgegeben wurde.

Die Diskussion brachte mehrere Punkte heraus. Dissens besteht in der Sprachverwendung, also darin, ob es für die Klärung der menschlichen Einflüsse, also von zuschreibbaren oder veränderlichen Verantwortlichkeiten in der Öffentlichkeit, besser sei, von algorithmischen Systemen zu sprechen, oder aber von Software, Maschinen, IT-Systemen, um in der Tat das ganze System im Luhmannschen Sinne zu erfassen. Eine Einigung war schließlich sogar dahingehend möglich, dass die mathematischen Eigenschaften von Algorithmen unwidersprochen blieben, der menschliche internationale Einfluss an vielen Stellen ebenfalls, wie indirekt und zeitlich verzögert auch immer. Es wurde darauf hingewiesen, dass es Situationen gibt, auf die man unmittelbar reagieren muss, wo keine Zeit bleibt, Verantwortlichkeiten zu diskutieren, z. B. bei Wetterkatastrophen, militärischen oder sonstigen Angriffen, wofür u. U. automatisierte Antworten vorzugeben sind.

Von allen wurde betont, dass menschliche Entscheidungen für die Software-Systeme an vielen Stellen Verantwortung tragen. Die Benennung „Algorithmisches System“ wird von manchen bevorzugt, denn es betone den Unterschied zwischen bzw. die Kombination von Algorithmus mit dem gesamten Zusammenwirken von Software-Produktion, -Anforderungen und -Gebrauch, also bis hin zum Luhmannschen Systembegriff, der den menschlichen sozialen Eingriff und Gebrauch mit behandeln soll.

Anmerkungen und Referenzen

1 *https://en.wikipedia.org/wiki/Algorithm_characterizations#1968.2C_1973_Knuth.27s_characterization*

2 *SEO (search engine optimization) versucht, Webseiten für User so zu verbessern, dass ihre Einträge in Rankings so weit oben wie möglich erscheinen. Bei der Suchmaschinenoptimierung werden neben Techniken für das Ranking über externe Verlinkungen (backlinks), Inhaltsdarstellung, Usability und Social Engineering verwendet.*

Jens Rinne

Workshop „ZensusVorbereitungsgesetz 2021“

Wir trafen uns in Jena auf der JaTa zum Workshop, um uns unter anderem über die Hintergründe, Konstruktion und Kosten der Volkszählung zu informieren und die Möglichkeiten einer neuen Verfassungsbeschwerde zu beraten. Die Ergebnisse werden im Folgenden zusammengefasst.

Zensus 2021

Die Volkszählung heißt nun Zensus, und zur ersten Neuauflage nach 1987 gab es 2011 Skepsis, ob eine Volkszählung notwendig ist, und vereinzelt Unmut in der Bevölkerung. Daraus resultierten Verfassungsbeschwerden (VB), die vom Bundesverfassungsgericht (BVerfG) nicht angenommen bzw. nicht verhandelt wurden und den Zensus 2011 nicht verhinderten. Die gewonnenen Ergebnisse der Erhebung, vor allem die Bevölkerungszahlen in Städten und Gemeinden, gefielen nicht allen Städten. Ihnen werden weniger EinwohnerInnen zugerechnet und somit Gelder des (Länder-)Finanzausgleichs gekürzt. Daher sind gegenwärtig Normenkontrollanträge von Berlin und Hamburg, die Verfassungsmäßigkeit des Zensusvorbereitungsgesetzes und Zensusgesetzes 2011 betreffend, beim BVerfG anhängig und zur Entscheidung 2018 durch den 2. Senat vorgesehen.[1] Bzgl. eines Eindrucks der mündlichen Verhandlung des BVerfG siehe den zugehörigen Bericht.[2]

Zensus schon wieder?

Der Zensus findet nach europäischer Vereinbarung[3] alle 10 Jahre statt. Diesem Turnus hat Deutschland zugestimmt und seine regelmäßige Teilnahme zugesichert. Der nächste Zensus 2021 wird gegenwärtig vorbereitet, dafür hat die Gesetzgeberin am 3. März 2017 das Zensusvorbereitungsgesetz (ZensVorbG 2021) veröffentlicht[4]. Auch dem Zensus 2011 ging im Jahre 2007 ein Vorbereitungsgesetz (ZensVorbG 2011) voraus[5]. Im ZensVorbG 2011 wurde das Gebäude- und Wohnungsregister zusammengestellt. Mit diesem Register wurde die Haushaltsstichprobe mit persönlicher Befragung erstellt. 2017 ist es ähnlich, Ziel vom ZensVorbG 2021 ist der Aufbau eines anschriftenbezogenen Steuerungsregisters, vor allem, um die Haushaltsstichprobe daraus zu ziehen. Für dieses Register werden alle EigentümerInnen von Gebäuden und Wohnungen befragt.

2011 fand der Zensus nicht mit einer vollständigen Haushaltsbefragung der Bevölkerung statt: primär wurden repräsentative 10 % der Haushalte für eine persönliche Befragung herangezogen, und diese Ergebnisse wurden auf die ganze BRD hochgerechnet. Bei dieser Konstruktion des Zensus ist entscheidend, dass die Ziehung der Haushaltsstichprobe tatsächlich repräsentativ erfolgt. Über die 10 % hinaus erfolgten weitere, umfassende Befragungen und Datenübermittlungen im Zusammenhang mit dem Zensus 2011.

Die Konstrukteure des Zensus sind die Statistiker – u. a. vom Statistischen Bundesamt (Destatis) sowie den Universitäten Bamberg und Trier – und sie argumentieren für die Repräsentativität und ihre komplexen statistischen Grundannahmen und Rechenoperationen. Im Kern klagen die Städte Berlin und Hamburg gegen diese Konstruktion und verweisen auf ihre eigene reale Ermittlung ihrer Bevölkerung in Form ihrer kontinuierlich geführten Melderegister.

Protest in der Bevölkerung

An weiten Teilen der Bevölkerung ging der Zensus 2011 vorbei. Sie wurden gar nicht gefragt, weil keine Vollerfassung stattfand. Breiter Protest gegen diese Volkszählung blieb aus. Dennoch hat der Zensus 2011 deutliche Auswirkungen auf weite Teile der Bevölkerung. Da insbesondere den großen Städten bisherige Einwohnerzahlen aberkannt wurden, verringerten sich die jährlichen Zahlungen aus dem Länderfinanzausgleich an diese Städte. Sie mussten sparen, und haben unter anderem an öffentlichen Einrichtungen wie Schulen, Kindertagesstätten oder Schwimmbädern gespart. Diese Zusammenhänge erscheinen verdeckt und werden weniger wahrgenommen, so bleibt die breite Aufregung aus.

Kosten

Die Gesamtkosten bei Bund und Ländern werden für das ZensVorbG 2021 auf 331 Millionen Euro geschätzt. Für den Zensus 2011 wurden im Jahr 2007 alleine für das Vorbereitungsgesetz 176 Mio. Euro veranschlagt, und für das Zensusgesetz 527 Mio. Euro. Die Gesamtkosten für 2011 werden vom Statistischen Bundesamt lediglich auf Basis der veranschlagten Höhe durch einfache Addition angegeben[6].

Ohne Datenlöschung

Trotz den in den Gesetzen zum Zensus 2011 gegebenen Fristen (§ 19 ZensG; § 15 ZensVorbG)[7] und Versprechen einer „frühestmöglichen Löschung" der personenbezogenen Daten, sind all diese Daten im Jahr 2018 immer noch nicht gelöscht. Derzeit wird vom BVerfG im Kontext der Normenkontrollklage die Löschung aufgeschoben. Dieses Aufschieben betrifft alle Daten, die im Rahmen des Zensus erhoben wurden. Somit insbesondere die sehr personenbezogenen Hilfsmerkmale, für die selbst das Statistische Bundesamt immer die Sensibilität betont hat.

Kritisches im ZensVorbG

Bereits im ZensVorbG 2011 wurde in § 8 eine Ordnungsnummer eingeführt und die „Nutzung allgemein zugänglicher Quellen" im § 12 erlaubt. Nach dem Volkszählungsurteil 1983[8] ist „ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal" unzulässig, welches „eine unbeschränkte Verknüpfung der erhobenen Daten mit den bei den Verwaltungsbehörden vorhandenen, zum Teil sehr sensitiven Datenbeständen" zusammen mit der „Zusammenführung einzelner Lebensdaten und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger" durch „Nutzung allgemein zugänglicher Quellen" (z. B. soziale Netzwerke wie Facebook oder Twitter) ermöglicht. Dies findet sich erneut im ZensVorbG 2021 im § 3 Ordnungsnummern und die Nutzung weiterer Quellen in § 13. Die Gesetzgeberin verpasst erneut die Klarstellung, dass keine Erstellung von Persönlichkeitsprofilen der BürgerInnen stattfinden darf.

Die Nicht-Löschung der Erhebungs- und Hilfsmerkmale wurde bereits thematisiert, zusätzlich ist zu kritisieren, dass im ZensVorbG 2011 die Löschung des erzeugten Anschriften- und Gebäuderegisters terminiert wird auf spätestens sechs Jahre nach dem Zensusstichtag (9.5.2011). Rechtzeitig vor diesem Löschtermin zum 9.5.2017 trat das ZensVorbG 2021 am 3.3.2017 in Kraft und erlaubt in § 13, die Angaben aus Bundes- und Landesstatistiken sowie aus statistikinternen Registern zu nutzen. Somit ist davon auszugehen, dass eine Quelle des neuen anschriftenbezogenen Steuerungsregisters das für den Zensus 2011 erstellte Gebäude- und Wohnungsregister ist.

Verfassungsbeschwerde

Im Workshop nahm der erste Informationsteil über das ZensVorbG und die Aktivitäten bei der VB zum ZensG 2011 viel Zeit in Anspruch. Die Kritik wurde anschließend zusammengetragen, und zum Abschluss der Arbeitsaufwand einer neuen VB abgeschätzt. Wir kamen zum Ergebnis, das eine VB nur mit einem ähnlichen Team wie 2010 zu bewerkstelligen ist. Eine VB innerhalb des ersten Jahrs nach Inkrafttreten eines Gesetzes konnte leider nicht realisiert werden, es bleibt jetzt der normale Klageweg durch die Instanzen übrig.

Anmerkungen und Referenzen

1 *http://www.bundesverfassungsgericht.de/DE/Verfahren/Jahresvorausschau/vs_2018/vorausschau_2018_node.html*
2 *https://freiheitsfoo.de/2017/10/26/bverg-verhandelt-zensus2011/*
3 *Verordnung Nr. 763/2008 des Europäischen Parlaments*
4 *http://dipbt.bundestag.de/extrakt/ba/WP18/769/76954.html; https://www.destatis.de/DE/Methoden/Rechtsgrundlagen/Statistikbereiche/Inhalte/1064_ZensVorbG_2021.html*
5 *https://www.destatis.de/DE/Methoden/Rechtsgrundlagen/Statistikbereiche/Inhalte/051_ZensVorbG_2011.pdf*
6 *https://www.zensus2011.de/SharedDocs/Aktuelles/Welche_Kosten_verursacht_der_Zensus.html*
7 *https://www.destatis.de/DE/Methoden/Rechtsgrundlagen/Statistikbereiche/Inhalte/051a_ZensG_2011.pdf*
8 *https://www.juraforum.de/lexikon/volkszaehlungsurteil; http://www.servat.unibe.ch/dfr/bv065001.html; http://www.servat.unibe.ch/dfr/bv027001.html*

Jens Rinne

Jens Rinne, FIfF-Mitglied aus Mannheim, war 2010 aktiv im Arbeitskreis Zensus und beteiligt an der Verfassungsbeschwerde gegen den Zensus 2011.

Eberhard Zehendner

Workshop „Handys – aber sicher!“

Der Workshop fand am Sonntag, den 22. Oktober 2017 von 8:00 bis 11:30 Uhr in einem Seminarraum der Friedrich-Schiller-Universität Jena statt. Es hatte im Vorfeld aus dem FIfF-Vorstand Bedenken gegeben, ob den Besucherinnen und Besuchern der FIfFKon eine derart frühe Anfangszeit zugemutet werden könne. Nachträglich kann ich nun ja zugeben, dass der an mich herangetragene Pessimismus dann auch mich etwas verunsicherte. Und so sah ich denn mit einer gewissen Nervosität der Eröffnung des Workshops entgegen, zumal wir am Abend zuvor noch bis 23 Uhr den Film „Zero Days“ gezeigt hatten. Doch der Seminarraum füllte sich zunehmend, und mit etwa 25 Anwesenden konnte es nun losgehen.

Die Teilnehmenden konnten über die Inhalte des Workshops höchstens spekuliert haben, da ich zwar den Workshop-Titel verbreitet, aber keine näheren Ausführungen zur Ausgestaltung hatte verlauten lassen. Nun gut, auf den beiden vorangehenden Konferenztagen hatte ich, im persönlichen Gespräch, die eine oder andere Konkretisierung erkennen lassen. Mit Gates'scher Chuzpe hätte ich ja nun behaupten können, der Informationsmangel sollte als Feature des Veranstaltungskonzepts verstanden werden. Das war er natürlich nicht. Aber ich hatte Glück im Unglück: Denn das Konzept, das ich ursprünglich verbreiten wollte, sah ganz anders aus als der tatsächliche Ablauf des Workshops. Ich hatte nämlich mit folgender Formulierung (die auch für eine breite Ankündigung gedacht war) bei etlichen Kandidatinnen und Kandidaten einige Wochen vor Beginn der Konferenz um Mithilfe im Workshop geworben:

> *„Der Workshop richtet sich vorwiegend an Jugendliche mit eigenem Handy. Es sollten dort praktische Elemente der IT-Sicherheit demonstriert und auf den individuellen Geräten eingerichtet werden, vor allem E-Mail-Verschlüsselung, sichere Messenger, Sicherheitseinstellungen und das Unterbinden von Datenabfluss. Lässt sich sicher auch in Teilen als eine Keysigning-Party gestalten. Wichtig wäre mir, dass auch das Zusammenspiel unterschiedlicher Plattformen klappt.“*

Der Rücklauf war dann doch ziemlich verhalten. Insbesondere schienen die meisten der Angesprochenen ihr Gerät unter Android zu betreiben, die nötige Breite für eine derart vollmundige Ankündigung wollte sich also nicht einstellen. Und so gab es denn auch keine detaillierten Werbemaßnahmen. Aus der ursprünglich eher wie ein Tutorium konzipierten Veranstaltung wurde eine lockere Gesprächsrunde, die dennoch das wichtigste Kriterium eines *Workshops* unzweifelhaft aufwies – es wurde heftig gearbeitet.

Themenfindung

Zunächst hatten alle Anwesenden die Möglichkeit, ihre Sichtweise auf den Problemkreis „Handy-Sicherheit“ darzustellen und bestimmte, sie vorwiegend interessierende Fragestellungen einzubringen. Dies führte schließlich auf eine ebenso umfangreiche wie bunte Themensammlung (Abbildung 1). Es wurde aus dem Kreis der Anwesenden darauf hingewiesen, dass zunächst *Ziele* formuliert werden müssten, an denen sich Beurteilungen ausrichten können.

Aus der Fülle der Themen schälten sich gewisse Bereiche als besonders interessant heraus, diese wurden dann vertieft diskutiert. Dies war zunächst der Komplex „Google“ mit folgenden Einzelfragestellungen:

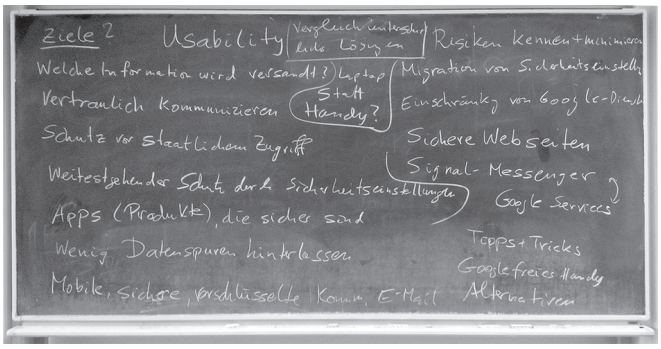


Abbildung 1: Themensammlung

- Inwieweit (und wie) können Google-Dienste eingeschränkt werden?
- (Wie) hängt der Signal-Messenger mit den Google Services zusammen?
- Wie kommen wir zu einem Google-freien Handy?
- Welche Alternativen zu Google auf dem Handy gibt es?

Ein weiterer Komplex betraf die *Vertraulichkeit der Kommunikation per Handy,* mit den Unterpunkten

- Verschlüsselung
- Sicherheit der Maßnahmen

sowie (auch andere Bereiche betreffend)

- Welche Information wird versandt?
- Wenig Datenspuren hinterlassen
- Schutz vor staatlichem Zugriff
- Apps (Produkte), die sicher sind

Dabei bestehen relevante Unterschiede zwischen der Kommunikation per E-Mail bzw. über einen Instant-Messenger.

Der Komplex *Geräteschutz* mit den Punkten

- Zugriffsschutz
- Produkte
- weitestgehender Schutz durch Sicherheitseinstellungen
- Migration von Sicherheitseinstellungen

konnte aus zeitlichen Gründen nur angerissen, aber nicht vertieft werden, desgleichen die übergreifenden Themen

- Vergleich unterschiedlicher Lösungen
- Risiken kennen und minimieren
- Tipps und Tricks
- Wie stark schränken Sicherheitsmechanismen die Usability ein?
- Sichere Webseiten
- Sind Handys sicherheitstechnisch so bedenklich, dass die Verwendung eines Laptops die angemessene Konsequenz ist?

Bedingt durch den Beginn parallel zum Workshop abgehaltener Vorträge wechselten nun einige der Anwesenden dorthin. Nach einer angemessenen Pause wurde der Workshop in kleinerer Runde fortgesetzt. Es dominierten nun speziellere Fragen das Gespräch, der Informationsstand erschien mir bereits sehr hoch. Der Begriff „Expertenrunde" wäre dafür vielleicht angemessen.

Handy ohne Google

Die Diskussion konzentrierte sich nun zunächst auf das Thema „Handy ohne Google" und kreiste dabei um folgende Fragestellungen (siehe Abbildung 2):

- Welche Betriebssysteme kommen als Google-freie Alternativen in Frage?
- Wie ist der Wechsel des Betriebssystems technisch zu vollziehen?
- Welche Recovery-Systeme kommen in Frage?
- Bestehen derartige Möglichkeiten auch für ältere Smartphones?
- Wird durch einen Wechsel die Herstellergarantie für das Gerät beeinträchtigt?
- Sind nach einem Wechsel weiterhin Updates möglich?
- Woher bekomme ich ohne Google meine Apps?
- Wo liegen meine bisherigen Daten?

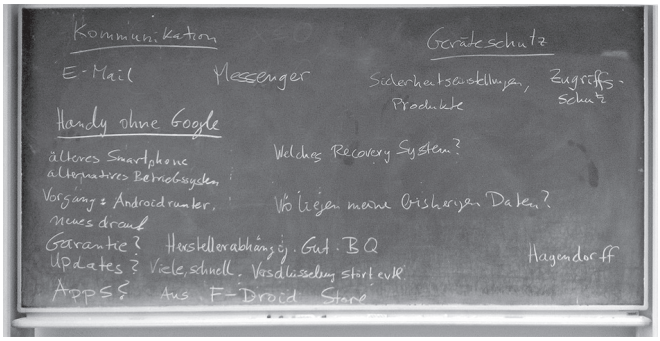


Abbildung 2: Vertiefung von Themen

Mobile Instant-Messenger

Nun wandte sich die Diskussion der Frage zu, welche Anforderungen an einen *mobilen Instant-Messenger* zu stellen seien und welche Anwendungen diese erfüllen könnten. Zunächst wurden die Anwesenden gebeten, an der Tafel (Abbildung 3) ihre persönliche Situation im Schema „Ich verwende … weil …" einzutragen. Dies ergab dann eine Zusammenstellung wie in Tabelle 1 (die Schreibweise dort sowie in den nachfolgenden Ausführungen orientiert sich an offiziellen Quellen und weicht dadurch teilweise vom Tafelbild ab).

Ich verwende …	weil …
Line	ich mit Asien schreibe
Signal	Open Source, verschlüsselt
Telegram	alle Freunde diesen verwenden
iMessage	
Conversations	besserer Metadatenschutz
Gajim	besserer Metadatenschutz
ChatSecure	
keinen	**keiner mich überzeugt**
WhatsApp	Gruppenzwang
Threema	verschlüsselt, simple, Schweiz, keine Telefonnummern
Facebook	Gruppe

Tabelle 1: Nutzung von mobilen Instant-Messengern durch Workshop-Teilnehmende und ihre Begründung

Die vorangestellten Striche im Tafelbild lassen erkennen, dass es eine Präferenz für *Threema* gab, gefolgt von *WhatsApp*. Ansonsten schienen die Anwesenden dann jeweils „ihren" persönlichen Messenger (manchmal auch mehrere) zu benutzen. Sicherheitsaspekte spielen anscheinend nur teilweise eine Rolle bei der Auswahl; ebenso entscheidend ist die „Community", mit der kommuniziert werden soll. Es könnte sogar sein, dass letzteres auch für die Wahl eines Messengers höherer Sicherheit (mit-)verantwortlich ist, falls „meine Community" dies von mir erwartet.

Besonders interessant fand ich die Antwort „Ich verwende keinen (Messenger), weil keiner mich überzeugt". Diese kam von einem Teilnehmer, der sich beruflich mit der Nutzung von Smartphones im gewerblichen Bereich beschäftigt. Dort wurden zu einem sehr frühen Zeitpunkt die Maßstäbe durch das *BlackBerry* geprägt, und generell liegen die Anforderungen an Verfügbarkeit, Zuverlässigkeit und Vertraulichkeit im gewerblichen Bereich höher als im privaten.

Die Aufzählung wurde dann noch erweitert um lediglich gelegentlich genutzte Messenger sowie solche, die evtl. auch noch von Interesse sein könnten. Dies ergab dann folgende Zusatzliste:

- SIMSme
- ICQ
- Riot
- Skype
- Hangouts
- qTox
- Briar
- Ring

Von einigen dieser Messenger hatte ich noch nie gehört. Daher habe ich im Nachgang ein wenig recherchiert und zunächst eine umfangreiche „Liste von mobilen Instant-Messengern" (*https://de.wikipedia.org/wiki/Liste_von_mobilen_Instant-Mes-*

sengern) mit Übersicht vieler Eigenschaften im Netz gefunden, die anscheinend noch laufend gepflegt wird. Doch selbst diese Übersicht führt nicht alle genannten Messenger auf. Es lohnt sich, dazu weiter im Netz zu stöbern und sich die tatsächlich interessanten Ansätze genauer anzusehen, zum Beispiel für *Briar* (*https://motherboard.vice.com/de/article/7xenwb/diese-app-will-den-messenger-markt-revolutionieren*) oder *Riot* (*https://www.deathmetalmods.de/messaging-und-open-source-ein-kurzer-blick-auf-riot-im-gastbeitrag/*).

Als Alternativen zur Verwendung eines mobilen Instant-Messengers wurde im Workshop auch die Kommunikation über *SMS* oder *E-Mail* genannt. Bemerkenswerterweise wurden bekannte Messenger wie *Signal* oder der von *Facebook* bereits um die Möglichkeit erweitert, dort direkt SMS verarbeiten zu können. Zum Abschluss sei daher noch auf eine (allerdings nicht ganz aktuelle) Übersicht zu „Sicherheit und Nachhaltigkeit von WhatsApp, E-Mail, SMS & Co." hingewiesen, zusammengestellt von der „Digitalen Gesellschaft" der Schweiz: *https://www.digitale-gesellschaft.ch/messenger/bewertung.html*.

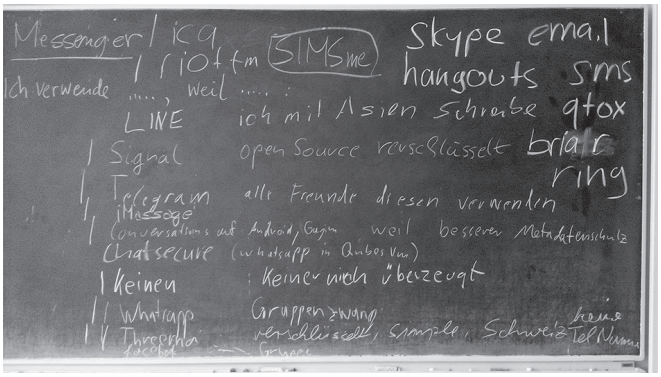


Abbildung 3: Tafelanschrift zur Nutzung von mobilen Instant-Messengern

Eberhard Zehendner

Workshop „IT-Sicherheit barrierefrei"

Der kleine, aber feine Workshop wurde mitveranstaltet von Henning Lübbecke, Sprecher der Fachgruppe „Informatik und Inklusion" im Fachbereich Informatik und Gesellschaft der Gesellschaft für Informatik (GI) und im FIfF schon bestens ausgewiesen durch seinen Workshop „Teilhabe an der allgegenwärtigen Kommunikation" auf der FIfFKon 2015 in Erlangen. Es war uns eine besondere Freude, den Beauftragten der Thüringer Landesregierung für Menschen mit Behinderungen, Joachim Leibiger, im Workshop begrüßen zu dürfen. Insofern hatte der Workshop eindeutig einen Vernetzungscharakter. Er war auch so konzipiert, die Zusammenarbeit zwischen der Fachgruppe „Informatik und Inklusion", dem FIfF, verschiedenen Landesverbänden und öffentlichen Beauftragten für die Belange von Menschen mit Behinderungen sowie interessierten Hochschulen mit einschlägigen Forschungsansätzen zu stärken.

IT-Sicherheit ist ein sehr sensibler Bereich, denn es geht unter anderem um persönliche Daten, den Schutz der eigenen digitalen Identität, Abwehr von betrügerischen Manipulationen, Zugang zu vertraulichen Unterlagen und nicht zuletzt den Zugriff auf das eigene Konto. Anders als Herr und Frau Mustermann, auf die gängige Hard- und Software für IT-Sicherheitszwecke typischerweise zugeschnitten sind, treffen Menschen mit Behinderung oft auf „Barrieren", die ihnen das Handhaben von üblichen Mechanismen der IT-Sicherheit erschweren oder sogar unmöglich machen. Das Problem trifft aber (vielleicht in geringerem Maße) auch Menschen mit Einschränkungen unterhalb der Schwelle einer amtlichen Behinderung, dazu zählen insbesondere viele ältere Menschen.

Spannende Fragen in diesem Umfeld sind zum Beispiel:

- Wie lässt sich Barrierefreiheit „by design" erreichen? Also Systeme von Anfang an so zu planen und zu gestalten, dass Barrierefreiheit gegeben ist, nicht eingeschränkte Personen aber Einstellungen zur Steigerung der Arbeitsleistung und des persönlichen Wohlgefühls verändern können. Bisher ist es meist genau anders herum: Systeme werden für eine Hauptbenutzergruppe optimiert, für alle anderen werden (im besten Fall) nachträglich Hilfen zur Verfügung gestellt.

- Welche „Mitspieler" müssen angesprochen und überzeugt werden, um Fortschritte in der Barrierefreiheit zu machen? Wo geht das eher über die politische Schiene (Vorschriften), wo besser über freiwillige Aktivitäten (z. B. zwecks Profitmaximierung durch Ausweitung des Nutzerkreises eines Systems)?

- Welche erprobten (oder vielleicht auch noch unerprobten) Methoden, Mittel und Systeme stehen bereits zur Verfügung, um konkrete Schritte in Richtung Barrierefreiheit zu unternehmen?

Im Workshop auf der FIfFKon 2017 wurden konkrete Pläne für eine Zusammenarbeit über Ländergrenzen hinweg gefasst. Thematisch soll es dabei um sogenannte *Tastbare Displays* gehen, vgl. z. B.

- *https://www.elektronikpraxis.vogel.de/hmi/articles/543342/*,
- *https://d-nb.info/1076314538/34*,
- *https://tu-dresden.de/ing/informatik/institut-fuer-angewandte-informatik/mci/ressourcen/dateien/Dissertation_DenisePrescher.pdf*

Die neue Technologie ist den Betroffenen noch weitgehend unbekannt, hier ist über die Blinden- und Sehbehindertenverbände Aufklärungsarbeit zu leisten. Außerdem sind administrative Regelungen zur Versorgung zu treffen, die Technik muss weiterentwickelt und tauglich für die Massenfabrikation gemacht werden.

Eberhard Zehendner

Das war die FIfFKon 2017

Nachbetrachtungen und Danksagungen

Wie war denn nun die FIfF-Konferenz 2017 in Jena? Auf jeden Fall bunt, vergleiche dazu das Programm in der tatsächlich durchgeführten Fassung[1]. Im Vorfeld gab es Bedenken, das Programm sei „sehr vollgepackt", lasse keinen Raum für individuelle Begegnung und Diskussion. Darüber mögen die Teilnehmenden nachträglich nun selbst befinden. Jede FIfFKon hat ihren eigenen Stil.[2]

Provokant hatte ich mir die Konferenz gewünscht, und auch das war sie. Der TLfDI rügte die Datenschutzpolitik der Bundesregierung, TDRM die Zurückhaltung belgischer Atombehörden. Cyber-Aktivitäten der Bundeswehr und Zensusvorbereitungsgesetz wurden zerlegt. Dazwischen, für die FIfFKon eher ungewöhnlich, konstruktive Vorträge zu Drohnenabwehr und ziviler Sicherheit. Heftig debattiert wurde die (Un-)Möglichkeit sicherer Handys. Nicht alle goutierten das Programm: „FIfFKon17 scheint eine ziemlich wirtschafts- und staatslastige Veranstaltung zu sein", schallte es aus dem Netz. Das Festhalten an Überzeugungen dürfte auch bei wechselnden Allianzen möglich sein, daran wird sich das FIfF vielleicht noch gewöhnen.

Das große Experiment: Beginn der Workshops um 8 Uhr! „Für eine freiwillige Veranstaltung schon recht ambitioniert." In der Tat. „Ich mache das Experiment gerne mit und wir können uns überraschen lassen." Halbwegs geglückt, würde ich sagen.

Angemessene Danksagung

Am Ende eines Films bin ich oft beeindruckt von der nicht enden wollenden Liste der im Abspann genannten Mitwirkenden. Besonders hervorheben möchte ich die kostenfreie Überlassung aller Räume und Dienstleistungen durch die *Friedrich-Schiller-Universität Jena,* die unentgeltliche Mitwirkung aller Vortragenden und „helfenden Hände" sowie die großzügige finanzielle und technische Unterstützung durch den *Chaos Computer Club.*

Ich habe ein wahrhaft wunderbares Verzeichnis aller an der FIfFKon 2017 Beteiligten zusammengestellt, aber dieser Rand ist zu schmal, es zu fassen.[3]

Trailer – War da nicht noch was...?

Zu meiner großen Freude war fast der gesamte FIfF-Vorstand durchgängig auf der FIfFKon 2017 anwesend – bis auf Werner Winzerling, der wegen eines Notfalls leider kurzfristig verhindert war. Auch von den ursprünglich zugesagten Veranstaltungen konnten die meisten realisiert werden.

Allerdings konnte Sascha Turban (HU Berlin) seinen bereits angekündigten Vortrag *It stays a matter of trust – Perspektiven für Open-Source-Software in der Post-Snowden-Ära* aus gesundheitlichen Gründen nicht halten. Überraschende Umstrukturierungen bei IANUS, einer Einrichtung zur wissenschaftlichen Friedensforschung an der TU Darmstadt, hinderten Thea Riebe am diesbezüglichen Vortrag und zugehörigem Workshop. Dorina Gumm (FH Lübeck) musste ihren geplanten Vortrag *Vertrauen ist gut, Verschlüsseln ist besser* bereits vor Programmerstellung leider wieder absagen. Und für Florian Mehnerts Ausstellung FREIHEIT 2.0 fehlten uns schließlich die finanziellen Mittel.

Der FIfF-Vorstand fand einen uns kurzfristig angebotenen Vortrag zu *Hubzilla* zwar durchaus interessant und auch zum Konferenz-Motto passend, konnte die nötigen Reisemittel aber nicht bereitstellen. Umso erfreulicher ist es, dass unser Heft-Schwerpunkt TRUST durch Gustav Walls auf Seite 68 beginnenden schriftlichen Beitrag *Informationelle Selbstbestimmung und Datenautonomie mit Hubzilla* sozusagen über die FIfFKon 2017 hinaus „verlängert" werden konnte.

Kurioses rund um die FIfFKon 2017

Das vom Fakultätsrechenzentrum an alle E-Mail-Accounts der Fakultät für Mathematik und Informatik verschickte Tagungsprogramm wurde durch die Spam-Filterung des Universitätsrechenzentrums abgefangen.

Ein Beamer für die Tagung verschwand auf ungeklärte Weise aus dem Dienstzimmer eines Mitarbeiters, und ebenso mysteriös erschien dort ein Flipchart, das ich auf der Tagung gut gebrauchen konnte.

Das Video-Team hatte im Catering-Bereich Spezialkabel in einem Müllsack deponiert, was erst entdeckt wurde, nachdem eine größere Menge Kaffeesatz dort entsorgt worden war.

Über die Berichte des Catering-Teams erfuhr ich erst Monate später, dass die speziell für die Tagung erworbene Großkaffeemaschine zwischendurch den Dienst versagt hatte.

John Perry Barlow, der 23C3 und „Trust"

Nachdem bekannt wurde, dass *John Perry Barlow* am 7. Februar 2018 verstorben war, beschloss die Redaktion der FIfF-Kommunikation den Abdruck seiner *Declaration of the Independence of Cyberspace* als Retrospektive. Mich interessierte darüber hinaus, welche Auffassung Barlow zum Thema *Trust* vertrat. Bei einer Recherche fand ich Erstaunliches: Der *23rd Chaos Communication Congress* (27.-30.12.2006, Berlin) des *Chaos Computer Clubs* stand unter dem Motto *Who can you trust?* Und die gleichnamige Keynote[4] hielt … John Perry Barlow!

Ins Zentrum seiner Ausführungen stellte Barlow einen einzigen Aspekt (auch wenn er mehr als die Hälfte seiner Vortragszeit brauchte, bis er auf den Punkt kam): Lange Zeit sei die Gruppe, die mit Netztechnologien sehr gut umgehen konnte, zahlenmäßig überschaubar geblieben und einer gemeinsamen *Kultur,* einer Ethik verpflichtet gewesen. Ihm sei daher relativ klar gewesen, wem er selbst im Netz vertrauen konnte. Aber dies hätte sich jetzt dramatisch geändert, dieselben Methoden würden

nun auch für kriminelle Zwecke eingesetzt: „But now I see other things going on in this environment […] that make me wonder very much about whether or not we can trust each other."

Barlow beschrieb, wie E-Mail, ein bisher für ihn essentielles Kommunikationsmedium, durch Spam unbrauchbar wurde. Wie sich Viren ausbreiten konnten, weil die Community nichts dagegen unternahm, nichts unternehmen wolle, derartige Angriffe sogar billigend als subversive Aktionsform missverstehe. Vielleicht seien bei seiner Ansprache sogar Übeltäter zugegen, meinte er, und schockierte die Anwesenden kollektiv: „I don't trust you!"

Die Erkenntnis, dass die Grenzen zwischen „gut" und „böse" im Cyberspace nicht mehr so einfach zu erkennen sind, anders verlaufen als früher, kann auch den Blick auf die FIfFKon 2017 klären. Ich hatte mir von Gabriele Schades Vortrag zur Glaubwürdigkeit (sie selbst formulierte es zu Beginn des Vortrags um in: Vertrauenswürdigkeit) der Medien eine akkurate Herausarbeitung der besonderen Güte öffentlich-rechtlicher Medien gegenüber denen der Privatwirtschaft erhofft. Und war dann – wie viele – enttäuscht, dass der Vortrag das nicht leistete. Aber vielleicht war genau das die *Message;* vielleicht gibt es ja keine prinzipiellen Unterschiede. Und sogleich fallen mir wieder die Bilder aus dem Irak ein, die Anfang der 90er-Jahre wochenlang unverändert, aber mit stets neuen „Nachrichten", auch über die Fernsehkanäle von ARD, ZDF, BR und ORF flimmerten. Wäre es nicht ehrlicher gewesen, nur Texte zu verlesen, und ansonsten den vom Militär gesteuerten Mangel an neuem Bildmaterial offensiv zu thematisieren?

Nun noch ein kleiner Ausflug zu Barlows früherem Schaffen, einem Ausschnitt aus einem von ihm verfassten Song-Text für die Rockgruppe *Grateful Dead:*

Strikes the morning, atomic dawn
Scramble back to cover
Quick, pop your mirrored sunglasses on

(J. P. Barlow, Picasso Moon, 1989)

Diese Verse klingen für mich wie eine sarkastisch eingedampfte Version des US-Zivilverteidigungsfilms *Duck and Cover*[5], der ab 1951 Kinder auf den Atomkrieg vorbereiten sollte[6] und noch Ende der 70er-Jahre in der westdeutschen Zivilschutzausbildung zum Einsatz kam. Interpretiert man das damalige Verhalten der Behörden nicht nur als Akt der Hilflosigkeit, sondern als bewusste Täuschung der Bevölkerung, schließt sich der Kreis zur Thematik aus dem TDRM-Artikel auf Seite 6.

Alle Vöglein sind schon da…

Wirklich alle? Natürlich nicht. Es war vorhersehbar, dass einige der erbetenen schriftlichen Beiträge nicht rechtzeitig zur Drucklegung dieses Hefts eintreffen würden. Doch gab es jemals eine FIfF-Konferenz, deren Beiträge ALLE abgedruckt wurden? Ich kann es mir nicht vorstellen. Oder ich habe es vergessen. Oder ich habe es vergessen.

Immerhin sind in diesem Heft erstaunlich viele unserer Vortragenden, Organisierenden und Mitwirkenden zu Wort gekommen. Ein Heft, so bunt wie die Konferenz selbst! Für unsere Online-Ausgabe der FIfF-Kommunikation gilt dies sogar im wörtlichen Sinne.

Zusätzlich enthielt bereits die FIfF-Kommunikation 4/2017 einen zusammenfassenden Bericht über die FIfFKon 2017 sowie das Beschlussprotokoll der FIfF-Mitgliederversammlung, die unmittelbar nach Ende der Konferenz stattfand. Das Heft dokumentierte überdies die Einführungsrede von Stefan Hügel zum FIfF-Studienpreis, die Laudatio für die Masterarbeit des Preisträgers Tobias Krafft und – unter dem Titel *Danke, Dietrich!* – eine Würdigung der Verdienste unseres Vorstandsmitglieds Dietrich Meyer-Ebrecht, der nicht mehr als stellvertretender Vorsitzender kandidierte und auch einige seiner zahlreichen Ämter weitergab – aber glücklicherweise weiterhin dem FIfF-Vorstand angehört. Der für das FIfF produzierte und auf der FIfFKon 2017 erneut gezeigte Kurzfilm *Cyberpeace statt Cyberwar* wurde bereits in der FIfF-Kommunikation 2/2017 vorgestellt.

Brave New World – Gestaltungsfreiheiten und Machtmuster soziotechnischer Systeme

Wir sehen uns dann auf der FIfFKon 2018 in Berlin!
https://2018.fiffkon.de/

Anmerkungen

1 *fiff.de/r/181033*
2 *Videomitschnitte der FIfFKon 2017 werden unter https://media.ccc.de/b/conferences/fiffkon sowie auf YouTube bereitgestellt, Bilder, Folien und Manuskripte auf der Website der FIfFKon 2017, https://2017.fiffkon.de/. Weitere Aufzeichnungen, bei denen z. B. die technische Qualität Defizite aufweist, sind über http://www2.informatik.uni-jena.de/~nez/ zu finden.*
3 *Stattdessen sei hier auf die Website der FIfFKon 2017 verwiesen, https://2017.fiffkon.de/*
4 *https://media.ccc.de/v/23C3-1256-en-who_can_you_trust*
5 *https://www.youtube.com/watch?v=IKqXu-5jw60*
6 *https://www.wikiwand.com/de/Duck_and_Cover*

Eberhard Zehendner

Prof. Dr. **Eberhard Zehendner** lehrt und forscht seit 1994 an der Friedrich-Schiller-Universität Jena u. a. im Bereich Informatik & Gesellschaft. Er arbeitete bereits in Schwerpunktredaktionen zu den Themen *Datenschutz* (FK 2/2015), *Cybercrime* (FK 4/2015) und *Datenschutz handhabbar* (FK 2/2017) mit. Dem FIfF-Vorstand gehört er seit 2013 an.

Gustav Wall

Informationelle Selbstbestimmung und Datenautonomie mit Hubzilla

Immer mehr Lebensbereiche erfahren durch die Digitalisierung einen Wandel. Viele Zeitgenossen reagieren auf diese Entwicklung mit wachsender Sorge um ihre Privatsphäre und sind auf der Suche nach Möglichkeiten, von den Vorteilen der Digitalisierung zu profitieren, ohne ihre Privatsphäre abgeben zu müssen und zu gläsernen Bürgern degradiert zu werden.

Ein Kooperationsverbund aus DENIC, 1&1 und Open-Xchange versucht diese Nachfrage mit einer Lösung namens *id4me* zur nutzerindividuellen Authentisierung für Internet-Services zu befriedigen. In der aktuellen Pressemitteilung[1] beschreibt DENIC die *id4me*-Lösung so:

> *„[…] der offene, freie und sichere Ansatz zur nutzerindividuellen Authentisierung für Internet-Services […] wird es dem Nutzer erlauben, sich mit einem einzigen Passwort bei einer Vielzahl von Diensten anzumelden und festzulegen, mit wem er wie lange welche Daten teilt."*

Beim Lesen der Pressemitteilung entsteht der Eindruck, die anvisierte *id4me*-Lösung könne dem Nutzer auch mehr Datenautonomie bieten.

Was bei *id4me wie* Zukunftsmusik klingt, ist bei der Open-Source-Lösung *Hubzilla*[2] schon Realität. Mit Hubzilla hat der Nutzer eine komfortable zeitsparende Möglichkeit, sich mit einem einzigen Passwort bei einer Vielzahl internetweiter Hubzilla-Dienste anzumelden und festzulegen, mit wem er welche Daten teilt.

Was ist Hubzilla?

Hubzilla – weiter Hbz genannt – ist ein dezentrales Netzwerk, dessen Erfinder und Macher sich das Ziel gesetzt haben, ein Medium zu realisieren, dessen Struktur und verwendetes Protokoll eine reibungslose zeitsparende Kommunikation ohne Zensur und ohne Überwachung ermöglichen. Hubzilla bietet viele nützliche Features. Die Relevanz jedes einzelnen Features hängt vom jeweiligen Anwendungsszenario ab.

Gefragte Features – Omnipräsenz, hohe Verfügbarkeit und Vertraulichkeit

Omnipräsenz, hohe Verfügbarkeit und Vertraulichkeit sind in vielen Anwendungsszenarien gefragt und werden von vielen Hbz-Teilnehmern sehr geschätzt.

Unter *Omnipräsenz im Hbz-Kontext* ist zu verstehen:

- Einerseits die wörtlich gemeinte *Omnipräsenz,* also eine Fähigkeit von und Möglichkeit für die Hubzilla-Teilnehmer, überall dort einen Zugang zu den Hbz-Diensten zu bekommen, wo Teilnehmer sich einloggen und ihre *nomadische Identität* kontaktieren können. Der Ausfall einzelner Hbz-Knoten hat keine spürbaren Auswirkungen sowohl auf die Arbeitsbedingungen der einzelnen Hbz-Teilnehmer als auch auf die Funktionsfähigkeit des Hbz-Netzes insgesamt.
- Hinzu kommt die *Omnipräsenz der nomadischen Identität* in der Hubzilla-Community in dem Sinne, dass die Teilnehmer ständig eine Möglichkeit haben, viele Hubzilla-Teilnehmer zu kontaktieren. Diese Omnipräsenz in der Community ist mit geringem Aufwand realisierbar: beim Verfassen von Nachrichten kann ein Hbz-Teilnehmer mit dem Eintippen des *@-Symbols* und einer Zeichenfolge alle Kontakte aus dem persönlichen Adressbuch einblenden, *die diese Zeichenfolge enthalten.* Ein derartiger Kontakt kann auch eine Mailingliste oder ein Forum sein. Auf diese Weise können Hbz-Teilnehmer miteinander *zeitsparend* Nachrichten austauschen, ohne zuvor ihre Kontaktdaten ausgetauscht zu haben.

Ungewöhnlich *hohe Verfügbarkeit der Hubzilla-Dienste* im Sinne einer ITIL[3] ist ein weiteres Hbz-Alleinstellungsmerkmal, das durch die Omnipräsenz der Teilnehmer gewährleistet ist. Die Verfügbarkeit des Netzes mit allen Diensten und die Omnipräsenz der Hbz-Teilnehmer sind zwei Seiten einer Medaille. Die Verfügbarkeit, Ausfallsicherheit des Hbz-Netzwerks ist umso besser, je größer die Hubzilla-Community ist.

Vertraulichkeit im Hubzilla-Kontext bedeutet für den Objekteigentümer die Möglichkeit einer vollständigen Kontrolle darüber, wer diese Objekte im Hbz-Raum sehen oder verändern darf.

Nomadische Identität und andere Annehmlichkeiten

Nomadische Identität ist einer der zentralen Begriffe im Hubzilla-Netzwerk, im Hubzilla-Konzept, und die nomadische Identität ist ein Mittel, um die Omnipräsenz zu verwirklichen. Das herausragende Omnipräsenz-Feature ist dadurch möglich, dass die Hubzilla-Teilnehmer eine Möglichkeit haben, in Eigenregie einen Klon ihres Hbz-Profils auf beliebig vielen Knoten im Netzwerk zu erstellen, wodurch die Verfügbarkeit des Accounts de facto 100 % erreicht. Die Änderungen im Profil auf einem der Klon-Knoten werden in Echtzeit in anderen Klonen abgebildet. Auf diese Weise besteht die Möglichkeit, eine oder mehrere stets aktuelle Sicherheitskopien des Profils zu unterhalten und zu nutzen.

Folgende Features stehen einem Eigentümer nach der Installation des Hbz-Knotens *standardmäßig* zur Verfügung (unvollständige Auflistung):

- Adressbuch (Kontakte)
- Website
- Content Management System
- Soziale Netzwerke
- Foren
- Kalender
- Wiki
- Chats

– Speichercloud
– Sammlung von Anwendungen (Apps), erweiterbar entsprechend den Bedürfnissen des Knoteneigentümers.

Kommunikation im Hubzilla-Netzwerk wird mittels HTTPS-Protokoll abgewickelt. Zusätzlich besteht die Möglichkeit, die Nachricht teilweise oder komplett mit einem Passwort zu verschlüsseln.

Vielseitig begabte nomadische Identität

Gesprächsfreudig – eine Fähigkeit, mit Teilnehmern aus anderen Netzwerken zu kommunizieren, bspw. aus *Diaspora*[4] oder *Friendica*[5].

Multiformatfähig – kann viele Formate (HTML, einfacher Text, BBCode, Markdown, application/x-php) verarbeiten, was den Anwendern ermöglicht, in ihren Veröffentlichungen die Inhalte aus unterschiedlichen Quellen mit geringem Aufwand zu integrieren.

Digitaler Raum – die Wirkungsstätte der nomadischen Identität

Zot ist ein für das Hubzilla-Netzwerk entwickeltes Protokoll[6]. Es ist zuständig für den Austausch von Mitteilungen, die Verwaltung der nomadischen Identität und die Zugangsverwaltung in einem dezentralen Netzwerk, bestehend aus einzelnen Knoten, genannt *Hubs*. Im Hbz-Kontext wird dieses Netzwerk oft *Grid* genannt. Hbz-Knoten haben viele Features; die wichtigsten für den Hub-Eigentümer sind:

- Die Bereitstellung eines digitalen Raums der *nomadischen Identität* des Hub-Eigentümers. Die nomadische Identität verfügt über:
  – das Adressbuch des Kanal-Eigentümers
  – einen Raum für die Treffen mit anderen nomadischen Identitäten
  – eine Art *Sendestation* mit einem oder mehreren Kanälen, oder einen *Verlag* mit einer oder mehreren Veröffentlichungen, Veröffentlichungsreihen
  – *ein System für eine vollständige Kontrolle* darüber, wer eigene Objekte im Hbz-Raum sehen oder verändern darf.

- Die nomadische Identität kommuniziert entsprechend der Vollmacht des Eigentümers der jeweiligen Identität mit anderen nomadischen Identitäten aus dem Hbz-Raum oder mit den Gästen.

- Ein *digitaler Raum,* der vom Hub-Eigentümer an fremde nomadische Identitäten *vermietet* werden kann. Jede fremde nomadische Identität hat die gleichen Fähigkeiten wie die nomadische Identität des Vermieters, vorausgesetzt der Mieter und der Vermieter vertrauen einander oder sie haben einen Mietvertrag geschlossen.

Demnach stellt das Hbz-Netzwerk einen Lebensraum für nomadische Identitäten dar, deren Fähigkeiten und Leistungsumfang durch den Eigentümer bestimmt werden.

Je nach Belastung des Hbz-Knotens, die von der Anzahl der registrierten Nutzer, von deren Kommunikationsfreudigkeit, von der Anzahl der Kontakte sowie der Anzahl der unangemeldeten Besucher abhängt, funktioniert Hbz auf einem Mini-PC Raspberry Pi[7] genauso zuverlässig wie auf den größten AMD- oder Intel-Xeon-Multiprozessor-Servern.

Vertiefung (Empfehlung des Autors)

Hubzilla-Projekt, https://project.hubzilla.org/

Hubzilla-Hilfe, https://project.hubzilla.org/help/

The history of Hubzilla, http://www.talkplus.org/blog/2016/the-history-of-hubzilla/

Hubzilla Community, Linkssamlung, http://hub2.sprechrun.de/page/hucope/hubzilla-community

Heliza: Considerations for Hubzilla mobile agent concept, http://hub2.sprechrun.de/page/flegno/heliza-considerations-for-one-hubzilla-mobile-agent-concept_en

Zukunftsfähige digitale Ökosysteme im Post-Google-Zeitalter, 13.10.2014, http://sprechrun.de/web21/?id=1708

Gustav Wall, Hubzilla – Einführung, Möglichkeiten, Hubzilla community, LVEE-2017, 24.6.2017, Vortragsvideo (russisch), http://0x1.tv/20170424C

Hubzilla – Interview zum dezentralen sozialen Netzwerk, 21.11.2017, https://greennetproject.org/2017/11/21/interview-zum-thema-hubzilla/

Anmerkungen

1 *DENIC (23. Februar 2018) Next-Level Evolution: Homo Digitalis; DENIC-Internetkonferenz Domain pulse 2018 im Zeichen von digitalem Wandel zwischen Freiheit und Sicherheit. Pressemitteilung. https://list.denic.de/arc/public-l/2018-02/msg00000.html*

2 *https://hubzilla.org/*

3 *https://de.wikipedia.org/wiki/IT_Infrastructure_Library*

4 *https://de.wikipedia.org/wiki/Diaspora_(Software)*

5 *https://de.wikipedia.org/wiki/Friendica*

6 *https://hub.libranet.de/help/developer/zot_protocol*

7 *https://www.raspberrypi.org/*

Gustav Wall

Gustav Wall … ist unterwegs im digitalen Raum für mehr Datenschutz, Nachhaltigkeit und freie Kommunikation. *https://hub.libranet.de/channel/nmoplus* führt zu seiner nomadischen Identität im Hubzilla-Grid.
Homepage: *http://sprechrun.de*

Visionär, Rebell und Lyriker – in memoriam John Perry Barlow

Vor wenigen Wochen starb John Perry Barlow im Alter von 70 Jahren. Vielen von uns dürfte seine „Declaration of the Independence of Cyberspace" (zumindest dem Namen nach) bekannt sein. Wir drucken dieses bemerkenswerte Dokument auf der nächsten Seite im vollen Wortlaut ab. Der Titel ähnelt dem der amerikanischen Unabhängigkeitserklärung von 1776, und das ist keineswegs Zufall, wie nicht nur Barlows Anspielung auf die dieser vorausgehende „Boston Tea Party" in seiner „Begründung" zeigt, sondern auch seine Bezugnahme auf Thomas Jefferson, (Haupt-)Verfasser der Unabhängigkeitserklärung und einer der „Gründerväter" der USA.

Barlows Begründung der Erklärung ist quasi das Anschreiben zu dieser: der Einleitungstext einer zornigen E-Mail vom 9. Februar 1996 (nachfolgend reproduziert), der die Hintergründe des Konflikts zwischen Netzgemeinde und damaliger US-Regierung weniger feinsinnig analysiert als die Erklärung selbst. Und durch die Nennung zweier nun auch im Internet unter Strafe gestellter „four-letter words" provozierend ebendiese Strafe riskiert.

Auch wenn es heute bei Eingriffen in das Netz nicht mehr um Sprachkosmetik geht, zeigen doch Regulierungsbemühungen wie jüngst das *NetzDG* (Dank an Ralf Graf für diesen Bezug), dass die alten „Tyrannen" noch immer die Vereinnahmung des öffentlichen Raumes betreiben, den Barlow als „Cyberspace" bezeichnete. Nur dass mittlerweile zusätzlich etliche Wirtschaftsgiganten auf deren Seite mitspielen.

Barlow war 1990 Mitgründer der *Electronic Frontier Foundation* (EFF), auch hier zeigt der Anlass Parallelen zu aktuellen Geschehnissen (siehe z. B. *https://www.eff.org/de/about/history*). 2012 gründete Barlow die *Freedom of the Press Foundation* (FPF) mit, deren Präsident derzeit Edward Snowden ist. Für die Rockband *Grateful Dead* schrieb Barlow zahlreiche bekannte Songtexte.

Date: Fri, 9 Feb 1996 17:16:35 +0100
To: barlow@eff.org
From: John Perry Barlow <barlow@eff.org>
Subject: A Cyberspace Independence Declaration

Yesterday, that great invertebrate in the White House signed into the law the Telecom „Reform" Act of 1996, while Tipper Gore took digital photographs of the proceedings to be included in a book called „24 Hours in Cyberspace."

I had also been asked to participate in the creation of this book by writing something appropriate to the moment. Given the atrocity that this legislation would seek to inflict on the Net, I decided it was as good a time as any to dump some tea in the virtual harbor.

After all, the Telecom „Reform" Act, passed in the Senate with only 5 dissenting votes, makes it unlawful, and punishable by a $250,000 to say „shit" online. Or, for that matter, to say any of the other 7 dirty words prohibited in broadcast media. Or to discuss abortion openly. Or to talk about any bodily function in any but the most clinical terms.

It attempts to place more restrictive constraints on the conversation in Cyberspace than presently exist in the Senate cafeteria, where I have dined and heard colorful indecencies spoken by United States senators on every occasion I did.

This bill was enacted upon us by people who haven't the slightest idea who we are or where our conversation is being conducted. It is, as my good friend and Wired Editor Louis Rossetto put it, as though „the illiterate could tell you what to read."
Well, fuck them.

Or, more to the point, let us now take our leave of them. They have declared war on Cyberspace. Let us show them how cunning, baffling, and powerful we can be in our own defense.

I have written something (with characteristic grandiosity) that I hope will become one of many means to this end. If you find it useful, I hope you will pass it on as widely as possible. You can leave my name off it if you like, because I don't care about the credit. I really don't.
But I do hope this cry will echo across Cyberspace, changing and growing and self-replicating, until it becomes a great shout equal to the idiocy they have just inflicted upon us.

I give you...

Foto: Joi Ito, CC BY 2.0

John Perry Barlow (3. Oktober 1947 – 7. Februar 2018)

A Declaration of the Independence of Cyberspace

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.

You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.

You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.

Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.

In the United States, you have today created a law, the Telecommunications Reform Act, which repudiates your own Constitution and insults the dreams of Jefferson, Washington, Mill, Madison, DeToqueville, and Brandeis. These dreams must now be born anew in us.

You are terrified of your own children, since they are natives in a world where you will always be immigrants. Because you fear them, you entrust your bureaucracies with the parental responsibilities you are too cowardly to confront yourselves. In our world, all the sentiments and expressions of humanity, from the debasing to the angelic, are parts of a seamless whole, the global conversation of bits. We cannot separate the air that chokes from the air upon which wings beat.

In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace. These may keep out the contagion for a small time, but they will not work in a world that will soon be blanketed in bit-bearing media.

Your increasingly obsolete information industries would perpetuate themselves by proposing laws, in America and elsewhere, that claim to own speech itself throughout the world. These laws would declare ideas to be another industrial product, no more noble than pig iron. In our world, whatever the human mind may create can be reproduced and distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish.

These increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers. We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.

We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.

Davos, Switzerland

February 8, 1996

Dietrich Meyer-Ebrecht

Zero Days

Dokumentarfilm über Geschichte und Hintergründe des Stuxnet-Angriffs

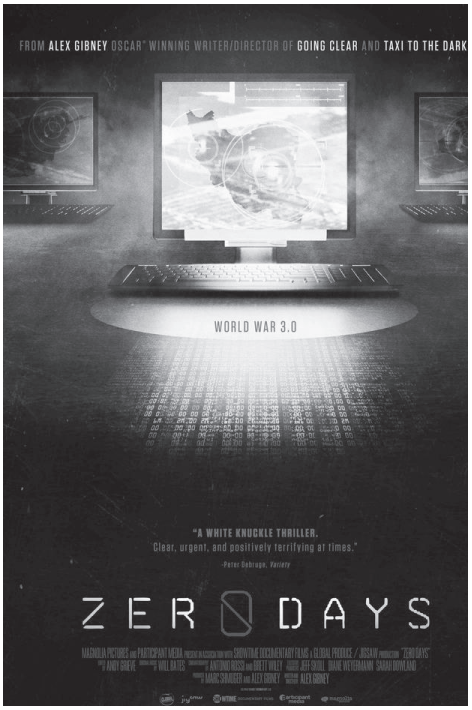
Dreimal habe ich mir den Film angeschaut. Jedes Mal eröffnete er mir mehr Details, jedes Mal war er wieder spannend bis zum Abspann. Und jedes Mal ging er mir tiefer unter die Haut. In *Zero Days* zeichnet der Regisseur und Oscar-Preisträger Alex Gibney die Geschichte der Entdeckung und Analyse des Computerwurms *Stuxnet* nach und versucht, die politischen und strategischen Hintergründe aufzudecken. Sein Publikum entlässt Gibney mit Denkanstößen, was Stuxnet für unsere Gesellschaft bedeuten kann und welche Folgen die durch Stuxnet offenbarte – technische, militärische, politische – Entwicklung für uns alle haben könnte. *Zero Days* ist ein gelungener Dokumentarfilm – unterhaltsam und spannend, dass er das Publikum erreicht und mitzieht, nicht ohne eine Position zu beziehen und eine Botschaft zu vermitteln. Er ist dabei ein anschauliches Beispiel, wie investigativer Journalismus geht.[1]

Wie ein Mosaik setzt Gibney den Plot aus Interviewschnitten zusammen, mit einem Minimum an Kommentar, und es ergibt sich am Ende ein schlüssiges Bild. So bringt Gibney die führenden Köpfe der Community, die sich mit der Aufdeckung der Rätsel um Stuxnet befasst hat, vor die Kamera und folgt mit Interviewschnitten der langwierigen Puzzlearbeit um die schrittweise Aufdeckung der Rätsel um Stuxnet. Politiker, Militärs, leitende Beamte, Journalisten lässt er zu Wort kommen, wenn es um Hintergründe und Folgen geht.

Am 17. Juni 2010 entdecken die „Woodpecker" der Computersicherheits-Unternehmen, zuerst in Weißrussland, einen neuen rätselhaften Typus von Schadsoftware im Internet. Sie nennen ihn *Stuxnet,* ein Amalgam aus zwei Codeschnipseln. Die Community der Sicherheitsanalysten, darunter führende Experten der Computersicherheits-Unternehmen Kaspersky Lab und Symantec, sind geschockt von der Komplexität dieser Schadsoftware. Für den *Dropper,* die für die Selbstausbreitung verantwortliche Softwarekomponente, werden vier Zero-Days genutzt – außergewöhnlich, wer kann sich einen derart hohen Aufwand leisten? Auch die *Payload,* die sich im Zielsystem aktivierende Softwarekomponente, überrascht bezüglich ihres Umfangs und ihrer Undurchschaubarkeit.

Die Zeichen verdichten sich, dass staatliche Akteure hinter dem Projekt stehen. In der *Payload* werden Hinweise auf PLC-Geräte gefunden, *Programmable Logic Controller* für die Steuerung von Maschinen und Geräten. Die Spur führt zu Siemens-Produkten. Offensichtlich identifiziert die *Payload* das Zielsystem anhand von Seriennummern für ein sehr gezieltes Zuschlagen. Die Seriennummern führen zu Zulieferern von Frequenzumrichtern und schließlich in den Iran. Aus US-Embargolisten kommt der Hinweis auf Anwendungen in nukleartechnischen Einrichtungen. Auf die Spur zum Ziel der Schadsoftware führt schließlich die Auswertung von Propagandafilmmaterial aus iranischen Atomforschungseinrichtungen: Entdeckt werden Korrespondenzen zwischen Zahlenmustern im *Payload*-Code und Gruppierungen der Urananreicherungszentrifugen in Anlagenplänen. Aber wer sind die Urheber? Was ist ihre Intention? Aus dem Off, „wo wir auch nachfragten, wir trafen auf eine Mauer des Schweigens, wir mussten uns andere Wege suchen".

Einen Ansatzpunkt liefert der Cyberwarfare-Experte David E. Sanger, Korrespondent der New York Times, mit einem Rückblick auf die Geschichte der politischen Beziehungen zwischen den USA und dem Iran. Ab 1959, unter Schah Reza Pahlavi, wird mit US-amerikanischer Unterstützung ein iranisches Atomforschungsprogramm aufgebaut. Die USA schenken dem Schah 1959 und 1967 jeweils einen Forschungsreaktor. Schon der Schah liebäugelt mit eigenen Atomwaffen. Nach 1979, dem Jahr der iranischen Revolution, wird Irans Streben nach eigenen Atomwaffen unüberhörbar. Der Iran treibt ihre Entwicklung voran, heimlich unterstützt von Pakistan. Die politische Situation im Nahen Osten wird zunehmend instabil. Israel sieht sich existenziell bedroht und bittet die USA um grünes Licht für Bombenangriffe auf iranische Nuklearanlagen. Die USA befürchten eine Eskalation, in die sie hineingezogen würden. Sie machen Israel das Angebot, einen „anderen Weg" zu finden. Die Militärs überzeugen Präsi-



Filmplakat, Magnolia Pictures[4]*: Zero Days (2016)*
Dokumentarfilm von Alex Gibney, 116 Minuten
Weitere Filmdaten: http://www.imdb.com/title/tt5446858/
Offizielle Filmseite: http://www.zerodaysfilm.com/

dent Bush von der Option eines Cyberschlags. Die Entwicklung wird im *Department of Defense* begonnen unter dem Codenamen „Olympic Games", später auf Drängen von Verteidigungsminister Gates in das neu geschaffene *US Cyber Command* verlagert. Beteiligt ist der israelische Geheimdienst.

Die Mauer des Schweigens. Bis heute gibt es zur Rolle der USA oder Israels keinerlei offizielle Erklärung, Aussage, Stellungnahme, Dementi. Nicht einmal ein Wort zur Existenz dieser Cyberwaffe. Selbst Sicherheitsorgane in den USA waren nicht informiert und glaubten an einen Angriff von außen, als Stuxnet auch heimische Systeme infizierte. Aber Washington sei nicht nur ein Ort der Geheimhaltung, sondern auch ein Ort der Lecks. Gibney findet seins. Vermutlich aus der Meisterklasse der NSA, der Abteilung TAO, zuständig für *Tailored Access Operations.* Vor die Kamera darf er diese Person (oder Personen?) natürlich nicht bringen. Ihre Aussagen lässt er von einer Schauspielerin mit verfremdeter Stimme sprechen, Aussagen über das Potenzial von Stuxnet, über die Rolle der NSA, über den schmalen Grat zwischen Ausspähung und Angriff – und über die Existenz einer noch weit mächtigeren Cyberwaffe für den Fall, dass die Verhandlungen mit dem Iran scheitern würden – *Nitro Zeus,* dazu bestimmt, die iranische Luftabwehr lahmzulegen und Teile des iranischen Stromnetzes auszuschalten.[2]

Dass die Existenz von Stuxnet aufgedeckt werden kann, verdanken wir dem israelischen Geheimdienst. Während man sich mit mehreren bestens getarnten Stuxnet-Vorversionen an den beabsichtigten Einsatz herantastet, modifizieren 2010 die Israelis die Software im Alleingang. Dabei unterläuft ihnen ein fataler Fehler, der zur Entdeckung führt – und die Zivilgesellschaft wird erstmals ganz konkret mit der potentiellen Bedrohung durch Cyberwaffen konfrontiert.

Stuxnet zerstört vermutlich um die tausend Zentrifugen in iranischen Nuklearanlagen. Die Produktion von angereichertem Uran wird, so die Kontrolleure der IAEA, ausgebremst – für ein Jahr. Danach nimmt sie erst richtig Fahrt auf. Der Iran baut seinerseits eine schlagkräftige Cyberwarfare-Einheit auf, Vergeltungsdrohungen richten sich an die USA. Im Iran vermutet man die Urheber folgenschwerer Cyber-Angriffe auf ein US-Unternehmen der Petrochemie und auf eine US-Bank. Zu den Folgen hat Ralph Langner, SPS-Sicherheitsberater, einen ausführlichen und lesenswerten Bericht veröffentlich.[3]

„Stuxnet hat die Büchse der Pandora geöffnet", O-Ton der anonymen Informantin. Oder Michael Hayden, „einmal ausgepackt, kann eine solche Waffe nicht mehr weggepackt werden". Die Zahl der Staaten und nichtstaatlichen Organisationen, die ein schlagkräftiges Cyberwaffen-Arsenal aufbauen, wird zunehmen, ebenso die nichtkalkulierbaren Risiken. Insider kommen zu Wort, die die Gefahren für die Gesellschaft noch über die der Atomwaffen stellen. Vor diesem Hintergrund appelliert der Terror-Experte Richard A. Clarke engagiert für einen Cyberwaffen-Bann. Auch wenn heute die praktische Unmöglichkeit einer Waffenkontrolle prophezeit wird. „Es hat 30 Jahre gedauert, und es wurde für unmöglich gehalten, aber heute haben wir wirksame Verbote von biologischen Waffen und Chemiewaffen und einige brauchbare Verträge für eine Atomwaffenkontrolle. Auch bei Cyberwaffen wird es Zeit brauchen. Aber es wird sich nur etwas bewegen, wenn wir anfangen!"

Ein hervorragender Einstieg in die Cyberpeace-Debatte, für öffentliche Veranstaltungen, für den Unterricht in Schulen und Ausbildungsstätten … könnte der Film sein, wenn die sprachliche Verständlichkeit nicht so schwierig wäre: Die Interviews werden auf Englisch geführt, und die Interviewten sind keine geschulten Sprecher (der Genderpunkt ist hier nicht nötig, bezeichnenderweise), sie sprechen teils sehr schnell, in knappen Sätzen, mit starkem Akzent, in Slang- und Fachtermini. Hinzu kommt die eigentlich unnötige und störende Verfremdung der Stimme der Schauspielerin. Ist man nicht im angelsächsischen Sprachraum unterwegs, zudem vielleicht auch mit den Fachbegriffen nicht vertraut, wird man ohne wiederholtes Abhören den Feinheiten der Aussagen kaum folgen und viele Zusammenhänge nicht erfassen können. Jedoch, durch eine Synchronisation oder überlagerte Kommentierung würde dem Film die Authentizität verloren gehen, und davon lebt der Film. Deswegen ist der Film doch unbedingt zu empfehlen. Auch für Veranstaltungen, wenn er moderiert, an wichtigen Stellen kommentiert und natürlich diskutiert wird.

> *"The title ZERO DAYS refers on one level to the multiple soft-ware vulnerabilities that made Stuxnet possible, as well as the infinite software vulnerabilities that will fuel the attacks of the future. But it is also a potent metaphor for this moment in time. We don't have a patch for this problem yet. From this moment forward, we're going to have to reckon with this new challenge of the potential of cyberwar. These are our 'Zero Days.' We're starting from zero. What are we going to do going forward?" — Alex Gibney*[5]

Zusätzliche Empfehlung der Redaktion: ZERO DAYS VR[6]

> *"How do you make a documentary where the lead character is code – where code could speak for itself? […] The true story of a clandestine mission hatched by the US and Israel to sabotage an underground Iranian nuclear facility told from the perspective of Stuxnet, a sophisticated cyber weapon, and a key NSA informant. Audiences experience the high stakes of cyber warfare placed inside the invisible world of computer viruses." – Scatter*[7]

Anmerkungen und Referenzen

1 *Vorgestellt am 17. Februar 2016 auf den Internationalen Filmfestspielen Berlin*

2 *Sanger DE, Mazetti M (16. Februar 2016) U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict. New York Times.* https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html

3 *Langner R (2017) Stuxnet und die Folgen. Langner Communications GmbH, Hamburg.* https://www.langner.com/wp-content/uploads/2017/08/Stuxnet-und-die-Folgen.pdf

4 Magnolia Pictures (2016) Zero days. Complete press kit. http://www.magpictures.com/resources/presskits/ZERODAYS.zip

5 *Magnolia Pictures (2016) Zero days; Final press notes.* http://www.magpictures.com/resources/presskits/zerodays/ZERODAYSfinalnotes.doc

6 *ZERO DAYS VR.* https://www.zerodaysvr.com/

7 *Scatter (Januar 2018) Zero days VR. Press kit.* https://www.zerodaysvr.com/s/1801_ZeroDays_PressKit.pdf

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

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*

Mitglieder-Wiki
https://wiki.fiff.de

FIfF-Beirat

Ute Bernhardt (Berlin); **Peter Bittner** (Kaiserslautern); **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** (Mannheim); 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); **Ingo Ruhmann** (Berlin); Prof. Dr. **Gerhard Sagerer** (Bielefeld); Prof. Dr. **Gabriele Schade** (Erfurt); **Ralf E. Streibl** (Bremen); Prof. Dr. **Marie-Theres Tinnefeld** (München); Dr. **Gerhard Wohland** (Waldorfhäslach)

FIfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Rainer Rehak (stellv. Vorsitzender) – Berlin
Michael Ahlmann – Kiel / Blumenthal
Sylvia Johnigk – München
Benjamin Kees – Berlin
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Prof. Dr. **Dietrich Meyer-Ebrecht** – Aachen
Kai Nothdurft – München
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	1 200 Stück
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck, Eberhard Zehendner
Schwerpunktredaktion	Hans-Jörg Kreowski, Eberhard Zehendner
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
Cover	Tagungsplakat der FIfFKon 2017 (Ausschnitt) von Benjamin Kees und Lena Schall
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 Autor.innen-Meinung wieder.

Die FIfF-Kommunikation ist das Organ des FIfF und den politischen Zielen und Werten des FIfF verpflichtet. Die Redaktion behält sich vor, in Ausnahmefällen Beiträge abzulehnen.

Nachdruckgenehmigung wird nach Rücksprache mit der Redaktion in der Regel gern erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

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

Aktuelle Ankündigungen

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

34. FIfF-Konferenz – #FIfFKon18
„Brave New World" – Gestaltungsfreiheiten und Machtmuster soziotechnischer Systeme
28. bis 30. September, Berlin

Bits & Bäume
Die Konferenz für Digitalisierung und Nachhaltigkeit
17. bis 18. November, Berlin

FIfF-Kommunikation

2/2018 „Staats-Hacking – Die ‚Gerätchenfrage'"
Rainer Rehak
Redaktionsschluss: 4. Mai 2018

3/2018 „Informatik und Gesellschaft"
Stefan Hügel u. a.
Redaktionsschluss: 3. August 2018

4/2018 „Alter(n)sgerechte Informatik"
Eberhard Zehendner, Stefanie Jäckel
Redaktionsschluss: 2. November 2018

1/2019 „Brave New World"
Rainer Rehak, Benjamin Kees, Anne Schnerrer u. a.
Redaktionsschluss: 1. Februar 2019

W&F – Wissenschaft & Frieden
4/17 Eingefrorene Konflikte (mit Dossier 85: Transhumanismus und Militär)
1/18 USA – eine Inventur

---

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik
#217 Der Islam als Herausforderung für das deutsche Religionsverfassungsrecht
#218 Rückkehr zum gerechten Krieg?
#219 Soziale Menschenrechte
#220 Europa in der Krise
#221 Datenschutz nach der DSGVO

DANA – Datenschutz-Nachrichten
1/17 – Verbraucherschutz
2/17 – BDSG-Nachfolgegesetz
3/17 – 40 Jahre DVD
4/17 – Gesundheitsdatenschutz

Das FIfF-Büro

Geschäftsstelle FIfF e. V.
Ingrid Schlagheck (Geschäftsführung), Michael Jacobsen
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

Hans-Jörg Kreowski

Mit Tränen in den Augen

Im Schlussplenum der FIfFKon 2017 habe ich zum Schluss das Wort ergriffen, um Eberhard Zehendner und seinem Organisationsteam noch einmal herzlich zu danken für die reibungslose und durchdachte Organisation und für die Gestaltung eines reichen und anregenden Programms mit vielen Höhepunkten. Mit zwei Elementen habe ich versucht, das auszudrücken.

Friedrich Schiller …

Die Friedrich-Schiller-Universität Jena gehört mit ihrem über 450-jährigen Bestehen zu den ältesten Einrichtungen dieser Art in Deutschland. Sie ist durch viele „Aufbrüche und Umbrüche" geprägt, wie es auf der Webseite heißt. Ein herausragendes Ereignis datiert auf den 26. Mai 1789: Friedrich Schiller hält als frisch berufener Professor für Geschichte seine Antrittsvorlesung zum Thema – und ich nehme hier eine kleine Fälschung vor – „Was heißt und zu welchem Ende studiert man Informatik". Unter anderem heißt es darin – wieder ein wenig gefälscht:

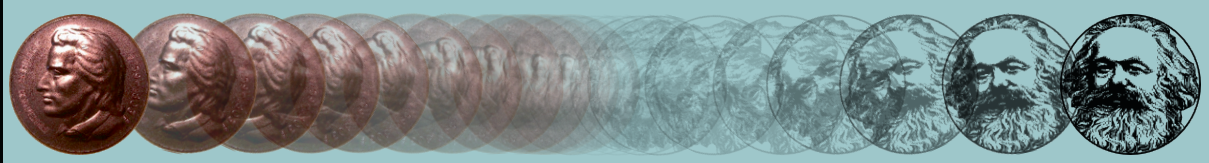
> *„Der Informatikprofessor hat umsonst gelebt und gearbeitet, wenn sich Technik und Wissenschaft für ihn nicht in Drittmittel, Medienecho und Politikerlob verwandeln."*

Die vollständige und bis heute äußerst lesenswerte Antrittsvorlesung ist auf vielen Webseiten im Internet zu finden, u. a. unter *https://www.uni-jena.de/Sonderausgabe_Schiller_AV*.

… und ein FIfFKon 2017-Gedicht

Wie schon zu anderen Gelegenheiten habe ich wieder einen Versuch zu konkreter Poesie unternommen. Das Gedicht spiegelt das weitgefächerte Programm wider, indem ich nach meinem persönlichen Geschmack aus allen Programmpunkten ein Schlüsselwort herausgepickt habe:

Schiller – Trusted – Datenschutz-Grundverordnung
Dummies – Cyber- und Informationsraum – The Making of …
Drohnenabwehr – Kampagne – Zero Days
Algorithmen – barrierefrei – Security
Gegenspieler – matter-of-trust – Spam
Schrott-Atomreaktoren – sozial und zivil – Rundfunk
Blick zurück – Danke – Preis
Zensus – Handys – Wardriving
Hands-on – Gesundheitswesen – Täter
Wie viele – Free-to-Play – FIfFKon 2017



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