H 7625

FIfF-Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

32. Jahrgang 2015 Einzelpreis: 7 EUR

3/2015 – September 2015

Rüstung und Informatik

ISSN 0938-3476

• Cyberpeace-Appell • FIfFKon 2015 • EU-Datenschutz-Grundverordnung •

Mit Dossier: Kriegführung im Cyberspace

FIfF Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V.

Titelbild: Landung des Euro Hawk (Global Hawk) auf dem Flugplatz Ingolstadt-Manching (ETSI) im Jahr 2011, Philipp Hayer, CC BY-SA https://commons.wikimedia.org/wiki/File:EuroHawk_Landing_ETSI_2011.jpg

Inhalt

Ausgabe 3/2015

inhaltt

Editorial

Rüstung und Informatik – das Gründungsthema des FIfF, heute so aktuell wie 1984. Ein Thema, das das FIfF immer beschäftigt hat, in Konferenzen, Schwerpunkten der *FIfF-Kommunikation*, im Arbeitskreis *RUIN* und in unserer aktuellen Kampagne *Cyberpeace*.

In dieser Ausgabe gibt es den Schwerpunkt gleich doppelt: in diesem Heft und zusätzlich – unter dem Titel *Kriegführung im Cyberspace* – als Dossier, das in bereits bewährter Zusammenarbeit mit der Zeitschrift *Wissenschaft und Frieden* entstanden ist und dieser Ausgabe beiliegt. Gleichzeitig ist die aktuelle Ausgabe der **vor***gänge*, der Zeitschrift für Bürgerrechte und Gesellschaftspolitik der Humanistischen Union dem Thema *Cybersecurity* gewidmet, ebenfalls mit Beiträgen aus dem FIfF. Der Schwerpunkt der **vor***gänge* hat einen stärkeren innenpolitischen Bezug und unterscheidet sich damit von unseren außenpolitisch fokussierten Schwerpunkten – doch die Frage ist die gleiche: Wie können wir uns und unsere Infrastruktur heute schützen, in der Zeit internationaler geheimdienstlicher Zusammenarbeit gegen die eigene Bevölkerung und der – zumindest aus technischer Sicht – unterschiedslosen Bedrohung aus dem nationalen und dem internationalen Netz? Was ist technisch, politisch und rechtlich erforderlich, um einen neuen *Wilden Westen* im Cyberspace zu verhindern?

Dietrich Meyer-Ebrecht, der sowohl Schwerpunkt als auch Dossier redaktionell betreut hat, weist in seinem Editorial zum Schwerpunkt zusätzlich auf die zunehmende Verwischung der Grenzen zwischen zivilen und militärischen Anwendungen hin. Es geht nicht nur um *Dual Use* – diese Diskussion führen wir bekanntlich schon lange – sondern auch um den fördernden Einfluss ziviler Lifestyleprodukte auf militärische Anwendungen: *„Technik ist per se eine unverzichtbare Grundlage für die Kriegführung, und alle technischen und technologischen Innovationen im zivilen Anwendungsbereich sind per se auch Stimuli und Ressourcen für die Rüstungstechnik."*

In den Schwerpunkt und seine Beiträge führt das Schwerpunkteditorial im Detail ein. Auf einen Beitrag will ich dennoch bereits hier hinweisen: Der Künstler *Florian Mehnert* berichtet in dieser Ausgabe von seinem Kunstprojekt *11 TAGE*, bei dem eine Waffe auf eine Ratte gerichtet ist, die – nach Ablauf von 11 Tagen – aus dem Internet ferngesteuert ausgelöst werden könne und damit die Ratte töten soll. Nur vorgeblich; es bestand nie die Absicht, die Ratte wirklich zu töten. Doch bereits die Ankündigung führte offenbar zu einem Shitstorm gegen den Künstler, der auf die Aufforderung, ihn zu lynchen, nicht verzichtete. *„Would like to put a gun against his head and well would say blow his brains out but he clearly has none"* – dies ist nur ein Beispiel dafür. Im *„Krieg gegen den Terror"* werden Menschen unter Terrorismusverdacht ohne rechtsstaatliches Verfahren durch Drohnen getötet, gemeinsam mit den Menschen, die sich zufällig in ihrer Nähe befinden, auch Kinder – ohne dass dies größere Proteste auslösen würde. Florian Mehnert sieht in dem Shitstorm so auch eine Ersatzhandlung: *„... Somit war der Fokus stark auf den Tod der Ratte und ihre lebensbedrohliche Lage gerichtet. Dennoch wurde die Situation der Ratte mit der Lage von Menschen in Syrien, Jemen, Waziristan etc., die durch Drohnen getötet wurden oder konstant mit einem Tod durch Drohnen rechnen müssen, assoziiert. Eine Diskussion darüber fand unter anderem in zahlreichen Foren statt."* Gegen den Drohnenkrieg können wir uns nicht wirksam einsetzen; den Tod einer Ratte glauben wir, durch unseren Einsatz gerade noch verhindern zu können. *„In diesem Zusammenhang"*, so Mehnert, *„kann der Shitstorm auf das Kunstexperiment 11 TAGE auch als Reaktionsventil der emotionalen und geistigen Überforderung im Umgang mit einer komplexen Realität angesehen werden, deren Durchdringung und Bewältigung immer schwieriger wird."* Mit diesem Schlaglicht auf die Problematik menschlicher Bewältigung von Komplexität weist der Beitrag über die Thematik des Schwerpunkts hinaus.

Aktuelle Themen ergänzen das Heft. Zu dem Versuch, die freie Presse durch den Vorwurf des Landesverrats gegen *netzpolitik.org* einzuschüchtern, hat das FIfF einen Kommentar veröffentlicht. Zur Debatte um die EU-Datenschutz-Grundverordnung veröffentlichen wir einen Beitrag, der für den aktuellen Schwerpunkt der Datenschutz-Nachrichten (DANA) entstanden ist und in dem, wir unsere *Roten Linien* darstellen – keinesfalls darf der Datenschutz-Standard hinter die heute gültige Richtlinie von 1995 zurückfallen. Die anlasslose Speicherung von Fluggastdaten in der EU lehnen wir ab, in den Plänen der Bundesregierung für eine Cybersicherheits-Strategie sehen wir die Ankündigung, gegen Regelungen der Genfer Konvention verstoßen zu wollen, da sie offensive Angriffe auf zivile Infrastrukturen vorsehen.

Sylvia Johnigk geht in einer Kolumne der Frage nach, warum Hacken überzeugt und IT-Sicherheit langweilt. Neuigkeiten im Bereich *Faire Computer* hat *Sebastian Jekutsch* zusammengestellt.

Die Retrospektive, Berichte über FIfF-Aktivitäten – diesmal in Wien und in Bremen – zwei Rezensionen und das Log runden diese Ausgabe der *FIfF-Kommunikation* ab.

Dazu gibt es die Vorschau auf unsere diesjährige FIfF-Konferenz 2015, die vom 6. bis 8. November 2015 in Erlangen stattfinden wird. Florian Mehnert wird von seinem bereits angesprochenen Kunstprojekt berichten; weitere Vorträge behandeln unter anderem *Privacy by Design* und die Datenschutzaspekte von *Smart-TVs.*

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

Stefan Hügel
für die Redaktion

cyberpeace

appell.cyberpeace.fiff.de

Frau von der Leyen, verzichten Sie auf Cyberwaffen für die Bundeswehr!

Mit seiner Kampagne Cyberpeace setzt sich das FIfF für eine ausschließlich friedliche Nutzung der Informations- und Kommunikationsnetze ein. Wir appellieren an unsere Regierung und an den Deutschen Bundestag, auf Cyberwaffen zu verzichten und sich für einen internationalen Bann dieser Waffengattung einzusetzen. Unterstützen Sie diesen Appell durch Ihre Unterzeichnung!

Militärische Operationen im Cyberspace bedrohen die Zivilgesellschaft

In nahezu allen Lebensbereichen hat sich die Zivilgesellschaft von digitaler Informationstechnologie abhängig gemacht. Das setzt uns neuen Risiken und Gefahren aus. Die Enthüllungen von Aktivitäten der Geheimdienste NSA, GCHQ und BND haben den virtuellen Raum als Ort einer Ausspähung in bisher nicht gekanntem Ausmaß enttarnt, damit aber nur die Spitze des Eisbergs gezeigt. Neben seiner umfassenden Nutzung für die Spionage hat der virtuelle Raum eine zentrale Funktion für die Militärs: Er ist Operationsraum für Cyberwaffen.

Die Entwicklung und der Einsatz von Cyberwaffen gefährden ein Internet, das durch weltweite Vernetzung großartige Chancen zur Förderung von Frieden und Völkerverständigung bieten könnte und sollte.

Szenarien des Cyberkriegs reichen von Destabilisierung durch Meinungsmanipulation über Sabotage bis zu Tod und Zerstörung verursachenden Eingriffen in die Computernetze kritischer Infrastruktur-Einrichtungen.

Die geduldete Öffnung des virtuellen Raums für Cyberangriffe setzt die Aushebelung von Grundrechten voraus. IT-Sicherheitsfunktionen werden mit staatlicher Billigung unterlaufen. Schon heute bedroht dies nicht nur unsere informationelle Privatsphäre, es setzt die Zivilgesellschaft unkalkulierbaren Risiken aus – toleriert von Politik und Wirtschaft.

Cyberwaffen sind unkontrollierbar

In ihrer Unfassbarkeit und Unkontrollierbarkeit stellen Cyberwaffen eine verschwiegene, aber höchst reale latente Gefahr für den Frieden dar. Im Gegensatz zu ABC-Waffen und konventionellen Waffen hinterlassen ihre Herstellung, Erprobung und Bereithaltung keine physischen Spuren. Damit fehlt die Grundlage für jede Art von Nichtweiterverbreitungs- oder Rüstungskontrollabkommen. Unberechenbar sind ihre Wirkungen, beabsichtigte wie unbeabsichtigte. Unvorhersehbar sind dauerhafte Beschädigungen unserer digitalen Kultur, gesellschaftlich wie wirtschaftlich. Unkalkulierbar sind Auswirkungen auf Innen- und Außenpolitik. Aufgrund dieser Risiken ist eine unheilvolle Entwicklung nur durch frühzeitiges Gegensteuern abwendbar.

Cyberpeace-Appell

Wir fordern die Bundesregierung und die Abgeordneten des Deutschen Bundestages auf, zum Schutz der Zivilgesellschaft zu handeln und sich dafür einzusetzen,

- **dass Deutschland auf eine offensive Cyberstrategie verzichtet,**
- **dass sich Deutschland verpflichtet, keine Cyberwaffen zu entwickeln und zu verwenden,**
- **dass sich die Bundesregierung für internationale Abkommen zu einem weltweiten Bann von Cyberwaffen einsetzt.**

Der Appell kann online *appell.cyberpeace.fiff.de* oder auf Unterschriftenlisten unterzeichnet werden. Wir bitten die diesem Heft beiliegenden Formulare auszulegen, wo immer es passt – und sie zum Einsenden wieder einzusammeln! Weitere Formulare können bei *cyberpeace@fiff.de* angefordert werden. Der Appell ist Teil der Cyberpeace-Kampagne, die durch die *Stiftung Bridge* gefördert wird.

Vielen Dank für Ihre, eure Unterstützung!

Der Brief

Überwachung – lebenslänglich

Liebe Leserinnen und Leser, liebe Mitglieder des FIfF,

über zwei Jahre dauert inzwischen an, was wir zu Beginn als *„NSA-Skandal"* bezeichnet haben und häufig immer noch bezeichnen. Die zugrunde liegende Ausspähung gibt es freilich schon länger; vom *„Skandal"* sprechen wir, seit die Veröffentlichungen von Edward Snowden sie öffentlich bekannt werden ließ.

Die Bezeichnung *NSA-Skandal* erscheint inzwischen aus zwei Gründen zweifelhaft:

- Zumeist verbinden wir mit einem Skandal ein zeitlich begrenztes Ereignis. Ein Missstand wird bekannt, er eskaliert zu einem Skandal, es entsteht öffentlicher Druck, der zu Konsequenzen führt, z. B. dem Rücktritt von verantwortlichen Akteuren. Der *NSA-Skandal* ist aber weder zeitlich begrenzt – denn es ist kein Ende abzusehen – noch sind Konsequenzen sichtbar: Es gab weder erkennbare personelle Konsequenzen in der Politik, noch wurden Überwachungsmaßnahmen erkennbar reduziert. Im Gegenteil: Die verantwortlichen Behörden fordern immer weitere Befugnisse, ohne dass dies zu öffentlicher Empörung oder Ablehnung führen würde.

- Als Urheber wird zumeist die US-amerikanische NSA – *National Security Agency* – genannt. Längst ist aber inzwischen klar, dass die NSA eng mit weiteren Behörden zusammenarbeitet, z. B. mit deutschen Geheimdienstbehörden und mit Wissen oder (zumindest stillschweigender) Duldung deutscher Regierungsbehörden.

Bereits die Ausspähung nach dem zweiten Weltkrieg wurde offenbar mit Wissen und Unterstützung deutscher Behörden durchgeführt. Josef Foschepoth weist in seiner bekannten Untersuchung darauf hin, dass 1955 auf ausdrücklichen Wunsch der Bundesregierung Besatzungsrechte der Alliierten in Kraft blieben, die die Überwachung des Postverkehrs juristisch legitimierten. Auch bei der aktuellen Debatte um die Freigabe der Selektoren für die Überwachung wurden US-Behörden verantwortlich gemacht: Diese hätten verlangt, dass die Informationen dem Untersuchungsausschuss nicht zugänglich gemacht werden dürften. Dieser Argumentation der Bundesregierung wurde dann offenbar durch US-Regierungsbehörden der Boden entzogen: Sie hätten zwar Bedenken geäußert, aber nicht verlangt, dass die Listen vor den Abgeordneten des Deutschen Bundestags geheim gehalten werden müssten. Das lässt wiederum die Folgerung zu, dass die Bundesregierung diese Entscheidung im eigenen Interesse getroffen hat. Es wäre interessant, die tatsächlichen Beweggründe zu erfahren. Konsequenzen gab es auch hier natürlich keine.

Auch die juristische Bewertung der Ausspähung durch den Generalbundesanwalt und die daraus resultierende Passivität bei ihrer Verfolgung ist kaum nachvollziehbar, nachdem es sich mutmaßlich um geheimdienstliche Agententätigkeit gegen deutsche Behörden und Wirtschaftsunternehmen handelt. Ist die Macht der US-Regierung über die Bundesrepublik Deutschland so groß, dass eine Verfolgung politisch nicht möglich ist? Steht es den Interessen der deutschen Akteure selbst entgegen, die Vorfälle zu untersuchen und zu verfolgen?

Nach der großen Zurückhaltung der Staatsanwaltschaft bei der Verfolgung der Ausspähung der deutschen Politik, Wirtschaft und Gesellschaft fällt das Verfahren gegen *netzpolitik.org* umso mehr ins Auge. Unabhängig von der juristischen Bewertung entsteht der deutliche Eindruck, dass hier eine kritische Stimme eingeschüchtert werden sollte. Merkwürdig war die sich anschließende Debatte, wer nun wen angezeigt haben will und wer was gewusst habe. Offenbar müssen wir uns glücklich schätzen, dass unsere Regierungsvertreter wenigstens Zeitung lesen – nur von dort scheinen sie ihre Kenntnis wesentlicher, ihr Ressort betreffender Vorgänge zu beziehen.

Der ganze Vorgang erinnert an die Spiegel-Affäre von 1962. Damals verbrachten Rudolf Augstein und weitere Reporter des *SPIEGEL* mehrere Wochen im Gefängnis. Soweit ist es dieses Mal zum Glück nicht gekommen.

Unabhängig von den ausbleibenden Konsequenzen – heute findet zumindest noch eine Diskussion über Überwachung statt, auch außerhalb der Fachcommunity – wenn sie sich auch häufig auf resignierend-sarkastische Bemerkungen beschränkt. Wird es solche Diskussionen in der Zukunft überhaupt noch geben? Angesichts der technologischen Entwicklung bei Smartphones und ihren Apps ist es wohl mittlerweile fraglich, ob die heute heranwachsende Generation ein Leben ohne ständige Überwachung überhaupt noch kennenlernen wird. Bereits in früher Kindheit können Kinder und ihr Aufenthaltsort auf Schritt und Tritt überwacht werden; Eltern werden sofort benachrichtigt, wenn *„erlaubte Zonen"* verlassen oder *„verbotene Zonen"* betreten werden. Die neue Microsoft-Betriebssystemversion Windows 10 erstellt offenbar auf Wunsch der Eltern ein vollständiges Protokoll aller Aktivitäten ihrer Kinder am Computer und im Internet. Die BigBrotherAward-preisgekrönte Spielzeugpuppe *Hello Barbie* zeichnet die Äußerungen von Kindern auf – selbstverständlich nur zur Spracherkennung. Diese Datensammlung bereits in frühester Kindheit wird dazu führen, dass alle Menschen zu jeder Zeit unter Überwachung stehen und sich dessen auch bewusst sind.

Die tägliche Überwachung in der Kindheit wird dann fortgesetzt – Smartwatches, die Gesundheitsdaten messen, aufzeichnen und weiterleiten, sind nur ein Beispiel dafür.

Werden die nächsten Generationen ein Leben ohne Überwachung noch kennenlernen? Ist dann eine freiheitliche Gesellschaft überhaupt noch möglich?

fragt mit FIfFigen Grüßen

Stefan Hügel

Sylvia Johnigk

Warum Hacken überzeugt und IT-Sicherheit langweilt

Neulich, in der Kantine bei einem Auftraggeber, sprachen wir über das Image von Hackern und IT-Sicherheitsspezialisten. IT-Sicherheitsspezialisten, vor allem Interne, also Angestellte, genießen in Unternehmen das Image des Spielverderbers. Das Management möchte neue innovative Produkte einsetzen und jedes Mal steht da ein IT-Sicherheitsspezialist, der seine Bedenken, also Sicherheitslücken, aufzeigt, die dazu führen, dass Unternehmensdaten oder gar Kundendaten abhandenkommen können. Für das Management ein Ärgernis, die Welt ist voller Möglichkeiten, die *„ganze Welt"* darf sie einsetzen und vor ihnen steht ein Bedenkenträger, der dies verhindern und ihnen das *Spielzeug* wegnehmen möchte.

Für das Management sind solche Unzulänglichkeiten lästig, sie wollen das Produkt trotzdem. Sie fordern vom IT-Sicherheitsspezialisten eine Lösung, die es ermöglicht, das Produkt möglichst in seiner ganzen Vielfalt nutzen zu können. Natürlich dürfen Sicherheitsmaßnahmen nur wenig kosten, es sei denn, die IT-Sicherheitsspezialisten erbringen den Beweis, dass ihre Befürchtungen nicht nur ihrer wild gewordenen Fantasie entspringen.

Der einzige Weg, dem Management Zustimmung und Budget abzuringen, ist, einen *externen* Hacker zu kennen, der nicht nur Hacken kann, sondern auch einen Anzug besitzt, ihn trägt und in einer Management-kompatiblen Sprache einen *Live Hack* zeigen kann. Das macht Eindruck. Zumindest für einen kurzen Augenblick, den die IT-Sicherheitsspezialisten schnell nutzen müssen, um ein Budget zu bekommen. Damit die Sicherheitsmaßnahmen umgesetzt werden können, die sie vorgeschlagen haben. Fazit: Sie bekommen ihr Budget, aber warum?

Live Hacken ist unmittelbar, man kann es *„fast anfassen"*. Zumindest kann man *es* mit eigenen Augen sehen. Das System ist gehackt, die Daten wurden entwendet. Der Beweis wurde erbracht. Wenn der *Live Hack* dann noch ein Spektakel ist, so hinterlässt das manchmal sogar einen bleibenden Eindruck.

Ganz anders ist es mit der IT-Sicherheit. Sie zu zeigen ist unspektakulär. Wenn IT-Sicherheitsspezialisten einen richtig guten Job gemacht haben, passiert nichts, was einer Erwähnung wert wäre. Das ist wie ein Krimi ohne Tote, ein Formel-Eins-Rennen ohne Unfall oder ein Fußballspiel ohne Foul und Tor. Das ist nicht nur langweilig, sondern richtig langweilig – leider. Machen wir einen Selbstversuch. Stehen Sie auf, gehen Sie vor einen Spiegel und stellen Sie sich vor, Sie stehen vor Ihren Managern. Und dann sagen Sie dynamisch und kraftvoll: *„Es ist nichts passiert! Ich möchte ein Budget, damit weiterhin nichts passiert."* Und? Haben Sie sich selbst überzeugt? Würden Sie sich ein Budget geben, damit nichts passiert? *„Nichts passiert"*, das ist wie Stillstand und ärgerlich für den IT-Sicherheitsspezialisten, der sich letztendlich dieselben Gedanken macht wie der Hacker, nur dass der IT-Sicherheitsspezialist die Sicherheitslücken voraussieht und gleich die notwendigen Sicherheitsmaßnahmen umgesetzt hätte, wenn das Budget da gewesen wäre. So muss er warten, bis das Produkt fertiggestellt ist und ein Hacker mittels eines Penetrationstests die Sicherheitslücken aufzeigt, die man schon vorher gesehen hat. Bei IT-Sicherheitsspezialisten kommt da ein wenig Frust auf.

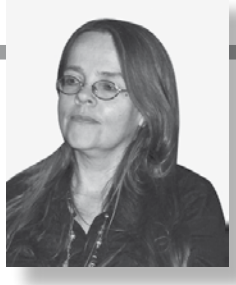
Hacken ist Aktivität. Der Hacker wirkt kraftvoll, dynamisch, belebend. Er ist ein Macher, der energiegeladen die Tür eintritt, wenn sie ihm nicht geöffnet wird. Er redet nicht nur davon, dass IT-Systeme verwundbar sind, er führt es den Zweiflern vor. Er zeigt damit den Stinkefinger. Und obwohl das Management darüber verärgert sein müsste, ist es begeistert. Endlich jemand, der mit der Faust auf den Tisch schlägt, sich durchsetzt und nicht nur so daher redet.

Das Problem ist, Hacker sind nötig, um das Management zu überzeugen, weil Taten offensichtlich besser wirken als Worte. Dabei darf man aber nicht vergessen, dass es wesentlich einfacher ist, ein existierendes System auseinander zu nehmen und es zu hacken, als ein neues IT-System zu entwickeln, das frei von Sicherheitslücken ist. Die Ungleichheit besteht darin, dass der Hacker nur eine einzige Sicherheitslücke finden muss, während der IT-Sicherheitsspezialist alle Sicherheitslücken finden und schließen muss, bevor das IT-Produkt ausgeliefert wird.

Das Beste wäre, wenn Hacker und IT-Sicherheitsspezialisten enger mit den Entwicklern zusammenarbeiten würden. Vor allem müssten beide in die gesamte Produktentwicklung integriert werden, um gemeinsam die Sicherheitslücken frühzeitig zu entdecken und zu schließen. Dazu müssten Hacker nicht nur *„destruktiv sein und kaputtmachen"*, sondern ihr Können nutzen, um Sicherheitslücken von vornherein zu vermeiden. Möglicherweise beißt sich da die Katze in den Schwanz, teure Sicherheitsmaßnahmen lassen sich nur rechtfertigen, wenn der Beweis erbracht wird, dass ein Sicherheitsproblem tatsächlich existiert und nicht nur ein Hirngespinst ist. Die Existenz eines Sicherheitsproblems lässt sich nur beweisen, wenn das System existiert und man es live hackt.

Im Übrigen, wenn ein IT-System mal nicht gehackt werden kann, so hat der IT-Sicherheitsspezialist noch lange keinen guten Job gemacht. Viel wahrscheinlicher ist, dass der Hacker seinen Job nicht gut genug gemacht hat. Oder?

Sylvia Johnigk



Sylvia Johnigk studierte Informatik an der TU Berlin und befasste sich schon im Studium mit Themen wie Datenschutz und Informationssicherheit. Sie arbeitete fünf Jahre in der Forschung und acht Jahre bei einem Finanzdienstleister. Seit 2009 ist sie selbständig und leitet ein kleines Unternehmen in München, das sich auf Beratung von Unternehmen zum Thema Informationssicherheitsmanagement mit dem Schwerpunkt Mitarbeitersensibilisierung spezialisiert hat.

Sebastian Jekutsch

Betrifft: Faire Computer

Fair wie in Fairer Fruchtsaft.

Was wirklich anders ist als früher, als zum Beispiel Foxconn in allen Zeitungen war: Es gibt keine Empörung mehr. Das beginnt schon damit, dass es kaum neue investigative Berichte aus den Elektronikfertigungshallen dieser Welt gibt. Von der Produktion der Apple Watch zum Beispiel liegen nur ein paar Bilder und ein kurzer Bericht vor. Da fällt für eine Kolumne wie diese kaum etwas ab. Die einschlägigen Organisationen sind anders unterwegs:

- Die eine investigativ recherchierende Organisation namens SACOM konzentriert sich auf die Bekleidungsindustrie, die andere namens *China Labor Watch* auf die Spielzeugindustrie.

- *ElectronicsWatch* ist das einzige europäische Projekt zur fairen IT, das allerdings in Sachen öffentlicher Beschaffung arbeitet, wichtig zwar, aber ein gähnend zähes Bürokratenthema.

- *GoodElectronics* arbeitet vor allem im Kleinen und unterstützt die Arbeit lokaler Arbeitsrechtsorganisationen, so dass dort gewerkschaftliche, aber auch arbeitsschutzrechtliche Trainings ermöglicht werden, z. B. auf den Philippinen oder in Mexiko. Sie veröffentlichten ansonsten gemeinsam mit SOMO zusammenfassende Dossiers über Nokia in Indien oder NXP in Indonesien. Ein Medienecho findet das nicht.

Es ist – das ist die gute Nachricht – eine Konzentration der Arbeit weg von Skandalisierung über Sweatshop-beauftragende Markennamen hin zu einer ergebnisorientierten Arbeit für die Betroffenen, auch bei den Teileherstellern und nicht mehr nur bei den Zusammenschraubern. Und wichtig: Unsere Einflussnahme, sei es durch Gesetzgebung, öffentliche Beschaffung oder alternative Unternehmen rückt in den Fokus.

Westliche Firmen haben nicht mehr die große Bedeutung. Zunehmend sind es die Günstiggerätehersteller aus zum Beispiel China, die den Markt bestimmen und die zunehmend reichen Schwellenländer beliefern. Kennt jemand *Huawai* oder *Xioami*? Bei denen ist Fairness noch nicht angekommen. So wie die Arbeitsplätze wandern inzwischen auch die Marken, so wie die Arbeitgeber nun also auch die Käufer. Die Hoffnung indes, die neuen Fertigungsländer Indien, Myanmar oder Vietnam könnten die Fehler Chinas vermeiden, ist nicht angebracht. Es bleibt bei der Unfairness, die letztlich auch die Industrialisierung unserer so genannten ersten Welt prägte.

In Sachen Krebsfälle bei Samsung hat das Panel der drei Parteien *Sharps* (kämpferische Opferorganisation), einzelner Familien (mit geringeren Forderungen) und Samsung selbst die Empfehlung veröffentlicht, eine Stiftung zu gründen, um Unfälle in der Display- und Halbleiterindustrie zu vermeiden. Samsung will das aber gar nicht unterstützen, sondern lediglich (zudem eingeschränkt) finanzielle Kompensation zahlen. Es gibt also eigentlich gar keinen Fortschritt in dieser Sache.

Ein US-Gericht hat sein eigenes Urteil bestätigt, dass Firmen entgegen einer Anweisung der US-Börsenregulierung ihren Kunden verschweigen dürfen, dass ihre Produkte „möglicherweise nicht konfliktfrei" sind, denn sie dürfen nicht gezwungen werden, schlecht über sich selbst zu reden. Das hat sich ein Industriekonsortium erkämpft, dem auch z. B. Intel, HP und Microsoft angehören, aber immerhin hatten die drei sich davon distanziert. Fakt ist, dass die große Mehrheit der Firmen bislang nicht herausfinden konnte, ob ihre Geräte nun konfliktfrei sind oder nicht. Derweil ist ein kritischer Film über die Probleme des dem Ganzen zu Grunde liegenden US-Dodd-Frank-Act 1502 unter dem Namen „We Will Win Peace" erschienen und sehr sehenswert.

Was machen die möglichst fairen Geräte? *Fairphone* hat zwar nun den Vorverkauf seiner zweiten, modulareren Generation von Geräten zu einem deutlich höheren Preis gestartet, zum namensgebenden Fairnessgrad der Geräte gab es anfangs aber keinerlei offizielle Verkündung. Inzwischen ist klar, dass es bei konfliktfreiem Zinn und Tantal bleibt, Wolfram kommt vielleicht hinzu, das mit dem Fairtrade-Gold klappt aber erstmal nicht. Auch wird sicher das Programm mit dem Fond für die Arbeiter fortgesetzt. Das ist gut, aber nichts Neues in dieser nach Neuem gierenden Branche. *Nager-IT* vermeldet, dass inzwischen 5 000 Computermäuse verkauft wurden. Mit *Shift* sind wir vom FIfF derzeit im Gespräch zur Einschätzung der angekündigten Fairness ihrer Geräte. Sie haben kurz vor Redaktionsschluss die mit dem Fertiger *Weihua* ausgehandelten Fairnessanforderungen veröffentlicht. Diese weisen u. a. ein ganz außergewöhnlich hohes Gehalt für die ArbeiterInnen aus. Wir bleiben am Ball.

Fairness im Elektroniksektor, so meine Einschätzung, macht nur ganz kleine Schritte. Fehlt uns und der Presse die verlorengegangene Empörung?

Sebastian Jekutsch

Sebastian Jekutsch ist Sprecher der AG Faire Computer des FIfF. Wer sich für die Quellen oder das Thema überhaupt interessiert, kann gerne Kontakt aufnehmen per *sj@fiff.de*.

FIfF e.V. – Pressemitteilung

Cybersicherheits-Strategie der Bundeswehr

FIfF fordert einen öffentlichen Diskurs

16. Juli 2015 – Die Pläne von Bundesverteidigungsministerin Ursula von der Leyen, das Internet zu einem Kriegsschauplatz zu erklären und die Fähigkeit der Bundeswehr auszubauen, offensiv Einsätze im In- und Ausland durchzuführen, ist eine Ankündigung Deutschlands, zukünftig wissentlich gegen die Genfer Konvention verstoßen zu wollen.

Deutschland ist aktuell nicht in der Lage, sein Parlament vor Angriffen zu schützen. Nach dem Bundestagshack steht die Regierungsfähigkeit unseres Landes auf dem Spiel. Aber statt kritische Infrastrukturen in Deutschland besser zu schützen und hierzu die IT-Fachkräfte des Landes einzusetzen, handelt die Verteidigungsministerin nach dem Motto einer amerikanischen Filmkomödie *„Angriff ist die beste Verteidigung"*.

Aus einem *„geheimen Dokument"*, das offenbar *SPIEGEL ONLINE* vorliegt, wird zitiert: *„[...] Bei Missionen im Ausland soll es zum Beispiel möglich sein, die Nutzung von Internet und Mobilfunk durch den Gegner ‚einzuschränken, gegebenenfalls sogar auszuschalten' [...] Möglicherweise könnten Reservesoldaten aus der IT-Wirtschaft ‚in hoheitlichem Auftrag' zur Unterstützung im Cybernotfall herangezogen werden."*

Um einen Gegner gezielt abzuwehren, müssen mindestens zwei Voraussetzungen erfüllt sein: Zum einen muss man den Angreifer in Echtzeit bzw. zeitnah zweifelsfrei identifizieren und lokalisieren können, gleichzeitig bräuchte man eine adäquate chirurgisch präzise Waffe, um diesen Angreifer virtuell schädigen zu können, ohne andere (‚*kollateral*') zu schädigen.

Beim Bundestagshack weiß man Monate später nur wenig über Hergang und Verursacher des Angriffs – und das trotz intensiver Untersuchungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) und externe IT-Dienstleister.

Für präzise Cyberoperationen wird ein Arsenal unterschiedlich wirkender Cyberwaffen und eine Vorratshaltung umfangreicher Kenntnisse über geheim gehaltene Schwachstellen für ihren Einsatz benötigt. Dabei ist jede geheim gehaltene Schwachstelle eine vertane Chance, sie zu schließen und damit unsere IT-Systeme sicherer zu machen.

Der Plan, offensive Angriffe auf zivile Infrastrukturen (Internet und Mobilfunk) im Ausland durchführen zu wollen, würde zu Kriegszeiten einen völkerrechtlichen Verstoß gegen die Genfer Konventionen darstellen. Ein solches Szenario zu Friedenszeiten zur erklärten Sicherheitsstrategie Deutschlands zu machen, bedeutet eine Ankündigung, zukünftig gegen die Genfer Konvention verstoßen zu wollen. *„Es wäre ein Skandal, deutsche IT-Fachkräfte zu missbrauchen und zwangszuverpflichten, um eine Sicherheitsstrategie zu unterstützen, die gegen das Völkerrecht verstößt"*, urteilt Sylvia Johnigk, Sprecherin der FIfF-Kampagne *Cyberpeace*.

„Wir sehen erheblichen Beratungsbedarf insbesondere der Bundesverteidigungsministerin, aber auch der Bundesregierung und des Bundestages und fordern einen öffentlichen parlamentarischen Diskurs unter Einbeziehung unabhängiger Berater.innen, um über die Risiken und Gefahren, die von einer derartig offensiven Sicherheitsstrategie im Cyberspace ausgeht, öffentlich zu diskutieren", fordert Werner Hülsmann, Beiratsmitglied des FIfF e.V.

FIfF e.V. – Pressemitteilung

FIfF kritisiert Entwurf zur europäischen Fluggastdatenspeicherung

4. August 2015 – Das FIfF fordert das Europäische Parlament auf, den Vorschlag des Innenausschusses zur Speicherung von Fluggastdaten abzulehnen. Der Entwurf zu einer EU-weiten Fluggastdatenspeicherung (*Passenger Name Records, PNR*) ist eine weitere Abkehr von der Unschuldsvermutung zugunsten einer Überwachungs- und Präventionsgesellschaft. Die anlasslose Massenüberwachung der Passagiere aller internationalen Flüge und Speicherung dieser Daten in Datenbanken steht im Widerspruch zu den Grundprinzipien der Europäischen Union.

Der Europäische Gerichtshof hat mit seinem Urteil zur Vorratsdatenspeicherung klargestellt, dass eine anlasslose Datenerhebung ein unverhältnismäßiger Eingriff in das EU-Grundrecht auf Privatsphäre und den Schutz personenbezogener Daten ist. Doch anstatt die Kritik an der Vorratsdatenspeicherung für eine Kurskorrektur zu nutzen, wird hier eine neue Massenüberwachung ins Leben gerufen.

Gespeichert werden sollen nicht nur Name, Abflugort und Ziel, sondern bis zu 60 Einzelangaben wie Essenswünsche, ob ein Hotel zusammen mit dem Flug gebucht wurde, und welche Tickets zusammen bestellt wurden. Damit lassen sich nicht nur Bewegungsprofile erstellen, sondern auch Aussagen über Beziehungen zwischen Fluggästen und eventuell sogar ihre Religion ableiten – hochsensible und schützenswerte Daten.

Die Zustimmung des Innenausschusses des Europäischen Parlaments zum Kommissionsentwurf zur Fluggastdatenspeicherung ist insbesondere im Licht der letzten PNR-Debatte enttäuschend: Im Jahr 2013 stellte sich das EU-Parlament noch gegen eine solche anlasslose Überwachung. Begründet wird die Maß-

nahme nun mit einem Bedarf zur Harmonisierung der Rechtslage in verschiedenen EU-Staaten. Doch dieser Harmonisierungsbedarf wurde überhaupt erst dadurch geschaffen, dass die EU-Kommission die Einführung der Fluggastdatenspeicherung in einzelnen EU-Ländern mit insgesamt 50 Millionen Euro unterstützt hat.

Der aktuelle Entwurf nimmt zwar innereuropäische Flüge von der Fluggastdatenspeicherung aus, tut ansonsten aber wenig, um die Privatsphäre der Fluggäste zu sichern: Die Daten dürfen von Strafverfolgungsbehörden nicht nur zur Aufklärung von Verbrechen, sondern auch für Profiling und Data-Mining verwendet werden. *„Dies stellt eine Abkehr von traditioneller Strafverfolgung hin zu einer digitalen Rasterfahndung dar"*, wie Kai Nothdurft, Vorstandsmitglied des FIfF, betont. Auch der Austausch mit anderen nationalen Polizeibehörden und der europäischen Polizeibehörde Europol ist erlaubt und kaum reguliert.

„Die Einführung einer anlasslosen Fluggastdatenspeicherung und -auswertung lehnen wir entschieden ab", betont Sylvia Johnigk, Vorstandsmitglied des FIfF.

FIfF e.V.

Rote Linien für die EU-Datenschutz-Grundverordnung

Nachdem die Datenschutzstandards in der Praxis des globalen Datenverkehrs immer mehr aufgeweicht wurden, schafft die Datenschutzgrundverordnung die Möglichkeit, bei einem europäischen Grundrecht in die Offensive zu gehen. Das FIfF hat sich in den Diskussionsprozess mehrfach eingebracht und Vorschläge für eine datenschutzfreundlichere Zukunft gemacht. Letzte Entwicklungen um den Entwurf des Ministerrates zeigen aber deutlich, dass der Wirtschaftslobbyismus funktioniert und nicht alle Interesse an einem starken europäischen Datenschutz haben. Es ist beschämend, dass gerade Deutschland mit allein 51 Forderungen den Parlamentsvorschlag beschädigt hat. Die gemeinsame Position des Rats der Europäischen Union vom 15. Juni 2015, 9565/15, überschreitet diverse rote Linien und fällt hinter die Standards der Datenschutz-Richtlinie von 1995 zurück.

Einwilligung

Bisher tun die Anbieter von Dienstleistungen im Internet häufig so, als bedeute schon die Nutzung eines Dienstes oder das Nichthandeln eine stillschweigende Einwilligung. In Artikel 7 wollen Parlament und Kommission sicherstellen, dass der betroffenen Person im Sinne einer informierten Einwilligung bewusst ist, dass sie ihre Einwilligung gibt. Eine ausdrückliche Handlung möchte der Rat vermeiden und fügt im Erwägungsgrund 25 ein, dass die Einwilligung auf *„beliebige"* geeignete Weise und nur *„eindeutig"* statt *„ausdrücklich"* erfolgen soll. Schon die Einstellungen des Browsers oder einer anderen Anwendung sollen eine Einwilligung signalisieren können.

Will eine Person eine Einwilligung widerrufen, soll das nach dem Wunsch des Europäischen Parlaments so einfach sein wie das Erteilen der Einwilligung, als die ja schon der Besuch einer Website gesehen werden kann. Diese Forderung im Artikel 7 hat der Rat gestrichen.

Bei diesem Grundpfeiler des Datenschutzes ist so viel Entgegenkommen gegenüber den Datenkraken mit uns nicht zu haben!

Datensparsamkeit

In Artikel 5 Satz 1 (c) haben Parlament und Kommission in wünschenswerter Klarheit festgelegt, dass die zu erhebenden personenbezogenen Daten auf das für die Zwecke *„notwendige"* Maß beschränkt sein müssen. Der Rat weicht den Zweckbezug zu *„verhältnismäßig"* auf. An anderer Stelle (Erwägungsgrund 39) will der Rat die Verhältnismäßigkeit den Betreibern von elektronischen Kommunikationsnetzen und -diensten sowie Anbietern von Sicherheitstechnologien und -diensten erlassen. Dagegen verlangt das Europäische Parlament, dass die Verarbeitung *„für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig"* sein muss.

An vielen Stellen hat der Rat die Vorgaben zur Datensparsamkeit gestrichen, die das Parlament eingeführt hat. In Erwägungsgründen 61 und 125 *„kann"* sie eine Maßnahme sein, in Artikel 23 wird sie lediglich als ein Beispiel genannt, die Rechte der Betroffenen zu schützen. Lobby-Arbeit hat wohl auch dazu geführt, dass laut Erwägungsgrund 30 personenbezogene Daten verarbeitet werden dürfen, wenn sich der Zweck anders nicht *„in zumutbarer Weise"* erreichen lässt. Schwammiger lässt sich die Datensparsamkeit kaum dem Ermessen der Unternehmen anheimstellen.

Bei der Verarbeitung personenbezogener Daten zu historischen, statistischen oder wissenschaftlichen Forschungszwecken (Erwägungsgrund 125) wünscht sich der Rat weitere Register mit den Daten großer Bevölkerungsanteile (auch Verstorbener, Erwägungsgrund 23). Das sind Sammlungen, die wachsende Begehrlichkeiten auf sich ziehen werden.

Datensparsamkeit als Anforderung endlich durchsetzbar zu machen, das wollen die Minister nicht. Wir bestehen auf den Formulierungen des Parlaments!

Zweckbindung

Der Entwurf des EU-Rats will es ins Ermessen der Unternehmen legen, den Zweck einer Verarbeitung nach Belieben neu zu definieren. Statt dass Daten gelöscht werden, wenn sie ihren

Zweck erfüllt haben, will der Rat in Erwägungsgrund 40 und Artikel 6 Satz 3a (a) eine Zweckänderung erlauben, wenn der neue Zweck mit dem ursprünglichen Zweck *„vereinbar"* ist.

Im Erwägungsgrund 39 haben die Minister zudem die *„Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung"* als berechtigtes Interesse definiert. – Wenn die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, soll das zwar ausgeschlossen sein, informationelle Selbstbestimmung sieht aber anders aus. Betroffene können nicht sicher wissen, ob bei der Verarbeitung *„für nicht konforme Zwecke aufgrund der berechtigten Interessen dieses [...] Verantwortlichen oder eines Dritten"* dessen Interessen überwiegen, was die Verarbeitung rechtmäßig macht (Artikel 6 Satz 4).

Bei diesem Grundpfeiler des Datenschutzes ist so viel Entgegenkommen gegenüber den Datenkraken mit uns nicht zu haben!

Profile

Als Profiling sieht der Rat erst die Nutzung personenbezogener Daten an, die verarbeitet wurden, damit eine Person bewertet oder ihr Verhalten analysiert oder vorhergesagt werden kann (Artikel 4 (12a)). Das Parlament definiert Profiling bereits über den Zweck, wodurch die Rechte der Betroffenen, beispielsweise Auskunfts- und Widerspruchsrecht, besser und früher greifen können, nicht erst dann, wenn womöglich eine Entscheidung gefallen ist. Der Rat hat das Profiling sogar aus dem Titel von Abschnitt IV und Artikel 20 gestrichen, um die automatisierte Entscheidungsfindung zum Ansatzpunkt für die Rechte der Betroffenen zu machen, nicht etwa schon das Profiling selbst. Es müssen rechtliche Folgen oder eine erhebliche Beeinträchtigung der Betroffenen vorliegen, bevor ihnen Möglichkeiten zum Widerspruch gegeben werden. Wo die Kommission noch von *„auf Profiling basierenden Maßnahmen"* spricht und das Parlament vom Profiling selbst, macht der Rat die Entscheidungsfindung zur Überschrift und das Profiling zur Nebensache.

Automatisierte Entscheidungsfindung und Profiling sogar auf der Grundlage besonderer Kategorien von personenbezogenen Daten sollen erlaubt sein, wenn eine Datenschutz-Folgenabschätzung stattgefunden hat (Erwägungsgrund 58), hier wird Diskriminierung zur Abwägungsfrage.

Wir im FIfF e.V. hatten eine Verschärfung der Profiling-Bestimmungen gefordert, der Rat schwächt sie noch weiter ab. So viel Entgegenkommen gegenüber den Datenkraken ist mit uns nicht zu haben!

Datenschutz durch Technik und Datenschutzfreundliche Voreinstellungen

Diese Prinzipien hatte die Kommission eingeführt und das Parlament zur Freude von Datenschützern zur Pflicht gemacht, der Rat hat sie abgeschwächt. Er will die Hersteller der Produkte, Dienste und Anwendungen lediglich *„ermutigen"*, Datenschutz bei der Entwicklung der Produkte, Dienste und Anwendungen zu berücksichtigen. Neben den Verantwortlichen für die Datenverarbeitung will das Parlament die Hersteller für solche datenschutzfreundlichen Produkte verantwortlich machen (Erwägungsgrund 61). Der Rat hat diese Vorgabe des Parlaments aufgeweicht. Das Parlament weist in Artikel 23 ausdrücklich darauf hin, dass sich Datenschutz durch Technik in der Technikfolgen-Abschätzung auf das gesamte Lebenszyklus-Management der Verarbeitung bezieht. Diesen Hinweis hat der Rat ebenso gestrichen wie in Artikel 33 die Forderung des Parlaments, zu dokumentieren, welche Maßnahmen getroffen wurden (Satz 3 g).

Wir haben die Neuerungen durch Parlament und Kommission begrüßt und hätten sie uns stärker gewünscht. Eine Abschwächung als Entgegenkommen gegenüber den Datenkraken ist mit uns nicht zu haben!

Unabhängige Kontrollen und Sanktionen

Entgegen dem Parlamentsbeschluss (Artikel 32a und 35) sieht der Rat keine *Pflicht* zur Einführung von Datenschutzbeauftragten vor, sie soll nur bestehen, wenn das nationale Recht dies vorsieht. Andernfalls *„kann"* oder *„darf"* der Verantwortliche einen Datenschutzbeauftragten benennen. Es muss nicht mehr sichergestellt sein, dass bei einer Gruppe von Unternehmen der Datenschutzbeauftragte von jedem Standort leicht zugänglich ist. Auch zur Vertraulichkeit über die Identität der betroffenen Person sollen Datenschutzbeauftragte nicht mehr verpflichtet sein (Artikel 36 Satz 4). Die vom Parlament geforderte Bereitstellung aller benötigten Mittel, darunter Personal, will der Rat nicht. In Artikel 35 Satz 10 wurde der Rechtsanspruch der Betroffenen, den Datenschutzbeauftragten zu Rate zu ziehen, abgeschwächt zu: *„Betroffene Personen* können *den Datenschutzbeauftragten [...] zu Rate ziehen."*

Im Artikel 79 haben sich nationale Interessen besonders deutlich niedergeschlagen, im vorauseilenden Gehorsam gegenüber den IT-Konzernen. Wo das Parlament Klartext redet und eine unabhängige Aufsichtsbehörde ermächtigt, Geldbußen bis zu 5 % (im EP-Beschluss) ihres (Konzern-)Umsatzes oder einer Milliarde Euro zu verhängen, da erteilt der Rat den *Mitgliedstaaten* die Befugnis, Gerichtsverfahren anzustrengen. Geldbußen dürfen die Aufsichtsbehörden selbst nur verhängen, wenn dies im nationalen Recht vorgesehen ist (Erwägungsgründe 100, 118 b, 120, 120 a und viele andere). Die Aufsichtsbehörde schrumpft zur rein nationalen Angelegenheit und ein Staat *„kann"* (Artikel 79 Satz 3 b und 5) entscheiden, ob überhaupt Geldbußen verhängt werden sollen. Wenn ja, kann die Aufsichtsbehörde nur noch maximal 2 % des Umsatzes festlegen. Die Mitgliedstaaten setzen damit einen der größten Vorteile einer europaweiten und durchsetzbaren Verordnung außer Kraft. Wir müssen davon ausgehen, dass sich große Konzerne nun weiterhin ihren Hauptsitz danach auswählen werden, wo die geringsten Kontrollen und Sanktionen zu befürchten sind.

Statt einheitliche Kontroll- und Sanktionsstandards zu schaffen, wollen die Minister nationale Standortvorteile behalten. Diese Egoismen zu Lasten des Datenschutzes sind mit uns nicht zu haben!

Drittstaaten-Regelung

Weil Datenschutz in Europa ein verbindliches Grundrecht mit Verfassungsrang in der EU-Grundrechtecharta ist, dürfen personenbezogene Daten grundsätzlich nur innerhalb Europas verarbeitet werden. Das scheint nicht zu den Interessen von Konzernen zu passen, die immer mehr Daten benötigen für ihre Geschäfte mit Big Data oder Scoring. Es ist ganz im Sinne der IT-Monopolisten, als *„Big Data"* alles zu speichern, was irgendwie verarbeitet werden kann. Regelungen aus der Parlamentsvorlage für die Übertragung von Daten in Drittstaaten (Nicht-EU-Staaten) hat der EU-Rat durchlöchert. Zu Recht sieht er vermutlich die Freihandelsabkommen TTIP und TiSA dadurch gefährdet. Insbesondere die regulatorische Zusammenarbeit wird fatale Folgen für die informationelle Selbstbestimmung und den Grundrechtsschutz in der EU haben.

Eine Aufweichung der Drittstaaten-Regelung als Entgegenkommen gegenüber den Datenkraken ist mit uns nicht zu haben!

Der Text ist eine Stellungnahme des FIfF zur EU-Datenschutz-Grundverordnung, die für die DANA – Datenschutz-Nachrichten, Ausgabe 3/2015, der Deutschen Vereinigung für Datenschutz erarbeitet wurde. Autorin ist Dagmar Boedicker mit Unterstützung von Martin Degeling.

FIfF e.V.

„Wir haben einen Abgrund von Landesverrat im Lande"

Kommentar zum Ermittlungsverfahren gegen netzpolitik.org

3. August 2015 – *Am 30. Juli 2015 wurde bekannt, dass der Generalbundesanwalt ein Ermittlungsverfahren wegen Landesverrats gegen die Journalisten und Blogger* Markus Beckedahl *und* André Meister *sowie gegen* Unbekannt *eröffnet hat – aufgrund einer Strafanzeige des Präsidenten des deutschen Inlandsgeheimdienstes* (Bundesamt für Verfassungsschutz). *Dieses Vorgehen hatte in der Geschichte der Bundesrepublik Deutschland zuvor nur zwei Beispiele: die Spiegel-Affäre (1962) – die mit dem Rücktritt des damaligen Verteidigungsministers* Franz Josef Strauß *endete – und die Affäre um die Zeitschrift* Cicero *(2005).*

Verfassungsschutzpräsident *Maaßen* begründet sein Vorgehen Zeitungsberichten zufolge damit, *„die weitere Arbeitsfähigkeit meines Hauses im Kampf gegen Extremismus und Terrorismus sicherzustellen"*. Um die Arbeitsfähigkeit des Verfassungsschutzes muss er sich in der Tat Sorgen machen – weder leistete die dem Bundesinnenministerium unterstehende Behörde einen erkennbaren Beitrag zur Verhinderung der rechtsgerichteten, terroristischen Morde des *Nationalsozialistischen Untergrunds (NSU)*, noch konnte sie bei der Spionageabwehr reüssieren, die ebenfalls zu ihren Aufgaben zählt. Die Ausspähung durch den US-Geheimdienst NSA – der dabei offenbar auch noch mit dem anderen deutschen Geheimdienst, dem Bundesnachrichtendienst (BND) zusammenarbeitet – konnte und kann sie offensichtlich nicht verhindern. Von Bundesregierung und Bundesbehörden wird nach wie vor behauptet, es gebe keine gerichtsverwertbaren Beweise für eine solche Ausspähung – angesichts der seit nun zwei Jahren beinahe wöchentlich neu an die Öffentlichkeit kommenden Indizien ist das nicht nachvollziehbar.

Gerade angesichts der offenkundigen Zurückhaltung bei der Aufklärung des NSA- und BND-Skandals ist das schnelle Handeln des Generalbundesanwalts nun besonders auffällig.

Zunehmend unklar wird inzwischen, wer die Strafanzeige und das Vorgehen der beiden Behörden – Verfassungsschutz und Generalbundesanwaltschaft – initiiert und getragen hat. Aussagen von Maaßen zufolge wurde lediglich Anzeige gegen Unbekannt erstattet, der Generalbundesanwalt bestreitet dies. Unklar auch die Rolle der beiden Ministerien, die die Fachaufsicht über die Behörden führen. Bundesjustizminister *Maas* distanziert sich vom Vorgehen des Generalbundesanwalts – dass aber, bei der zu erwartenden Öffentlichkeitswirkung, der zuständige Minister vom Ermittlungsverfahren nicht vorab informiert wurde, ist nur schwer vorstellbar und war, anderen Presseberichten zufolge, auch nicht der Fall. Damit muss Maas wohl eine Mitverantwortung zugeschrieben werden. Gleiches gilt für Bundesinnenminister de Maizière, dessen Fachaufsicht der Verfassungsschutz untersteht. Inzwischen ließ selbst Bundeskanzlerin Merkel durch eine Sprecherin erklären, sie hätte Zweifel am Vorwurf des Landesverrats. Bundesjustizminister Maas hatte nach seiner Kehrtwende bei der Vorratsdatenspeicherung – die er selbst freilich immer noch bestreitet – ohnehin bereits einiges an Vertrauen in der netz- und bürgerrechtspolitischen Öffentlichkeit verspielt.

Über die Motive kann nun munter spekuliert werden:

- Ist das Ganze ein Versuchsballon, um die Reaktion der Öffentlichkeit zu testen? Gut vorstellbar. In diesem Fall könnten wir zunächst beruhigt sein – die heftige Reaktion in großen Teilen der Presse zeigt, dass solch ein Versuch, die Pressefreiheit einzuschränken, (noch) nicht hingenommen wird.

- Es kann auch der erste Schritt einer Gewöhnungsstrategie sein. So heftig die Reaktionen dieses Mal ausfielen – es ist abzusehen, dass im nächsten derartigen Fall die Empörung bereits deutlich geringer sein wird. Ebenso wie Überwachungsmaßnahmen Schritt für Schritt zum Normalzustand werden, lässt sich so auch Schritt für Schritt die Pressefreiheit – und weitere Grundrechte – abbauen.

- 2014 wurden im Bundeskanzleramt Referenten mit verhaltensökonomischem Hintergrund eingestellt, von denen angenommen wird, dass sie sogenannte *Nudging*-Techniken in die Regierungsarbeit einführen werden. Ist also die Strafanzeige ein *„Stups"*, um kritische Presse im eigenen Sinn zu beeinflussen?

- Der Gesetzentwurf zur Vorratsdatenspeicherung sieht den Zugriff auf die gespeicherten Daten nur bei schweren Straftaten vor. Journalismus zählt bisher nicht dazu, Landesverrat schon.

Bereits jetzt ist abzusehen, dass die politischen Konsequenzen nicht mit der Spiegel-Affäre vergleichbar sein werden – noch wurde allerdings auch auf Vollstreckungsmaßnahmen gegen *netzpolitik.org* verzichtet. Zunächst wurde offenbar externe (!) Expertise eingeholt, ob der Vorwurf des Landesverrats überhaupt berechtigt ist. Noch ruht das Verfahren offenbar, kann aber jederzeit wieder aufgenommen werden. Das Verfahren gegen Beckedahl und Meister wurde inzwischen eingestellt, gegen *Unbekannt* jedoch nicht; Generalbundesanwalt Range musste seinen Posten aufgeben (Anm. d. Red.). Überwachungsmaßnahmen sind weiterhin möglich.

Davon unabhängig ist der Vorgang beunruhigend. Zu viel spricht dafür, dass hier eine kritische Presse eingeschüchtert werden soll. Ermutigend ist dagegen, dass sich am Samstag, dem 1. August 2015 in Berlin rund 2.500 Menschen zu einer spontanen Demonstration zusammengefunden haben.

Gleichzeitig steht eine juristische Untersuchung des geheimdienstlichen Ausspähskandals immer noch aus. Doch hier ist nach zwei Jahren ein Gewöhnungseffekt schon eingetreten – neue Veröffentlichungen werden mittlerweile eher schulterzuckend hingenommen. Aber gerade Blogs wie netzpolitik.org werden der Verantwortung der Presse gerecht, wenn sie die Öffentlichkeit unermüdlich und umfassend über einen Skandal informieren, der jeden Tag, an dem Regierung und ihr unterstehende Behörden nichts unternehmen, ungeheuerlicher wird.

„Man darf nicht warten, bis der Freiheitskampf Landesverrat genannt wird" – gerne wird in diesen Tagen Erich Kästner zitiert. Ist es etwa schon wieder so weit?

FIfF e.V. und Fachgruppe Informatik & Ethik der Gesellschaft für Informatik e.V. – Pressemitteilung

Ermittlungsverfahren gegen netzpolitik.org

3. August 2015 – Die Fachgruppe Informatik und Ethik der Gesellschaft für Informatik *(@gewissensbits)* und das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung *(@FIfF_de / fiff.de)* missbilligen das juristische Vorgehen von Verfassungsschutz, Generalbundesanwalt und Bundesjustizministerium gegen ein Presseorgan. Sie fordern klare Stellungnahmen und Positionierungen von allen Regierungsministerien. Die Mitglieder beider Vereinigungen sehen sich verpflichtet, allgemeine moralische Prinzipien, wie sie in der Allgemeinen Deklaration der Menschenrechte formuliert sind, zu wahren. Zu diesen essentiellen Rechten gehören die Meinungs- und Pressefreiheit sowie die Freiheit, mit Zivilcourage gegen offenkundige Missstände einzutreten. *„Die Geschichtsvergessenheit ist mit das Erschreckendste am Verfahren gegen netzpolitik.org"*, empört sich der Sprecher der GI-Fachgruppe Informatik und Ethik, Stefan Ullrich. *„Als die Wochenzeitschrift Weltbühne die heimliche, rechtswidrige Aufrüstung der Deutschen Luftwaffe 1929 öffentlich machte, wurden Herausgeber und Informanten wegen Landesverrats verurteilt. Nun erleben wir, wie mit der Berichterstattung an einem heimlichen, moralisch fragwürdigen Wettrüsten im Cyberspace umgegangen wird: Mit einer Ermittlung wegen Landesverrats."*

Die Informationsgesellschaft erwartet von Informatikerinnen und Informatikern, eine ihrer Gestaltungsmacht angemessene individuelle und gemeinschaftliche Verantwortung zu tragen. Für die Herausbildung der dazu notwendigen Urteilskraft jedoch ist eine unabhängige, engagierte Presse unabdingbar, eine Presse, die schon längst nicht mehr mit Bleilettern hantiert, sondern vorwiegend digitale Medien nutzt. Das FIfF-Vorstandsmitglied Rainer Rehak kritisiert: *„Die Integrität und Vertraulichkeit informationstechnischer Systeme wird systematisch und mit voller Absicht von geheim operierenden Diensten im Auftrag verschiedener Staaten unterminiert; doch nicht gegen die für die Grundrechtsverletzungen Verantwortlichen, sondern gegen die darüber berichtenden Journalisten wird ermittelt."*

Das Ermittlungsverfahren des Generalbundesanwalts wurde aufgrund der Berichterstattung von netzpolitik.org angestoßen, die wir hier prominent noch einmal verlinken wollen:

- *https://netzpolitik.org/2015/geheimer-geldregen-verfassungsschutz-arbeitet-an-massendatenauswertung-von-internetinhalten/*

- *https://netzpolitik.org/2015/geheime-referatsgruppe-wir-praesentieren-die-neue-verfassungsschutz-einheit-zum-ausbau-der-internet-ueberwachung/*

(Die von *netzpolitik.org* veröffentlichten Dokumente werden unter *http://landesverrat.org/* gespiegelt.)

Die Fachgruppe *Informatik und Ethik* der Gesellschaft für Informatik und das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung rufen die politisch Verantwortlichen zur Raison sowie ihre Mitglieder zur erneuten Lektüre der höchstrichterlichen Grundsatzurteile auf.

FIfF e.V.

FIfF-Konferenz 2015
Kommerzialisierung des Sozialen –
Markt und Macht im Zeitalter digitaler Kompletterfassung

Commercialisation of the Soci(et)al – Markets and Power in the Age of Total Datafication

Vom 6. bis zum 8. November 2015 laden das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) *und der* Lehrstuhl für Informatik 1 *der* Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) *zur wissenschaftlichen Tagung* **FIfFKon31** *in Erlangen ein.*

Digitale Sensorik durchdringt zunehmend unser Leben und generiert und speichert unaufhörlich Daten, von deren Existenz wir oft gar nichts wissen. Die Daten entstehen in Computern und Smartphones, aber auch in Navigationsgeräten, Fitnesstrainern und digitalen Implantaten. Jeder Mensch, jede menschliche Interaktion hinterlässt dadurch digitale Spuren, ein Umstand, den nicht nur Suchmaschinen und soziale Netzwerke zu einem Geschäftsmodell gemacht haben. Nachdem der Mensch als Arbeitskraft und Konsument umfassend überwacht, analysiert und kommerzialisiert worden ist, folgt mit dem *Internet der Dinge* nun die Kommerzialisierung des privaten und sozialen Lebens? Welchen Wert haben unsere privaten und sozialen Daten und wer verdient an ihnen? Welche Konsequenzen haben *Likes*, *LifeStyle* Apps und das Internet der Dinge auf das Machtgefüge der Gesellschaft? Dieser Themenbereich steht im Zentrum der diesjährigen FIfF-Konferenz 2015 in Erlangen.

Programm (kurzfristige Änderungen vorbehalten)	
Freitag, 6. November 2015	
18:00 Uhr	Eröffnung und Impulsreferat zum Tagungsthema **Miika Blinn** (Verbraucherzentrale Bundesverband, vzbv) *Individuelle Preise – Eine Herausforderung für Verbraucher*
18:45 Uhr	Eingeladener **Vortrag** **Andreas Sachs** (Bayerisches Landesamt für Datenschutzaufsicht) *Smart-TVs im Fokus der Datenschutzaufsichtsbehörden*
ab ca. 19:45	Stehempfang und Get-together im Medical Valley Center

Samstag, 7. November 2015	
09:30 Uhr	Eingeladener **Vortrag** **Florian Mehnert** *Das Kunstexperiment 11 TAGE*
10:30 Uhr	*Kaffeepause*
11:00 Uhr	**Workshops**
12:30 Uhr	*Mittagessen*
14:00 Uhr	Eingeladener **Vortrag** **Sebastian Hahn** (The Tor Project) *Privacy by Design in a Digital World*
15:00 Uhr	*Kaffeepause*
15:30 Uhr	**Workshops**
17:00 Uhr	**Veranstaltung** *Cyberpeace*
18:00 Uhr	**Verleihung** des FIfF-Studienpreises 2015
19:00 Uhr	Abendveranstaltung in der Steinbach Bräu, Vierzigmannstr. 4, 91054 Erlangen
Sonntag, 8. November 2015	
10:00 Uhr	Eingeladener **Vortrag** **Sebastian Jekutsch** *Was gibt's Neues in Sachen Faire Computer?*
11:00 Uhr	**Mitgliederversammlung** des FIfF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Veranstaltungsort: Medical Valley Center, Henkestraße 91, 91052 Erlangen.
Alle eingeladenen Vorträge werden bei Erlaubnis der Referenten durch das RRZE der FAU ins Netz übertragen. Details folgen.

Details zu Referenten und Vorträgen

Miika Blinn:
Individuelle Preise – Eine Herausforderung für Verbraucher

Der Einsatz von Big Data verändert Wettbewerb und Marktprozesse fundamental. Wenn zunehmend selbstlernende Algorithmen auf Basis von Big Data Preise gestalten, führt dies zu einer erheblichen Informations-Asymmetrie zugunsten der Anbieter. Wenn sich Preise auf Grund nicht nachvollziehbarer Mechanismen im Minutentakt ändern, kann dies die Verbraucher stark verunsichern. Können Preisvergleiche überhaupt noch stattfinden, wenn Preise individuell an die vermeintliche Zahlungsbereitschaft einzelner Nutzer angepasst werden? Dieses Impulsreferat möchte zum Nachdenken darüber anregen, was es für Verbraucher bedeutet, wenn Preise in der digitalen Ökonomie an einzelne Nutzer individuell angepasst werden.

Dr. **Miika Blinn** ist Referent für das Thema Digitales und Medien beim Verbraucherzentrale Bundesverband (vzbv). Als Ökonom befasst er sich mit Fragestellungen im Themenfeld Wettbewerb in der digitalen Welt.

Andreas Sachs: Smart-TVs im Fokus der Datenschutzaufsichtsbehörden

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

Andreas Sachs ist Informatiker und leitet das technische Referat beim Bayerischen Landesamt für Datenschutzaufsicht in Ansbach. Zu seinen Aufgaben gehören die Beratung und Kontrolle von in Bayern ansässigen Unternehmen in den Bereichen IT-Sicherheit und technischem Datenschutz.

Florian Mehnert:
Das Kunstexperiment *11 TAGE*

Das Kunstexperiment *11 Tage* untersuchte als Folge der Überwachung den Einsatz von ferngesteuerten bewaffneten Drohnen. Eine Laborratte wurde über einen Livestream permanent überwacht. Nach Ablauf des Countdowns von 11 Tagen am 25. März 2015 um 19:00 Uhr (CET), sollte die steuerbare Waffe scharf geschaltet werden. Die Ratte hätte dann von jedem Smartphone, von jedem Computer aus über das Internet getötet werden können. Die internationalen Reaktionen auf das Projekt waren extrem kontrovers, es folgte ein Shitstorm und Morddrohungen, die Behörden reagierten nervös. Warum wurde das Projekt nach sechs Tagen beendet? Zu welchen Ergebnissen hat das Kunstexperiment geführt? Warum waren die Reaktionen derart ambivalent und kontrovers? Eine Aufarbeitung des Projekts hinsichtlich seiner Reaktionen und aufgeworfenen Fragen.

Der deutsche Künstler **Florian Mehnert** erlangte mit mehreren Kunstprojekten und Ausstellungen zum Thema Überwachung international Aufmerksamkeit. In seinem Kunstprojekt „Waldprotokolle" verwanzte er Wege und Lichtungen in Wäldern mit Mikrofonen, die vorbeigehende Passanten abhörten. In seiner Videoinstallation „Menschentracks" zeigte er 42 Videosequenzen gehackter Smartphones, deren Kameras und Mikrofone ferngesteuert aktiviert wurden. In dem Echtzeit-Videoprojekt *11 TAGE* ließ er Besucher einer Website per Mausklick eine Paintball-Pistole steuern, die eine Ratte in einer weißen Box bedrohte. Nach elf Tagen sollte der Besucher die Möglichkeit bekommen, die Ratte abzuschießen. Das Projekt wurde nach sechs Tagen vorzeitig beendet.

Sebastian Hahn:
Privacy by Design in a Digital World

Historisch betrachtet war das Internet nie dazu gedacht, die Daten seiner Nutzer zu schützen. Die Protokolle, die im Internet Verwendung finden, müssen daher mühevoll erweitert oder ersetzt werden, um die informationelle Selbstbestimmung möglich zu machen. Gleichzeitig werden die Qualitätsprobleme unserer Softwarei-Infrastruktur immer deutlicher sichtbar, ein neuer, ganzheitlicher Ansatz würde der digitalen Welt gut tun. Am Beispiel von Tor wird aufgezeigt, welche Probleme Overlay-Netzwerke lösen können und wo sie versagen, welche typischen Fehler im Entwicklungsprozess auftreten können und wie versucht wird, diese zu identifizieren und zu beheben, bevor ein Schaden entstehen kann.

Sebastian Hahn ist seit 2008 im Tor-Projekt engagiert. Seine Aktivitäten beinhalten die (Weiter-)Entwicklung der Software, das Schulen von Nutzern im sicheren Umgang mit dem Internet und den Betrieb einer der zentralen Verzeichnisserver im Tor-Netzwerk. Derzeit studiert Hahn Informatik an der Universität Erlangen-Nürnberg.

Sebastian Jekutsch:
Was gibt's Neues in Sachen Faire Computer?

Vor knapp drei Jahren fragte ich „Sind faire Computer möglich?" *(http://events.ccc.de/congress/2012/Fahrplan/events/5121.de.html)* und die Antwort war: „Im Prinzip ja ... aber einfach wird es nicht." Was ist seitdem geschehen und in welche Richtung entwickeln sich die Szene und die AG Faire Computer des FIfF e.V.?

Nach einer kurzen Einführung für diejenigen, denen das Thema *sozialverträgliche IT-Produktion* neu ist, geht es zur Sache: Apple und Samsung, ein Siegel und viele Rankings, Konfliktfreiheit und Sklavenarbeit, Unternehmens- und Konsumentenverantwortung, Fairphone und die faire Nager-IT-Maus.

Man erkennt, dass praktisch alle Fortschritte auf Druck aus der Zivilbevölkerung und professionellen Nichtregierungsorganisationen zustande kamen. Ich stelle die Szene vor, in der sich auch das FIfF bewegt. Es folgen Hinweise, wie man sich als Konsument und Aktivist beteiligen kann, wenn einem Fairness wichtig ist.

Am Schluss stehen Forderungen, aber nicht an die Hersteller oder uns Konsumenten, sondern an die, die tatsächlich die Macht haben: an die Politik.

Sebastian Jekutsch recherchiert und informiert seit nun fünf Jahren über sozialverträgliche IT-Produktion. Er ist Sprecher der AG Faire Computer des FIfF und Initiator des *blog.faire-computer.de.*

Workshops

Am Samstag sind traditionell wieder eine Reihe von Workshops geplant, für die wir um Vorschläge bitten. Im Programm sind dafür zwei 90-Minuten-Slots am Samstagvormittag und -nachmittag vorgesehen.

Workshops müssen nicht notwendigerweise inhaltlich mit dem Tagungsthema verwandt sein, sondern können aus dem gesamten Themenspektrum der kritischen Informatik stammen. In einem Workshop kann man ein solches Thema innerhalb von 90 Minuten gemeinsam mit interessierten Teilnehmern erarbeiten. Im Rahmen der Tagung haben wir Raum für bis zu vier parallele Workshops.

Wer einen Workshop vorschlagen möchte, sende bitte einen *Titel, ein paar Stichworte zum Inhalt und den/die Namen der Verantwortlichen* per E-Mail an die Tagungsleitung (präferiert als verschlüsselte E-Mail an Andreas Cavazzini). Einreichungsdeadline ist der 26. Oktober 2015. Über die Einrichtung der Workshops informieren wir dann kurzfristig.

Veranstaltungsort

Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU),
Medical Valley Center, Henkestraße 91, 91052 Erlangen

Anreise mit der Bahn: Bahnhof Erlangen. Das Tagungsgebäude ist ca. 1,4 km vom Bahnhof entfernt, Fußweg etwa 15-20 Minuten, Taxi 5 Minuten. Karte gibt es online.

Anreise mit dem Auto: Über die A73, Ausfahrt Erlangen-Zentrum/Ost, auf vierspuriger Werner-von-Siemens-Straße stadteinwärts, vorbei an zahlreichen Siemens-Gebäuden, an Ampel nach der Tankstelle rechts in die Henkestraße. Karte gibt es online.

Der Parkplatz hinter dem Gebäude ist ab Freitagnachmittag für Sie geöffnet. Bitte parken Sie **nicht** bei den lokalen Einkaufszentren, Dauerparker wurden in der Vergangenheit abgeschleppt.

Anlaufstelle ist zunächst der große Hörsaal im 1. OG. Spätere Programmpunkte finden auch in den Seminarräumen im Eingangsbereich statt.

Organisation

Prof. Dr. Felix Freiling

Andreas Cavazzini
E-Mail: *andreas.cavazzini@informatik.uni-erlangen.de*

Kristin Sutara-Kleinemeier
Telefon: +49 9131 85 69917
Fax: +49 9131 85 69919

Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)
Lehrstuhl für Informatik 1
Martensstr. 3, 91058 Erlangen

Webseite

http://2015.fiff.de
https://www.fiffkon.de
https://www1.cs.fau.de/fiff

Einladung zur Mitgliederversammlung 2015

des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF e.V.)

Wir laden fristgerecht und satzungsgemäß zur ordentlichen Mitgliederversammlung 2015 ein.

Sie findet am Sonntag, den 8. November 2015, von 11:00 Uhr bis voraussichtlich ca. 14:00 Uhr an der Universität Erlangen-Nürnberg, Henkestraße 91, 91052 Erlangen, statt.

Vorläufige Tagesordnung

1. Begrüßung, Feststellung der Beschlussfähigkeit und Festlegung der Protokollführung
2. Beschlussfassung über die Tagesordnung, Geschäftsordnung und Wahlordnung
3. Bericht des Vorstands einschließlich Kassenbericht
4. Bericht der Kassenprüfer
5. Diskussion der Berichte
6. Entlastung des Vorstands
7. Neuwahl des Vorstands
8. Neuwahl der Kassenprüfer
9. Diskussion über Ziele und Arbeit des FIfF, aktuelle Themen, Verabschiedung von Stellungnahmen, Berichte aus den Regionalgruppen
10. Anträge an die Mitgliederversammlung
    - Themenbezogene FIfF-SprecherInnen
    Weitere Anträge müssen schriftlich bis drei Wochen vor der Mitgliederversammlung bei der FIfF-Geschäftsstelle eingegangen sein
11. Verschiedenes

gez. Stefan Hügel
für den Vorstand und die Geschäftsstelle des FIfF

Sara Stadler

Log 3/2015

Ereignisse, Störungen und Probleme der digitalen Gesellschaft

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

Mai 2015

12. Mai 2015: Im Kontext der BND-Affäre veröffentlicht *ZEIT ONLINE* neue Informationen zur Weitergabe von Metadaten über Kommunikationsvorgänge an die NSA. Hatte Edward Snowden zunächst von 500 Millionen Daten im Monat gesprochen, die der BND der NSA liefere, gibt die Zeitung jetzt an, diese Angaben auf 1,3 Milliarden nach oben korrigieren zu können. Dabei handele es sich nicht um durch die Selektoren vorsortierte Daten, die im Kern der aktuellen Affäre stehen, sondern um Daten aus einem parallel laufenden Prozess. Weiter gehe aus einer der Zeitung vorliegenden, vertraulichen Akte hervor, dass auf Basis der Daten sowie von aufgezeichneten Kommunikationsinhalten sogenannte *Meldungen* an US-amerikanische, britische und multinationale Verbündete übermittelt würden. Auf Rohdaten „ausgewählter Auslands-Auslands-Übertragungswege in Krisengebieten" gebe es zudem einen Vollzugriff für die *Special U.S. Liaison Activity Germany* (SUSLAG), nachdem diese um Daten mit Deutschlandbezug bereinigt worden seien. (Quelle: *DIE ZEIT*)

15. Mai 2015: Nach Informationen, die dem *SPIEGEL* vorliegen, hat der BND entgegen anderer Behauptungen sehr wohl für die NSA Behörden, Unternehmen und andere Ziele in Europa ausgespäht und dabei in größerem Ausmaß als bisher angenommen gegen „deutsche und österreichische Interessen" gehandelt. So seien dem Nachrichtenmagazin zufolge rund 25.000 der 40.000 Suchbegriffe, die der BND angeblich ausgeschaltet habe, durchaus aktiv gewesen, bis ihre Problematik im Rahmen einer internen Untersuchung erkannt worden sei. (Quelle: *DER SPIEGEL*, *Heise*)

15. Mai 2015: Der *SPIEGEL* berichtet erstmals von einem Angriff von Hacker.innen auf die IT-Systeme des Deutschen Bundestages. Später wird bekannt, dass dabei große Mengen von Daten abgegriffen wurden. Um wen es sich bei den Angreifer.innen handelt, bleibt unklar. (Quelle: *DER SPIEGEL*, *Heise*)

18. Mai 2015: Des Einkaufs von Kampf- und Aufklärungsdrohnen aus den USA und Israel überdrüssig geworden, haben Deutschland, Frankreich und Italien den Entschluss gefasst,

fortan an der Entwicklung einer eigenen Drohne zu arbeiten. Ziel des voraussichtlich milliardenschweren Projekts soll es Bundesverteidigungsministerin Ursula von der Leyen zufolge sein, zukünftig „selber entscheiden" zu können, wo die waffenfähigen Drohnen eingesetzt werden. (Quelle: *Heise*)

22. Mai 2015: Der *SPIEGEL* berichtet vom Fund einer neuen Liste mit 459.000 NSA-Selektoren auf Rechnern des BND, von denen lediglich 400 aussortiert worden seien. Die Selektoren stammen aus den Jahren 2005 bis 2008 und deuten auf ein großes Interesse an europäischen Wirtschaftsunternehmen hin. Besonders interessant sei auch, dass die Daten aus der BND-Zentrale in Pullach und nicht wie die bisherigen aus dem BND-Horchposten in Bad Aibling stammten. (Quelle: *DER SPIEGEL*)

27. Mai 2015: Trotz heftiger Kritik hat das Bundeskabinett den Neuentwurf zur Vorratsdatenspeicherung beschlossen. Bis zu 10 Wochen sollen Telekommunikationsanbieter Informationen zu IP-Adressen von Computern und Verbindungsdaten von Telefongesprächen aufbewahren, Standortdaten bei Handy-Gesprächen sollen bis zu vier Wochen gespeichert werden. Von der Speicherung ausgenommen sind Daten zum E-Mail-Verkehr und Kommunikationsinhalte. (Quelle: *Heise*)

27. Mai 2015: Das Bundeskabinett beschließt den *Gesetzentwurf für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen* (E-Health-Gesetz), welches die Schaffung einer umfangreichen digitalen Infrastruktur im Gesundheitswesen vorsieht. Datenschützer.innen kritisieren, dass in dem Entwurf Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder nach einer Zugriffsmöglichkeit der Patient.innen auf ihre gespeicherten Daten nicht umgesetzt würden und diese so von ihrem Recht auf Auskunft und Löschung keinen Gebrauch machen könnten. Außerdem bestehe deutlicher Nachholbedarf bezüglich der Sicherheit der sehr sensiblen Personendaten. (Quelle: *Datenschutzbeauftragter INFO*)

Juni 2015

2. Juni 2015: Einer zwischen Anfang 2012 und Ende 2014 durchgeführten Studie der Bürgerrechtsorganisation *Big Brother Watch* zufolge ersuchen britische Ermittler 670 mal am Tag – oder alle zwei Minuten – um bei Providern gespeicherte Vorratsdaten. Nur 4 % der Anfragen würden abgelehnt. (Quelle: *Heise*)

3. Juni 2015: Nachdem die regierungskritische türkische Zeitung *Cumhuriyet* Aufnahmen veröffentlicht hat, die eine Waffenlieferung für jihadistische Gruppen in Syrien aus der Türkei Anfang 2014 belegen sollen, droht ihrem Chefredakteur wegen einer Anzeige des türkischen Präsidenten Recep Tayyip Erdoğan unter anderem wegen politischer und militärischer Spionage lebenslange Haft. Kritiker.innen im In- und Ausland sehen in der Anzeige einen neuerlichen Angriff auf die Pressefreiheit in der Türkei. (Quelle: *Heise*)

4. Juni 2015: 17 von *Wikileaks* veröffentlichte Geheimpapiere zum geplanten Dienstleistungsabkommen TiSA *(Trade in Services Agreement)*, über das EU, USA und 23 weitere Länder verhandeln, weisen auf zukünftig weitere Einschränkungen bezüglich des Datenschutzes und der Internetfreiheit in Europa hin. (Quelle: *Heise*)

4. Juni 2015: Während einer Debatte im Innenausschuss des EU-Parlaments fordert die konservative Europäische Volkspartei (EVP) eine deutliche Ausweitung des EU-Fluggastdatensystems. Wenn es nach Agustín Díaz de Mera García Consuegra und seiner Partei geht, sollen *Passenger Name Records* (PNR) künftig 7 statt 5 Jahre gespeichert werden. Weiter sollten auch innereuropäische Flüge einbezogen und die Möglichkeiten für Sicherheitsbehörden erweitert werden, auf die Datenpools zuzugreifen. Vertreter.innen anderer Parteien weisen die Vorschläge entschieden zurück. Das bereits bestehende, von Bürgerrechtsorganisationen scharf kritisierte Abkommen zur Vorratsdatenspeicherung von Fluggastdaten (vgl. dazu auch die Pressemitteilung des FIfF in diesem Heft) liegt aktuell noch dem Europäischen Gerichtshof zur Prüfung vor. (Quelle: *Heise*)

6. Juni 2015: In Großbritannien sind etwa 700.000 Patient.innen des *National Health Service* von einer unautorisierten Weitergabe ihrer vertraulichen Gesundheitsdaten betroffen. Alle hatten eine Weitergabe der bei ihren Hausärzt.innen gespeicherten Daten ausdrücklich untersagt. Der Vorfall macht auch deutlich, welche Konsequenzen unzureichende Regelungen von Datenschutz und Datensicherheit im Rahmen des kürzlich in der Bundesrepublik verabschiedeten E-Health-Gesetzes haben können. (Quelle: *Heise*)

7. Juni 2015: Das höchste Gericht Saudi-Arabiens bestätigt das heftig kritisierte Urteil gegen den Blogger Raif Badawi. Der wegen Beleidigung des Islams angeklagte Badawi kann nun keine Rechtsmittel gegen die Strafe von 1000 Peitschenhieben und 10 Jahren Gefängnis mehr einlegen. *Amnesty International* spricht von einem „schwarzen Tag für die Meinungsfreiheit". (Quelle: *Heise*)

8. Juni 2015: Nachdem Hessen *Body-Cams* bei Polizei-Einsätzen bereits seit 2013 testet, erwägen trotz erheblicher Bedenken von Datenschützer.innen nun weitere Bundesländer ihre Einführung. Rheinland-Pfalz startet im Juli zwei Pilotprojekte in Mainz und Koblenz und die Hamburger Polizei beginnt noch im Juni mit dem probeweisen Einsatz auf St. Pauli. Auch in Baden-Württemberg wird ein Pilotprojekt geplant. Forderungen der Gewerkschaft der Polizei, Body-Cams auch in Wohnungen einsetzen zu dürfen, wird derzeit noch nicht entsprochen; Lewentz, gegenwärtig Chef der Innenministerkonferenz, lehnt diese jedoch nicht kategorisch ab: „Möglicherweise werden wir da noch eine Fortentwicklung anstreben müssen". (Quelle: *Heise*)

10. Juni 2015: Das Oberhaus des kanadischen Bundesparlaments nimmt das sogenannte *Anti-Terror-Gesetz* an, welches die Befugnisse von Polizei und Geheimdiensten deutlich erweitert. Das Unterhaus hatte dem Gesetz bereits am 7. Mai zugestimmt. Sobald die zu erwartende Zustimmung des Generalgouverneurs erfolgt, entfallen in Kanada Schranken beim Informationsaustausch zwischen Behörden und es werden *No-Fly*-Listen erstellt, die mit ausländischen Regierungen geteilt werden können. Besonders hervorzuheben ist auch Abschnitt 3 des Gesetzes, demzufolge jegliche (auch fahrlässige und rein private) Äußerungen, die als Unterstützung von „Terrorismus im Allgemeinen" interpretiert werden können, mit bis zu 5 Jah-

ren Gefängnis bestraft werden sollen. Der bisher nur mit der Überwachung beauftragte Geheimdienst CSIS soll fortan die Sicherheit des Landes (auch die wirtschaftliche) weltweit aktiv verteidigen. (Quelle: *Heise*)

12. Juni 2015: Die Kompetenzen des Schweizer Nachrichtendiensts (NDB) und der Strafverfolgungsbehörden könnten künftig erheblich ausgeweitet werden. Das neue Nachrichtendienstgesetz würde es dem NDB erlauben Telefone anzuzapfen, in Computer und Netzwerke einzudringen und Privaträume zu verwanzen. Nachdem der Nationalrat bereits im März zugestimmt hat, wird das Gesetz nun vom Ständerat diskutiert. Dieser macht seine Zustimmung noch von Detailentscheidungen abhängig. Eine Woche später stimmt der Schweizer Nationalrat einer Verschärfung des *Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs* (BÜPF) zu. Diese umfasst unter anderem den Einsatz von Staatstrojanern, um verschlüsselte Kommunikation noch vor der Verschlüsselung auf den Geräten abfangen zu können, sowie eine Verlängerung der Vorratsdatenspeicherung von 6 auf 12 Monate. Gegen beide Vorlagen wurde bereits von verschiedenen Gruppen ein Referendum angekündigt. (Quelle: *Heise*)

15. Juni 2015: Innen- und Justizminister der EU-Mitgliedsländer haben sich auf eine Position zur geplanten Datenschutzverordnung geeinigt, die deutlich hinter der bisherigen Datenschutzrichtlinie, wie auch hinter Vorschlägen der EU-Kommission und des Parlaments zurückbleibt. So werden etwa die Möglichkeiten der Unternehmen und Behörden zur Verarbeitung personenbezogener Daten ausgebaut und das Prinzip der Datensparsamkeit aus dem Artikel für grundlegende Prinzipien gestrichen. Die Bürgerrechtsorganisation *European Digital Rights* (EDRi) bezeichnet die Vereinbarung als einen Vorstoß „Europas weltweit führenden Datenschutzansatz zu zerstören." Siehe FIfF Stellungnahme in diesem Heft. (Quelle: *Heise*)

20. Juni 2015: Die SPD stimmt dem vom Bundeskabinett auf den Weg gebrachten neuen Gesetz zur Vorratsdatenspeicherung mit knapper Mehrheit zu. Justizminister Heiko Maas geht von einer Verabschiedung des Gesetzes nach der Sommerpause aus. (Quelle: *Heise*)

22. Juni 2015: Das für die Geheimdienstaufsicht zuständige britische Gericht IPT (*Investigatory Powers Tribunal*) macht die rechtswidrige Überwachung von Nichtregierungsorganisationen durch den britischen Geheimdienst GCHQ öffentlich. Die Rechte der beiden NGOs – des südafrikanischen *Legal Resources Centre* (LRC) und, wie sich später herausstellt, *Amnesty International* – seien dadurch verletzt worden, dass die abgefangenen Kommunikationsdaten länger als erlaubt gespeichert und zudem auf ungesetzmäßige Art und Weise ausgewertet worden seien. (Quelle: *Privacy International*)

24. Juni 2015: Neuen, von *Wikileaks* veröffentlichten Dokumenten zufolge hat die NSA mindestens die drei letzten französischen Präsidenten, Jaques Chirac, Nicolas Sarkozy und François Hollande überwacht. (Quelle: *Heise*)

24. Juni 2015: Das französische Parlament beschließt ein umstrittenes Gesetz, welches die Befugnisse der eigenen Geheimdienste ausweitet. Für die in dem Gesetz geregelten Überwachungsaktivitäten wie Lauschangriffe, Videoüberwachung, den Einsatz von Spionagesoftware und die Erfassung von Verbindungsdaten gelten zukünftig geringere Hürden. Internetkommunikation einschließlich deren Metadaten kann fortan nicht mehr nur zwecks „Terrorbekämpfung" oder „Verteidigung der Nation", sondern auch zum Schutz gegen „umfassende ausländische politische Interessen" oder drohende „Angriffe auf die institutionelle Form der Republik" aufgezeichnet und durchsucht werden. Die Vorratsdatenspeicherung in Frankreich wird zudem auf 5 Jahre ausgeweitet und der inländische Geheimdienst zum Abhören von Internet-Telefonaten oder unbemerktem Durchführen von Online-Durchsuchungen mit einem Trojaner ausgestattet. (Quelle: *Heise*)

30. Juni 2015: Dass auch die französische Wirtschaft über Jahre hinweg von der NSA ausspioniert wurde, legen neue, auf *Wikileaks* veröffentlichte Dokumente nahe. (Quelle: *Heise*)

Juli 2015

1. Juli 2015: Auf *Wikileaks* werden geheime NSA-Dokumente aus unbekannter Quelle veröffentlicht, die Aufschluss über das Ausmaß der Spionage durch die NSA in der Bundesrepublik geben sollen. Laut der *Süddeutschen Zeitung*, der die Dokumente ebenso wie dem NDR und dem WDR im Vorfeld zugänglich gemacht wurden, zeugen die Dokumente von einer weit über die Bundeskanzlerin hinausgehenden Ausspähung der Bundesregierungen mindestens seit den 1990er-Jahren, wobei das Interesse vor allem der Währungs- und Handelspolitik gegolten habe. (Quelle: *Süddeutsche Zeitung*)

3. Juli 2015: Wie *CNN* und *DER SPIEGEL* berichten, hat die NSA in der Bundesrepublik auch Journalist.innen ausspioniert. Dem Nachrichtenmagazin zufolge sei der Geheimdienstkoordinator im Bundeskanzleramt, Günter Heiß, im Frühsommer 2011 von der CIA-Spitze vor angeblichen Kontakten des *SPIEGEL* in deutsche Regierungsstellen gewarnt worden, worüber auch das Kanzleramt informiert worden sei. Letzterem sei die Überwachung von Journalist.innen und Regierungsstellen durch die NSA also bereits 2 Jahre vor Snowden bekannt gewesen. Der *SPIEGEL* gibt an, bei der Bundesanwaltschaft Anzeige „wegen des Verdachts der geheimdienstlichen Agententätigkeit und der Verletzung des Fernmeldegeheimnisses" erstattet zu haben. (Quelle: *DER SPIEGEL, Heise*).

3. Juli 2015: Einem Bericht von *L'Observateur* zufolge zapft der französische Auslandsgeheimdienst DGSE seit 2008, autorisiert durch den damaligen Staatspräsidenten Nicolas Sarkozy, die internationale Telekommunikation über mindestens 5 große Unterseekabel an. Die Operation, von der unter anderem Leitungen in Richtung USA, Indien, Südostasien und Westafrika betroffen seien, sei mit Unterstützung des Betreibers *Orange* und des Netzwerkausrüsters *Alcatel-Lucent* und teilweise in Kooperation mit dem britischen Geheimdienst GCHQ erfolgt. François Hollande habe die Operation sogar noch erweitert und mit dem jüngst beschlossenen Gesetz zur Geheimdienstreform zu legalisieren gesucht. (Quelle: *L'Observateur, Heise*)

3. Juli 2015: Der Bundestag verabschiedet den von der Bundesregierung auf den Weg gebrachten Gesetzesentwurf zur

Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes. Künftig wird das *Nachrichtendienstliche Informationssystem* (Nadis) der Staatsschutzbehörden von Bund und Ländern, das bislang eine Indexfunktion hatte, zum beliebigen Speichern, Austauschen und Auswerten von Volltextdateien genutzt. Zudem wird der Bundesnachrichtendienst auch für Cyberangriffe zuständig und die *strategische Fernmeldeüberwachung* auf diesen Bereich ausgedehnt. Die Opposition stimmte geschlossen gegen den Entwurf, kritisiert wurde unter anderem, dass nicht nur in Rahmen der Späh-Affäre zum Vorschein gekommene Defizite der deutschen Geheimdienste nicht behoben würden. (Quelle: *Heise*)

3. Juli 2015: Wie aus der Antwort der Bundesregierung auf eine Anfrage der Grünen Verteidigungsexpertin Agnieszka Brugger hervorgeht, will das Kabinett die Aufklärungsdrohne *Euro Hawk* für 32,7 Millionen Euro wieder flugfähig machen. Die Kosten für die anstehenden Flüge, in deren Rahmen das Aufklärungssystem ISIS mindestens ein Jahr lang getestet und weiterentwickelt werden soll, werden auf 160 Millionen Euro geschätzt. (Quelle: *Heise*)

6. Juli 2015: Hacker.innen hacken den italienischen Überwachungssoftware-Hersteller *Hacking Team* und legen damit interessante Details über dessen Geschäftspolitik offen. E-Mails und Rechnungen belegen den Verkauf ihrer Software an autoritäre Regimes. Aus Äthiopien erhielt *Hacking Team* gar ein Dankschreiben für die softwaretechnische Hilfe, oppositionelle Ziele schnell identifizieren zu können. Auch mehrere deutsche Unternehmen gehören zu den Kund.innen von *Hacking Team*. (Quelle: *Heise*)

8. Juli 2015: Aus neuen, von *Wikileaks* veröffentlichten Dokumenten geht hervor, dass nicht nur die Regierung der Bundeskanzlerin Angela Merkel, sondern auch die ihrer Vorgänger Gerhard Schröder und Helmut Kohl von der NSA überwacht wurden. Insgesamt umfasst die veröffentlichte Liste 56 Telefonnummern. (Quelle: *Süddeutsche Zeitung*)

10. Juli 2015: *Wikileaks* veröffentlicht rund eine Million E-Mails des jüngst gehackten italienischen Überwachungssoftware-Hersteller *Hacking Team*. Diesen zufolge hatte auch das BKA 2012 Mitarbeiter.innen nach Mailand entsandt, um sich über das *Remote Control System* (RCS) zu informieren. Anscheinend hat sich das BKA dann aber doch für den Bau eines eigenen Staatstrojaners entschieden. Der Leiter des Geheimdienstes von Zypern tritt wenige Tage später wegen des Einkaufs von Sicherheitslücken bei *Hacking Team* zurück und auch der Chef der Kantonspolizei Zürich gerät wegen des Einkaufs von *Hacking-Team*-Software in die Kritik. (Quelle: *Heise*)

20. Juli 2015: Erneut veröffentlicht *Wikileaks* eine Liste mit NSA-Suchbegriffen. Diesmal handelt es sich um 20 Telefonnummern, die dem Auswärtigen Amt und Bundesaußenminister Walter Steinmeier zuzuordnen seien. Für letzteren ist das Abhörprotokoll eines Gesprächs oder eines Telefonats vom 29. November 2005 besonders unangenehm. Von einer USA-Reise zurückgekehrt, in deren Vorfeld die Medien über CIA-Entführungsflüge und -Gefängnisse in Europa berichtet hatten, sei Steinmeier laut dem Protokoll „erleichtert" gewesen, von Seiten der USA keine klaren Antworten zu diesem Thema erhalten zu haben. Wie ausführlich dokumentiert ist, hatten Entführungsflüge in mindestens einem Fall über den US-Luftwaffenstützpunkt im rheinland-pfälzischen Ramstein geführt, Ermittlungen der für Ramstein zuständigen Staatsanwaltschaft gegen Unbekannt wegen Freiheitsberaubung und Nötigung mussten jedoch eingestellt werden. (Quelle: *Süddeutsche Zeitung*)

24. Juli 2015: Das IT-Sicherheitsgesetz tritt in Kraft. Neben erhöhten Sicherheitsanforderungen an Betreiber.innen von Webservern, der Pflicht zur Meldung von schweren IT-Sicherheitsvorfällen für Betreiber.innen von Kernkraftwerken und Telekommunikation und dem Ausbau des BSI zur internationalen Zentralstelle für IT-Sicherheit umfasst das Gesetz auch die von Bürgerrechtler.innen kritisierte „freiwillige Vorratsdatenspeicherung". So dürfen Provider künftig Verbindungsdaten bis zu 6 Monaten speichern, wenn Probleme mit Cyberattacken oder Spam auch nur entfernt zu vermuten sind. (Quelle: *Heise*)

30. Juli 2015: Es wird öffentlich bekannt, dass die Bundesanwaltschaft gegen zwei Blogger von *netzpolitik.org*, Markus Beckedahl und André Meister aufgrund deren Berichterstattung wegen des Vorwurfs des Landesverrats ermittelt. Konkret geht es unter anderem um die Veröffentlichung und Kommentierung eines als geheim eingestuften Budgetplans für das Bundesamt für Verfassungsschutz im Februar diesen Jahres, aus dem unter anderem hervorgeht, dass die Staatsschützer zu diesem Zeitpunkt an der Massenauswertung von Internetdaten (unter anderem aus sozialen Netzwerken) arbeiteten und dafür ein Budget von 2,75 Millionen Euro zur Verfügung hatten. Zu den zahlreichen Kritiker.innen der Ermittlungen gehört auch das FIfF (siehe den Kommentar und die Pressemitteilung in diesem Heft). Anderthalb Wochen später werden die Ermittlungen eingestellt; der Generalbundesanwalt wird im Rahmen der Affäre abgelöst. (Quelle: *Heise*)

31. Juli 2015: Aus neuen, von *Wikileaks* veröffentlichten Dokumenten geht hervor, dass auch die politische Führung und Wirtschaft in Japan zu den Zielen der NSA-Spionage gehören. (Quelle: *Heise*)

Sara Stadler

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

A MQ-9 Reaper during a training mission, U.S. Air Force photo by Paul Ridgeway

Dietrich Meyer-Ebrecht

Rüstung und Informatik – Editorial zum Schwerpunkt

Schon gegen Ende der 1950er-Jahre umwarb die damals noch junge Bundeswehr uns frisch eingeschriebene Ingenieurstudenten, und ich erinnere unsere bange Frage in einer Werbeveranstaltung, ob wir nun – die allgemeine Wehrpflicht wurde gerade eingeführt – mitten in unserem Studium zum Pflichtdienst eingezogen werden würden. Die Tragweite der Antwort – „uns ist viel mehr damit gedient, wenn Sie Ihr Studium brav absolvieren und in Ihrem Beruf erfolgreich sein werden" – ist mir erst viel später bewusst geworden. Was wir aus unserer zivilen Perspektive nicht sehen konnten oder in einer Zeit des Umbruchs nach einem schrecklichen Krieg auch nicht sehen wollten, war den Militärs spätestens seit Beginn des 20. Jahrhunderts selbstverständlich: Technik ist per se eine unverzichtbare Grundlage für die Kriegführung, und alle technischen und technologischen Innovationen im zivilen Anwendungsbereich sind per se auch Stimuli und Ressourcen für die Rüstungstechnik.

Zunehmend erfahren wir, dass wir zwischen ziviler Technik und Rüstungstechnik keine klare Trennlinie mehr ziehen können, auch und gerade in der Informatik und Informationstechnik. In der Rückschau war es besonders in der Forschung und Entwicklung auf diesem Gebiet immer schon eine Illusion, dass wir trennen könnten, was einmal der Zivilgesellschaft dienen würde und was ausschließlich den Militärs. Gerade die Entwicklung der digitalen Technologien und Systeme war von Anbeginn militärisch motiviert und finanziert. Das Internet startete als militärisches Projekt ARPAnet. Das Silicon Valley, Brutplatz für die Cybertechnologie, verdankt sein Entstehen großzügigen Förderprogrammen aus den Töpfen der Militärs – „cyber-militärischer Komplex" nennt *Daniel Leisegang* diese Liaison in seinem Beitrag in diesem Heft.

Treibende Kraft des Evolutionsprozesses, der mit der rasanten Entwicklung und globalen Ausbreitung digitaler Technologien und Methoden einherging, war die Zivilgesellschaft mit ihrem ungehemmten Konsum informationstechnischer Produkte. Wenn heute auf 3x3x1 mm³ Silizium für fünf US-Dollar ein Gyroskop, ein Beschleunigungssensor, ein Magnetometer – alles in drei Achsen! – zusammen mit einem Prozessor für die Datenaufbereitung untergebracht werden können,[1] verdanken wir dies dem Masseneinsatz in Lifestyleprodukten. Produkte wie dieses und ihre Derivate landen umgehend in Waffensystemen, erfüllen preisgünstig eine geforderte Aufgabe oder inspirieren sogar neue Waffenfunktionen.

„Macht Eure Arbeit gut und wir schauen Euch dabei über die Schulter" – so fließen die Innovationen der Informatik und Informationstechnik ständig aus allen Anwendungsbereichen in die Rüstungstechnik ein – auch ungewollt von ihren Schöpfern, vor allem unkontrollierbar durch die Gesellschaft. Junge Menschen an der Schwelle von einer technischen Ausbildung in eine berufliche Laufbahn, zumal in der Informatik und Informationstechnik, stehen in der Wahl ihres zukünftigen Tätigkeitsfeldes vor zunehmend schwierigen Entscheidungen: Zu fließend sind die Grenzen zwischen ziviler und militärischer Technik, um vorausschauend erkennen zu können, ob der anvisierte Arbeitsplatz die gesuchte rüstungsferne Perspektive bietet. Zu sehr verlocken die Gelder der Militärs die Leitungen von Unternehmen und Forschungsinstituten, die vorgetragenen moralischen Ansprüche alsbald hintanzustellen.

Rüstung und Informatik ist ein zentrales Thema des FIfF seit seiner Gründung vor nunmehr 31 Jahren. Eines der Ziele ist es,

Dietrich Meyer-Ebrecht

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

diese Wechselwirkungen transparenter zu machen. Dazu dienen auch die in unregelmäßiger Folge erscheinenden Schwerpunkthefte der FIfF-Kommunikation zu diesem Themenbereich, so auch wieder dieses Heft. In seinem Schwerpunktteil *Rüstung und Informatik* werden dieses Mal vor allem ethische Fragen gestellt. Aus ethischer Blickrichtung reflektiert *Thomas Gruber* die Rolle der Informatik in der modernen Kriegführung. Wie die neuerlich einsetzende Aufrüstungsspirale auf die Hochschulforschung Einfluss nimmt, beschreiben *Reiner Braun* und *Lucas Wirl*, und auch welche Rolle Zivilklauseln in der universitären Forschung spielen. Dass die Vorbehalte gegen eine militärische Finanzierung von Forschung und Entwicklung in den USA deutlich weniger ausgeprägt sind, beschreibt Daniel Leisegang, oben bereits genannt, beispielhaft mit der „dunklen Seite" des Silicon Valley. Welchen Einfluss die alle Räume und alle Dimensionen durchdringende technische Vernetzung mit ganz neuen Verknüpfungen der Einflussgrößen, der Dimensionen und Akteure auf die globale Entwicklung von Konflikten, Gewalt und Krieg hat, analysiert *Jürgen Scheffran*. Auch wenn Vernetzung nicht allein die technische Domäne betrifft, sind Wissenschaft und Technik grundlegend beteiligt und mit in die Verantwortung zu nehmen.

Hans-Jörg Kreowski schreibt über eine Waffe, die aus ethischen Erwägungen besondere Aufmerksamkeit fordert, die Drohne. Sie wird vermutlich die erste Waffe sein, mit der bereits in naher Zukunft die Schwelle zu einem autonom operierenden Kampfgerät überschritten werden wird. Unkalkulierbare Konsequenzen und Risiken des Einsatzes autonomer Waffen haben eine Gruppe von über 2.000 Wissenschaftlern der Künstlichen Intelligenz und Robotik bewogen, zu einem Bann autonomer Waffen aufzurufen, den wir in diesem Heft abdrucken. Nochmals *Hans-Jörg Kreowski* und *Aaron Lye* kommentieren diesen dringend zu unterstützenden Aufruf. Zum Thema Drohnen und insbesondere zu ihrem Einsatz für die Tötung unter Terrorverdacht gesuchter Personen hat der Künstler *Florian Mehnert* ein bemerkenswertes Experiment gemacht, das er in diesem Heft beschreibt. Mit der Situation eines „High Value Targets" im Fadenkreuz des fernab agierenden Drohnenpiloten, abgebildet auf einen Rattenkäfig, führt er unsere Gesellschaft vor, die den Künstler ob des angedrohten (aber nie beabsichtigten) Todesschusses auf die Ratte lynchen möchte, jedoch hinterhältige, völkerrechtswidrige Drohnenoperationen auf fremder Staaten Terrain schweigend hinnimmt.

Wie sich die Aktivitäten der Geheimdienste seit Turings Entschlüsselung der Enigma zu einem unerklärten Informationskrieg entwickelt haben, in den wir längst verstrickt sind, und zu welchen Absurditäten die Geheimniskrämerei unserer Politiker führt, nehmen *Ute Bernhardt* und *Ingo Ruhmann* in ihrem Beitrag *Das Blaumilch-System* aufs Korn. Ihr Artikel und ein Interview mit dem Hacker *Felix FX Lindner* zur Frage, wie weit Cyberwar einen Angriff auf Freiheit und Demokratie darstellt, stimmen auf unser Dossier *Kriegführung im Cyberspace* ein, das der Ausgabe beiliegt, siehe Kasten.

Anmerkung

1 *InvenSense Inc. 9-Axis Gyro+Accel+Magn MPU-9250*

Dossier *Kriegführung im Cyberspace*

Diesem Heft liegt das 20 Seiten starke Dossier *Kriegführung im Cyberspace* bei, das das FIfF gemeinsam mit der Zeitschrift *Wissenschaft & Frieden* herausgibt. Es ist gleichzeitig Beilage der *W&F 3/15,* August 2015.

Während die Medien die ungebremste Ausspähung in den digitalen Netzen aufmerksam verfolgen, dient der virtuelle Raum weitgehend unbemerkt von der Öffentlichkeit den Militärs als Operationsraum. Militärische Szenarien beziehen Cyberoperationen als entscheidende Elemente der Kriegführung ein – für Spionageaktionen bis hin zum Einsatz von Cyberwaffen. Ihre beabsichtigte Wirkung reicht von Destabilisierung über Sabotage bis zu Eingriffen in digitale Infrastrukturen mit weitreichenden Folgen für die Zivilbevölkerung. In ihrer Unfassbarkeit und Unkontrollierbarkeit stellen die Cyberaktivitäten der Geheimdienste und Militärs eine verschwiegene, aber höchst reale Gefahr für den Frieden dar. Die fünf Beiträge des Dossiers umreißen die Problematik und machen die Notwendigkeit eines Gegensteuerns deutlich, wie es das FIfF in seiner Kampagne Cyberpeace fordert.

Die Herausgabe des Dossiers wurde im Rahmen dieser Kampagne durch die Stiftung *bridge* finanziell unterstützt.

Hans-Jörg Kreowski

Unbemannte Waffensysteme – nicht ohne Informatik

Die deutsche Verteidigungsministerin Ursula von der Leyen hat laut Medienberichten vor kurzem angekündigt, dass die Bundeswehr bewaffnungsfähige Drohnen anschaffen und Deutschland zusammen mit Frankreich und Italien eine eigene Kampfdrohne entwickeln will. Als kurzfristige Lösung ist wohl an die amerikanische Drohne Reaper *gedacht. Diese Nachricht sollte nicht nur alle friedliebenden Menschen in Deutschland alarmieren, sondern insbesondere auch alle Informatikerinnen und Informatiker. Ohne den Beitrag der Informatik wären unbemannte Waffensysteme nach Art der Kampfdrohnen völlig undenkbar.*

Ein Blick über den großen Teich

Die Entwicklung unbemannter Waffensysteme ist in den USA am weitesten fortgeschritten und durch diverse Quellen öffentlich zugänglich dokumentiert. Das US-amerikanische Verteidigungsministerium plant nach dem 160-seitigen Konvolut *Unmanned Systems Integrated Roadmap FY 2013-2038* einen erheblichen Teil der Bewaffnung der US-Streitkräfte in der Luft, am Boden sowie auf dem und unter Wasser auf unbemannte Systeme umzustellen. Ein Teil dieser Entwicklung ist bereits seit einiger Zeit im Gange, wie der 1000-fache Einsatz von Kampfdrohnen in Afghanistan, Pakistan und dem Jemen zeigt.

Was macht unbemannte Systeme für das Militär interessant?

In der Roadmap werden drei Attribute als Antwort genannt: *dull, dirty, dangerous.* Ein unbemanntes System mit Kamera und anderen Sensoren kann eine Szene stunden- und tagelang beobachten, ohne zu ermüden, abgelenkt zu werden oder auf dumme Gedanken zu kommen, auch wenn die meiste Zeit nichts passiert und die Aufgabe total langweilig ist. Ein unbemanntes System kann sich „unbeschadet" und mit vergleichsweise geringem Risiko in einem biologisch, chemisch oder nuklear verseuchten Gebiet aufhalten und agieren. Ein unbemanntes System kann viel unbedenklicher einer gefährlichen Situation ausgesetzt werden als ein Soldat oder eine Soldatin. Es kann einsturzgefährdete Gebäude inspizieren, es kann durch Gegenden fahren, die von Heckenschützen bedroht sind, es kann in Kampfhandlungen einbezogen werden, ohne dass direkt eigene Gefallene zu beklagen sind, sondern höchstens „Blechschaden". Für den Gegner bleibt das gefährlich, und genau genommen wird die Gefahr lediglich verlagert, denn während an der einen Stelle unbemannte Systeme schießen, jagen sich an anderer Stelle Selbstmordattentäter in die Luft.

In der Roadmap wird noch ein weiterer wichtiger Grund genannt, der sich durch das ganze Dokument zieht: das Geld. Unbemannte Systeme sind kleiner, leichter, weniger gepanzert als entsprechende bemannte Systeme und deshalb billiger. Sie werden angesichts nicht mehr allzu stark wachsender oder sogar sinkender Rüstungsetats als eine Option betrachtet, militärische Stärke und Überlegenheit zu wahren trotz knapper Kassen.

Und noch ein Argument spielt bei der Entwicklung unbemannter Waffensysteme eine wichtige Rolle: die Entwicklung unbemannter Waffensysteme. Einmal in die Welt gesetzt, folgen viele andere Länder der Welt dem US-amerikanischen Beispiel. Ein gigantisches Wettrüsten ist entbrannt. Die USA wollen gemäß ihrer spätestens seit dem Ende des Zweiten Weltkriegs herrschenden Allmachts- und Weltbeherrschungsphantasie auf allen technologischen Gebieten mit Priorität für die Kriegstechnik überlegen sein. Die Führungsposition ist aber nur dann zu halten, wenn man massiv weiter aufrüstet.

Sind unbemannte Waffensysteme kriegstauglich?

Wenn der Einsatz von Kampfdrohnen in den letzten zehn Jahren in Afghanistan, Pakistan, Jemen und Somalia typisch ist dafür, wie auch zukünftig unbemannte Waffensysteme verwendet werden, lässt sich Folgendes festhalten:

1. Sie dienen gezielten Tötungen *(targeted killings)*, bei denen bestimmte Personen anhand von Todeslisten aufgespürt, angegriffen und „ausgeschaltet" werden.

2. Sie dienen sogenannten *signature strikes*, bei denen Personen einzeln oder in Gruppen ins Visier genommen und getötet werden, weil sie nach einer Checkliste verdächtig aussehen oder sich verdächtig verhalten.

3. Sie bringen viele zivile Tote mit sich, weil die Zielpersonen nach den Punkten 1 und 2 selten allein angetroffen werden, sondern sich in normalen Wohnräumen, auf öffentlichen Plätzen, im Kreis ihrer Familie oder bei Freunden aufhalten, und weil die Zielpersonen nach Punkt 2 tatsächlich selbst oft Zivilpersonen sind.

Tötungen von Menschen nach den Punkten 1 bis 3 sind nach dem humanitären Völkerrecht Kriegsverbrechen und deshalb ethisch völlig unvertretbar.

Hans-Jörg Kreowski

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

Gladiator Tactical Unmanned Ground Vehicle at Redstone Arsenal, Gladiator des United States Marine Corps

Von diesem Umstand ist, was wohl nicht wirklich überrascht, in der Roadmap nicht die Rede. Dort wird davon ausgegangen, dass unbemannte Systeme die Möglichkeiten der Kriegführung wesentlich erweitern. Wenig bis gar nichts findet sich zu den Einsatzgrenzen dieser Waffen. Beispielsweise wird kaum darauf eingegangen, dass heute verfügbare Drohnen von Luftabwehrsystemen leicht abgeschossen werden können, sodass Einsatzgebiete nur dort liegen, wo Luftabwehr fehlt.

Nicht ohne Wissenschaft und Technik, nicht ohne Informatik

Um unbemannte Waffensysteme bauen zu können, werden die Erkenntnisse und Hervorbringungen vieler wissenschaftlicher und technischer Bereiche benötigt: Materialforschung, Optik, Sensorik, Nachrichtentechnik, Ballistik, Maschinenbau und andere mehr. Ohne die Beiträge der Informatik käme man allerdings nicht sehr weit. Jedes System benötigt einen eingebetteten Computer, auf dem die eingehenden Daten aller Sensoren gesammelt, zusammengeführt, aufbereitet, interpretiert, ausgewertet und zu Kommandostationen übertragen werden. Durch den Bordcomputer werden alle Geräte einschließlich der Waffen gesteuert. Die Kommandostation verfügt notwendigerweise auch über ein Computersystem, mit dem die vom unbemannten System eingehenden Daten aufbereitet und ausgewertet werden, soweit das nicht bereits auf dem unbemannten System selbst erfolgt ist. Auf der Basis der enthaltenen Daten entscheidet der Kommandeur dann über den nächsten Waffeneinsatz.

In der Roadmap sind in Kapitel 4 – *Technologies for Unmanned Systems*, das mit über 50 Seiten längste – bestehende technologische Lücken und offene Forschungsfragen ausführlich dargelegt. Es werden sechs Problembereiche beschrieben:

- Interoperability and Modularity,
- Communication Systems, Spectrum and Resilience,
- Security: Research and Intelligence/Technology Protection (RITP),
- Persistent Resilience,
- Autonomy and Cognitive Behavior,
- Weaponry.

Bei der *Interoperabilität* und der *Modularität* geht es darum, dass der Datenaustausch zwischen den verschiedenen Komponenten (insbesondere Sensoren und Bewaffnung) innerhalb eines unbemannten Systems sowie zwischen unbemannten und bemannten Systemen reibungslos funktioniert, trotz unterschiedlicher Datenformate und ständiger Fortentwicklung der Sensor- und Waffentechnologie sowie der algorithmischen Prozesse.

Die heutigen unbemannten Systeme sind extrem abhängig von *Kommunikationssystemen*, wobei die Funktionsfähigkeit der Kommunikationslinks, ihre Bandbreite, ihr Frequenzspektrum und ihre Härtung gegen jede Art von Interferenz signifikant sind.

Unbemannte Systeme sind in der Regel mit kritischen Programmen und klassifizierten (d. h. geheim zu haltenden schutzwürdigen) Daten ausgestattet, um ihre Aufgaben erledigen zu können. Deshalb spielen *Sicherheitsmaßnahmen* eine wesentliche Rolle, um unautorisierten Zugriff zu vermeiden, unabsichtliche Offenlegung der Daten zu verhindern und die technologische Überlegenheit zu wahren.

Persistenz verweist auf die Verkleinerung, Gewichtsreduktion, Energieersparnis und verbesserte Kühlung bei gleichzeitiger Erhaltung von Zuverlässigkeit, Wartbarkeit und Lebensdauer. Unbemannte Systeme besitzen ein erhebliches Potenzial in dieser Hinsicht.

Praktisch alle im Einsatz befindlichen unbemannten Systeme bedürfen der aktiven Kontrolle durch geeignetes Personal bei der Analyse gesammelter Daten und der Planung und Durchführung von Steuerung und Waffengebrauch. Da vor allem Personalkosten das Budget des *U.S. Department of Defense* belasten, hat die Entwicklung *autonomer Waffensysteme* höchste Priorität. Autonomie bedeutet dabei, dass die Systeme selbst die Signifikanz der gesammelten Informationen erkennen und eigenständig über weitere Aktionen entscheiden, ohne dass Menschen direkt eingreifen. Die Entscheidung über Leben und Tod wird also auf die Maschine verlagert, wobei aber Autonomie technisch zu verstehen ist. Das autonome Waffensystem wird programmierte Entscheidungsalgorithmen ausführen. In dieser Phase greift der Mensch nicht ein, aber die Algorithmen stammen immer noch von menschlichen Akteuren.

An Unmanned Surface Vehicle demonstration at Hampton, Virginia, January 2009, U.S. Navy photo by Mass Communication Specialist Seaman Apprentice Joshua Adam Nuzzo

Bei der *Bewaffnung* geht es darum, Waffen und unbemannte Plattformen aufeinander abzustimmen, spezifische Waffen und neue Munition für unbemannte Systeme zu entwickeln und perspektivisch auch Waffen auf der Basis der Nanotechnologie zur Verfügung zu stellen. Es wird davon ausgegangen, dass die Weiterentwicklung der Bewaffnung davon abhängt, ob die vorgenannten Technologien zum Durchbruch gebracht werden.

Auch wenn die Analyse der militärischen Wünsche an Wissenschaft und Technik viel vertiefter und detaillierter durchgeführt werden müsste, um verlässliche Schlussfolgerungen zu treffen, zeichnet sich auch schon bei einer ersten flüchtigen Sichtung ab, dass insbesondere von der Informatik viel erwartet wird. Als Forschungsgebiete der Informatik sind vor allem Datenfusion, Big Data, cyberphysikalische Systeme, sichere Systeme, Robotik, Künstliche Intelligenz und Autonome Systeme gefordert. Sind das nicht auch genau die Gebiete, die in der zivilen Informatik gerade mit immensen Finanzmitteln besonders gefördert werden? Ein Schelm, der Böses dabei denkt. Aber wenn dem so ist, wäre interessant zu untersuchen, ob immer noch wie in den 1950er- bis 1980er-Jahren der militärische Komplex die Entwicklung der Informatik maßgeblich bestimmt, oder ob das Militär sich einfach die aktuellen Hervorbringungen der zivil emanzipierten Informatik zunutze und zu eigen macht.

Was will die Bundeswehr mit Kampfdrohnen?

Waffentragende Drohnen werden bisher und vor allem für gezielte Tötungen, *signature strikes* und unter Inkaufnahme vieler Ziviltoter eingesetzt, sodass mit ihnen in den meisten Einsatzfällen Kriegsverbrechen begangen werden. Will die Bundeswehr auch solche Kriegsverbrechen begehen können? Wenn JA, wo soll das zukünftig geschehen? Welche Feinde Deutschlands sollen so bekämpft werden? Was hätte das mit dem Verteidigungsauftrag der Bundeswehr zu tun? Wenn NEIN, was sonst? Aus politischen und militärischen Kreisen hört man dazu oft litaneiartig wiederholt: Die Kampfdrohnen sollen dem Schutz der Soldaten bzw. dem Schutz von Feldlagern dienen. An welche zukünftigen Feldlager in welchen Ländern der Welt ist dabei gedacht?

A BAE Raven during flight testing, Brigadier Lance Mans, Deputy Director, NATO Special Operations Coordination Centre

Auf welche Kriegseinsätze bereitet sich die Bundeswehr vor? Welche Angreifer werden nicht über eine Flugabwehr verfügen, sodass Drohnen überhaupt dort fliegen können?

Hoffnung

Trotz der vielen Gegenbeispiele habe ich die Hoffnung nicht aufgegeben, dass Menschen vernünftig denken und handeln können, und dass sich insbesondere in einer Demokratie die Vernunft bei politischen Entscheidungen durchsetzen kann. Bezogen auf die Entwicklung unbemannter Waffensysteme hoffe ich, dass sich Informatikerinnen und Informatiker wo und wie immer möglich diesem Irrsinn verweigern. Bezogen auf bewaffnungsfähige Drohnen hoffe ich, dass die deutsche Regierung auf ihre Beschaffung und Neuentwicklung verzichtet, weil die immensen notwendigen Finanzmittel besser verwendet werden können, weil diese Waffen keinen Verteidigungsbedarf decken, weil diese Waffensysteme mit oder ohne Autonomie unüberwindliche ethische Probleme aufwerfen.

Daniel Leisegang

Der cyber-militärische Komplex

Die dunkle Seite des Silicon Valley

Den Begriff „militärisch-industrieller Komplex" prägte US-Präsident Dwight D. Eisenhower vor gut 50 Jahren. Er beschrieb damit eine Entwicklung, in der die Rüstungsindustrie durch den Zweiten Weltkrieg und im Zuge des Kalten Krieges erheblich an Einfluss auf die politischen Entscheidungen in Washington gewann. Die technische Entwicklung ist seither rasant fortgeschritten; es sind vollständig neue Technikfelder entstanden, in aller Regel mit erheblichem militärischen oder Dual-Use-Potenzial. Im digitalen Bereich, im „Cyberraum", ist die Verknüpfung von Militär und Industrie besonders eng, wie der Autor hier an zahlreichen Beispielen aufzeigt.

Das Silicon Valley gilt als die postindustrielle Innovationsschmiede der USA. Die dort angesiedelten IT- und Hightech-Unternehmen sind überzeugt, dass ihre *smarten* Produkte selbst die kompliziertesten Probleme des Alltags lösen können. Und in der Tat: Apples iPhone hat die Kommunikation von Millionen Menschen geradezu revolutioniert. Facebook verbindet über 1,3 Milliarden Menschen miteinander, derweil Google nicht weniger als sämtliche Fragen der Menschheit beantworten will.

Doch das sonnige Tal südlich von San Francisco steht nicht nur im Dienst der guten Sache, sondern ist bereits seit Jahrzehnten auch Teil des militärisch-industriellen Komplexes der USA. Die

enge Zusammenarbeit zwischen Nachrichtendiensten, der US-Armee und den IT-Unternehmen lässt die Trennlinie zwischen militärischen Anwendungen auf der einen und zivilen Produkten auf der anderen Seite mehr und mehr verschwimmen. Die Ursache dafür liegt nicht zuletzt in der zunehmenden Verbreitung des Internets und der Digitalisierung unserer Kommunikation.

Electronic Warfare: Die Entstehung des Silicon Valley

Die Verbindungen zwischen dem Silicon Valley und dem US-amerikanischen Militär reichen bis weit in die erste Hälfte des vergangenen Jahrhunderts zurück. Eine wichtige Rolle spielte dabei die Stanford University. Sie liegt etwa 60 Kilometer südöstlich von San Francisco nahe der Kleinstadt Palo Alto. Bereits in den 1930er-Jahren ermunterten die dort lehrenden Professoren ihre Studenten, in der näheren Umgebung Unternehmen zu gründen. Aus diesen ging unter anderem der Weltkonzern Hewlett-Packard hervor: Er wurde 1939 in einer Garage in Palo Alto ins Leben gerufen. Diese Garage gilt heute als die eigentliche Geburtsstätte des Silicon Valley.

Die wirtschaftliche Entwicklung der Region gewann 1951 an Fahrt. Damals wurde der Grundstein für den *Stanford Industrial Park* gelegt, den weltweit ersten Industriepark, der auf die Erforschung und die Produktion technologischer Produkte spezialisiert war. Der Park gehörte damals der Universität Stanford; heute ist er unter anderem Sitz des Facebook-Hauptquartiers.

Für die Herausbildung des Silicon Valley spielte *Frederick Terman* eine entscheidende Rolle. Der Professor für Ingenieurwissenschaften gilt – neben dem Physiker und Nobelpreisträger *William Bradford Shockley* – als einer der beiden Begründer des IT-Standorts.

Terman genoss in den 1930er-Jahren den Ruf, einer der besten Funktechniker der Vereinigten Staaten zu sein. Während des Zweiten Weltkrieges leitete er das streng geheime Electronic Warfare Lab an der Harvard University. Terman sollte erforschen, wie sich das deutsche Radarsystem effektiv stören ließ, um so Verluste auf Seiten der alliierten Luftstreitkräfte zu reduzieren.

Nach dem Krieg kehrte Terman 1946 an die Stanford University zurück. Er verfolgte das Ziel, das dortige Ingenieurinstitut zu einem weltweit anerkannten Zentrum für Mikrowellen- und Elektrotechnik zu machen, und gründete das Electronics Research Lab (ERL). Das ERL wurde von Beginn an auch vom US-Militär finanziert; im Gegenzug nutzte die Armee dessen Erkenntnisse während des Kalten Krieges, um die Sowjetunion auszuspionieren.[1]

Das ERL war jedoch nicht das einzige Labor in Stanford, das im Dienste der US-Armee stand. Auch die Forschungsergebnisse des Applied Electronics Lab (AEL), das sich der Störung von Radarsignalen und der elektronischen Aufklärung verschrieben hatte, wurden militärisch genutzt – vor allem während des Vietnamkriegs. Im April 1969 besetzten allerdings Studenten das Labor und verlangten dessen Schließung – mit Erfolg.

Einige der Forscher wechselten daraufhin in die Privatwirtschaft und gründeten rund um Palo Alto Start-ups, die sich auf Mikrowellen- und Radartechnik spezialisierten. Damit bestärkten sie zum einen den Aufstieg des Silicon Valley als IT-Standort. Zugleich festigten sie die Zusammenarbeit der dortigen Unternehmen mit dem Militär und den amerikanischen Geheimdiensten.

Google: Verwurzelt im militärisch-industriellen Komplex

Die Kooperationen zwischen dem Silicon Valley und der US-Regierung in Washington D.C. bestehen bis heute fort. Auch der Internetkonzern Google ist im Bereich der Militärforschung aktiv – ungeachtet seines inoffiziellen Firmenmottos „Don't be evil".

Google Inc. wurde 1998 von den Informatikern *Larry Page* und *Sergey Brin* gegründet. Bereits deren Forschungsprojekt an der Stanford University, aus dem der Konzern hervorging, wurde unter anderem von der Defense Advanced Research Projects Agency (DARPA) finanziert.[2] DARPA besteht seit 1958 und soll als Forschungsbehörde des US-Verteidigungsministeriums die „technische Überlegenheit des US-Militärs aufrechterhalten".

Nach der Unternehmensgründung arbeitete Google eng mit dem amerikanischen Auslandsgeheimdienst National Security Agency (NSA) und der National Geospatial-Intelligence Agency (NGA) zusammen, der zentralen US-Behörde für militärische und geheimdienstliche kartografische Aufklärung.

Im Jahr 2003 stattete Google die NSA beispielsweise intern für mehr als zwei Mio. US$ mit seiner Suchtechnologie aus. Zwar verlängerte die NSA den Vertrag nach einem Jahr nicht, dennoch stellte Google dem Nachrichtendienst seine Suchwerkzeuge noch ein weiteres Jahr zur Verfügung – ohne dies in Rechnung zu stellen. 2004 beauftragte auch die Central Intelligence Agency (CIA) Google, den Nachrichtendienst intern mit seiner Suchtechnologie auszustatten.[3]

Zudem bietet Google verschiedenen US-Geheimdiensten und dem Militär *geospatial intelligence services* an.[4] Bei diesen handelt es sich im Kern um *raumbezogene Aufklärungsdienste*,[5] welche die Kartenanwendung *Google Earth* nutzen. Insbesondere die NGA nutzt diese, um geografische Daten mit Geheimdienstinformationen anzureichern und zu visualisieren, und unterstützt damit, so Google, unter anderem die US-Regierung im Bereich der Sicherheitspolitik.[6]

Von Keyhole zu Google Earth

Auch Googles Kartentechnologie wurde maßgeblich von den Geheimdiensten finanziert. Google Earth ging aus den Produkten des Start-ups Keyhole hervor. Keyhole wurde 1990 gegründet und hatte sich frühzeitig auf dreidimensionale Kartentechnologie spezialisiert. Als dem Unternehmen 2001 die Insolvenz drohte, half ihm *In-Q-Tel* mit einer Finanzspritze aus der Not.

In-Q-Tel (IQT) war 1999 von der CIA gegründet worden und fungiert als dessen Capital-Venture-Arm. Das „Q" im Namen steht für die fiktive Forschungsabteilung des britischen Geheim-

dienstes MI6 in der James-Bond-Reihe, die dessen Agenten mit Armbanduhrenlaser und explodierenden Schlüsselringen versorgt. IQT verfolgt das Ziel, in neue Technologien zu investieren, die sich kurzfristig für geheimdienstliche oder militärische Zwecke einsetzen lassen. Bislang hat IQT mehr als 3,5 Mrd. US$ in ausgewählte IT-Unternehmen gesteckt. Auf Regierungsseite kooperiert das Unternehmen mit der Defense Intelligence Agency (DIA), dem US-Heimatschutzministerium sowie der NGA. Die Mittel des Unternehmens stammen allerdings in der Regel aus dem Haushalt der CIA.[7]

Die finanzielle Rettung von Keyhole zahlte sich aus: Die CIA und die NGA wirkten im Anschluss gezielt darauf hin, dass die Produkte von Keyhole an militärische und geheimdienstliche Zwecke angepasst wurden. Die Kartentechnologie unterstützte die US-Armee unter anderem bei der Invasion des Irak ab dem Jahre 2003.

Im Jahr 2004 kaufte Google Keyhole und nutzte dessen Technologie, um seinen eigenen dreidimensionalen Kartendienst Google Earth zu entwickeln. Gleichzeitig setzte Google die Kooperation mit den Nachrichtendiensten wie auch mit dem US-Militär fort. Die CIA macht aus der Zusammenarbeit keinen Hehl: Auf ihrer Website beschreibt sie Google Earth als „CIA-unterstützte Technologie".

Die Kooperation mit der NGA baute Google im Jahr 2008 sogar aus: Gemeinsam schickten sie einen Beobachtungssatelliten ins All – den *GeoEye-1*. Dieser galt damals als der kommerzielle Beobachtungssatellit mit der höchsten Bildauflösung: Täglich erfasst er eine Fläche doppelt so groß wie die Bundesrepublik. Google darf diese Aufnahmen verwerten, jedoch nur in einer reduzierten Auflösung. Zwei Jahre danach ging Google eine „formelle Beziehung zum Informationsaustausch" mit der NSA ein. Der Geheimdienst sollte dem Konzern dabei helfen, einen ausgeklügelten Angriff chinesischer Hacker auf dessen Dateninfrastruktur aufzuklären.[8] Welche Inhalte Google in diesem Rahmen mit der NSA austauschte, unterliegt bis heute der Geheimhaltung.

Google-Manager mit militärischen Erfahrungen

Die enge Bindung Googles an den militärisch-industriellen Komplex[9] spiegelt sich auch in der Unternehmensführung wider. Eine Reihe von Google-Managern kommt aus dem US-Militär oder hat zuvor für Nachrichtendienste gearbeitet.

Michele R. Weslander Quaid zum Beispiel ist seit 2011 Googles *Innovation Evangelist* und technische Leiterin der Google-Abteilung, die für öffentliche Aufträge zuständig ist. Das *Entrepreneur Magazine* zählte sie im vergangenen Jahr zu einer der sieben mächtigsten Frauen der Welt. Der Zeitschrift gegenüber beschrieb Weslander Quaid ihre Tätigkeit als „Brückenbauerin" zwischen dem Silicon Valley und den Regierungsbehörden in Washington. Dabei kommt der Google-Managerin zugute, dass sie zuvor unter anderem bei der NGA, dem Direktor der nationalen Nachrichtendienste, dem Nationalen Aufklärungsamt sowie dem US-Verteidigungsministerium tätig war.

Shannon Sullivan hingegen leitet bei Google die Abteilung für Verteidigung und Aufklärung. (Sein offizieller Titel lautet *Head of Defense & Intelligence*.) Er ist dafür zuständig, Google-Dienste für das Verteidigungsministerium bereitzustellen. So hatte eines von Sullivans Projekten zum Ziel, 50.000 US-Soldaten mit angepassten Google-Applikationen auszustatten.[10] Zuvor hatte Sullivan über zwei Jahrzehnte bei der *U.S. Air Force* gearbeitet – unter anderem in der Geheimdienstabteilung.

Kriegsroboter im Dienste der Kunden?

Google hilft jedoch nicht nur bei der Auswertung von Daten, sondern ist seit Kurzem auch im Robotergeschäft unterwegs. 2013 kaufte der Konzern in nur sechs Monaten acht Roboterfirmen auf, darunter Boston Dynamics. Das Unternehmen wurde 1992 von *Marc Raibert* gegründet, einem ehemaligen Professor am Massachusetts Institute of Technology (MIT); Raibert gilt in den Vereinigten Staaten als *Vater* der Laufroboter. Boston Dynamics hatte vor allem im Auftrag des US-Militärs gearbeitet, und nach der Firmenübernahme sicherte Google zu, die bestehenden Verträge zu erfüllen. Mit dem Unternehmen hat Google nicht nur 80 Ingenieure und Wissenschaftler *eingekauft*. Zudem verfügt der Internetkonzern nun über den weltschnellsten Laufroboter, genannt *Cheetah* (Gepard). Dieser hat vier Beine, erreicht eine Geschwindigkeit von knapp 47 Stundenkilometern und ist damit etwas schneller als der mehrfache Olympiasieger über 100 Meter, *Usain Bolt.*

Der Bau, der Verkauf und der Einsatz von Robotern ist ohne Frage ein großer Zukunftsmarkt, insbesondere im Bereich der Automatisierung und der Erforschung künstlicher Intelligenz. Welche Ziele Google allerdings genau mit dem Kauf der Roboterfirmen verfolgt, ist derzeit noch offen.

Drohnen: Der Wettkampf um den Luftraum

Klarer sind die Ziele bei der Entwicklung unbemannter Flugzeuge erkennbar. Anfang 2014 erwarb Google den Drohnenhersteller Titan Aerospace. Das Unternehmen stellt riesige, solarbetriebene Flugzeuge her. Diese können mehr als drei Millionen Flugkilometer zurücklegen, bevor sie wieder landen müssen. Aus einer Höhe von 30 Kilometern sollen sie weltweit unwegsame Gebiete mit Internetzugang versorgen.

In diesem Bereich bewegt sich insbesondere Facebook in direkter Konkurrenz zu Google. Die *Social Community* übernahm den britischen Drohnenentwickler *Ascenta* und plant ebenfalls den Bau tausender Flugdrohnen. Diese sollen die Spannweite von Jumbo-Jets haben und, so der Plan, vier Milliarden Menschen mit drahtlosem Internetzugang versorgen.[11]

Ein weiterer Konzern – allerdings mit Sitz in Seattle – interessiert sich ebenfalls für Drohnen: Amazon. Der Internethändler möchte die unbemannten Fluggeräte nutzen, um Bestellungen an die Kunden auszuliefern. Bisher stehen diese Pläne noch am Anfang, allerdings ist das Vorhaben gewiss mehr als ein reiner Marketing-Gag: Für sein Vorhaben hat Amazon unter anderem Ingenieure der NASA und der *U.S. Navy* abgeworben: *Neil Woodward* leitet seit April 2014 die Abteilung, die für Testflüge und Zertifizierungen zuständig ist; zuvor war er NASA-Astronaut und Navy-Flugoffizier. *Mark Sibon* ist seit September 2014

Operations Program Manager bei Prime Air. Davor leitete er drei Jahre lang bei der US-Navy die Abteilung Unmanned Aerial Vehicle (Unbemannte Flugkörper).

Die CIA in der Amazon-Cloud

Nicht nur zur Armee, auch zu den US-Geheimdiensten pflegt Amazon enge geschäftliche Beziehungen. Seit Jahren nutzen über 300 amerikanische Regierungsbehörden, darunter das US-Finanzministerium, die so genannte *GovCloud*. Diese ist Teil der *Amazon Web Services*, mit denen Unternehmen wie auch Privatkunden Speicherplatz auf den Amazon-Servern nutzen können. Im Juli 2013 – und damit inmitten der NSA-Enthüllungen – gab der Konzern bekannt, ausgerechnet von der CIA den Zuschlag für einen Großauftrag erhalten zu haben: Für die Dauer von vier Jahren stellt Amazon dem Auslandsgeheimdienst der USA ein eigens auf sie zugeschnittenes Cloud-Computing-System bereit – Kostenpunkt: mehr als 600 Mio. US$.

Durch diese einträgliche Public Private Partnership befindet sich Amazon in großer wirtschaftlicher Abhängigkeit von der CIA und der US-Regierung. Möglichen Forderungen, Einblicke in die Amazon-Kundendaten oder gar eine direkte Schnittstelle zu den Unternehmensservern zu erhalten, wird sich der Online-Händler wohl kaum entziehen können, ohne gleichzeitig Gefahr zu laufen, eine Reihe wichtiger Großkunden zu verlieren.

Die Suche nach der Nadel im Big-Data-Heuhaufen

Weitaus weniger bekannt als Google, Facebook oder Amazon ist das ebenfalls im Silicon Valley beheimatete Unternehmen Palantir Technologies. Palantir verfügt über keine direkte Konsumentenbindung, sondern unterhält vor allem Geschäftsbeziehungen zum US-Militär – und zur CIA.

Wie kaum ein anderes Unternehmen des Silicon Valley ist Palantir ein technisch-militärischer Hybrid: Zur einen Hälfte ist das Unternehmen in Washington angesiedelt, zur anderen in Palo Alto.[12] Gegründet wurde es 2004 von dem heutigen Geschäftsführer *Alex Karp* und dem PayPal-Gründer *Peter Thiel*. Thiel investierte gut 28 Mio. US$ in Palantir, weitere zwei Millionen kamen von In-Q-Tel. Heute ist das einstige Start-up eines der am schnellsten wachsenden Unternehmen im Silicon Valley; sein Marktwert wird derzeit auf über acht Mrd. US$ geschätzt.

Der Firmenname leitet sich von den *Sehenden Steinen* aus der Fantasiesaga *Der Herr der Ringe* ab. Dementsprechend hat sich Palantir auf die Entwicklung hochkomplexer Software auf der Grundlage von PayPals Betrugserkennungssoftware spezialisiert. Diese ist in der Lage, verschiedene Datenbanken über einen gemeinsamen Index zu erschließen und deren Inhalt mit menschlicher Sprache abzufragen. Das Suchwerkzeug genießt den Ruf, einfach und intuitiv anwendbar zu sein.

In Geheimdienstkreisen genießt Palantir den Ruf, das effizienteste Werkzeug zu besitzen, um terroristische Netzwerke aufzufinden und zu untersuchen. Dafür prüft und kategorisiert Palantir unterschiedliche Datenquellen – ganz gleich, ob es sich dabei um Namen, Telefonnummern oder Kontobewegungen handelt – und stellt eigenständig Beziehungen zwischen diesen her.[13] Auf diese Weise kann Palantir die sprichwörtliche Nadel im Big-Data-Heuhaufen finden – und bietet damit aus Sicht der Geheimdienste die *Killer-App* schlechthin an.[14]

Die Software wird bislang vor allem im Bereich der militärischen und geheimdienstlichen Aufklärung eingesetzt. So soll Palantir in der Vergangenheit unter anderem Mitglieder eines mexikanischen Drogenkartells ausfindig gemacht haben, nachdem diese einen US-Agenten getötet hatten. Die US-Truppen in Afghanistan hingegen nutzen die Software, um Aufständische aufzuspüren, die mit selbstgebauten Sprengsätzen US-Soldaten töten.[15]

Das Potenzial von Palantir ist damit aber bei Weitem nicht ausgeschöpft. Zu den Beratern des Unternehmens gehören neben der Nationalen Sicherheitsberaterin unter *George W. Bush*, *Condoleezza Rice*, auch der ehemalige CIA-Direktor *George Tenet*. Dieser sagte über Palantirs Software, er wünschte, die CIA hätte ein derart machtvolles Programm vor dem 11. September 2001 besessen. Palantir sei in der Lage, Verbindungen aufzuzeigen, „die fünf, sechs, acht, zehn Jahre zurückreichen". Etwas Vergleichbares habe damals keine Anwendung vermocht.[16]

Daher überrascht es nicht, dass zu Palantirs Kunden neben der CIA längst auch die NSA, das FBI, die Defense Intelligence Agency, das Department of Homeland Security, das National Counterterrorism Center, das U.S. Marine Corps, das U.S. Special Operations Command sowie – nicht zuletzt – die Polizeibehörden in Los Angeles und in New York City gehören.

Der cyber-militärische Komplex

Dank der voranschreitenden Digitalisierung wird die Zusammenarbeit zwischen dem Silicon Valley und Washington in Zukunft noch enger werden. Denn längst gehen *Big Brother* – die globale Ausspähung durch die US-Geheimdienste – und *Big Data* – die massenhafte Anhäufung von Kommunikationsdaten – Hand

Daniel Leisegang

Daniel Leisegang ist Politikwissenschaftler und Redakteur bei der Monatszeitschrift *Blätter für deutsche und internationale Politik (blaetter.de)*.

in Hand. Zugleich sind die US-Armee und die Geheimdienste damit auf Analysewerkzeuge angewiesen, die die richtigen Punkte in der schier unendlichen Masse an Informationen finden und miteinander verbinden können.

Fest steht damit auch, dass der cyber-militärische Komplex weiter anwächst – und nach und nach den militärisch-industriellen Komplex ablösen wird, der seine Wurzeln in den 1950er-Jahren hat. Allein in diesem Jahr stehen dem US-Verteidigungsministerium 5,5 Mrd. US$ für Investitionen im Bereich der *Cybersicherheit* zur Verfügung. Ein Großteil davon wird ins sonnige Silicon Valley fließen – und damit in die smarte, neue Überwachungswelt.

Der Beitrag ist in *Wissenschaft & Frieden* 2015-2: *Technikkonflikte, Seite 27–30* erschienen.
http://wissenschaft-und-frieden.de/seite.php?artikelID=2042

Anmerkungen

1 *Steve Blank: The Secret History of Silicon Valley Part VI: Every World War II Movie was Wrong. steveblank.com, 27.4.2009.*
2 *Dazu auch: Nafeez Ahmed: How the CIA made Google. medium.com, 22.1.2015.*
3 *Douglas Edwards (2012): I'm feeling lucky: Confessions of Google Employee Number 59. Boston: Mariner Books.*
4 *Der US-Regierung bietet Google zudem für 6,7 Mio. US$ seine Cloud-basierten E-Maildienste an. Vor diesem Hintergrund ist wenig verwunderlich, dass Länder wie Russland oder China Googles Dienste aussperren; vgl. dazu: Evgeny Morozov: Who's the true enemy of internet freedom – China, Russia, or the US? The Guardian, 3.1.2015.*
5 *Seit 2010 bietet Google der NGA zudem für 27 Mio. US$ „geospatial visualization services" an. Den Auftrag erhielt Google direkt und ohne Ausschreibung, was die NGA damit begründete, dass sie bereits erhebliche Investitionen in die Google-Earth-Technologie getätigt habe, die man nicht verlieren wolle.*
6 *Google Earth Builder supports NGA geospatial efforts. Official Google for Work Blog, 20.4.2011.*
7 *Das Geld, mit dem Keyhole vor der Pleite gerettet wurde, kam allerdings von der NGA. Die NGA verfügt über ein etwa halb so großes Budget wie die NSA; damals gab sie an, das Geld anstelle der »Intelligence Community« zur Verfügung zu stellen.*
8 *Ellen Nakashima: Google to enlist NSA to help it ward off cyberattacks. The Washington Post, 4.2.2010.*
9 *Google arbeitet auch eng mit Rüstungsunternehmen wie Lockheed Martin und Northrop Grumman zusammen. Lockheed erhielt von Google »geospatial technologies«. Northrop zahlte rund eine Million US$ für eine maßgeschneiderte Google-Earth-Anwendung.*
10 *Yasha Levine; The revolving door between Google and the Department of Defense; pando.com, 23.4.2014. Jeremy Scahill: Blackwater for Sale. The Nation, 8.6.2010.*
11 *Derzeit verfügt gerade einmal gut ein Drittel der Weltbevölkerung über einen Zugang zum Internet: Vgl. den Bericht der Internationalen Fernmeldeunion ITU (2014): Measuring the Information Society Report 2014. Genf.*
12 *Daneben unterhält Palantir ein weiteres Dutzend Büros in der ganzen Welt, unter anderem in Tokio, Sydney, Singapur und Tel Aviv.*
13 *Siobhan Gorman: How Team of Geeks Cracked Spy Trade. The Wall Street Journal, 4.9.2009.*
14 *Palantirs Software ist damit das kommerzielle Gegenstück zum NSA-Tool XKeyscore. Mit ihm kombiniert und durchsucht der Geheimdienst Telekommunikationsdaten aus verschiedenen Quellen. Aus diesem Grund sehen Bürgerrechtsorganisationen wie die American Civil Liberties Union in Palantir auch einen „wahren totalitaristischen Albtraum", da die Software es ermögliche, das Leben unschuldiger Amerikaner in nie gekanntem Ausmaß zu überwachen. Andy Greenberg and Ryan Mac: How A »Deviant« Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut. Forbes, 2.9.2013.*
15 *Rowan Scarborough, Military leaders urgently push for new counterterrorism software. The Washington Times, 27.8.2012.*
16 *Ryan Mac: National Security Darling – Why Condoleezza Rice, David Petraeus and George Tenet Back Palantir. forbes.com, 19.8.2013.*

Gertrud Maria Vaske

Cyberwar – die digitale Front: Ein Angriff auf Freiheit und Demokratie?

Interview mit Felix *FX* Lindner, Hacker

Felix *FX* Lindner *legte die Energieversorgung der Stadt Ettlingen lahm und hackte Blackberry sowie die Netzwerkstruktur von Cisco. Als ausgewiesener Experte in der Computer-Security-Szene präsentiert* „FX" *seine Forschungsergebnisse bereits seit über zehn Jahren weltweit auf Konferenzen und macht sie frei im Netz zugänglich. Er ist Gründer, technischer und Forschungsleiter von* Recurity Labs GmbH*, einem Beratungs- und Forschungsunternehmen für IT-Sicherheit im High-End-Bereich, das sich auf Code-Analyse und das Design von sicheren Systemen und Protokollen spezialisiert hat. Das Interview führte* Gertrud Maria Vaske*.*

Gertrud Maria Vaske (GMV): *Was ist Ihrer Meinung nach die größte Bedrohung im Cyberwar? Was war Ihrer Meinung nach die größte Bedrohung für Datensicherheit und Datenschutz im Jahr 2014?*

Felix *FX* Lindner (FX): Die größten Bedrohungen erwachsen meiner Meinung nach durch den Mangel an Verständnis bei vielen der verantwortlichen Personen. Dadurch bestimmten in 2013 und 2014 einige wenige Personen das mediale Narrativ und die politische Agenda. Eine sachliche Diskussion über Datensicherheitsstrategien ist leider so selten wie sie dringend angeraten ist.

GMV: *Welche Cyberwar-Gefahren gibt es vor allem militärisch, aber auch für die Privatbevölkerung und für Unternehmen?*

FX: Das Hauptproblem in allen drei Bereichen ist die blinde Digitalisierungswut. Wir schaffen es nicht, unsere existierenden Computersysteme und Netzwerke abzusichern, bauen aber überall noch mehr und tiefer vernetzte Computer ein, sei das

nun in Waffensysteme oder Versorgungsinfrastruktur für Strom, Wasser oder Gas. An vielen Stellen ist der Nutzen bestenfalls ein Mythos, die zusätzlichen Gefahren sind aber sehr reell.

GMV: *Mit Cyberattacken können Waffensysteme wie z. B. Flugabwehrraketen lahm gelegt werden. Warum wird das so selten gemacht?*

FX: Einerseits ist das notwendige Wissen und Personal mit den entsprechenden Fähigkeiten dünn gesät. Solange man konventionelle Mittel zur Verfügung hat, um den gleichen Effekt zu erzielen, lohnt sich der Einsatz dieser knappen Ressource nicht. Zum anderen haben die verantwortlichen Personen in Militär und Politik aufgrund ihres mangelnden Fachwissens auch eine berechtigte Angst vor Sekundäreffekten, welche sie nicht einschätzen können.

GMV: *Könnte man mit Cyberattacken die aktuellen Konflikte (Syrien/Ukraine) eindämmen?*

FX: Cyberattacken sind für diesen Zweck ungeeignet. Offensivmittel sind ja generell eher das falsche Mittel der Wahl, um Konflikte zu entschärfen.

GMV: *Sollte ich als Verteidigungsministerin lieber in Cyberwaffen oder Cybersicherheit investieren oder lieber in herkömmliche Waffen?*

FX: Das sollte ein Ergebnis einer sicherheitspolitischen Gesamtstrategie sein, welche eine Verteidigungsministerin hoffentlich hat. Der Aufbau von Offensivfähigkeiten *on par* mit denen anderer Länder ist sicherlich ein Muss, denn die fünfte Domäne wird nicht einfach wieder verschwinden, und genauso wie man keine Luftwaffe vom einen Tag zum anderen bei *Amazon* bestellen kann, so müssen auch Cyberoffensivkräfte viele Jahre trainieren, bevor sie einsatzbereit sind. Die sogenannte Cybersicherheit ist eher eine gesamtpolitische Aufgabe.

GMV: *Was brauche ich, um die Infrastruktur eines Landes lahm zu legen?*

FX: Bezogen auf einen Cyberangriff reichen hier ein paar fähige Angreifer mit schiefem moralischem Kompass und das entsprechende Geld, um diese zu bezahlen. Hat man es aber nicht eilig damit, bietet sich auch umfangreiche Privatisierung als ein sehr effektives Mittel an.

GMV: *Aufsehen haben die Cyberwaffen* Stuxnet *und* Flame *erregt. Damit wurde das iranische Atomwaffenprogramm ausgespäht und angegriffen. Was war daran besonders gefährlich?*

FX: Besonders gefährlich daran sind die Kollateralschäden – und zwar nicht die direkt ersichtlichen. Beispielsweise wurde für *Flame* eine kryptographische Signatur erzeugt, damit es so aussah, als ob die Datei von *Microsoft* selbst kam. Dadurch wurden viele Sicherheitsprüfungen umgangen, welche essenziell für eine ganze Reihe von Schutzmaßnahmen in der Computersicherheit sind. Diese Methode funktioniert auch heute noch, die Schutzmaßnahmen können aber nicht einfach mal ausgetauscht werden. Dadurch wurde die ganze Welt verwundbarer als sie es vorher war.

GMV: *Entmystifizierung des Cyberwar – oft heißt es, den gebe es nicht und der sei nicht neu. Sie haben auf unserer Berliner Podiumsdiskussion zu der Behauptung, Schadsoftware trüge keine Uniform, gesagt, die militärischen Angriffe im Netz trügen mehr Uniform als russische Soldaten auf der Krim – was meinen Sie damit genau?*

FX: Fast alle Staaten haben wenig Hoffnung auf mittelfristig verfügbare Defensivmaßnahmen und konzentrieren sich daher auf Offensivmittel. Dementsprechend soll allen anderen gezeigt werden, was man kann, also eine Art *Show of Force*. Die Hoffnung ist, einen gewissen Grad von Abschreckung zu erreichen. Dazu muss aber offensichtlich sein, von wem der Angriff entwickelt und durchgeführt wurde. Es wird also wenig verschleiert.

GMV: *Wieviel Cyberpower hat China oder Russland im Vergleich zu den USA?*

FX: China und Russland sind offensiv vergleichbar stark wie die USA, wenn auch in jeweils etwas anderer Ausprägung.

GMV: *Wer sind derzeit die Cybersupermächte?*

FX: *Google*, China, Russland und die USA.

GMV: *Also Länder, die selbst Computer bauen, haben gute Chancen, Cyberpower zu sein oder zu werden. Wie stehen da derzeit die Chancen für Deutschland? Werden wir nach Zuse überhaupt noch computertechnisch wahrgenommen in der Welt?*

FX: Nein, Deutschland spielt hier keine besondere Rolle mehr. Das ist besonders schade, da die Fähigkeiten durchaus vorhanden sind, aber leider nicht genutzt werden.

GMV: *Wie gehen Cyberangreifer vor? Was tun sie, wenn sie ein Land, Konzerne, Firmen, den Staat oder den Geheimdienst angreifen wollen?*

FX: Der Vorgang ist grob vergleichbar mit einem Einbruch: Hintergrundinformationen beschaffen, auskundschaften, an Türen und Fenstern rütteln, Werkzeuge auswählen und dann den Einbruch durchführen. Im Unterschied zu einem Einbruch flüchtet man nicht danach, sondern verbarrikadiert sich möglichst unauffällig im Objekt.

GMV: *Welche Abwehrmechanismen gibt es, um sich gegen Eindringlinge zu wappnen? Müssen wir nicht eigene Computer bauen?*

FX: Ja, wir müssten wirklich eigene Computer bauen. Wenn wir für diese im Unterschied zu allen anderen auch eine Produkthaftung übernehmen würden, wären sie zwar deutlich teurer, aber auch der Exportschlager schlechthin.

GMV: *Gibt es ein Patentrezept gegen Cyberangreifer, z. B. wieder auf Schreibmaschine umzustellen?*

FX: Wenn Sie ein Geheimnis bewahren wollen, sollten Sie es heutzutage nicht in einen Computer stecken.

GMV: *Blicken wir auf das kommende Jahr. Nationalstaaten, die sich mehr und mehr gegenseitig mit Schadsoftware angreifen. Der jeweilige Privatsektor ist betroffen und auch Aktivisten werden das Internet weiterhin für eigene Zwecke nutzen – was wäre der „Supergau" für Deutschland? Welches Szenario könnte schnell wahr werden?*

FX: Deren gibt es leider viele. Ich vertrete aber die Auffassung, dass man keine Anleitungen öffentlich zur Verfügung stellen sollte.

GMV: *Wie kann man ein solches Szenario verhindern?*

FX: Eine gesamtpolitische Auseinandersetzung mit dem Thema wäre ein erster Schritt.

GMV: *Kann man mit einem anständigen Computer einen Flughafen lahmlegen? Nennen Sie uns bitte eine grobe Schätzung. Wie viele Menschen können das Ihrer Meinung nach?*

FX: Einige tausend Personen weltweit sind es bestimmt.

GMV: *Manche Stimmen werden lauter: Panikmache und Forderung nach Aufklärung – worin sehen Sie die Aufgaben von Produzenten von Soft- und Hardwareprodukten, um die Computersicherheit zu verbessern?*

FX: Es wäre schön, wenn die Produzenten endlich ehrlich zur Politik wären. Immer neue Versprechen vom nächsten Wundermittel bringen uns nicht weiter. Das Eingeständnis, dass die nicht vorhandene Haftung ihrerseits das Kernproblem darstellt, würde eine Menge ändern. Die Politik wird nicht sofort eine solche Haftung fordern, denn niemand will SAP & Co. ruinieren. Doch leider ist die momentane Scharlatanerie zu einträglich, als dass sie freiwillig aufgegeben würde.

GMV: *Laut Thomas Ried ist Cyberwar nur eine clevere Strategie von Sicherheitsfirmen, denn eigentlich gibt es ihn seiner Meinung nach nicht. Was halten Sie von der Ried-These?*

FX: Der Begriff *Cyberwar* eignet sich ausgezeichnet, um den Verkauf des nächsten Wundermittels anzukurbeln. Er erklärt aber weder die Hunderte von Soldaten und die Horden von Experten in der Verteidigungsindustrie verschiedener Länder, die sich mit dem Thema Offensivkapazitäten befassen, noch die großen Summen in den entsprechenden Etats. Herr Ried beschreibt ein Symptom, nicht die Krankheit.

GMV: *Wie schätzen Sie die Sicherheitslage deutscher Firmen generell ein?*

FX: Deutsche Firmen sind meiner Meinung nach hochgradig exponiert. Wir sind ein Exportland, spezialisiert auf Prozess- und Produktionswissen. Anders als Rohstoffe ist unser Exportgut also perfekt geeignet, um aus unseren Computern entwendet (d. h. kopiert) zu werden, ohne dass wir es merken.

GMV: *Experten gehen davon aus, dass gezielte Hackerangriffe jährlich Schäden in Millionenhöhe verursachen – glauben Sie, dass die Mehrheit der CIOs und IT-Leiter derzeit in der Lage sind richtige und sinnvolle Schutzmaßnahmen zu ergreifen?*

FX: Nein, was unter anderem daran liegt, dass der CEO es zur Aufgabe des IT-Leiters macht, als hätte der CEO damit nichts zu tun.

GMV: *Wird Sicherheit künftig der Bequemlichkeit geopfert? Internet in Bundeswehrkasernen – wie sicher ist eine E-Mail-Adresse innerhalb der Bundeswehr vor Hackern?*

FX: Sicherheit wird immer der Bequemlichkeit oder Eitelkeit geopfert. Unternehmen haben jahrelang großen Aufwand betrieben, um mit *BlackBerry* eine halbwegs verlässliche Infrastruktur zu schaffen, und dann wollten die CEOs lieber *iPhones*. Die Sicherheit einer E-Mail innerhalb der Bundeswehr kann man einfach mal testen lassen. Leider wird auch das fast nie gemacht, denn die befürchtete Antwort will keiner hören.

GMV: *Wie sicher ist mein Smartphone (Samsung) vor Ihnen?*

FX: Vor mir ist es sicher. Ich habe kein Interesse daran.

GMV: *Manche Experten behaupten, dass es bislang keinen einzigen Cyberangriff gegeben hat. Trotzdem wird immer wieder vom Cyberwar gesprochen. Ist dies eine Strategie von Sicherheitsfirmen, Marketing- und Medienexperten und ist Cyberwar gar unreal?*

FX: Ob es Cyberangriffe gegeben hat, ist eine Definitionsfrage und daher strittig. Nationalstaatliche Aktivitäten nehmen allerdings definitiv kontinuierlich zu, das ist leider kein Marketing, so sehr ich mir das auch wünschen würde.

GMV: *Was macht einen guten professionellen Hacker aus?*

FX: Integrität, Passion, Fachwissen und Fähigkeiten sowie die Kirche im Dorf lassen.

GMV: *Müssen Hacker um ihr Leben fürchten bzw. wie zimperlich sind Geheimdienste?*

FX: Gewaltsame Todesfälle mit möglichem geheimdienstlichem Hintergrund sind eher selten bekannt geworden. Hacker, die für

Gertrud Maria Vaske

Gertrud Maria Vaske ist Chefredakteurin des E-Journals *Ethik und Militär*.
vaske@zebis.eu

kriminelle Vereinigungen gearbeitet haben, werden schon häufiger mal tot aufgefunden, wenn der Job erledigt ist.

GMV: *Unterhalb der Schwelle eines bewaffneten Konflikts – was gibt es für einen Regelungsbedarf?*

FX: Wie gesagt sehe ich den größten Bedarf in der Einführung von Produkthaftungen für Hard- und Software, zumindest wenn die Produkte an den Staat oder das Militär geliefert werden. Solange es einträglicher ist, völlig kaputtes Zeug zu verkaufen, damit man dann auch noch die nächste Version verkaufen kann, gibt es kein Geld mit sicheren Computern zu verdienen, also baut sie auch keiner.

GMV: *Eine Frage nach dem Ausmaß und der Bedrohung durch Überwachung. Was würden Sie einem Regierungschef sagen, der* Google Mail *nutzt, mit dem* Google-*Browser* Chrome *surft und ein Smartphone mit dem* Google-*Betriebssystem* Android *benutzt?*

FX: Ich würde fragen, warum er oder sie das Geld der Bürger an Ministerien für Verteidigung, Spionage und Spionageabwehr verschwendet, da dieses Verhalten deren Arbeit *ad absurdum* führt. Außerdem würde mich interessieren, inwieweit der Amtseid mit einer fahrlässigen vollständigen Auslieferung des Staates an eine transnationale Supermacht vereinbar ist.

GMV: *NATO-Experten haben mit dem* Tallinn Manual *2013 ein Handbuch bereitgestellt, das sich mit der Anwendbarkeit des Völkerrechts im Cyberspace beschäftigt. Spielt das Handbuch bei Hackern eine Rolle?*

FX: Nein, das sind *Policy*-Fragen.

GMV: Google/Apple/Microsoft – *inwieweit sind diese Firmen eine Gefahr für die persönliche und nationale Sicherheit?*

FX: *Googles* Kontrolle über das gesamte Internet sollte bei Fragen der nationalen Sicherheit eine prominente Stellung einnehmen.

GMV: *Welche internationalen Cyberschutzgesetze brauchen wir?*

FX: Wir sollten internationale Regeln aufbauen, welche die Kontrolle über das Internet in der Hand der demokratischen Länder der Welt belassen, obwohl diese die Minderheit aller Länder darstellen.

GMV: *Und welche Gesetze, etwa zur Produkthaftung, brauchen wir für die Sicherheit von Computern oder Software?*

FX: Volle Produktlieferung (keine Lizenz) und entsprechende Produkthaftung für vom Bund oder der Bundeswehr beschaffte Software ist der erste und wichtigste Schritt. Nach chaotischen Anfängen werden Sie einen dramatischen Qualitätsanstieg bemerken, Sicherheit inklusive.

GMV: *Im Cyberangriffsfall, rein hypothetisch gefragt: Würden Sie im Tarnanzug für Deutschland hacken?*

FX: Ich helfe verschiedenen Ländern, ihre Infrastruktur besser zu verteidigen. Einen Tarnanzug habe ich dafür bis jetzt noch nie gebraucht.

Der Beitrag wurde übernommen aus *Ethik und Militär*, Ausgabe 2014/2 *Cyberwar – die digitale Front: Ein Angriff auf Freiheit und Demokratie?*, E-Journal-Special *(http://www.ethikundmilitaer.de/index.php?id=26).*

Reiner Braun und Lucas Wirl

Aufrüstung, Militarisierung und Rüstungsforschung an Hochschulen

Die Aussage Ban Ki Moons vor der NPT-Konferenz 2010, die Welt sei überrüstet und der Frieden unterfinanziert, trifft heute – 5 Jahre später – mehr zu denn je. Durch die globale Finanzkrise liegen die globalen, jährlichen Rüstungsausgaben zwar seit einigen Jahren stabil bei ca. 1,7 Billionen US-Dollar, jedoch verfällt die deutsche, europäische und internationale Politik in Praktiken und Gebaren, die nach zwei Weltkriegen und dem Wegfall des „Gleichgewichts des Schreckens" und des ideologisch bedingten Ost-West-Konfliktes überwindbar zu sein schienen: Deutschland stellt sich mit einer „Armee im Einsatz" zur Sicherung wirtschaftlicher Interessen als internationaler militärischer Faktor auf, der Krieg ist zurück in Europa – in der Ukraine und auch in Griechenland – und der global geführte „Krieg gegen den Terror" stellt in einer Reihe von Brüchen des Völkerrechts den wohl universellsten dar. Von der Illusion einer Friedensdividende musste schnell Abstand genommen werden.

In unserer multipolaren Welt ist die Schwelle militärischer Gewaltanwendung und Interessensdurchsetzung gesunken. Nach dem Kalten Krieg und den kurzen Jahren der Kooperation befinden wir uns in einer Phase der Konfrontation mit der Tendenz zu einer Neuaufteilung der Welt, die (bisher) durch hohe Komplexität und Unübersichtlichkeit geprägt ist. Ein Ausdruck dessen ist eine neue Rüstungsspirale und eine Militarisierung der Außen- und Innenpolitik.

Eine neue Rüstungsspirale und Revolutionen des Militärwesens

Aus Obamas berühmter Rede in Prag ist nur noch „but not in my lifetime" in bitterer Erinnerung geblieben, und die Welt befindet sich heute in einer neuen Rüstungsspirale. An oberster Stelle, angeführt von den USA und der NATO, ersetzen alle Atomwaffenstaaten ihre nuklearen Arsenale durch hochmoderne High-

tech-Atomwaffensysteme. Sie nennen es Lebensverlängerung, aber es ist eine Weiterentwicklung des Damoklesschwertes für das 21. Jahrhundert. Bezeichnend ist, dass der nukleare Abrüstungsprozess mit dem Nichtzustandekommen eines Abschlussdokuments der Vertragsstaaten des Atomwaffensperrvertrags vollends ins Stocken geraten ist und die Kündigung des INF-Vertrages zur Stationierung von Mittelstreckenraketen in Europa durch die USA angedroht wurde. Schon Ende 2014 stellte die vielleicht renommierteste Zeitschrift der Friedenswissenschaft, das *Bulletin of the Atomic Scientists*, die Weltuntergangsuhr auf 3 Minuten vor 12. Auch in einem weiteren Rahmen der Abrüstung und Rüstungskontrolle unterhalb der allzerstörenden Atomwaffen sind keine Fortschritte zu verzeichnen, so unter anderem bei einer Konvention zur Verhinderung der Militarisierung des Weltraums, dessen militärische Nutzung stetig ausgeweitet wird.

Während die Zeichen in wichtigen Arenen auf Aufrüstung stehen, verpflichten sich die NATO-Mitgliedsstaaten auf eine Steigerung ihrer Rüstungshaushalte auf 2 % ihres BIP. Werden diese Ziele umgesetzt, steigen die Militärausgaben der NATO-Mitgliedsstaaten von 880 Milliarden US-Dollar in 2014 auf 980 Milliarden US-Dollar – in Zeiten wachsender globaler Herausforderungen eine unglaubliche Fehlleistung, die nicht nur Menschen in zukünftigen Kriegen schadet, sondern auch all denen, denen hier und jetzt mit einer humanistischen oder auch „lediglich" mit einer solidarischeren Finanzpolitik geholfen werden könnte. Ziel der NATO-Aufrüstung ist die Umsetzung der 2010 verabschiedeten Strategie eines doppelt entgrenzten Interventionsbündnisses, das global agieren und weit über die Bündnisverteidigung hinaus in Aktion treten kann. Wie am Beispiel der Bundeswehr erkennbar, sollen Dislozierungsfähigkeiten für eine Armee im globalen Einsatz geschaffen werden und über die Technisierung des Krieges – z. B. mittels Kampfdrohnen oder verbesserter Informationsgewinnung, -auswertung und -verwertung – die eigenen Verluste minimiert werden.

Das die NATO-Staaten verbindende Großprojekt, die Errichtung eines Raketenabwehrschirms zur Verhinderung der atomaren Erstschlagsfähigkeit Russlands, wird das geopolitische Gefüge nachhaltig stören, und dies provoziert heute bereits Aufrüstungsschritte anderer Länder. Eine wichtigere Rolle wird auch Cyberwarfare für Präventivschläge und Kriegsvorbereitungen spielen. Die Versicherheitlichung von Gesellschaftsbereichen und der damit einhergehende Führungsanspruch der Militärs weiten sich nicht nur in der Digitalwelt, sondern auch in fast allen anderen Bereichen aus. Die Dimensionen der Militarisierung gesellschaftlicher Bereiche lassen sich erahnen, wenn man einige der Aufgabenbereiche nimmt, die sich die NATO selbst gegeben hat: So definiert das Bündnis in einem neuen Papier unter anderem den Klimawandel, den Zugang zu Ressourcen und die Migration als Sicherheitsfaktoren. In diesem Sinne bestimmt das Weißbuch zur Sicherheitspolitik Deutschlands und zur Zukunft der Bundeswehr von 2006 zur staatlichen Sicherheitsvorsorge eine „vernetzte Sicherheit": Zur Konfliktverhütung und Krisenbewältigung wird eine enge Integration politischer, militärischer, entwicklungspolitischer, wirtschaftlicher, humanitärer, polizeilicher und nachrichtendienstlicher Instrumente gefordert.

Hochschulen – Dienstleister eines neuen Todes gegen das alte Leben?

Die Wechselwirkung zwischen der von den Nationalstaaten und von den Militär- und Verteidigungsbündnissen angestoßenen Rüstungsspirale und der universitären und außeruniversitären Rüstungsforschung ist ein von der Friedenswissenschaft kaum wahrgenommenes Forschungsthema. So gibt es zum Beispiel wenig wissenschaftliche Erkenntnis über einen Zusammenhang zwischen der Prekarisierung von WissenschaftlerInnen und der Bereitschaft, Drittmittel für Rüstungsforschung einzuwerben und anzunehmen. Dagegen steht die Prekarisierung von WissenschaftlerInnen selbst oftmals im Mittelpunkt wissenschaftlicher Untersuchungen. Durch die Ökonomisierung der Wissenschaft und die verstärkte Ausrichtung des wissenschaftlichen Betriebs auf die Verwertungslogik und Profitabilität werden starke Zwänge auf WissenschaftlerInnen ausgeübt und neue Abhängigkeitsverhältnisse aufgebaut. Sich diesen zu entziehen wird vor allem jungen WissenschaftlerInnen immer schwieriger. Oftmals verhindert oder behindert die Prekarisierung hochschulpolitisches Engagement und trägt zu einer Entdemokratisierung von Hochschulen bei. Die Dimension der Aufrüstung sollte der Friedenswissenschaft Anlass sein, sich mit der Auswirkung auf Wissenschaft und Forschung stärker zu befassen.

Im deutschen Hochschulraum werden Vorhaben der Rüstungsforschung im Wesentlichen durch parlamentarische Anfragen, Senatsanfragen an Universitäten sowie durch investigativen Journalismus bekannt. Angaben zu den Finanzvolumina und zu den Auftragnehmern militärischer Forschungs- und Entwicklungsvorhaben, die im Bundeshaushaltsgesetz in Kapitel 1420 unter *Wehrforschung, wehrtechnische und sonstige militärische Entwicklung und Erprobung* aufgeführt sind, unterliegen dem Geheimnisschutz. 2012 betrugen die Gesamtausgaben des BMVg für diesen Bereich knapp eine Milliarde Euro. Wofür das Geld im Einzelnen verwendet wurde, muss in minutiöser Recherche herausgefunden werden.

Es ist auffällig, dass Rüstungsforschung in allen wissenschaftlichen Bereichen stattfindet, natürlich an erster Stelle immer noch im MINT-Bereich, aber zunehmend auch in den Geistes-, Sozial- und Rechtswissenschaften. Forschung im Dienste des Militärs betrifft heute bei Weitem nicht mehr allein technische Probleme wie beispielsweise die Verbesserung der Sensorik für kleine Flugobjekte, sondern auch so unterschiedliche Themen wie die Akzeptanz von Interventionsarmeen, für Militärinterventionen relevante völkerrechtliche Fragen oder Methoden der psychologischen Aufstandsbekämpfung. In vielen Fällen lassen sich durch die Beschreibung des Forschungsprojekts Rückschlüsse auf einen Rüstungsforschungshintergrund ziehen – aber nicht in allen Fällen. Spätestens jedoch beweist die Quelle der Drittmittel auch bei zivil anmutenden Vorhaben ein primäres Interesse der Militärs, wenn wir einmal davon ausgehen, dass beispielsweise das Verteidigungsministerium wenig Interesse an einer Forschung hat, deren Ergebnisse voraussichtlich keinen militärischen Nutzen haben werden. Dennoch ist meist eine Prüfung des Einzelfalls notwendig.

Wer Rüstungsforschung betreibt, stellt seine Vorhaben nicht selten als Grundlagen-, Dual-Use- oder Sicherheitsforschung dar, um den militärischen Charakter zu verschleiern oder gar abzustreiten. Will man Forschung in zivile und militärische Forschung

durch rote Linien trennen, bedarf es Kommissionen, welche Zugriff auf unterschiedlichstes Expertenwissen haben und dieses diskursiv zur Entfaltung bringen. Aufgrund der mit militärisch geförderten Drittmittelprojekten verbundenen Geheimhaltung wird es hier jedoch schwer werden, objektives Wissen zur Geltung zu bringen. Auch hier wäre ein Ansatzpunkt für die Friedenswissenschaften, um einen Beitrag zu mehr Erkenntnis in dem Dickicht der Rüstungsforschung zu leisten.

Insbesondere bei Dual-Use- und Sicherheitsforschung wäre wissenschaftliche Expertise zur Einordnung von Forschungsprojekten hilfreich. Denn die Forschungsrahmenprogramme der EU sowie der BRD streben beabsichtigt eine multiple Einsetzbarkeit von Forschungsergebnissen an, und das provoziert das Verschwimmen der Grenzen zwischen ziviler und militärischer Forschung. Nach dem Spin-off-Prinzip soll militärisches Wissen der Zivilgesellschaft nutzen, nach dem Add-on-Prinzip sollen zivile Fähigkeiten militärischen Zwecken dienen. Das Bundesforschungsministerium legt im *Horizon-2020*-Forschungsrahmenprogramm ein eigenes Programm für Sicherheitsforschung auf. Rüstungsforschung und -technologie sollen auf europäischer Ebene durch die Europäische Verteidigungsagentur koordiniert werden. Innerhalb der NATO wird von zivil-militärischen Fähigkeiten und einer besseren und effektiveren Koordination der Entwicklung aller relevanten Fähigkeiten gesprochen.

In die Logik der Ausweitung militärischer (Forschungs-)Vorhaben in Deutschland passen die Ende 2013 von NDR und SZ an 22 deutschen Universitäten und mehreren Forschungsinstituten aufgedeckten Rüstungsforschungsprojekte des Pentagons. Zwar handelte es sich bei den Fördermitteln nicht um hohe Summen. Dies ist jedoch eine ‚Türöffnerpolitik'. Brücken vom Militär zur Wissenschaft werden gebaut, um eine Verstetigung der Kooperation zwischen Hochschulen und Militär zu erreichen und sowohl die Militarisierung der Wissenschaft als auch eine Verwissenschaftlichung des Krieges voranzutreiben. Wenn zehn dieser 22 Hochschulen Zivilklauseln besitzen und dennoch Forschungsgelder des Pentagon annahmen, stellt sich die Frage, wie ernst deutsche Hochschulen ihre selbstauferlegten Regeln nehmen und warum kein Kontrollmechanismus auf die Quelle dieser Forschungsgelder aufmerksam wurde.

Ein immer stärker in den Fokus der Rüstungsindustrie rückender Wissenschaftsbereich ist die Informatik. Im digitalen Zeitalter spielt die IT so wie im zivilen Alltagsleben auch im militärischen Umfeld eine immer bedeutendere Rolle. Allen voran wird die Versicherheitlichung ziviler Bereiche immer stärker ausgebaut. So ist z. B. 2010 unter der Beteiligung der Universität Potsdam, EADS, Rolls-Royce und IABG das Brandenburgische Institut für Gesellschaft und Sicherheit (BIGS) gegründet worden. Es versteht sich als Institut für die zivile Sicherheitsforschung und forscht und lehrt u. a. zum Schutz kritischer Infrastrukturen. Seitdem das BMBF im Jahre 2007 das Rahmenprogramm *Forschung für die zivile Sicherheit* aufgelegt hat, steigt die Anzahl an Sicherheitsforschungsprojekten. Geht es nach der Bundesregierung, wird Deutschland in den nächsten Jahren zu einem Leitmarkt für Sicherheitstechnologie. Neben dem Schutz vor Naturkatastrophen stehen auch internationale Handels- und Reiseströme, Warenketten, der weltweit operierende Terrorismus und die organisierte Kriminalität im Fokus der von der Bundesregierung geförderten Sicherheitsforschung. Der Schritt zur Rüstungsforschung ist nicht weit, sodass mit der Sicherheitsforschung ein neuer Dual-Use-Forschungsbereich geschaffen wurde, der in einigen Bereichen sogar offen Rüstungsforschung betreibt. Dies belegen nicht nur die Akteure der Sicherheitsforschung, sondern auch deren Forschungsgebiete. „Freie Kommunikation", eines der Themen des Rahmenprogramms *Forschung für zivile Sicherheit*, wird beispielsweise am *Institute of Computer Science* der Universität Bonn innerhalb von Projekten über robuste Verfahren zur Erkennung von Angriffen sowie über sinnvolle Gegenmaßnahmen in taktischen *Multi-Hop*-Netzen erforscht. Passend dazu sind auf der Website der Universität Soldaten im Einsatz abgebildet. Projekttitel sind u. a. *Wireless Sensor Network Lab* oder *Mobile Intrusion Detection for Tactical Environments*. Auch im Institut für Nachrichtentechnik der Universität Karlsruhe wird auf diesem Bereich geforscht, genauer an *Cognitive Radio*, einem rechnergestützten Breitbandkommunikationssystem für multinationale Interventionstruppen. Ein ähnliches multilinguales Forschungsprojekt an der Universität Saarbrücken wurde vom *U.S. Army Research Laboratory* 2013 mit ca. 125.000 US-Dollar finanziert. Die Liste lässt sich weiterführen und um die Bereiche Cyberwarfare, Überwachung, Nanotechnologie und autonome Maschinen ergänzen. Eine intensivere Auseinandersetzung mit Rüstungsforschung im Bereich der Informatik und IT sowie mit der Sicherheitsforschung ist vonnöten, die FIfF-Kampagne *Cyberpeace* mit Sicherheit ein guter Anfang, der hoffentlich ausgeweitet wird und Nachahmer findet.

Friedenspolitisches Engagement ist auch an den Hochschulen nötig

Die in Universitäten und Forschungsstätten akkumulierte Intelligenz ist wichtig für die zukünftige Entwicklung einer Gesellschaft. Auf welche Seite sich die Intelligenz schlägt, ob zum

Reiner Braun und Lucas Wirl

Reiner Braun ist Geschäftsführer der IALANA und im *Netzwerk Hochschulen für den Frieden – Ja zur Zivilklausel* aktiv.

Lucas Wirl ist Geschäftsführer der *NaturwissenschaftlerInnen-Initiative Verantwortung für Frieden und Zukunftsfähigkeit* (NatWiss) und ebenfalls im *Netzwerk Hochschulen für den Frieden – Ja zur Zivilklausel* aktiv.

Krieg oder zum Frieden, ist ausschlaggebend für die Gesellschaft und das gesellschaftliche Klima. 1914 wurden im August die Seminare geschlossen und die Studierenden zogen gemeinsam in den Ersten Weltkrieg. Sie folgten den nationalistischen Prophezeiungen, die ihre Professoren und ihre Hochschule vertraten.

Produktionsfähigkeit innovativer Produkte erfordert einen Vorlauf der Forschung und Entwicklung von zehn bis fünfzehn Jahren. So wird an den von Verteidigungsministerin von der Leyen heute neu beschafften Bundeswehrmaterialien bereits seit den 1990er-Jahren geforscht und weiterentwickelt. Entsprechend kann aus den politischen Vorgaben und den darauf fußenden Forschungsprogrammen, auch an den sich auf rüstungs- und sicherheitsrelevante Aufgabenstellungen ausdehnenden Programmen öffentlicher Forschungseinrichtungen und Wissenschaftsinstitutionen, ein qualitativer Sprung in der Rüstungstechnik prognostiziert werden. Dies zu verhindern oder zumindest einzudämmen ist eine große Herausforderung für die Friedensbewegung.

Zivilklauseln sind ein wichtiges Mittel, Militarismus an den Hochschulen in die Öffentlichkeit zu bringen und die Diskussion darüber wach zu halten.[1] 21 Zivilklauseln sind mittlerweile an deutschen Hochschulen etabliert, 51 weitgehend studentische Zivilklausel-Bewegungen existieren im gesamten Bundesgebiet. Sie sind von besonderer Bedeutung, um den Diskurs über friedenspolitische und gesellschaftspolitische Themen, über Krieg und Frieden in die Universitäten zu transportieren. Mit dem *Netzwerk Hochschulen für den Frieden – Ja zur Zivilklausel* gibt es ein Dach, unter dem Studierende, GewerkschaftlerInnen und Friedensbewegte um eine friedliche und nachhaltige Ausrichtung von Wissenschaft ringen. Auch einzelne WissenschaftlerInnen sind in diesem Netzwerk engagiert. Das Einbringen von Wissen und Expertise, das Einbinden von ForscherInnen und Lehrenden ist hier von elementarer Bedeutung, eine Stärkung unbedingt vonnöten. Der Diskurs über den Sinn und Zweck der Wissenschaft und über die Verantwortung der Wissenschaft muss noch viel weiter auf die Tagesordnung des wissenschaftlichen Betriebes gebracht werden. Dies geht nicht ohne die ProfessorInnen und ohne den Mittelbau. Es ist ohne spezifisches Expertenwissen nicht möglich, Rüstungsforschung als solche zu erkennen und Forschungsprojekte entsprechend einzuordnen. Ein intensiveres Eingreifen der Wissenschaft in gesellschaftliche Konflikte wäre sehr wünschenswert. Denn nur wo die Zivilklausel ein aktiver, verankerter Teil der Kultur der Universität und der Wissenschaft ist, kann sie zur Entfaltung kommen.

Krieg erfordert eine „innere Militarisierung". Die Menschen müssen in den Köpfen bereit sein für den Krieg. Rüstungsforschung in all seinen Facetten bereitet nicht nur den Weg zum „intelligenteren" Krieg und zu technisch raffinierterem Töten, sie ist auch ein Mittel zur Erzeugung von Akzeptanz für Krieg und Gewalt und damit auch zu ideologischer Kriegsvorbereitung. „Du Forscher im Laboratorium. Wenn sie dir morgen befehlen, du sollst einen neuen Tod erfinden gegen das alte Leben, dann gibt es nur eins: Sag NEIN", schreibt Wolfgang Borchert in seinem Gedicht „*Dann gibt es nur eins!*" – dieser Aufruf ist heute aktueller denn je.

Anmerkungen

1 *Reiner Braun et al.: Zivilklauseln – Lernen und Forschen für den Frieden. Wissenschaft & Frieden 2-2015, Dossier 78*

Jürgen Scheffran

Vom vernetzten Krieg zum vernetzten Frieden: Die Rolle von Wissenschaft und Technik

In Grenzbereichen des westlichen Zivilisierungsprozesses entstehen immer neue Muster von Gewalt und Krieg. Mithilfe von Technik durchdringen sie alle Räume und Dimensionen der Gesellschaft, von kleinsten Räumen über unsere Lebenswelt bis zu unserem Planeten und dem Weltraum. Die Vernetzung zwischen Krieg und Gesellschaft betrifft die Ursachen und Folgen ebenso wie ihre Rechtfertigung und Realisierung, die Rolle zivil-militärischer Verflechtungen und die besondere Bedeutung der wissenschaftlich-technischen Entwicklung. Zur Problemlösung bedarf es neuer Konzepte nachhaltigen und vernetzten Friedens.

Ursachen, Folgen und Rechtfertigungen vernetzter Kriege

Die heutigen Krisen und Konflikte lassen sich nur verstehen, wenn die systemischen Ursachen in den Blick genommen werden. Im Prozess der expansiven Globalisierung, die die vergangenen Jahrzehnte und Jahrhunderte beherrscht hat, konnten die westlich geprägten Industriestaaten eine ökonomische und technologische Dominanz entwickeln, deren Akzeptanz durch universelle Prinzipien und Werte (Freiheit, Gleichheit, Demokratie, Wohlstand, Toleranz, Menschenrechte und Gewaltfreiheit) hergestellt wird. Während das westliche Erfolgsmodell eine hohe Anziehungskraft ausübt und für einen relevanten Teil der Menschheit Wohlstand bedeutet, ist es im globalen Maßstab widersprüchlich.

Basierend auf dem Prinzip permanenten Wachstums gerät die kapitalistische Wirtschaft in Widerspruch zu natürlichen Grenzen, allen Versuchen der wissenschaftlich-technischen Naturbeherrschung zum Trotz. Zudem führt sie zur Akkumulation von Wohlstand in den Händen weniger auf Kosten vieler, die daran nur wenig oder gar nicht teilhaben. Dies steht in Widerspruch zum propagierten Wertesystem, das nur für einen Teil der Weltgesellschaft realisierbar ist. Das Versprechen von Wohlstand, Freiheit und Demokratie wird zwar über die Massenmedien in alle Welt transportiert, lässt sich aber nicht überall einlösen. Aufgrund seiner Widersprüchlichkeit erzeugt das globalisierte Wachstumsmodell Differenzen, Grenzen und Spannungen, die Auslöser für Konflikte und Krisen sind.

In diesem Spannungsgefälle versucht das System eine Stabilisierung nach innen mit einer Abgrenzung nach außen zu verbinden, wobei die Grenzen dynamisch auf Druck von beiden Seiten reagieren. Das westliche Entwicklungsmodell hat in den vergangenen Jahrzehnten eine beispiellose Expansion erlebt, wobei das Überschreiten von Grenzen mit teilweise gewalttätigen Konflikten verbunden war. Hierzu gehören die Konflikte im Gefolge des Ost-West-Konflikts im ehemaligen Jugoslawien und in der Sowjetunion ebenso wie die Konflikte in Nahost und in Nordafrika im Gefolge des *Arabischen Frühlings*. Hier zeigten sich politische Grenzen der Expansion, etwa durch Konkurrenzen um Einflusszonen mit anderen Mächten wie Russland und China oder durch eine fehlende Akzeptanz gegenüber westlichen Werten. Zu nennen sind religiöse Differenzen, die zum Nährboden für Islamismus und Terrorismus werden, rechtspopulistische Strömungen gegen Gleichheit und Toleranz ebenso wie radikale Bewegungen gegen Ausbeutung und Ungerechtigkeit oder auch Differenzen zwischen moderner Stadtbevölkerung und traditioneller Landbevölkerung in vielen Teilen der Erde. Verstärkt werden solche Spannungen durch Krisenerscheinungen im kapitalistischen System, die dessen Attraktivität untergraben wie die Finanzkrise von 2008 oder die Griechenlandkrise, die tief gehende Bruchlinien in Kernzonen des Systems offenbaren und Widerstände verstärken. Langfristig konfliktär sind die ökologischen Grenzen des Wachstums aufgrund der begrenzten Verfügbarkeit natürlicher Ressourcen und der Klimawandel, die dem Streben nach Wohlstand für alle im Wege stehen.

Das komplexe Ursachengeflecht heutiger Krisen schafft Auslöser für Gewaltkonflikte, die sich zu kaum lösbaren vernetzten Kriegen aufschaukeln können. Die Konfliktlinien verlaufen überall dort, wo das Spannungsgefälle widersprüchlicher Tendenzen am größten ist: im Mittelmeerraum zwischen Südeuropa, Nordafrika und Nahost, innerhalb der Ukraine zwischen Ost und West, in den Drogenanbaugebieten Afghanistans und Mittelamerikas und in den Rohstoffgebieten Afrikas, in den Regenwäldern der Welt und in ökologisch degradierten Zonen, ebenso in den Slumgebieten der Megastädte, an den Bruchlinien der Religionen und generell zwischen Arm und Reich.

Das System reagiert auf Krisenerscheinungen und damit verbundene Risiken mit immer neuen Interventionen, die eine Kontrolle herstellen sollen. Wenn von einer Verantwortung Deutschlands in der Welt die Rede ist, geht es weniger um die eigene (Mit-) Verantwortlichkeit für die Krisen der Welt, sondern vielmehr um die Verantwortbarkeit von Eingriffen, ungeachtet der Frage, ob damit Öl ins Feuer gegossen wird oder eigene Prinzipien (etwa gegen Gewalt) über Bord geworfen werden. Der Verweis auf die moralische Verantwortung ermöglicht Handlungen gegen jedwede Bedrohung eigener Werte von außen und lenkt zugleich ab von den systemimmanenten Gefährdungen eben dieser Werte von innen, durch Demokratieabbau, Geheimdienste, Umweltzerstörung und Ungerechtigkeit. So wird es möglich, zur Abwehr von Terroristen oder Migranten weit höher in einen Sicherheitsapparat zu investieren als in die Vermeidung des Klimawandels oder ökonomischer Krisen, selbst wenn diese weit größere Probleme darstellen und Ursachen eben jener Phänomene sind.

Netzwerke der Gewalt

So sehr bei vernetzten Kriegen die Ursachen, Folgen und Rechtfertigungen aufs Engste mit den gesellschaftlichen Strukturen verbunden sind, so sehr gilt dies für ihre Umsetzung und Durchführung. Wenn die gesamte Gesellschaft vom Krieg betroffen ist, verliert die klassische Trennung zwischen Soldat (lat. *miles*) und Bürger (lat. *civilis*) an Bedeutung. Die „Bürger"-Kriege in Ruanda und Ex-Jugoslawien ebenso wie die gewaltsamen Konflikte in Afghanistan, im Libanon, in Syrien oder im Irak durchziehen die Gesellschaften dieser Länder. Ohne klare Fronten agieren Streitkräfte innerhalb der Gesellschaften und sind damit deren Logiken unterworfen. Das Gegenstück zu einem entgrenzten, alles durchdringenden Krieg findet sich auch in den westlichen Industrienationen, trotz aller Versuche der Abgrenzung und Ausgrenzung. Die Terroranschläge des 11. September, die auch in den USA vorbereitet wurden, verwendeten zivile Passagierflugzeuge, um zivile Ziele inmitten einer Großstadt zu treffen. Der daraufhin erklärte „Krieg gegen den Terror" durchzieht die Zivilgesellschaften des Westens, lässt Koffer in einem Flughafen oder Bahnhof oder jede Cyberattacke als möglichen Teil eines kriegerischen Gewaltakts erscheinen. Die Flüchtlinge aus den Krisengebieten, die nach Europa „vordringen", werden zu unfreiwilligen Kombattanten an einer „Heimatfront", an der innere und äußere Sicherheit verschmelzen, was im Begriff der *Homeland Defense* in den USA offenkundig wird. Bezeichnenderweise war die erste Belastungsprobe für die Heimatverteidigung in den USA nicht ein Terroranschlag, sondern eine Naturkatastrophe, der Wirbelsturm *Katrina* 2005. Sie ist gründlich schief gegangen.

Noch desaströser war der Versuch der USA, mit überwältigender Militärmacht den Irak besetzt zu halten – ignorierend, dass eine Demokratisierung des Irak eine gesellschaftliche Aufgabe ist, die ganz andere, vor allem zivile Mittel erfordert. Statt den

Jürgen Scheffran

Jürgen Scheffran ist Professor am Institut für Geographie der Universität Hamburg. Er leitet dort die Forschungsgruppe *Klimawandel und Sicherheit*. Er arbeitet in der Redaktion der Zeitschrift *Wissenschaft und Frieden* mit und ist Mitglied in verschiedenen Wissenschaftsorganisationen (Natwiss, VDW, INES, BdWi, FONAS).

Irak zu „befrieden“ wurde noch Öl ins Feuer gegossen. Der gewaltsame Widerstand gegen die als Besatzer empfundenen US-Truppen konnte sich an jeder Hausecke oder Straßenkreuzung entzünden und hat letztlich zur Entstehung des *Islamischen Staates* beigetragen.

Damit einher ging eine Privatisierung der Sicherheitsdienste, das Entstehen moderner Söldnerheere. Die Fraktionierung der Gewaltstrukturen bringt unermessliches Leid über die Zivilbevölkerung, sie zerstört soziale und politische Strukturen – u. a. in zahlreichen Ländern Afrikas. Dauerkriege, verbunden mit Massenmord und millionenfacher Flucht und Vertreibung, sind die Folge. An der gesellschaftlichen Basis wächst damit ein Potenzial der Verarmten und Entwurzelten, der Missachteten und Empörten heran, das einen Nährboden für jede Form der Radikalität bietet, dem Islamismus Menschen zutreibt. Durch Vernetzung kann die Unzufriedenheit auf der lokalen Ebene in nationale und globale Netzwerke der Gewalt einbezogen werden. Verbrecher- und Terrornetze agieren weltweit, der Drogen- und Waffenhandel floriert und ist über eine Schattenwirtschaft mit der globalen Ökonomie verknüpft.

Zivil-militärische Verflechtungen

Die Vernetzung des Krieges betrifft auch die Vorbereitung, Planung und Durchführung von Gewalteinsätzen in Industrieländern, die sich gesellschaftliche Strukturen zunutze machen und mit struktureller Gewalt einhergehen. Dies erfolgt unter Ausnutzung fließender Übergänge zwischen zivilen und militärischen Infrastrukturen, inklusive Wissenschaft und Technik, Information, Kommunikation und Medien, Wirtschaft und kritischen Infrastrukturen bis hin zu den politischen Entscheidungsebenen.

Im Rahmen einer gesellschaftlichen Gesamtmobilisierung nutzt das Militär die zivil-militärische Zusammenarbeit, die dem Militär neue Spielräume eröffnet und zivile Ressourcen in die Militärplanung einbezieht. Entsprechend widmet sich die Bundeswehr verstärkt der Koordinierung zivil-militärischer Beziehungen sowie der Unterstützung von bewaffneten Streitkräften und der zivilen Umgebung. Hierzu gehören die Koordinierung von Planungen der zivilen und militärischen Verteidigung ebenso wie Vorsorgemaßnahmen für die Zivilbevölkerung und die Streitkräfte, die Einbindung der Streitkräfte in die Zivil- und Katastrophenschutzplanung und in die Einsatzplanung bei sogenannten Großschadensereignissen. Im Weiteren geht es um die Zusammenarbeit in allen Bereichen des Umweltschutzes, der Raumordnung und der Konversion.

Dabei wird ausdrücklich zwischen Truppenführung im Kampf und bei Friedensmissionen unterschieden, wobei der Kampf nicht nur auf herkömmliche Kriege, sondern mit dem Oberbegriff des bewaffneten Konfliktes auf alle Erscheinungsformen sozialer Gewalt ausgedehnt wird, die mit Waffen ausgefochten werden. Bei der Informationsgewinnung wird auch auf internationale und Nicht-Regierungs-Organisationen zurückgegriffen, die über zusätzliche Informationen verfügen. Damit verbundene Probleme bei der Einbindung in militärische Befehlsstrukturen werden anerkannt, das unterschiedliche Selbstverständnis ziviler Organisationen und das Primat der Politik werden nicht bestritten.

Auch wenn eine Zusammenarbeit zwischen zivilen und militärischen Einrichtungen bei Friedensmissionen erfolgt, ist die grundsätzliche Unvereinbarkeit ziviler und militärischer Aufgaben und Einsatzmittel nicht zu übersehen. Nicht geeignet ist das Militär für den Prozess der Staatenbildung und Demokratisierung, für den Aufbau einer Volkswirtschaft, für die nachhaltige Ressourcensicherung und für den Umweltschutz. Genauso wenig lassen sich zivilgesellschaftliche Kräfte einfach in militärische Strukturen und in den gewaltsamen Konfliktaustrag einbinden. Die Logik betriebswirtschaftlicher Rationalisierung verbirgt, dass sich das Militär ziviler Ressourcen bedient, um eigene Budgets zu schonen. Im Kontext von Krisenreaktionskräften und Antiterrorkriegen kann eine gesellschaftliche Mobilisierung unter militärischen Kalkülen eine Totalisierung von Konflikten befördern und den Einsatz von Gewalt legitimieren. Statt Unterschiede zwischen zivil und militärisch zu verwischen, sollten sie deutlicher gemacht werden.

Wissenschaft und Technik in vernetzten Kriegen

Wissenschaft und Technik spielen eine Schlüsselrolle im Netz globalisierter Gewalt. Getrieben von dem Streben nach militärischer Überlegenheit macht sich das Militär die Ergebnisse wissenschaftlicher Forschung immer umfassender zunutze, von der Grundlagenforschung bis hin zur anwendungsnahen Entwicklung. Atomwaffen und Raketen, Satelliten, Anti-Satellitenwaffen, Raketenabwehr und Lasertechnologie, technische Intelligenz, Drohnen, Robotik und Cyberspace erlauben Macht- und Gewaltprojektionen über den ganzen Planeten und in den erdnahen Weltraum. Die Hochtechnologieentwicklung wird als Ganzes militärischen Verwertungsinteressen unterworfen, unter Ausnutzung des zivilen Technologiezweigs im Dual-Use-Sinn. Nach Ende des Ost-West-Konflikts wurde aufgrund der Notwendigkeit von Kosteneinsparungen und geringerer öffentlicher Akzeptanz für den Militärsektor die Ambivalenz der Forschungsergebnisse systematisch genutzt.

Dies betrifft zum einen die globale Vernetzung moderner Transport-, Informations- und Kommunikationssysteme ebenso wie die Verschmelzung von Mikro-, Nano- und Biotechnologien, die Macht- und Gewaltprojektionen in kleinsten Räumen erlaubt. Sie verknüpfen die Globalisierung der Gewalt mit der Miniaturisierung von Gewalt, was in den Informationskriegen auf unseren Computern ebenso zum Ausdruck kommt wie im Krieg der Mikroben oder Mini-Kampfroboter. Durch sie findet der Krieg Einzug in unseren Nahbereich, in unsere Wohnung, ja in den menschlichen Körper, der über technische Systeme mit globalen Strukturen vernetzt ist. Globale (Un-)Sicherheit und menschliche (Un-)Sicherheit sind so aufs engste verbunden.

Technisch vermittelte Netzwerke haben einen immer wichtigeren gesellschaftlichen Stellenwert. Auch und gerade in den Kriegen des 21. Jahrhunderts spielt eine technologisch realisierte Vernetzung eine zentrale Rolle, von der Vernetzung der Gefechtsfelder zu Luft, Wasser und Boden, im Weltraum und im Cyberspace über die Robotisierung und Automatisierung bis hin zur Heimatfront und zur Medienwelt.

Technikentwicklung zwischen Wirtschaftswachstum und Naturzerstörung

Der Multiplikator- und Vernetzungseffekt der Technik spielt eine besondere Rolle in der auf Wachstum ausgerichteten kapitalistischen Ökonomie, die technische Produktionsmittel in Form von Kapital anhäuft. Das Baconsche Programm der wissenschaftsgeleiteten Technikentwicklung konnte in Teilen der Welt die Mühsal der menschlichen Existenz erleichtern und dafür sorgen, dass trotz begrenzter Ressourcen rund zehnmal so viele Menschen auf der Erde existieren können wie vor der Industrialisierung. Es stellt sich die Frage, wie lange sich Wohlstand noch steigern lässt, ohne dass die Folgen der Technik dessen Grundlagen untergraben. In der wirtschaftlichen Konkurrenz führen effektivere Produktionstechniken zu Wettbewerbsvorteilen durch Profitsteigerung und letztlich zur Ausschaltung von bzw. Fusion mit Konkurrenten, um deren Kapazitäten einzubinden – ein Äquivalent zur Konzentration in der Gewaltspirale.

Eine zentrale Rolle spielt Technik auch für den Konflikt zwischen Mensch und Natur. Dies betrifft zum einen die technischen Systemen zugrunde liegenden natürlichen Faktoren und Ressourcen, zum anderen die Wirkung des Technikeinsatzes auf die Natur, die zur Zerstörung von Ökosystemen, Lebensräumen und Artenvielfalt führt und diese zu Konfliktfeldern macht. Der von Malthus vor mehr als 200 Jahren prognostizierte baldige Zusammenbruch der menschlichen Population konnte mit neuen Erfindungen immer wieder verschoben werden. Ging es bei der Industrialisierung darum, Naturressourcen in großem Maßstab in die Erzeugung von Produktions- und Destruktionsmitteln zu schieben, so werden heute die Grenzen des expansiven und verschwenderischen Umgangs mit der Natur in Umwelt- und Ressourcenkonflikten sichtbar.

Neben dem Naturverbrauch auf der Verursacherseite tritt die destruktive Seite der Technik auch auf der Folgenseite immer deutlicher hervor. Dies wird sichtbar bei der fossilen Energieversorgung, die ein breites Feld für Technikkonflikte aller Art war und ist, so bei der Einbeziehung von Kohle, Erdöl und Erdgas – als Ressource wie als Konfliktgegenstand – in die Kriegführung im Ersten und Zweiten Weltkrieg, im Kalten Krieg sowie in diversen Kriegen in Nahost und in der Kaukasusregion. Unkonventionelle Methoden der Gewinnung fossiler Energieträger sind nicht nur mit steigenden Kosten, sondern auch mit Umweltfolgen verbunden, so bei der Gewinnung von Ölsänden, Schiefergas oder Erdgas durch Fracking, was ebenso zu Protesten führt wie Ölbohrungen zur See oder in der Arktis.

Am deutlichsten wird dies beim Klimawandel, der durch die Freisetzung fossiler Treibhausgasemissionen das gesamte Erdsystem zu destabilisieren droht und damit neue Sicherheitsrisiken und Konfliktfelder eröffnet. Erscheint der Klimawandel zunächst noch als unbeabsichtigte Nebenfolge des fossilen Entwicklungspfades der Menschheit, so könnte der Versuch, mit Hilfe von Geoengineering im Anthropozän die Kontrolle über den Planeten zurückzugewinnen, zum Fiasko einer wider die Natur handelnden Technikgläubigkeit geraten.

Risikogesellschaft, technische Verwundbarkeit und gesellschaftliche Umbrüche

Auch das Versagen der Technik birgt erhebliche Risiken und Konfliktpotenziale, insbesondere in großtechnischen Systemen, in denen sich kleine Fehler zu Katastrophen aufschaukeln können. Spektakuläre Unfälle mit Risikotechnologien (Bhopal, Challenger, Tschernobyl) zeigten, dass Großtechnologien (Chemie- und Atomtechnik, Bio- und Gentechnologie, Luft- und Raumfahrt, Rüstungstechnik) nicht vollständig beherrschbar sind und ein „Restrisiko“ schaffen, das mit Naturkatastrophen vergleichbar sein kann. Bei der Kernenergie treten Risiken über die gesamte nukleare Kette auf: von Uranminen über Unfälle beim Transport radioaktiver Materialen bis zur ungelösten Endlagerproblematik. Da bei komplexen Systemen nicht alle Eventualitäten vorherbestimmbar sind, genügt ein geringfügiges Ereignis, um eine Ereigniskette auszulösen, die bei gekoppelten Mensch-Maschine-Systemen als „normale Katastrophe“ erscheint.

Ein spektakuläres Beispiel für eine Risikokaskade, in der Natur und Technik zusammenwirkten, war das Erdbeben in Japan vom 11. März 2011, das eine Kette von Ereignissen mit globaler Wirkung in Gang setzte. Die Tsunami-Welle zerstörte in Fukushima mehrere Reaktoren, deren radioaktives Inventar sich über die Atmosphäre und den Ozean nicht nur lokal, sondern auch global ausbreitete. Direkt oder indirekt davon betroffen waren das japanische Stromnetz, die Nuklearindustrie, Aktienmärkte, der Ölpreis und die Weltwirtschaft. Autohersteller und Elektronikfirmen drosselten weltweit die Produktion, weil wichtige Teile aus Japan nicht mehr geliefert wurden. Die Schockwellen der Nuklearkatastrophe lösten in Deutschland die Energiewende aus. Diese Katastrophe zeigt eindrücklich, wie ein Einzelereignis kaskadenartig über globale Netzwerke verschiedene Prozessketten in Gang setzen und miteinander verknüpfen kann. Sie zeigt auch, wie die Risikohaftigkeit von Technik Widerstände und Proteste auslöst.

Neben Erdbeben oder technischen Unfällen können auch Klimawandel und Wetterextreme kritische Infrastrukturen und Versorgungsnetze treffen, die für die Aufrechterhaltung menschlicher Existenz wichtig sind. Hierzu gehören Systeme für die Versorgung mit Wasser, Nahrung und Energie, mit Gütern und Dienstleistungen, Systeme für die Bereitstellung von Kommunikations-, Gesundheits-, Transport- und Sicherheitsdienstleistungen sowie menschliche Siedlungen und politische Institutionen. Dabei ist nicht nur das Versagen von Teilsystemen von Bedeutung, sondern auch die Möglichkeit, dass sich das Versagen über Kopplungen ausbreiten und das gesamte System gefährden kann. So führten Wetterextreme in Deutschland, wie die Hitzewelle 2003, die Sturmflut 2013 oder das Elbehochwasser im selben Jahr zu Beeinträchtigungen des (Zug-)Verkehrs und der Energieversorgung. Im November 2005 ereignete sich nach heftigen Schneefällen in Nordrhein-Westfalen und Niedersachsen einer der größten Stromausfälle in der deutschen Geschichte.

Mit der wachsenden Abhängigkeit von technischen Infrastrukturen nimmt auch ihre Verwundbarkeit gegenüber Angriffen oder Missbrauch zu. Wenn der Mensch Teil der Maschine ist, kann er sie willentlich in den Untergang steuern, indem die ein-

gebauten Wirkmechanismen einem von den Konstrukteuren nicht geplanten Zweck zugeführt werden. Durch den „Missbrauch“ wird aus der Möglichkeit einer nicht intendierten Nebenfolge die konkrete Gefahr, dass diese absichtlich ausgenutzt wird. Flugzeuge, Fahrzeuge, Schiffe, Reaktoren, die Chemieindustrie, das Internet oder Stromnetze können nicht nur Ziel von Gewalthandlungen sein, sondern auch selbst zur Waffe werden. Die von Allmachtsphantasien getriebene Wahnsinnstat wird nicht nur ergriffen, weil sie gewollt ist, sondern auch, weil sie durch den Verstärker- und Multiplikatoreffekt der Technik möglich wird und dazu verführt. Durch das Internet erhält das Individuum Zugriff auf riesige Informationsmengen und damit auch die Macht, gezielt Knoten des globalen Netzes nicht nur auszuschalten, sondern für destruktive Zwecke einzusetzen. Das Netz wird Ziel von Gewalthandlungen, alle daran angebundenen Systeme werden zur potenziellen Waffe.

Durch technologische Umwälzungen beschleunigt sich die gesellschaftliche Entwicklung rasant und erlaubt es, Energie- und Informationsflüsse über wachsende Entfernungen in immer kleineren Zeiträumen auszutauschen. Alle jederzeit erreichen zu können, bedeutet auch, für Alle immer erreichbar zu sein. Der Prozess der permanenten Grenzüberschreitung durch Technik bestimmt so die menschliche Lebenswelt und macht immer mehr Lebensfunktionen von technischen Systemen abhängig. Die Beherrschung komplexer technischer Systeme bedarf eines fortwährenden Lernprozesses der Anpassung in technisch konstruierten Welten, die den Menschen zum Teil der Maschinerie machen.

Dies gilt für Individuen ebenso wie für staatliche Organe. Mit vernetzter Technik wird der Einflussbereich des Staates auf alle gesellschaftlichen Bereiche ausgedehnt. Polizei, Justiz, Militär und Geheimdienste nutzen die neuen Machtmittel und lassen sich nur widerwillig dabei einschränken, wie der NSA-Skandal demonstrierte. Bei der Steuerung sozialer und politischer Prozesse kann Technik bestehende Macht- und Herrschaftsstrukturen verstärken, aber auch überwinden helfen. Technik dient als gesellschaftliches Herrschaftsinstrument, das die Macht staatlicher Institutionen stärkt und die Bereitschaft zur Machtteilhabe einschränkt, oft mit dem Argument, Technik dürfe nicht in „falsche“ Hände geraten. Dies gilt auch für die Mittel der Überwachung und Steuerung. Wer glaubt, die Welt durch Spionagesoftware, Drohnen oder Mikroroboter sicherer zu machen, wird sich am Ende durch diese Instrumente selbst bedroht sehen.

Vernetzter Frieden und soziale Bewegungen

Was kann getan werden, um die Teufelskreise vernetzter Kriege zu durchbrechen? Netzwerke können die Entstehung demokratischer und partizipativer Strukturen fördern und Chancen für Zusammenarbeit, Friedenssicherung und Konfliktlösung auf lokaler, regionaler und globaler Ebene eröffnen. Jedes Individuum ist Knoten im globalen Netzwerk, und es kann sich die Strukturen als Machtverstärker zunutze machen, auch die Kritiker und die Aktivisten. Netzwerke für den Frieden gab es auch ohne Internet, so die Friedensbewegung Anfang der achtziger Jahre, die weltweit die öffentliche Debatte beherrschte. Die globale Protestbewegung gegen den Irakkrieg konnte diesen 2003 zwar nicht verhindern, jedoch mithilfe digitaler Netze eine relevante Gegenmacht aufbauen. Beim *Arabischen Frühling* waren soziale Medien bereits ein bestimmendes Moment, auch wenn die Bewegung einen friedlichen Umbruch nicht auf Dauer erreichen konnte. Statt nur auf Probleme zu reagieren, ist es für eine nachhaltige Friedenssicherung wichtig, Konfliktursachen präventiv zu vermeiden: durch Naturschutz und Ressourceneffizienz, Begrenzung des ökologischen Fußabdrucks, angepasste Technologien und Lebensweisen, durch gerechte Verteilung und Kooperation, Dialog und Partizipation.

Es gibt auch eine lange Geschichte sozialer Bewegungen, die sich kritisch mit den Folgen der Technik auseinandersetzten, von den Maschinenstürmern über die Arbeiterbewegung bis zur Studenten- und Umweltbewegung. Dabei geht es um den Streit, welche Richtung die technische Entwicklung nehmen oder nicht nehmen soll, um Interessengegensätze und um den Umgang mit Risiken. Dabei können Protest, Widerstand und Whistleblowing helfen, negative Entwicklungen an die Öffentlichkeit zu bringen, inakzeptable Folgen und Risiken zu vermeiden oder Win-Win-Lösungen zu stärken.

Um mit solchen Fragen umzugehen, bedarf es geeigneter Entscheidungsprozesse im Lebenszyklus der Technikentwicklung, von der Grundlagenforschung über die Erprobung bis zu Einsatz, Recycling und Abfallverwertung. Es geht auch um Lern- und Aushandlungsprozesse, die Differenzen und Konflikte auf konstruktive Weise lösen und kooperative Strukturen schaffen. Verschiedene Konzepte können im Rahmen des vernetzten Friedens zusammenwirken: präventive Rüstungskontrolle und Zivilklauseln zur Eindämmung der militärischen Verwendung von Forschung und Technik; nachhaltige und effiziente Ressourcennutzung, um die Belastung für Mensch und Natur durch Technik auf der Verursacher- und Folgenseite zu verringern; die Nutzung von Technologien, die die soziale Kompetenz stärken und gemeinsames Handeln zur Problem- und Konfliktbewältigung ermöglichen; Partizipation der Bevölkerung an Entscheidungs- und Nutzungsprozessen, um demokratisch legitimierte Entscheidungen und einen Interessenausgleich zwischen gesellschaftlichen Gruppen und Stakeholdern zu ermöglichen; und politische Regulierungsmechanismen, die die Entwicklung einer verantwortlichen Technikfolgenabschätzung und Technikgestaltung erlauben.

Referenzen

Dieser Beitrag basiert auf:

Scheffran, J. (2015) Vernetzter Krieg, Vortrag bei der Beiratssitzung der NaturwissenschaflerInnen-Initiative Verantwortung für Frieden und Zukunftsfähigkeit, Berlin, 20.02.2015.

Scheffran, J. (2015) Technikkonflikte in der vernetzten Welt, Wissenschaft und Frieden, 02/2015, S. 6-10.

Thomas Gruber

Die Informatik in der modernen Kriegsführung

Die Berührungspunkte der Informatik mit militärischen Interessen sind zahlreich. Nicht wenige Forschungsgebiete der Informatik werden – meist durch Drittmittelprojekte oder Honorarprofessuren – erheblich von der Rüstungsindustrie oder den nationalen Verteidigungsministerien kofinanziert. In den Universitäten entwickelt sich immer wieder punktueller Widerstand, aus dem ein grundlegender Diskurs über die Militarisierung der Wissenschaften hervorgegangen ist.

Wenn Forschung relevant für militärische Zwecke wird, betrifft dies nicht allein die Forschungseinrichtungen und die ihr angehörenden Forschungsgruppen, es wirkt auch auf die Gesellschaft im Ganzen. Forschung mit militärischen Zielen oder militärisch verwendbaren Ergebnissen arbeitet den aktuellen und den zukünftigen Kriegen zu, und diese führen unabdingbar zu einschneidenden Folgen für die Gesellschaft. Hier steht zunächst einmal die Verantwortlichkeit von Wissenschaftler.innen für die Folgen ihrer Forschungsergebnisse auf dem Prüfstand. Aufgrund der Auswirkungen dieser Ergebnisse auf gesellschaftliche Prozesse außerhalb der Universitäten scheint es deshalb notwendig, den Diskurs auf eine gesamtgesellschaftliche Ebene zu heben.

Trotz einiger medialer Aufmerksamkeit, die vom Pentagon in deutschen Forschungseinrichtungen geförderte militärrelevante Drittmittelprojekte im Jahr 2013 erhielten,[1] bleibt eine gesellschaftliche Diskussion über die universitäre Militärforschung weitgehend aus. Der Blick von außen in den Elfenbeinturm der Wissenschaften scheint ebenso schwer wie der Blick von ihm herab auf die Gesellschaft. Das Ziel dieses Artikels ist es, die Einbettung des Diskurses über Forschung für militärische Zwecke an zivilen Forschungseinrichtungen und über die diesbezügliche Verantwortlichkeit von Forscher.innen in einen gesamtgesellschaftlichen Kontext zu motivieren. Der Fokus soll daher im Folgenden auf zwei zentralen Aspekten dieser Einbettung liegen:

1. Ist die Anwendung einer Erkenntnis, einer Methode oder eines Verfahrens der Informatik in der Technologie oder der Methodik der modernen Kriegsführung ohne Weiteres erkennbar? Und weiter: Wo sind diese Technologie und Methodik ohne Forschungsergebnisse aus der Informatik undenkbar?

2. Welche Fragen und Anforderungen ergeben sich aus dieser Verflechtung bezüglich der Verantwortlichkeit von Forscher.innen? Welche Sonderstellung nehmen die gesellschaftlichen Grundwerte des Friedens und der Wissenschaftsfreiheit in diesem Diskurs ein?

Die erste Fragestellung kann aufgrund der Vielfalt militärrelevanter Forschungsergebnisse aus der Informatik nur exemplarisch behandelt werden. Dabei sollen im Folgenden drei prominente Beispiele aus verschiedenen Bereichen der modernen Kriegsführung auf ihre Abhängigkeit von Forschungsergebnissen aus der Informatik überprüft und einige weitere Beispiele dieser Verflechtung gegeben werden.

Die Informatik im Krieg

Als vergleichsweise junges Forschungsfeld arbeitet kriegsrelevante Forschung in der Informatik vorwiegend einer Kriegstechnologie und -methodik zu, die seit dem Zweiten Weltkrieg entstanden ist. Mit dem Begriff ‚moderne Kriegsführung' werden die aktuellen strategischen Entwicklungen von den historischen Mechanismen des Krieges abgegrenzt. In einer Analyse der historisch einschneidenden Änderungen in der Schlachttaktik und der Modernisierung von Kriegsgerät seit dem Zweiten Weltkrieg[2] lassen sich drei Parallelen in den Anforderungen an die Forschung und Entwicklung für eine moderne Kriegsführung erkennen: die Neu- und Weiterentwicklung von Kriegstechnologie, Methoden für eine kriegsrelevante Informationsakquise sowie Prädiktoren und Analysemodelle zur Unterstützung der Schlachttaktik[3]. In jeder dieser Anforderungen finden sich erhebliche Schnittpunkte zu Forschungsfeldern der Informatik. Gerade in der Steuerung computergestützter Kriegstechnologie sowie der militärischen Informations- und Datenverarbeitung sind diese Überschneidungen am deutlichsten sichtbar – ein Umstand, dem auch in den nachfolgenden Beispielen Rechnung getragen werden soll.

Die Erschließung des Weltraums mittels militärisch genutzter Satelliten steht auf der Agenda beinahe jeder so genannten militärischen Großmacht. Die taktischen Vorteile eines eigenen, sicheren Kommunikations-, Aufklärungs- und Navigationssystems im Kriegsfall sind schwer von der Hand zu weisen. Satellitenbilder sind in der Durchführung eines vermeintlich präzisen militärischen Schlags oft eine Voraussetzung. Neben den dazu benötigten Methoden zur Informationsverarbeitung und -übertragung lässt sich an Militärsatelliten darstellen, wie unverzichtbar eine tiefgehende theoretische Forschung in den Bereichen Informatik, Mathematik und Elektrotechnik, hier speziell Regelungstech-

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.

nik, ist. Ohne sie wäre beispielsweise eine ausreichend präzise Bahnsteuerung undenkbar. Ein mit genügender Geschwindigkeit in die Erdumlaufbahn geschossener Körper wird sich ohne weitere Steuerung durch die Triebwerke in eine elliptische Bahn um die Erde begeben, die durch viele Einflussfaktoren bestimmt ist. Für künstliche Satelliten, gerade auch die militärisch genutzten, muss eine vorbestimmte Bahn präzise erreicht werden. Kommunikationssatelliten sollen sich als fest ansteuerbare Punkte geostationär, das heißt über einem fixen Punkt der Erdoberfläche, bewegen. Überwachungssatelliten dagegen sollen sich geosynchron bewegen, um einen gewünschten Bereich der Erdoberfläche möglichst regelmäßig abzudecken. Einen Satelliten präzise auf eine vorbestimmte Bahn zu bringen, ist eine hochkomplexe Aufgabe. Zur Realisierung der gewünschten Flugeigenschaften werden Triebwerke benötigt, die zum genau richtigen Zeitpunkt und mit der richtigen Stärke feuern, und das ist ohne eine komplexe algorithmische Unterstützung undenkbar. Bei einer ungewünschten Neigung des Satelliten während des Fluges, sei es durch äußere Einflüsse oder durch eine Fehlzündung der eigenen Triebwerke, muss der Satellit dem Fehlverhalten gegensteuern, da sonst der künstlich erzeugte Orbit verlassen würde. Das dazu implementierte Programm im Steuerungssystem des Flugkörpers muss mathematische Grundlagen der Kontrolltheorie mit der ingenieurswissenschaftlichen Umsetzung in der Regelungstechnik verbinden. Eine zuverlässige, schnell reagierende und minutiös arbeitende Ausgleichssteurung für die Flugbahn des Satelliten ist ohne umfassende theoretische Forschung nicht realisierbar. Die Forschungsergebnisse aus der Informatik bezüglich der flugstabilisierenden und steuernden Algorithmen sind daher eine unverzichtbare Voraussetzung für die Nutzung eines militärischen Satelliten.

Eine Technologie, die neben der Nutzung durch zivile Sicherheitsinstitutionen vor allem in der asymmetrischen Kriegsführung wie in Guerilla- oder Bürgerkriegen Anwendung findet, ist die militärische Überwachung und Spionage. Überwachungs-Hardware des deutschen IT-Sicherheitskonzerns *Utimaco* wurde beispielsweise an das syrische Assad-Regime verkauft, das diese Ausrüstung zum Ausspionieren syrischer Demonstrant.innen nutzte.[4] Die von Utimaco so genannten *Lawful Interception Management Systems* (LIMS) sind vollständige funktionale Überwachungssysteme zum Abfangen privater Kommunikation u. a. über E-Mail, SMS und MMS. Verschlüsselte Kommunikation wird dabei mittels eines integrierten *LIMS-Decoders* gebrochen, und für ihre Weiterverarbeitung werden die gesammelten Kommunikationsdaten vom System wieder verschlüsselt[5] – ein erheblicher kryptographischer Aufwand also, der einer theoretischen Auseinandersetzung mit den verwendeten Kryptosystemen und mit einer algorithmischen Umsetzung der Decodier- und Codiervorgänge bedarf. Solche kryptoanalytischen und kryptographischen Anforderungen sind aktueller Forschungsstand in Mathematik und Informatik, und sie sind daher ohne Forschungsergebnisse aus diesen Disziplinen nicht umsetzbar.

Ein weiteres, viel diskutiertes Beispiel für die Modernisierung der Kriegsführung ist der militärische Einsatz von Drohnen. Überwachungs- oder Kampfdrohnen werden weltweit für Aufklärungs- oder Kriegseinsätze genutzt. Sie tragen zur Entstehung einer Asymmetrie zwischen den Parteien aktueller Konflikte bei. Dabei sind die verwendeten Drohnen nicht einfach ferngesteuerte Kampfflugzeuge, sondern sie sind umfangreich mit schlachtunterstützender Technologie ausgerüstet, die den Pilot.innen die durchzuführenden militärischen Schläge erheblich vereinfacht. Der US-amerikanische Rüstungskonzern *Northrop Grumman* entwickelt derzeit Drohnen mit einer automatisierten Zielerkennung, die aus den im Einsatzgebiet gesammelten Oberflächendaten selbstständig potenzielle militärische Ziele erkennt und identifiziert.[6] Eine solche Zielerkennung erfordert zuverlässige Klassifikatoren, die lernfähig sind und fehlertolerant arbeiten – eine typische Problemstellung im Forschungsbereich des Maschinellen Lernens und der Künstlichen Intelligenz. Hier lässt sich auch ohne genaue Kenntnis des Forschungs- und Entwicklungsstands der Drohnenkomponenten ein unmittelbarer Bezug zur Forschung in der Informatik herstellen, ohne die ein so mächtiger Klassifikator nicht realisierbar wäre.

Als weitere Beispiele könnten die Steuerung autonomer Fahrzeuge, die Forschung an *augmented reality* für das Militär, die Verschlüsselung kriegsrelevanter Daten oder das Brechen etablierter Kryptosysteme genannt werden. All dies sind Beispiele für die vielfältigen Anwendungen informatischer und informationstechnologischer Forschung in der modernen Kriegsführung. Dabei würde eine vollständige Analyse der Verflechtung zwischen Informatik und moderner Kriegsführung ins Uferlose führen.

Der gesellschaftliche Diskurs

Die Methoden der modernen Kriegsführung sind von der Informatik geprägt. Erkennbar ist dies nicht nur für die beteiligten Wissenschaftler.innen, sondern auch bei der Analyse der Kriegstechnologie aus einer gesellschaftskritischen Sicht. Die gesellschaftlichen Auswirkungen dieser Technologie stehen dem gesellschaftlichen Grundwert Frieden entgegen. Gelte es dann nicht, die Rolle von Informatiker.innen in aktuellen Kriegen in den allgemeinen Diskurs um den Krieg einzubinden? Was sind die Punkte, auf die sich dieser Diskurs stützen würde? Wo gestaltet sich ein breiter gesellschaftlicher Diskurs schwierig? Und welche Lösungsansätze gibt es für diese Problematik?

Eine der zentralen Fragestellungen für die Diskussion um friedliche Forschung ist zunächst die Verantwortlichkeit von Forscher.innen: Sind Informatiker.innen für die Nutzung ihrer Forschungsergebnisse verantwortlich, vielleicht sogar, wenn die Anwendung gar nicht ihrer Intention entsprach? Eine militärische (Mit-) Nutzung der Forschungsergebnisse in den Grundlagen oder für zivile Anwendungen (*Dual-Use*) ist kein Novum, doch könnten gerade die Wissenschaftler.innen fachlich am kompetentesten gegen die militärische Nutzung ihrer Forschungsergebnisse argumentieren. Eine solche Ausweitung der Verantwortung wäre also keine utopische Forderung der Gesellschaft an die Forschenden, es wäre die logische Konsequenz einer in allen Teilen nach Frieden strebenden Gesellschaft.

Natürlich gibt es Wissenschaftler.innen, die bewusst und gewollt für militärische Zwecke forschen. Insofern ist außerdem die Rangfolge der Werte *Frieden* und *Wissenschaftsfreiheit* zu klären. Denn sollte die Gesellschaft die Kriegsforschung für unverträglich mit ihren Werten erklären, dann ließe sich diese auch von der Wissenschaftsfreiheit ausnehmen, wie es beispielsweise bereits beim Embryonenschutzgesetz der Fall ist.

Auf Grundlage dieser Diskursansätze ließe sich die universitäre Militärforschung auch in die aktuelle Diskussion um Kriegseinsätze und so genannte Friedensmissionen einbinden. Das wäre ein wichtiger politischer Faktor, um auch auf universitärer Ebene gegen die Forschung für militärische Zwecke argumentieren zu können.

Problematik und Lösungsansätze

Während einige Ideen zur Ausgrenzung militärischer Forschung an Universitäten auf institutioneller Ebene existieren, fehlt für einen breiten gesellschaftlichen Diskurs vor allem eines: die Transparenz. Zivilklauseln, Ethikkommissionen und wissenschaftsethische Reflexion sind institutionelle Lösungsansätze, die zwar dem Ziel friedlicher Forschung zuarbeiten, die öffentliche Diskussion allerdings weitgehend unbeachtet lassen. Mit Geheimhaltungsklauseln versehene oder anderweitig intransparente Forschungsprojekte verhindern bisher die oben geforderte öffentliche Anfechtbarkeit von Forschungsprojekten, die in diesem Sinne fragwürdig sind. Transparenzklauseln zur Offenlegung von Drittmittelförderung oder Landesgesetze zur Transparenz von Forschungsprojekten[7] scheinen daher unabdingbar.

Anmerkungen

1 *Aus dem Fernsehprogramm „NDR Info" vom 25.11.2013*
2 *Vgl. hierzu beispielsweise: David Jordan et al., Understanding Modern Warfare, Cambridge University Press, 2008*
3 *Vgl. hierzu: Thomas Gruber, Verquickung mathematischer und informationstechnologischer Forschung an deutschen Forschungseinrichtungen mit der modernen Kriegsführung, Dissertation im Fachbereich Mathematik an der Universität Bremen, noch unveröffentlicht*
4 *Vgl. hierzu: http://www.bloomberg.com/news/articles/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear, aufgerufen am 22.7.2015*
5 *https://www.wikileaks.org/spyfiles/docs/UTIMACO-2010-UtimLIMSLawf-en.pdf, aufgerufen am 22.7.2015*
6 *http://www.northropgrumman.com/Capabilities/Triton/Documents/pageDocuments/Triton_data_sheet.pdf, aufgerufen am 23.7.2015*
7 *Wie beispielsweise im März 2015 vom Bremer Senat verabschiedet: http://landesportal.bremen.de/senat/44488385, aufgerufen am 24.7.2015*

Ute Bernhardt und Ingo Ruhmann

Das Blaumilch-System

Der unerklärte *Information Warfare*

1940 knackten die Briten erstmals mit programmierbaren Rechnern die deutsche ENIGMA-Verschlüsselung. Dieses Wissen wurde bis 1974 als Staatsgeheimnis gehütet. In den dazwischenliegenden 30 Jahren wurde die auf der ENIGMA beruhende kompromittierte Verschlüsselungstechnik weiter von staatlichen Stellen genutzt – und von den Briten geknackt. Dank Edward Snowden haben die Angreifer heute diesen Zeitvorsprung verloren. Wenig mehr als zehn Jahre nach der Entwicklung von digitalen Überwachungs- und Angriffswerkzeugen wie Turmoil, Turbulence *und deren Schwestersystemen wie* XKeyscore *wissen wir heute, in welchem Umfang Datenkommunikation weltweit überwacht und Computer mit solchen Werkzeugen angegriffen und manipuliert werden. Was macht den Unterschied aus?*

Otto Leiberich, lange Jahre Leiter der westdeutschen Zentralstelle für das Chiffrierwesen und nach deren Umwandlung in das Bundesamt für Sicherheit in der Informationstechnik (BSI) auch dessen erster Präsident, konnte sich noch in den 90er-Jahren im Verlauf von Interviews, Gesprächen und in Beiträgen mächtig darüber echauffieren, dass erst 1974 bekannt wurde, dass das ENIGMA-Verschlüsselungsverfahren kompromittiert war[1]. Heute sorgt es hingegen kaum noch für Aufregung, dass aktuelle und ehemalige Kabinettsmitglieder im Dutzend und Regierungsmitarbeiter in Kohortenstärke abgehört wurden, dass Verschlüsselungsverfahren und grundlegende IT-Sicherheitsmechanismen ausgehebelt sind. Und dass das alles nicht einmal bemerkt wurde.

Liegt es daran, dass zum Glück kein Krieg mehr herrscht und Politiker sowieso all ihre Kommentare an die Medien geben? Und wir alle dann weiter nur das Glück haben, diese ungefilterte Mitteilungswut der Politik nicht erdulden zu müssen, weil wohlmeinende Journalisten uns nicht damit behelligen? Oder liegt es doch eher daran, dass Politiker auch nur Menschen sind und mit vielerlei missliebigen und politisch inkorrekten Äußerungen aus vielfältig belauschter Kommunikation genauso kompromittierbar sind wie ihre IT-Systeme? Was sollten denn sonst die Anlässe und Motive für die lange Zeit unerkannten Angriffe auf die Server des Deutschen Bundestages sein, wenn nicht die aus der Überwachung gewonnenen Kenntnisse über Absprachen oder persönliche – digital übermittelte – Äußerungen von Politikern, die nicht mit deren öffentlicher Kommunikation übereinstimmen?

Das Schöne Neue daran ist: Wir werden es erfahren! Und zwar nicht erst in 30 Jahren, sondern bei passender Gelegenheit. Denn zur Kernkompetenz der Geheimdienste gehört nicht nur das Ausspähen, sondern auch das Nutzen der erlangten kompromittierenden Informationen.

Der Rücktritt von Roderich Kiesewetter, CDU-Obmann im NSA-Untersuchungsausschuss, wegen BND-Informanten in seinem Umfeld – oder doch wegen russischer Agenten? – lupft die Decke ein ganz kleines Stückchen von diesem schmuddeligen Tun[2]. Zum Vorschein kommt die munter betriebene Manipulation des politischen Betriebs durch die Dienste, zum Vorschein kommen

düpierte Abgeordnete, die sich von Geheimdiensten in der Ausübung ihres Mandates auch zu Recht manipuliert sehen.

Abgehörte und durch das erlangte Wissen kompromittierbare Beamte könnten keine Sicherheitsüberprüfung überstehen. Diverse Kabinettsmitglieder, nach dem gleichen Muster als Geheimnisträger bewertet, dürften nicht einmal ihre eigenen Kabinettssachen lesen, weil sie nicht durch die Sicherheitsüberprüfung kämen – zum Glück aber gelten die Regeln für den Beamtenapparat nicht für sie.

Dumm nur, dass sich nicht nur der politische Betrieb Berlins vor der Fremdsteuerung ängstigt. Auch wir Bürgerinnen und Bürger werden manipuliert – durch jene Medienberichte, die dunkle Quellen zu genehmer Zeit lancieren, um politische Karrieren zu stutzen oder zu verändern: Medial von gezielt gestreuten Meldungen manipulierte WählerInnen sind das Gegenstück zu kompromittierten Politiker.innen.

So geht Information Warfare.

Und damit gilt es, noch einen weiteren Irrtum auszuräumen. Denn natürlich herrscht Krieg – Informationskrieg. Darin macht es keinen Unterschied, ob wahre Meldungen belauscht und zur rechten Zeit publiziert werden, oder ob Falschmeldungen kunstvoll fabriziert und an die Medien lanciert werden.

Das heutige politische Italien zeigt unsere Zukunft: Nach dem Klima des politischen Misstrauens aus Unkenntnis folgten eine Welle von publizierten Abhörprotokollen aus unterschiedlichsten Quellen und entsprechende Skandale. Das Ergebnis ist heute der Wunsch nach Ehrlichkeit, Purismus und Klarheit – den letztlich aber nur Populisten und sektiererische Ideologen in Reinkultur liefern können, solange die geheimen Manipulateure der öffentlichen Meinung ungestört weiter arbeiten können.

Offenheit und Klarheit in der Politik ist gut. Aber sie stört den politischen Aushandlungsprozess. Denn Politik beruht auf Aushandlung und Kompromissen. Bis Kompromisse erzielt sind, sind notwendigerweise die Verhandlungen zwischen gegensätzlichen Positionen erforderlich. Die inhaltliche Differenz solcher Verhandlungen ist das Spielfeld für Manipulation und Kompromittierung. Ideologen und Populisten dagegen verhandeln nicht. Sie sind nicht kompromittierbar, wenn sie nicht verhandlungs- und kompromisswillig sind.

Die Kompromittierung von Politiker.innen durch die Kompromittierung ihrer IT-Systeme untergräbt die Möglichkeit der Verhandlung und des Kompromisses. Die Kompromittierung liegt im Interesse einer der Parteien im Verhandlungsprozess. Sie hebelt zum Nachteil anderer die Verhandlungen aus.

So geht Information Warfare.

Das zu leugnen und sich stattdessen zum Spielball derer zu machen, die Kompromisse und politisches Handeln in ihrem Sinne manipulieren wollen, ist ein schädliches Versagen von Politik und Medien zugleich. Denn Bürgerinnen und Bürger verstehen durchaus die aufgabenbedingte Doppelbödigkeit von Politik und schätzen auch kluge politische Schachzüge. Sie schätzen aber nicht Feigheit und Unehrlichkeit gegenüber Fakten und Zwängen. Manipulation im *Information Warfare* ist ein solches Faktum und schafft Zwänge.

Doch die heutigen Spielbälle der Dienste – genau: unsere Politiker.innen, deren PARLAKOM-Netzwerk im Bundestag so verwurmt ist, dass es aufgegeben werden muss – wollen sich zu Spielern wandeln. Regierungsmitglieder sind digital nackt, das Parlament digital handlungsunfähig und seiner Infrastruktur beraubt – man könnte fast sagen: Opfer eines digitalen Enthauptungsschlages – und doch wollen beide nicht nur etwas mehr Schutz für ihre IT-Systeme, sondern vor allem mehr Personal und Technik für den Angriff auf die IT-Systeme anderer. Gut möglich, dass die Dienste der potenziellen Zielländer dieser Angriffe schon die Cyberwar-Pläne gelesen haben, bevor sie von Regierung und Parlament beraten und verabschiedet sind. Egal.

Mit dem IT-Sicherheitsgesetz verbessert sich allein die Lage für die IT des Bundes durch BKA-Sonderermittler, durch mehr Personal beim BSI und mehr Personal im Bundesamt für Verfassungsschutz – letzteres heute schon auf besondere Weise bekannt für seine Variante einer „Cyberspionage-Abwehr“ gegen NSA, GCHQ und andere. Vom BND weiß man nicht, ob er sich vielleicht sogar durch falsch selektierte Selektoren auch noch als Cyberspion-Gehülfe im eigenen Haus herausstellt. Davon ungerührt rüsten BND und Bundeswehr derweil auf: Der BND beantragt zehnmal mehr Mittel für Personal, Wissen und Mittel für Cyberangriffe als die Bundesregierung pro Jahr für die IT-Sicherheitsforschung zur Verfügung stellt. Das Verteidigungsministerium arbeitet an einer Strategie für Cyberangriffe der Bundeswehr und hat eine „Strategische Leitlinie“ erlassen[3].

Das ist Information Warfare.

Ist das auch klug? Und selbst wenn man an die Richtigkeit von Krieg glauben würde, muss sich jeder Stratege fragen: Lässt sich damit etwas gewinnen? Strategie – nur zur Erinnerung – ist der zielgerichtete Einsatz meist militärischer Gewalt oder die Gewaltandrohung zur Erreichung politischer Ziele. Wenn man also glaubt, militärisch aktiv werden zu müssen: Was ist die Information-Warfare-Strategie der Bundeswehr?

Denn um Gewinnen geht es. Für die Verteidigung hat die Bundeswehr seit Jahren das CERTBw. Das ist die zur Abwehr konkreter Angriffe gerufene Einheit, die öffentlich seit mindestens 2007 erklärt, dass auch befreundete Nachrichtendienste die Netze der Bundeswehr angreifen. Und weil es von der Arbeit von Zivilisten und seiner Mitgliedschaft im CERT-Verbund abhängig ist, ist das CERTBw beim IT-Amt der Bundeswehr angesiedelt und strikt getrennt von den Cyber-Angreifern im Kommando Strategische Aufklärung (KSA).

„Offensive Cyber-Fähigkeiten der Bundeswehr haben grundsätzlich das Potenzial, das Wirkspektrum der Bundeswehr in multinationalen Einsätzen signifikant zu erweitern“, so die neuen Leitlinien des BMVg. Was also will die Bundeswehr im *Information Warfare* gewinnen? Und gegen wen? Um welchen Krieg geht es dabei genau? Wer hat den erklärt? Unter welcher Flagge führt die Bundeswehr diesen? Das Verteidigungsressort erklärt *False-Flag*-Aktionen als „Kriegslist“ für zulässig[4]. Und der Angriff auf zivile Netzwerke? Auch das ist nach Ansicht des zuständigen Parlamentarischen Staatssekretärs zulässig[5].

Oder wollen auch die Bundeswehr oder die Bundesregierung mitmischen im Spiel der Kompromittierung, der Ausspähung und Manipulation, der Falschmeldung und Sabotage? Und geht es gar um die Manipulation physischer Systeme – die Fernsteuerung der Autos und Flugzeuge von *Value Targets* – oder um die Destruktion von Maschinen und Anlagen?

Information Warfare ist eine Strategie für ein garantiertes Desaster moderner Gesellschaften. Verantwortungsvolle Zeitgenossen – auch solche, die sich in Uniform mit diesem Thema praktisch beschäftigt haben – konzentrieren sich auf Begrenzung und Abwehr. Wer daran glaubt, als konventionelle Streitkraft mit *Information Warfare* irgendetwas gewinnen zu können, sollte mindestens erkennen lassen, welche Antworten er oder sie für die Fragen und Probleme bedacht hat, die sich aus einer solchen Strategie ergeben.

Derzeit beschleicht den oberflächlichen Betrachter aber das ungute Gefühl, dass hier ebenso wenig überlegt wird wie zu Beginn des Ersten Weltkriegs auf allen Seiten – oder zu verschiedenen Zeiten im Zweiten Weltkrieg, als polnische Ulanen zu Pferd gegen angreifende deutsche Panzer anritten, Rotarmisten zu Beginn des Krieges oder der Volkssturm an dessen Ende jeweils ohne Waffen gegnerische Panzer aufhalten sollten. Immerhin wird der Wahnsinn für jeden greifbarer, wenn man Panzer sehen, hören und intensiv spüren kann. Bei Bits und Bytes ist die Vermittlung derselben Fakten wohl etwas schwieriger.

Die Bundesregierung will ihre Rechenzentren konsolidieren und kommt den Angreifern mit der Zentralisierung der Ziele sehr entgegen. Ist das hoffnungslos naive Feindesliebe oder soll mit dem republikweit größten Honeypot für Cyberkrieger eine besonders gekonnte Strategie verbunden werden?

BND und Verfassungsschutz haben die von der NSA entwickelte integrierte Cyberwar-Softwaresuite *XKeyscore* eingesetzt[6]. Angeblich erkannten beide aber nicht, welche Cyberwaffe sie da nutzen. Ist das eine dreiste Lüge oder die Wahrheit? Und welche dieser zwei Möglichkeiten ist die bessere Variante?

BND und Verfassungsschutz haben trotz des Wissens um Cyberangriffe von „befreundeten Diensten" die Angreifer weder verfolgt noch eingegrenzt. Auch für die Zukunft ist nicht zu erkennen, dass die in Deutschland verantwortlichen Cyberkriegs-Akteure ihre angreifenden Gegner überhaupt erkennen.

Bei genauer Betrachtung erstaunen die *Information-Warfare*-Krieger in Deutschland auf allen Ebenen. Sie haben keine Strategie. Sie können keine Ziele ihres Tuns benennen. Sie erkennen keine Angriffe auf die politischen Spitzen des Staates und das gesamte Parlament. Sie erkennen weder ihre Gegner, noch deren Waffen. Sie leisten keinen Beitrag zur politischen und militärischen Sicherheit und schon gar nicht zur IT-Sicherheit – letzteres leistet seit langem eine nach zivilem Muster aufgebaute CERT-Einheit der Bundeswehr. Sie riskieren stattdessen mit ihrem Tun ihre eigene Infrastruktur und die der Zivilgesellschaft. Sie drohen, politische Krisen durch ihr Tun militärisch zu eskalieren.

Wenn man zurück kommt zu den Ausgangsfragen und wenn man dabei an die Richtigkeit von Krieg glauben würde, wird sich jeder Stratege angesichts dieser Lage nur an den Kopf fassen wollen. Statt Mittel zu investieren, um die erkannten Probleme zu lösen, wird für jene Geld bereitgestellt, die umfassend bewiesen haben, dass sie von sicherer IT im Zivilleben und der IT in der Welt der heutigen Geheimdienste zwar frei von Kenntnissen sind, aber leider nicht frei von Wünschen.

Zurück zur ENIGMA. Ihre Entschlüsselung war ein Staatsgeheimnis, das Jahrzehnte von höchster strategischer Bedeutung war. Die meisten Staatsgeheimnisse sollen aber nur die Schwächen und vor allem das untaugliche Tun von verantwortlich Handelnden im Staate verheimlichen. Legt man diese Auslegung der Facetten der Ausspähung und des *Information Warfare* zugrunde, so darf sich niemand mehr ernsthaft fragen, warum der NSA-Skandal und seine Details mit allen Mitteln geheim gehalten werden müssen.

Loriot hat wunderbare Satiren über Konstellationen geschrieben, in denen ein starrköpfiges Familienmitglied einfach irgendein verrücktes „Dings" haben oder machen musste. Ebenso treffend ist Ephraim Kishons „Blaumilchkanal" über einen aus der Heilanstalt entflohenen Verrückten, der die Straßen einer Stadt nacheinander mit dem Presslufthammer aufmeißelt, wobei das Versagen, ihm Einhalt zu gebieten, am Ende als genialer staatlicher und politischer Plan verkauft wird.

Der Blaumilchkanal ist heute noch lustig. *Information Warfare* ist genauso verrückt. Nur lustig ist daran nichts.

Ingo Ruhmann und Ute Bernhardt

Ingo Ruhmann ist Informatiker und arbeitet im Bereich Technikfolgenabschätzung, Forschungspolitik, IT-Sicherheit, Information Warfare, *Cyberwar*, Geschichte der Geheimdienste und Datenschutz. Er ist Lehrbeauftragter im Studiengang *Security Management* der Fachhochschule Brandenburg. Er ist Mitglied des FIfF und war Vorstandsmitglied von 1991 bis 1998.

Ute Bernhardt ist Informatikerin und beschäftigt sich seit Jahren mit Forschungspolitik, Datenschutz und IT-Sicherheit, dem Verhältnis von Wissenschaft und Frieden sowie der Beziehung von Informatik und Militär. Sie hat Lehraufträge an der Fachhochschule Bonn-Rhein-Sieg und der FernUni Hagen. Sie ist Mitglied des FIfF und war FIfF-Vorstandsmitglied von 1991 bis 1998.

Anmerkungen

1 *Vgl. etwa: Otto Leiberich: Vom diplomatischen Code zur Falltürfunktion. In Spektrum der Wissenschaft, 01.06.1999. Vgl. auch: http://www.spektrum.de/magazin/vom-diplomatischen-code-zur-falltuerfunktion/825487*

2 *Politiker im NSA-Ausschuss verlangen Aufklärung. Die Welt, 08.02.2015, http://www.welt.de/politik/deutschland/article137244296/Politiker-im-NSA-Ausschuss-verlangen-Aufklaerung.html und: Verwirrung komplett. Süddeutsche Zeitung, 21.07.2015, http://www.sueddeutsche.de/politik/nsa-ausschuss-verwirrung-komplett-1.2575592?reduced=true*

3 *Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg, dokumentiert unter: https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/#Strategische-Leitlinie-Cyber-Verteidigung*

4 *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan van Aken, Andrej Hunko, Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE, „Elektronische Kampfführung der Bundeswehr", BT-Drs. 18/3963, Antwort auf Fragen 30–33*

5 *Plenarprotokoll der Fragestunde der 16. Sitzung des Deutschen Bundestages vom 19.02.2014, Antwort auf Frage 8, S. 1165 f.*

6 *Schnüffelsoftware XKeyscore: Deutsche Geheimdienste setzen US-Spähprogramm ein. SPIEGEL ONLINE, 20.07.2013, http://www.spiegel.de/politik/deutschland/bnd-und-bfv-setzen-nsa-spaehprogramm-xkeyscore-ein-a-912196.html*

Florian Mehnert

Das Kunstexperiment *11 TAGE*

Die gezielte Tötung als Konsequenz einer totalen Überwachung

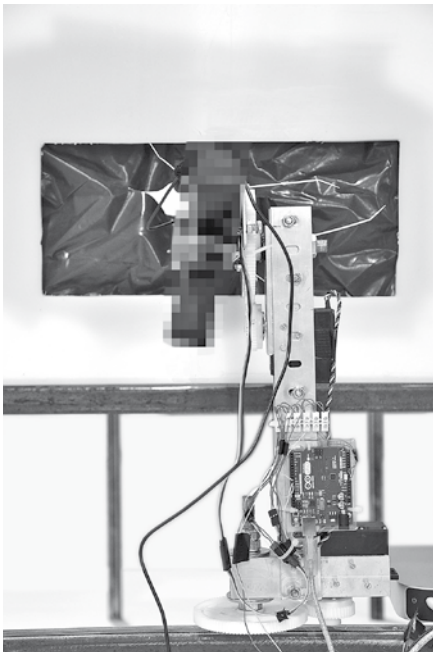
Die Installation 11 TAGE

Nach den vorhergehenden Kunstprojekten, die sich vor allem mit der Veranschaulichung der Überwachung auseinandersetzen, ging es mir wieder darum, eine Arbeit zu schaffen, in der die Folgen der Überwachung deutlich werden, aber hier vor allem, dass der Rezipient selbst partizipieren kann. Es war mir wichtig, dem Rezipienten eine entscheidende Rolle zu geben, ihn in eine kritische Situation zu bringen, in der er selbst Überwacher und Entscheider ist.

Der Aufbau

Die Installation *11 TAGE* besteht aus einer weißen Polyethylen-Box mit den Maßen 150 x 60 x 60 cm³. In der Box ist ein Rattengehege eingerichtet, in dem sich eine lebende weiße Ratte befindet. Die Box steht auf einer Stahlkonstruktion, an der eine über das Internet steuerbare Waffe angebracht ist. Die Rückwand der Box ist auf 4 cm verstärkt, um den Projektilen der Druckluftwaffe zu widerstehen. Drei Servomotoren sind für die Bewegung und das Auslösen der Waffe zuständig. Diese Motoren werden über ein *Arduino*-Board geregelt, das per USB-Verbindung mit einem Computer verbunden ist. Auf dem Waffenlauf ist eine Webcam montiert. Die gesamte Installation ist 195 cm lang, 60 cm breit und 145 cm hoch.

Auf dem dazugehörigen Computer befinden sich Skripte, die das Kontrollieren der Waffe über die Internetseite ermöglichen und den Lifestream im Internet auf dem Server bereitstellen. Die



Ansicht der Waffensteuerung der Installation 11 TAGE

Internetseite *(11tage.florianmehnert.de)* ist ein elementarer Bestandteil der Installation, sie ermöglicht die Steuerung der Waffe und zeigt den Livestream. Die Installation ist voll funktionsfähig und ermöglicht das Zielen sowie das Auslösen der Waffe.

Die Installation versetzt den Rezipienten in die Position des Überwachers und des Drohnenpiloten. Durch die Kameraposition auf dem Gewehrlauf – der typischen Egoshooter Perspektive – entsteht eine Spielsituation, die an Videospiele erinnert.

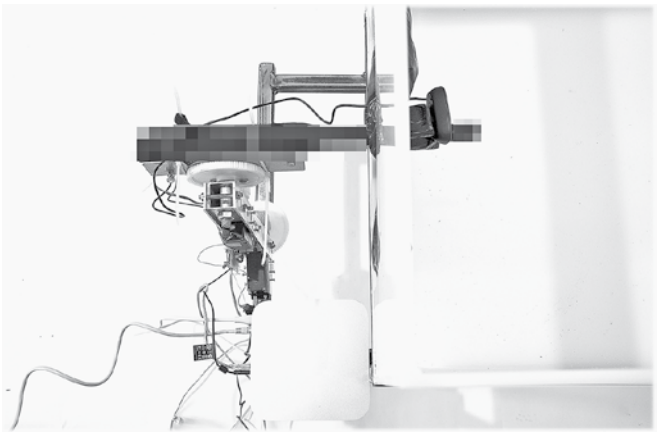
Die Intention

Das Kunstexperiment *11 TAGE* untersucht die Folgen der Überwachung, den Einsatz von ferngesteuerten bewaffneten Drohnen. Einem Drohneneinsatz geht eine umfassende Überwachung voraus, die sich dabei hauptsächlich auf private Daten von Mobiltelefonen stützt.

Wer durch Überwachung die Bewegungsprofile seiner Zielperson kennt, weiß wohin er tödliche Drohnen schicken muss. Bei der Installation *11 TAGE* spielt auch Gamification eine essentielle Rolle. Der Rezipient versetzt sich in die Position des Drohnenpiloten. Das Prinzip entspricht einerseits der Steuerung beim Einsatz von bewaffneten Drohnen und andererseits dem Prinzip des Egoshooter-Videospiels. Der Einsatz der Gamification führt zu einer Herabsetzung der Hemmschwellen. Hier bezieht sich *11 TAGE* auf die zahlreichen Spiele, in denen die Aggressionsbereitschaft und die Bereitschaft zum Töten in Szene gesetzt und initiiert werden.

11 TAGE inszeniert den bewaffneten Drohneneinsatz und zeigt, was er ist: Die gezielte Tötung als Konsequenz der totalen Überwachung.

Die Laborratte wurde über einen Livestream per Webcam permanent überwacht. Nach Ablauf des Countdowns von 11 Tagen, am 25. März 2015 um 19.00 Uhr (CET), sollte die steuerbare Waffe scharf geschaltet werden. Die Ratte hätte dann von



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

jedem Smartphone, von jedem Computer aus über das Internet getötet werden können. Jeder hätte zum anonymen Täter werden können.

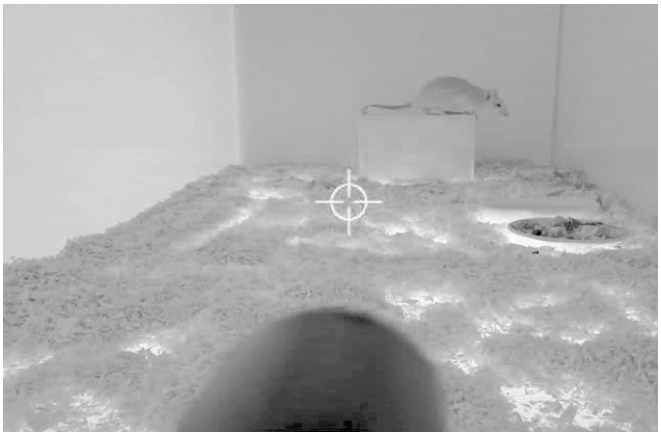
Es war jedoch nie geplant, die Ratte wirklich töten zu lassen.

Der Ablauf des Projekts

Der Countdown des Projekts wurde am Samstag, den 14. März, offiziell gestartet. Ich informierte die Presse vorher am Abend des 12. März.

Die Presse reagierte sofort und am späteren Abend kamen die ersten Anfragen, am Freitagmorgen führte ich um 9 Uhr das erste Interview mit der Süddeutschen Zeitung. Die darauf folgenden sechs Tage waren ein Pressemarathon, in denen ich zahlreichen Medien Interviews gab. In weniger als 12 Stunden entwickelte sich im Internet ein Shitstorm über Facebook, Twitter und in zahlreichen Foren sowie Kommentarbereichen der Online-Zeitungen. Ich erhielt hunderte von E-Mails mit Beschimpfungen und Morddrohungen.

Die täglichen Zugriffe auf die Webseite des Projekts stiegen von zunächst einigen Tausend über Nacht auf ca. 30.000 pro Tag. Am Ende des Projekts waren über 100.000 Zugriffe zu verzeichnen.



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

Ich musste mehrfach den Webserver wechseln, nach zwei Tagen einen Cloud-Server mieten, der dem Ansturm an Zugriffen einigermaßen gewachsen war. Unter den – teilweise auch angekündigten – DOS-Attacken von Hackern brach der Server aber trotzdem regelmäßig zusammen.

Am Samstagmorgen erschienen zwei Beamte der örtlichen Polizei, die sich die Installation, die Waffe und die Haltung der Ratte ansehen wollten.

Das Kunstexperiment *11 TAGE* lief nicht wie ursprünglich vorgesehen 11 Tage, sondern nur sechs Tage. Es wurde von mir vorzeitig am 17. März 2015 um 19.00 Uhr (CET) beendet. Warum? Das Kunstexperiment *11 TAGE* hat sein Ziel erreicht!

Bereits am Samstag, als der 11-Tage-Countdown erst am Abend gestartet wurde, gab es über 30.000 Zugriffe auf die Webseite. Bis zum Sonntagabend hatten viele Medien in Deutschland, Österreich, Schweiz und England über das Projekt berichtet. Das Projekt *11 TAGE* hatte in kurzer Zeit mehr Aufmerksamkeit erzeugt, als ich erwartet hatte. Es wurde über das Projekt und seine Thematik kontrovers diskutiert. Insofern war das Ziel des Kunstexperiments *11 TAGE* schon nach wenigen Tagen erreicht. Das Projekt bis zum Ende des Countdowns weiterlaufen zu lassen, war daher nicht unbedingt notwendig.

Zahlreiche Morddrohungen zeitigten ihre Wirkung. Ich fühlte mich nicht mehr sicher, befürchtete eine mögliche Eskalation und fing an, darüber nachzudenken, wann ich ein vorzeitiges Ende des Projekts einleiten könnte. Am Montagabend beantragte ich Personen- und Objektschutz bei der örtlichen Polizei. Zunächst wurden nächtliche Kontrollfahrten vor meinem Wohn- und Arbeitshaus bewilligt.

Am Mittwoch, den 17. März erhielt ich Besuch von drei zivilen Vertretern der Behörden: ein Hauptkommissar, ein Tierarzt des Landratsamtes Freiburg und ein Dezernatsleiter. Sie baten um Besichtigung der Installation, daraufhin um ein Gespräch, in dem mir unmissverständlich klargemacht wurde, dass ich das Projekt freiwillig beenden sollte, da sonst Mittel und Wege gegen mich gefunden werden würden, das Projekt von offizieller Seite aus zu beenden.

Weder die Belastung des Shitstorms, noch der Pressemarathon, noch das Gespräch mit den Behördenvertretern führten letzten Endes zu der Entscheidung, das Ende des Kunstexperiments am Abend des 16. März nach sechs Tagen einzuleiten, sondern der tatsächliche, erreichte Erfolg des Projekts.

Der Shitstorm: Abbild der sozialen Wirklichkeit im Netz?

Der Shitstorm entwickelt eine starke negative Wucht. Am Anfang habe ich noch die E-Mails gelesen, dann nur noch überflogen und später fing ich an, sie nach den Hinweisen im Betreff auszusortieren. Die Konfrontation mit den negativen Inhalten erschwerten eine konstruktive Auseinandersetzung mit dem Kern der Arbeit. Darüber hinaus verschärfte sich die Lage zum Einen durch das kontinuierliche Eintreffen der E-Mails und zum Anderen durch die unüberschaubaren Kommentare auf Online-Plattformen wie Facebook, Twitter, Reddit sowie in zahlreichen Zeitungsforen. Zudem wurden mehrere internationale Online-Petitionen von Tierschützern gegen das Projekt gestartet. Eine Petition, die mir vorgelegt wurde, hatte über 12.000 Unterschriften von internationalen Unterzeichnern, weitere hatten insgesamt 11.000 Unterschriften. Zahlreiche Anzeigen gegen mich wurden bei der Staatsanwaltschaft eingereicht.

Die Reaktionen sind zu differenzieren. Es können ein paar grobe Zahlen in Bezug auf die Webhits genannt werden: In fünf Tagen haben etwa 100.000 Menschen die Webseite besucht. Aufgrund der zahlreichen Berichte in den Medien hatten allerdings weitaus mehr Menschen Kenntnis von dem Projekt. Rund 20.000 Menschen haben Online-Petitionen unterschrieben und ca. 500 eine negative oder drohende E-Mail an mich geschrieben. Somit haben sich ca. 20 % der Besucher der Webseite persönlich gegen mich gewendet.

Die Aussagen der „Shitstormer" reichen von Beschimpfungen bis hin zu Gewalt- und Morddrohungen. Die Mehrzahl schlug vor, man möge mich in die Installation setzen und erschießen. Hier nur einige der vielen Beispiele:

> *„Would like to put a gun against his head and well would say blow his brains out but he clearly has none." (Linda Moorhouse , Cleckheaton, UK)*

> *„He should be killed instead." (Filip Vavra, Prague, Czech Republic)*

> *„I think we should put him in a box and let anyone of the internet kill him." (M. Ridway, Manchester, UK)*

> *„What a sick bastard. Aim the gun at his head and let everyone go for it. See how he likes it." (Cathy Nowland, Bribie, Australia)*

Florian Mehnert

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

„... This person needs to be prosecuted!!" (Antoinette Kruger, East London, South Africa)

„Florian Mehnert YOU need to be shot!" (Victoria Coleman, Pittsburgh, PA, USA)

„Wo finde diesen so genannten Künstler ich glaube der braucht eine Kugel durch den Kopf!" (Christian Weltin, Deutschland)

David Pella (Twitter) „@FlorianMehnert ich hoffe Sie werden eines Tages erschossen."

Warum kam es zu dieser Reaktion des Publikums? Wie ist diese zu bewerten? Kam es durch die Rattenfokussierung zu einer Überlagerung der Intention?

Die Ratte war ein wichtiger kalkulierter Bestandteil der Installation. Sie bekam implizit die Rolle des unschuldigen Opfers, und fungierte hervorragend als Auslöser von Aufmerksamkeit und Emotionen. Das Ziel des Projekts war es, eine kontroverse Diskussion über die Konsequenzen der Überwachung und den Einsatz von bewaffneten Drohnen anzustoßen. Über die Identifikation der Rezipienten mit der Ratte gelang es, die Aufmerksamkeit auf das Projekt zu lenken. Jeder konnte den klaren Aufbau und die Funktionsweise der Installation verstehen. Jeder hatte bewusst oder unbewusst wahrgenommen, dass das *11 TAGE*-Projekt in seinem Aufbau eine Parallelsituation zur Wirklichkeit geschaffen hatte.

Der *11 TAGE*-Shitstorm war keinesfalls Ausdruck einer reinen Verunglimpfung meiner Person, sondern Ausdruck einer Überforderung und Hilflosigkeit der Rezipienten. Der Lifestream zeigte eine offensichtlich vom Tod bedrohte Ratte. Die Gefahr, dass die Ratte am Ende des 11 Tage dauernden Countdowns getötet werden würde, war für viele der Rezipienten eine unausweichliche Tatsache.

Somit war der Fokus stark auf den Tod der Ratte und ihrer lebensbedrohlichen Lage gerichtet. Dennoch wurde die Situation der Ratte mit der Lage von Menschen in Syrien, Jemen, Waziristan etc., die durch Drohnen getötet wurden oder konstant mit einem Tod durch Drohnen rechnen müssen, assoziiert. Eine Diskussion darüber fand unter anderem in zahlreichen Foren statt.

Die Hilflosigkeit, sich gegen den Drohnenkrieg nicht wirksam einsetzen zu können, manifestierte sich für die „Shitstormer" um so mehr in einer Rettung der Ratte, in einer Verurteilung des Kunstprojekts und seines Urhebers. Der Shitstorm verdeutlichte jedoch, dass Menschen durchaus bereit sind, sich gegen bestehendes Unrecht auch politisch zu mobilisieren.

Die Tragweite und Auswirkungen des Drohnenkriegs sind vielen Menschen nicht bewusst oder werden nicht als Unrecht wahrgenommen. Demnach schien die Rettung der Ratte lohnenswerter zu sein, als sich gegen eine oder mehrere Regierungen und Institutionen als Urheber des Drohnenkriegs zu wehren. Dies scheint aufgrund der Komplexität der Thematik, die wesentlich von Angst vor Terror gesteuert wird, verständlich.

In diesem Zusammenhang kann der Shitstorm auf das Kunstexperiment *11 TAGE* auch als Reaktionsventil der emotionalen und geistigen Überforderung im Umgang mit einer komplexen Realität angesehen werden, deren Durchdringung und Bewältigung immer schwieriger wird.

Hans-Jörg Kreowski und Aaron Lye

Ein kurzer Kommentar zu einer bemerkenswerten Initiative

Wie auf der nächsten Seite abgedruckt, ist vor kurzem ein offener Brief unter dem Titel Autonomous Weapons: an Open Letter from AI and Robotics Researchers *erschienen, für den die Erstunterzeichnerinnen und -unterzeichner Unterschriften sammeln (siehe http://tinyurl.com/awletter). In dem Brief wird dazu aufgerufen, offensive autonome Waffen zu ächten.*

Das ist ein wirklich bemerkenswerter Vorgang, weil Fachwissenschaftlerinnen und Fachwissenschaftler äußerst selten kollektiv zu den politischen und gesellschaftlichen Auswirkungen ihrer Wissenschaft öffentlich Stellung nehmen. Der offene Brief entstammt einer Initiative aus dem *Future of Life Institute*, das in Boston angesiedelt ist, mit vielen bekannten und weniger bekannten Persönlichkeiten aus Wissenschaft, Kultur und Wirtschaft. Es verfolgt folgende Mission:

„To catalyze and support research and initiatives for safeguarding life and developing optimistic visions of the future, including positive ways for humanity to steer its own course considering new technologies and challenges." *(Quelle: http://futureoflife.org)*

Der offene Brief wurde am 28. Juli 2015 auf der *International Joint Conference on Artificial Intelligence* öffentlich vorgestellt. Die Unterschriftensammlung lief zu der Zeit bereits über vier Wochen und wies bis zum 30. Juli über 2.400 Unterzeichnerinnen und Unterzeichner aus dem KI- und Robotik-Bereich auf, sowie fast 14.000 Unterschriften von weiteren Unterstützerinnen und Unterstützern. Es handelt sich also um eine begrüßenswerte Initiative mit erstaunlicher Resonanz. Einige Argumente im offenen Brief sollten aber nicht unkommentiert bleiben.

Wir teilen die Auffassung, dass durch technologische Fortschritte in Bilderkennung, Künstlicher Intelligenz, Ontologien, neuronalen Netzen, Sensorfusion und Big Data autonome Waffensysteme in naher Zukunft entwickelt werden können, die gegenüber herkömmlicher Waffentechnologie neue Möglichkeiten

eröffnen, und dass auf technischer Ebene autonome Waffen, wenn sie zum Einsatz kommen, Ziele auswählen und angreifen werden, ohne dass Menschen direkt den Befehl dazu geben. Aber solche Waffensysteme sind nur in einem technischen Sinne intelligent und autonom. Ihre Intelligenz und Autonomie sind künstlich; sie sind selbstlernende, regelbasierte Softwaresysteme, die aufgrund von Mustern Entscheidungen treffen. Ihre Lernalgorithmen, Regeln und Entscheidungsverfahren sind von Menschen konzipiert und programmiert. Der menschliche Faktor ist lediglich verlagert.

Auf der Basis der immer umfassenderen Vernetzung, der immer weiter voranschreitenden Verbreitung von Informationstechnologien in unserer Gesellschaft und der immer effizienteren Rechner werden auch die Anwendungen immer anspruchsvoller. Auch für die Anwendungen in der Kriegsführung trifft dies zu. Die Entwicklung autonomer Waffen ist ein Ausdruck einer maßlosen Technikeuphorie. Aber handelt es sich wirklich um eine Revolution, um die dritte nach Schießpulver und Atombombe? Mittlerweile wird fast alles als Revolution oder Game-Changer bezeichnet, sei es Cyberwarfare, Drohnen oder autonome Waffen. Wie bei Pfeil und Bogen, beim Schießpulver, bei Flugzeugen oder bei den ABC-Waffen handelt es sich um Entwicklungsschritte der Militärtechnik. Dabei ist nicht klar und vielleicht auch nicht wirklich wichtig, ob es sich um evolutionäre oder revolutionäre Phänomene handelt. In allen Fällen geht es aber um immer perfidere Methoden des Tötens. Dabei sind, wie im Open Letter richtig beschrieben, autonome Waffensysteme aufgrund ihrer vergleichsweise geringen Kosten und ihrer einfach zu beschaffenden Materialien für Militärs besonders attraktiv. Das kann aber momentan auch einfach an der asymmetrischen Kriegsführung und Drohneneinsätzen in Gebieten ohne Luftabwehr liegen. Autonome Waffen könnten gegen einen technologisch gleich starken Gegner völlig nutzlos sein.

Weltweit wird schon jetzt an autonomen Waffen geforscht, und diese Forschung wird ganz massiv von den jeweiligen Regierungen gefördert. Deshalb ist es richtig und wichtig, einen Appell an die Vereinten Nationen zu richten mit der Forderung, autonome Waffen zu verbieten. Allerdings sollte diese Forderung nicht wie im offenen Brief auf offensive Systeme eingeschränkt werden, weil defensive autonome Waffen dieselbe Problematik mit sich bringen wie offensive (ganz abgesehen davon, dass sich bei vielen Waffen offensiv und defensiv gar nicht unterscheiden lassen). Auch wäre zu überlegen, ob nicht ferngesteuerte Waffen wie Kampfdrohnen in die Ächtung einbezogen werden müssten, weil sie ebenfalls zu einem unsinnigen Rüstungswettlauf führen, ähnliche ethische Probleme mit sich bringen und ihr derzeitiger Einsatz praktisch immer ein Kriegsverbrechen darstellt. Außerdem ist ein Verbot allein noch keine Lösung. Damit Militärs eine Technologie nutzen können, bedarf es immer Menschen, die diese entwickeln. Daher ist auch ein Appell an alle Menschen, die Waffensysteme entwickeln, nötig, denn ohne sie geht es nicht.

Autonomous Weapons: an Open Letter from AI & Robotics Researchers

Autonomous weapons select and engage targets without human intervention. They might include, for example, armed quadcopters that can search for and eliminate people meeting certain pre-defined criteria, but do not include cruise missiles or remotely piloted drones for which humans make all targeting decisions. Artificial Intelligence (AI) technology has reached a point where the deployment of such systems is — practically if not legally — feasible within years, not decades, and the stakes are high: autonomous weapons have been described as the third revolution in warfare, after gunpowder and nuclear arms.

Many arguments have been made for and against autonomous weapons, for example that replacing human soldiers by machines is good by reducing casualties for the owner but bad by thereby lowering the threshold for going to battle. The key question for humanity today is whether to start a global AI arms race or to prevent it from starting. If any major military power pushes ahead with AI weapon development, a global arms race is virtually inevitable, and the endpoint of this technological trajectory is obvious: autonomous weapons will become the Kalashnikovs of tomorrow. Unlike nuclear weapons, they require no costly or hard-to-obtain raw materials, so they will become ubiquitous and cheap for all significant military powers to mass-produce. It will only be a matter of time until they appear on the black market and in the hands of terrorists, dictators wishing to better control their populace, warlords wishing to perpetrate ethnic cleansing, etc. Autonomous weapons are ideal for tasks such as assassinations, destabilizing nations, subduing populations and selectively killing a particular ethnic group. We therefore believe that a military AI arms race would not be beneficial for humanity. There are many ways in which AI can make battlefields safer for humans, especially civilians, without creating new tools for killing people.

Just as most chemists and biologists have no interest in building chemical or biological weapons, most AI researchers have no interest in building AI weapons — and do not want others to tarnish their field by doing so, potentially creating a major public backlash against AI that curtails its future societal benefits. Indeed, chemists and biologists have broadly supported international agreements that have successfully prohibited chemical and biological weapons, just as most physicists supported the treaties banning space-based nuclear weapons and blinding laser weapons.

In summary, we believe that AI has great potential to benefit humanity in many ways, and that the goal of the field should be to do so. Starting a military AI arms race is a bad idea, and should be prevented by a ban on offensive autonomous weapons beyond meaningful human control.

Reinhold Franck, Jürgen Gerloff, Wilfried Hardt, Rainer Isle, Hans-Jörg Kreowski, Inger Kuhlmann, Peter Löhr, Ludwig Voet, Anne Wilharm

Militärische Probleme mit der Software – Kann STARS sie meistern?

1982 brachte das Verteidigungsministerium der Vereinigten Staaten von Amerika (das Department of Defense*, das im folgenden mit* DoD *abgekürzt wird) ein Informatik-Förderungsprogramm unter dem Titel* Software Technology for Adaptable, Reliable Systems (STARS) Program Strategy *heraus. Die Förderung durch STARS begann im Finanzjahr 1984 und soll eine Laufzeit von sieben Jahren haben. In dieser Zeit sollen einige Hundert Millionen US-Dollar für Software, genauer für die Verbesserung des Herstellungsprozesses von Software, ausgegeben werden.*

STARS ist in Art und Umfang ein Musterbeispiel, wie und warum der militärische Bereich auf die Informatik als Wissenschaft vom Computer und seinem Einsatz massiv einwirkt. Um die Mechanismen besser erkennen und verstehen zu können, die zur engen Verflechtung von Militär und Informatik beitragen, werden in diesem Abschnitt einige Aspekte des STARS-Programms vorgestellt und kurz kommentiert. Dem geht ein knapper historischer Abriss voraus, der zeigt, dass STARS nur ein Glied in einer langen Kette militärischer Einflussnahmen auf die Entwicklung des Computers und der Informatik ist.

1. Ein Wunderwerk

Und nun komm, du alter Besen!
Nimm die schlechten Lumpenhüllen;
Bist schon lange Knecht gewesen:
Nun erfülle meinen Willen!
Auf zwei Beinen stehe,
Oben sei ein Kopf,
Eile nun und gehe
Mit dem Wassertopf!

Walle! walle
Manche Strecke,
Daß, zum Zwecke,
Wasser fließe
Und mit reichem, vollem Schwalle
Zu dem Bade sich ergieße.

Seht, er läuft zum Ufer nieder,
Wahrlich! Ist schon an dem Flusse,
Und mit Blitzesschnelle wieder
Ist er hier mit raschem Gusse.
Schon zum zweiten Male!
Wie das Becken schwillt!
Wie sich jede Schale
Voll mit Wasser füllt!

In den 40er Jahren werden die ersten elektronischen Rechenanlagen gebaut und für ballistische Berechnungen, zur Weiterentwicklung der Atombombe und beim Bau der ersten Wasserstoffbombe erfolgreich eingesetzt. Der atemberaubende „Siegeszug" der Computertechnik beginnt, die Computerwissenschaft wird gegründet. Die Verbreitung der Computer erfasst alle Bereiche der Produktion, Verteilung und Verwaltung, macht auch nicht halt vor der Privatsphäre. Doch wie in ihren Anfängen bleiben die Computertechnik und die Informatik als ihre Wissenschaft bis heute eng verzahnt mit dem militärischen Bereich. Die Geschichte des Computers ist vor allem von waffentechnischen und strategischen Erfordernissen beherrscht und vom Zugriff und Geld der Militärs bestimmt. In kaum einem Waffensystem wird auf die Hilfe von Rechnern verzichtet. Aufklärung und Logistik basieren auf Computereinsatz. Aus den Kommandozentralen sind rechnergestützte Informationssysteme nicht mehr wegzudenken. Frühwarn- und weltweite Kommunikationssysteme sind ohne Computer nicht möglich. Die Kriegsmaschinerie hängt, scheint es, völlig und unauflöslich vom Funktionieren der Computer ab, so dass Informatiker inzwischen zu den wichtigsten Beratern des Militärs zählen. Im STARS-Programm liest sich das so:

> *„Während der letzten 25 Jahre hat sich die ursprünglich untergeordnete Rolle, die der Computer in militärischen Systemen spielte, zu einer von größter Wichtigkeit verändert. Buchstäblich jedes System im gegenwärtigen und geplanten militärischen Arsenal macht extensiven Gebrauch von Computertechnologie ... Die militärische Stärke der Vereinigten Staaten ist unauflöslich gebunden an den programmierbaren Digitalrechner." (S. VIII)*

2. Schwachstellen

Stehe! Stehe!
Denn wir haben
Deiner Gaben
Vollgemessen! –
Ach, ich merk es! Wehe! wehe!
Hab ich doch das Wort vergessen!

Ach, das Wort, worauf am Ende
Er das wird, was er gewesen.
Ach, er läuft und bringt behende!
Wärst du doch der alte Besen!
Immer neue Güsse
Bringt er schnell herein,
Ach! und hundert Flüsse
Stürzen auf mich ein.

Welche Zwänge, Wünsche, Erfolge auch immer dazu führen, dass sich die Militärherren ganz dem Computer verschreiben, alle Nachteile und Mängel der neuen Technik gehören dazu. Schon frühzeitig wird deutlich und mit den immer umfangreicheren und anspruchsvolleren Aufgaben für die verwendeten Rechner bald unübersehbar, dass Wissen, Erfahrung und Einsicht nicht Schritt halten mit der rein technischen Entwicklung der Rechner, dass Fachkräfte fehlen, dass die Herstellung von Software und damit der eigentlichen Voraussetzung für den (flexiblen) Computereinsatz teuer ist. Wer sich umfassend der Computer bedient, erfährt schmerzlich ihre Fehleranfälligkeit, die Verletzlichkeit ihrer Systeme und die Unzuverlässigkeit ihrer Programme. Beispielsweise berichtete die International Herald Tribune in ihrer Ausgabe vom 30.10.1980, dass das Computergestützte nordamerikanische Frühwarnsystem in 18 Monaten 147 Fehlalarme auslöste.

Im US-amerikanischen Militärapparat wirken sich die Engpässe, Schwierigkeiten und Risiken, die mit dem Computereinsatz verbunden sind, besonders nachhaltig und spürbar aus, weil hier nicht nur „bewährte" Systeme verwendet werden, sondern neue Entwicklungen noch unausgegoren und zu früh umgesetzt oder überhaupt erst forciert in Gang gesetzt werden. Im STARS-Programm kann man einige Hinweise darauf finden:

> *„Mehrere Jahre lang haben Experten angeregt, dass das DoD etwas gegen das ‚Software-Problem' tun sollte." (S. IX)*

Hinter dem Schlagwort vom *Software-Problem* verbirgt sich tatsächlich eine Vielzahl an Ungereimtheiten und an offenen Fragen, die Hersteller von Software heutzutage nicht beherrschen:

> *„Eher gibt es viele Schwierigkeiten einschließlich einer inadäquaten Technologie, unangemessener Beschaffungs- und Managementpraktiken und einer ernsten Knappheit an fähigen Leuten." (S. 4)*

> *„Die gestiegenen Kosten sind manchmal nur der sichtbare Effekt einer grundlegenden Schwierigkeit: armselig definierte und sich ändernde Anforderungen." (S. 5)*

> *„Andere Schwierigkeiten stammen von der Notwendigkeit ultra-hoher Zuverlässigkeit und dem Zwang, fortgeschrittene, ausgeklügelte Anwendungen auszuführen. Zuverlässigkeit ist für das DoD wesentlich wegen der kritischen Aufgaben und Abhängigkeit menschlichen Lebens vom korrekten Funktionieren der Systeme." (S. 5/6)*

3. Maßnahmen

Nein, nicht länger
Kann ichs lassen;
Will ihn fassen.
Das ist Tücke!
Ach! nun wird mir immer bänger!
Welche Miene! welche Blicke!

O du Ausgeburt der Hölle!
Soll das ganze Haus ersaufen?
Seh ich über jede Schwelle
Doch schon Wasserströme laufen.
Ein verruchter Besen,
Der nicht hören will!
Stock, der du gewesen,
Steh doch wieder still!

Es ist deshalb kein Wunder, dass die wichtigsten Impulse, die Missstände abzustellen, von militärischer Seite und vor allem aus dem US-amerikanischen Verteidigungsministerium und der Bürokratie des Nordatlantikpaktes (NATO) kommen. 1968 werden die wichtigsten Vertreter der praktischen Informatik aus aller (westlichen) Welt zu einer NATO-Tagung geladen, auf der über Ursachen und Abhilfe der „Softwarekrise" beraten wird: Die Informatik wird mit dem neuen Fachgebiet *Software Engineering* beglückt. In den siebziger Jahren startet das Department of Defense (DoD) der Vereinigten Staaten ein gigantisches Projekt mit immensem finanziellem Aufwand zur Entwicklung einer neuen Programmiersprache. Hunderte von Fachleuten aus Industrie und Hochschule beteiligen sich. Unter militärischer Kontrolle und nach militärischen Ansprüchen entsteht ADA, eine ganz „normale" universelle Programmiersprache, die aber insbesondere zur Programmierung „eingebetteter Systeme", also von Computern in Raketen, Bombern, Panzern, Radarnetzen u.ä. dienen soll. Ende der 70er Jahre wird der Hardware-Entwicklung ein weiterer Schub erteilt mit der Zielsetzung eines *very high speed integrated circuit*, das 1000 mal schneller und obendrein zuverlässiger arbeiten soll als herkömmliche Chips. Im Umfang ist dieses Projekt mit der ADA-Entwicklung vergleichbar. Das STARS-Programm erwähnt beide Projekte lobend:

> *„Das Programm wird vollständig und vorteilhaft die jüngsten Fortschritte auf dem Gebiet der Computer-Hardware nutzen, die in den VHSIC- und VLSI-Programmen des DoD erzielt wurden ..." (S. 15)*

> *„Das ADA-Programm mag als ein dieser Initiative vorausgehender Schritt betrachtet werden, weil es die soziologische und technologische Basis legt für eine gemeinsam (von den Land-, Luft- und Seestreitkräften) genutzte, automatisierte (Software-) Entwicklungsumgebung." (S. 40)*

Erhebliche Anstrengungen werden momentan unternommen, um ADA zur Programmiersprache der 90er Jahre zu machen – im militärischen, ökonomischen und universitären Bereich. Das wird vielleicht das Schreiben von Programmen rationalisieren können, alle anderen Schwierigkeiten mit der Software jedoch wird das kaum verkleinern. Erfolge auf dem Hardware-Sektor durch das VHSIC-Programm werden das „Software-Problem" eher verschärfen, weil bessere Chips zu waghalsigen, unbeherrschbaren und unprogrammierbaren Anwendungen in Waffensystemen weit über das heute üblichen Maß hinaus verführen.

4. Ein erneuter Anlauf

Willst's am Ende
Gar nicht lassen?
Will dich fassen,
Will dich halten
Und das alte Holz behende
Mit dem scharfen Beile spalten.

Seht da kommt er schleppend wieder!
Wie ich mich nur auf dich werfe,
Gleich, o Kobold, liegst du nieder;
Krachend trifft die glatte Schärfe.
Wahrlich, brav getroffen!
Seht, er ist entzwei!
Und nun kann ich hoffen,
Und ich atme frei!

1982 startete das DoD eine neue Initiative, der Bedeutung der Softwaretechnologie für die militärische Schlagkraft gerecht zu werden und den anhaltenden, ja wachsenden Problemen mit der Software im militärischen Bereich zu begegnen: *Software Technology for Adaptable, Reliable Systems (STARS) Program Strategy*.

Erklärtes Ziel von STARS ist, die Softwareproduktivität zu erhöhen und dabei gleichzeitig eine größere Zuverlässigkeit und Anpassbarkeit der Systeme zu erreichen:

„Das Ziel ist, die Softwareproduktivität zu erhöhen, während größere Systemzuverlässigkeit und Anpassbarkeit erreicht werden soll. ... Angesichts wachsender Nachfrage nach mehr Software und des Mangels an Leuten mit geeigneten Fähigkeiten besteht die Herausforderung darin, die technologische Basis voranzubringen ..." (S. X)

Das Ziel soll dadurch erreicht werden, dass der Werkzeugcharakter vorhandener und verfügbarer Methoden, Sprachen und Programmiersysteme, stärker zur Geltung kommt, die Personalknappheit überwunden wird und so die Umgebung verbessert wird, in der Softwareentwicklung und -weiterentwicklung erfolgen kann.

Um alle derartigen Aktivitäten bündeln zu können, ist ein Softwaretechnik-Institut vorgesehen (und mittlerweise an der Carnegie-Mellon-Universität eingerichtet), das verschiedenste Forschungs- und Entwicklungsaktivitäten zu einer Softwareumgebung zusammenfasst, ihre Einführung und Verwendung in militärischen Softwareentwicklungen unterstützt und ein Trainingsprogramm zur Einarbeitung in die Softwareumgebung erstellt. Das Personal des Instituts wird sich aus dem DoD, der Industrie und den Hochschulen rekrutieren.[1]

5. Die Nöte bleiben

Wehe! wehe!
Beide Teile
Stehn in Eile
Schon als Knechte
Völlig fertig in die Höhe!
Helft mir, ach! ihr hohen Mächte!

Und sie laufen! Naß und nässer
Wirds im Saal und auf den Stufen.
Welch entsetzliches Gewässer!
Herr und Meister! hör mich rufen! –

Hinter all den Facetten, die das STARS-Programm ausmachen, dürfen jedoch zwei Aspekte nicht übersehen werden, die vielleicht Hinweise liefern, was die eigentlichen Absichten des DoD sind.

Erstens werden im STARS-Programm die laufenden jährlichen Kosten des DoD allein für Software eingebetteter Systeme auf 5-6 Milliarden US-Dollar beziffert und bis 1990 eine Steigerung auf 32 Milliarden US-Dollar prognostiziert. Eine Verdoppelung der Softwareproduktivität (eine angeblich bescheidene Zielvorstellung für STARS) ist also notwendig, damit zukünftig Softwareerstellung im militärischen Bereich bezahlbar bleibt.[2]

Neben den finanziellen und ökonomischen Zwängen, die das STARS-Programm dämpfen soll, gibt es eine immens politisch-ideologische Komponente:

„Computersoftware ist eine wesentliche Komponente militärischer Systeme. Tatsächlich etabliert und kontrolliert Software zunehmend die Funktionsfähigkeit von Militärsystemen. Software jedoch ist ein zweischneidiges Schwert: sie kann auch unser (US-amerikanisches) zukünftiges militärisches System in einer Weise zum Scheitern bringen, die ein Desaster für unsere nationale Sicherheit darstellen könnte." (S. 1)

Doch was hier noch wie Sorge um (vielleicht berechtigte) Sicherheitsinteressen klingt, entpuppt sich an anderer Stelle als unverhohlenes Streben nach militärischer Überlegenheit:

„Die Vereinigten Staaten haben ihre Führungsrolle in vielen hochentwickelten Technologien eingebüßt, auf denen unsere (US-amerikanische) industrielle Basis und militärische Stärke aufgebaut waren. Ein ähnlicher strategischer Verlust droht nun der Elektronik-, Computer- und Software-Industrie. Das darf nicht passieren, weil wir (die USA) so stark von Computern abhängen in unseren zentralen militärischen Systemen. Aggressive Aktion ist jetzt erforderlich, wenn wir unsere militärische Überlegenheit durch den Einsatz von Computertechnologie behaupten sollen." (S. VIII)

„Das VHSIC, ADA und STARS-Programm zusammen bilden ein ausgewogenes Portefeuille, um die US-militärische Überlegenheit durch die Führungsrolle in der Computertechnologie zu erhalten." (S. 84)

6. Schluss (damit)

Goethe schilderte im *Zauberlehrling*, wie sich die Menschen (und insbesondere die Herrschenden und ihre Gefolgsleute) Natur und Technik zu eigen machen: ohne unerwünschte und fatale Folgen zu bedenken. Die Strophen waren ein trefflicher Begleiter durch den Abriss, wie militärisches Denken die Informatik in den letzten 40 Jahren befördert hat. Vielleicht kann sogar der Schluss des Gedichtes (der alte Hexenmeister kommt nach Hause und beendet den Spuk mit den Worten: *„In die Ecke, Besen! Besen! Seid's gewesen ..."*) einen Hinweis geben, wie der faule Zauber des Computereinsatzes im militärischen Bereich beendet werden kann: *„In die Ecke, Rechner! Seid's gewesen."*

Dieser Gedanke soll aber nicht weitergesponnen werden, um keine Illusionen zu schüren. Computerfachleute und Informatiker könnten sich vielleicht einige ihrer Gewissensbisse sparen, wenn der Computer nicht mehr als Kriegsgerät genützt würde, doch an der eigentlichen Problematik kann das nichts ändern. Denn Krieg wird nicht wegen der Computer geführt, sondern Computer werden für den Krieg genutzt und nach den Erfordernissen des Krieges gestaltet. Beseitigt werden müssen die ökonomischen und gesellschaftlichen Voraussetzungen, die Krieg möglich und erstrebenswert machen. Es muss verhindert werden, dass Staaten unter dem Vorwand, sich zu verteidigen, ihre militärische Stärke einsetzen, um andere Völker zu unterdrücken und auszubeuten.

---

aus: Informatik 2000 – Kampf um Märkte und Vorherrschaft, Informatik-Bericht 5/87, Universität Bremen 1987, S. 5-10, alle Zitate im Text mit Seitenangaben sind Übersetzungen aus DoD: Software Technology for Adaptable and Reliable Systems (STARS) Program Strategy, ACM SIGSOFT Software Engineering Notes, 2 (1983), S. 56-108)

Anmerkungen

1 vgl. ebenda, S. xii

2 vgl. ebenda, S. xiii

Hans-Jörg Kreowski

FIfF auf dem *IS4IS Summit Vienna 2015*

Vom 3. bis 7. Juni 2015 führte die International Society for Information Studies (IS4IS) *als erste Konferenz dieser Art den* IS4IS Summit Vienna 2015 *durch, mit dem Titel* The Information Society at the Crossroads – Response and Responsibility of the Sciences of Information*. Sie fand mit über 300 Teilnehmerinnen und Teilnehmern an der Technischen Universität Wien unter der Leitung von Wolfgang Hofkirchner statt.*

IS4IS dient als Schirm mehrerer Netzwerke, Institutionen und Organisationen, die sich wissenschaftlich mit Information im weitesten Sinne auseinandersetzen, insbesondere auch in ihrem gesellschaftlichen Kontext. Vier Konferenzen fanden in diesem Rahmen statt:

- die sechste *International Conference on the Foundations of Information Science*,
- die fünfte *ICTs and Society Conference*,
- die zweite I*nternational Conference on Philosophy of Information* sowie
- die dritte *International Conference on the Difference that Makes a Difference (DTMD)*.

Außerdem fanden parallel dazu noch weitere Tracks statt, so dass teilweise bis zu acht Sektionen parallel liefen. Das thematische Spektrum umfasste die Grundlagen von Informationsprozessen in Natur und Gesellschaft mit besonderer Berücksichtigung der sozialen, kulturellen, politischen, ökonomischen, ökologischen, geschichtlichen, philosophischen und technologischen Aspekte und Probleme.

Einen Track hat das FIfF organisiert: *Cyberpeace is more than the absence of cyberwar*. Er bestand aus zwei 90-minütigen Sektionen und wurde von Kai Nothdurft und Britta Schinzel moderiert. Sylvia Johnigk hielt einen Hauptvortrag zum Thema *Let's Clear Up the Debris – What the Snowden Leaks Mean for Our IT Security.* Außerdem gab es vier weitere Präsentationen: Stefan Hügel sprach über *Cyberpeace: Promoting civil rights and peaceful use of the Internet*, Hans-Jörg Kreowski (in Kooperation mit Dietrich Meyer-Ebrecht) über *Revolution in Military Affairs – Not without information and communication technology*, Henning Lübbecke über *Ubiquitous Computing and Privacy*. Ein weiterer vorgesehener Hauptvortrag von Mariarosaria Taddeo zum Thema *Just Information Warfare* musste leider ausfallen, weil die Referentin ihr Flugzeug verpasste. Das FIfF hatte sich kurzfristig zur Beteiligung am Summit entschlossen, so dass nur wenig Zeit für die Einwerbung von Beiträgen blieb. Das gab uns andererseits Gelegenheit, die Cyberpeace-Kampagne ausführlich vorzustellen.

Mehr Information zum Summit findet man unter *http://summit.is4is.org/programme.* Die extended Abstracts der meisten Vorträge der Konferenz sind auf der Webseite *http://sciforum.net/conference/isis-summit-vienna-2015/page/allcontributions* gesammelt und speziell die des FIfF-Tracks unter *http://sciforum.net/conference/isis-summit-vienna-2015/isis-T1.4.* Nach meiner Einschätzung passte der FIfF-Track bestens in das Gesamtprogramm und so manche der an der IS4IS beteiligten Organisationen sind interessante Kooperationspartner für das FIfF. Deshalb wäre es erstrebenswert, dass sich das FIfF wieder und vielleicht sogar verstärkt am nächsten Summit 2017 in Göteborg beteiligt.

Im Rahmen des Summit hat sich ein Arbeitskreis der Leibniz-Sozietät der Wissenschaften zu Berlin zum Thema *Emergente Systeme, Information und Gesellschaft* gegründet, in dem sich auch einige Mitglieder des FIfF engagieren werden. Der Arbeitskreis wird insbesondere auch versuchen, das Fachgebiet *Informatik und Gesellschaft* zu stärken. Wolfgang Hofkirchner hat dazu den folgenden Text verfasst, in dem Ziele und Hintergründe des Arbeitskreises skizziert werden.

Wolfgang Hofkirchner

Emergente Systeme, Information und Gesellschaft – Informatik und Gesellschaft bilden mit Systemwissenschaften einen Arbeitskreis

Am 5. Juni 2015 wurde der Arbeitskreis *Emergente Systeme, Information und Gesellschaft* gegründet. Die Gründung erfolgte im Rahmen des *IS4IS Summit Vienna 2015*, einer Tagung zur Zukunft der Informationsgesellschaft, die an der Fakultät für Informatik der Technischen Universität Wien stattfand. Die Leibniz-Sozietät war dabei unter den Koorganisatoren.

Einer spontanen Idee auf der wissenschaftlichen Konferenz der Leibniz-Sozietät *Vom Mineral zur Noosphäre* über V. I. Vernadskij 2013 folgend, waren der Gründung diverse Gespräche vorausgegangen, die auf Anregung von Klaus Fuchs-Kittowski immer stärker in eine bestimmte Richtung führten.

Inhaltlich geht es bei dem Arbeitskreis um ein wissenschaftliches, disziplinübergreifendes Verständnis von Information in Natur, Technik und Gesellschaft und um die Wechselbeziehungen zwischen Systemansätzen und Informationswissenschaften mit besonderer Berücksichtigung von Informatik und Gesellschaft. In dem Maße, in dem Information und Informationstechnik zum Schlüssel für die zukünftige Gestaltung der menschlichen Gesellschaft werden, kommt es auf einen verantwortungsvollen Umgang mit den Beiträgen von Systemtechnik, Systemwissenschaften und Informatik zur weiteren Entwicklung der Informationsgesellschaft an – weit über eine rein technologische Betrachtung hinaus.

Ein Gespräch zwischen dem Präsidenten der Leibniz-Sozietät, Gerhard Banse, und dem Präsidenten des *Bertalanffy Centers for the Study of Systems Science* (BCSSS), Wolfgang Hofkirchner, auf dem *European Meeting on Cybernetics and Systems Research* (EMCSR) 2014 in Wien verabredete weitere Schritte. Die Tagung *Informatik und Gesellschaft 2015* in Berlin, von der Leibniz-Sozietät und der Hochschule für Technik und Wirtschaft (HTW) zu Ehren Klaus Fuchs-Kittowskis aus Anlass seines 80. Geburtstages veranstaltet, bereitete die Gründung des Arbeitskreises vor, der auf dem Lebenswerk Fuchs-Kittowskis aufbauen kann.

Der Arbeitskreis ist eine Kooperation mit dem Bertalanffy Center und der International Society for Information Studies. Er ist deckungsgleich mit einer Research Group des BCSSS und einer Special Interest Group der IS4IS (in Beantragung) unter dem englischen Titel *Emergent Systems, Information and Society*. Wolfgang Hofkirchner (Technische Universität Wien) ist Leiter des Arbeitskreises und Hans-Jörg Kreowski (Universität Bremen) sein Stellvertreter. Interessentinnen und Interessenten mögen sich bitte an sie wenden: *wolfgang.hofkirchner@tuwien.ac.at* oder *kreo@informatik.uni-bremen.de.*

Birgit und Michael Ahlmann

Bericht zur Fragebogenaktion

im Rahmen der Cyberpeace-Veranstaltung am 14. April 2015 in Bremen im Haus der Wissenschaft

Im Zuge der ersten öffentlichen Veranstaltung der Bremer Cyberpeace-Kampagne des FIfF führte die Arbeitsgruppe Cyberpeace eine Fragebogenaktion unter den Veranstaltungsteilnehmer.innen durch. Einerseits war es Ziel der Befragung, anhand der Antworten herauszufinden, ob und in welchem Maße sich die Veranstaltungsteilnehmer.innen durch Missbrauch und Missmanagement digitaler Produkte bedroht fühlen. Andererseits erhoffte sich die Arbeitsgruppe auch weitere Impulse für die Fortsetzung der Cyberpeace-Kampagne.

Von den ausgelegten Fragebögen kamen knapp die Hälfte ausgefüllt zurück. Außer der grundsätzlichen Frage, ob die zunehmende Digitalisierung generell als bedrohlich empfunden wird, wurden in weiteren zehn Fragen verschiedene mögliche Bedrohungsszenarien angesprochen. Man sollte hierzu ankreuzen, wie sehr oder wie wenig man sich als Individuum durch die aufgezeigten Gefahren bedroht fühlt.

Unter den Rückläufern war nur ein einziger Fragebogen, in dem ausschließlich die erste Frage verneint worden war, und ein weiterer, dessen Antworten auf die weiteren zehn Fragen aber genau dieser Aussage widersprachen. Etwa 80 % der Antworten insgesamt bestätigen eine reale Furcht vor den Risiken und dem Missbrauch der Digitalisierung. Als die beiden größten Gefahren wurden die permanente totale Überwachung jeder und jedes Einzelnen sowie mögliche Hackerangriffe auf die Versorgung mit Trinkwasser, Energie, medizinischen Apparaten etc. genannt.

Die in den Fragen dargestellten exemplarischen Szenarien wurden überwiegend als bedrohlich oder sehr bedrohlich eingeschätzt. Es gab insgesamt nur wenige Rückläufer, in denen „wenig bedrohlich“ oder „nicht bedrohlich“ angekreuzt war.

Diese Ergebnisse der Fragebogenaktion bestätigen der Arbeitsgruppe, dass es notwendig ist, sich verstärkt für eine friedliche Nutzung der digitalen Möglichkeiten einzusetzen und sich für den Schutz der Privatsphäre und den Erhalt der informationellen Selbstbestimmung zu engagieren.

Die im Fragebogen vorgesehene Möglichkeit des freien Kommentars zum Thema Cyberpeace wurde zwar nur von sehr wenigen genutzt. Dennoch spiegeln auch diese Kommentare den Eindruck wider, der schon in der Diskussion während der Veranstaltung entstanden war: Es besteht eine relativ große Unsicherheit im Umgang mit der wachsenden Digitalisierung und der Bedarf an Information, Diskussion und Klärung ist groß, z. B. wie eigene Daten in der Öffentlichkeit geschützt werden.

Einer der Kommentare zeigt, dass befürchtet wird, die Lebens-, Lern- und Bildungsqualität würde letztendlich unter der Digitalisierung aller Lebensbereiche leiden, weil die Menschen aus Bequemlichkeit das eigene Nachdenken und die eigene Kreativität immer weniger nutzen. In einem weiteren Kommentar wurde dafür plädiert, den Umgang mit IT und IT-Sicherheit als festen Unterrichtsbestandteil in die Lehrpläne der Schulen aufzunehmen.

Alle Ergebnisse der Fragebogenaktion bestätigen folglich die Notwendigkeit, die Bremer Veranstaltungsreihe innerhalb der Cyberpeace-Kampagne mit verschiedenen ausgesuchten Schwerpunktthemen wie Datenschutz und insbesondere für Arbeitnehmerdatenschutz fortzusetzen.

Cyberwar – Cyberpeace 2015 – Umfrage

Die Digitalisierung beeinflusst in immer stärkerem Maße das Leben der Gesellschaft und des Individuums. Digitale Steuerung ermöglicht beispielsweise die Kommunikation mit den Freunden und Verwandten auf anderen Kontinenten. Das Öffnen oder Schließen Ihres Autos funktioniert über eine Distanz – Ähnliches gilt für Fernwärme, Wasser- oder medizinische Versorgung oder Verkehrsleitsysteme. Ferngelenkte Roboter können in verseuchte Gebiete hineinfahren oder fliegen, aber eben auch in kriegerische Missionen eingebunden werden. Vielfältige Missbrauchsmöglichkeiten durch Kriminelle, Terroristen oder Machthaber stellen eine reale Bedrohung dar.

Bitte füllen Sie den Fragebogen aus – er bleibt selbstverständlich anonym!

1. Digitalisierung bedeutet Segen oder Fluch. Fürchten Sie sich vor den Risiken der Digitalisierung?

ja ☐ nein ☐ weiß nicht ☐

2. Welchen „Grad der Bedrohung" ordnen Sie konkreten Gefahren durch die Digitalisierung zu:

a. Hackerangriffe auf die Versorgung mit Trinkwasser, Energie, medizinischen Apparaten (im Krankenhaus)

sehr bedrohlich ☐ bedrohlich ☐ kaum bedrohlich ☐ nicht bedrohlich ☐ weiß nicht ☐

b. Die permanente totale Überwachung jedes/jeder Einzelnen

sehr bedrohlich ☐ bedrohlich ☐ kaum bedrohlich ☐ nicht bedrohlich ☐ weiß nicht ☐

c. Wirtschaftsspionage

sehr bedrohlich ☐ bedrohlich ☐ kaum bedrohlich ☐ nicht bedrohlich ☐ weiß nicht ☐

d. Sabotageakte / Störung von Flugverkehr, Polizei, Zoll, Bundeswehr (Jamming)

sehr bedrohlich ☐ bedrohlich ☐ kaum bedrohlich ☐ nicht bedrohlich ☐ weiß nicht ☐

e. Digitale (unbemannte) Kriegführung, u. a. Waffen-Drohneneinsätze

sehr bedrohlich ☐ bedrohlich ☐ kaum bedrohlich ☐ nicht bedrohlich ☐ weiß nicht ☐

f. Zusammenbrechen vieler wichtiger Systeme durch Überlastung

sehr bedrohlich ☐ bedrohlich ☐ kaum bedrohlich ☐ nicht bedrohlich ☐ weiß nicht ☐

g. Zündung von Atom-, Bio- oder Chemiewaffen durch „Irre" oder Terroristen

sehr bedrohlich ☐ bedrohlich ☐ kaum bedrohlich ☐ nicht bedrohlich ☐ weiß nicht ☐

h. Die beabsichtigte oder unbeabsichtigte Auslösung eines Krieges durch Angriff oder Fehlfunktionen bewaffneter Drohnen

sehr bedrohlich ☐ bedrohlich ☐ kaum bedrohlich ☐ nicht bedrohlich ☐ weiß nicht ☐

i. Mobbing / Verleumdung im Internet

sehr bedrohlich ☐ bedrohlich ☐ kaum bedrohlich ☐ nicht bedrohlich ☐ weiß nicht ☐

j. Identitätslöschung Einzelner durch Hacker oder totalitäre Staaten oder Fehlfunktion der Systeme in der Verwaltung

sehr bedrohlich ☐ bedrohlich ☐ kaum bedrohlich ☐ nicht bedrohlich ☐ weiß nicht ☐

3. Wenn Sie noch etwas bemerken möchten, bitte auf der Rückseite ...

Herzlichen Dank für Ihre Mühe – FIfF Bremen – www.fiff.de – cyberpeace.fiff.de

FIfF-Regionalgruppe Bremen – Prof. Dr. Hans-Jörg Kreowski – Goetheplatz 4 – 28203 Bremen

Nils Erik Flick

„Smart City" – alternativloser Selbstläufer oder abgekartetes Spiel?

Aufruf zur Diskussion

Türen, die Dich freundlich grüßen.[1] Kühlschränke, die mit Autos über Deine Gewohnheiten reden, und andere wahr gewordene Wahnvorstellungen. Straßenlaternen, die Menschen ansprechen oder welche melden, die sich komisch verhalten. Eine Umgebung, die Dich kennt. Was kann schon schiefgehen? Oder ist schon etwas schiefgegangen, wenn niemand mehr einen Schritt machen kann, ohne verfolgt, erfasst, erkannt, profiliert, von Maschinen mit dem Vornamen angesprochen und dabei hinterrücks analysiert zu werden, zum Zweck individualisierter Abrechnung, Marktforschung, Infrastrukturplanung und natürlich besserer Anpassung an die eigenen (selbstverständlich messbaren, modellierbaren und beliebig extrapolierbaren) Bedürfnisse? „The spectrum of control: A social theory of the smart city", *ein Beitrag von* Jathan Sadowski *und* Frank Pasquale *im* First Monday Peer-Reviewed Journal on the Internet *gab Anlass, die dort aufgestellten Thesen zu reflektieren und zur Diskussion zu stellen.[2]*

Was ist Überwachungskapitalismus, was ist eine Kontrollgesellschaft, und was haben beide mit dem Schlagwort *„smart"* zu tun? Ist *die Stadt der Zukunft*, in der *alles vernetzt* ist, Segen oder Desaster? Wem nutzen all die Vernetzungsvisionen? Werden hier wichtige Punkte unterschlagen? Sadowski und Pasquale üben pointierte Kritik an Plänen zur Vernetzung von Infrastrukturen, Objekten, Menschen in der Stadt. Sie zeigen, dass der Diskurs ein erhebliches Framing durch die Marketing-Rhetorik der *„Smart"*-Vertreter erfahren hat, die ihr Vorgehen gern als pragmatische Problemlösung darstellen.[3] Diese Mär wird ebenso widerlegt wie die ideologische Neutralität einer *„Smart City"*, deren Mehrwert auf einer neoliberalen Kommodifizierung persönlicher Daten beruht. Der folgende Text bezieht sich auf Sadowski und Pasquale, streut aber eigene Betrachtungen ein.

Ein unsichtbares Wurzelgeflecht

Wir leben in einem überwachungskapitalistischen System, in dem alltägliche Daten über uns gesammelt, aufbereitet und gehandelt werden.[4,5] Aus Mobilfunk-Standortdaten entstehen Bewegungsprofile,[6] Buchungen und Online-Äußerungen landen bei Kredit-Auskunfteien.[7] Auswertungen, denen niemand informiert zugestimmt hätte, werden auf Infrastrukturen gesetzt und verändern deren Charakter essenziell – *Function Creep* verwässert die Zweckbindung von Daten.[8,9] Die Industrie will mehr: sie propagiert ein *Internet der Dinge* – im Englischen noch viel treffender *internet of everything* genannt –, in dem noch mehr Daten[10] anfallen. Immer mehr Geräte funktionieren nur noch mit Internetverbindung.[11] In Politik und Verwaltung arbeitet es, „warum nicht alles effizienter machen, womöglich in öffentlich-privater Partnerschaft?". Verwaltungsdaten eignen sich zur Vermarktung.[12] So wuchert in harmonischer Symbiose mit kommerzieller Überwachung auch der Staat in die elektronischen Netze, kann der Verlockung der Macht nicht widerstehen und wird zunehmend zu einer Gefahr für sich selbst. Nach dem Willen der Branchenriesen[13] steht mehr Vernetzung bevor. Manchmal muss die Entwicklung durch Werbung, Gruppenzwang oder Verordnungen forciert werden, letzteres im Fall des *Smart Meter*, das als Teil des Wurzelgeflechts Daten ausleitet,[14] oder im Fall der *eHealth* – ein eigenes Thema.[15] Trotz mangelhafter Argumente wird die *smarte Zukunft* zur Erlösung verklärt. In ihr ist alles gut, optimiert, optimal. *Big Data* ist der große Bruder von *„Smart"*: ein Solutionismus, der mit Technik und Statistik gesellschaftliche Probleme lösen will, ohne neue zu schaffen.[16]

Jathan Sadowski, Frank Pasquale: The spectrum of control: A social theory of the smart city, München: Knaur Verlag, http://firstmonday.org/ojs/index.php/fm/article/view/5903

Wir übernehmen die Konvention aus Sadowski und Pasquale (s. o.), *„smart"* in Anführungszeichen zu setzen, weil es nie definiert wird, nur als vage positives Label dient. *„Smart City"* meint ein integriertes Informationsnetzwerk aus Objekten (und Menschen) mit einer Vielzahl möglicher Anwendungen: die Stadt als ungenutzte Datenquelle. Die typischen Szenarien wirken plastikartig, die Phrasen abgedroschen – die *„smarte Welt"*, in der „alles vernetzt" ist: Man achte auf bestimmte Artikel („*die* Stadt *der* Zukunft"). Werden diejenigen, die *nicht* wollen oder können, ausgeschlossen oder assimiliert? Eventuell sind diese Floskeln bloß rhetorische Missgriffe: die konkreten Projekte unterscheiden sich durchaus voneinander. Sadowski und Pasquale kritisieren dubiose Kosten-Nutzen-Rechnungen und die Tendenz, den Sozialvertrag durch einen Unternehmensvertrag zu ersetzen (Abschnitt III).

Die Kontrollgesellschaft und die Beziehung zwischen Verwaltung und Gesellschaft in der *„Smart City"*: ein kybernetischer Regelkreis?

Schwerer zugänglich ist vielleicht die Deleuzesche Philosophie, auf der die Kritik in den späteren Abschnitten von Sadowski und Pasquale basiert.[17] Drei Grundbegriffe werden im Text erklärt und spielen eine wichtige Rolle: *Dividuen* (*dividu-*

als), *Wurzelgeflechte* (*rhizomes*), *Passworte* (*passwords*). Ein *Dividuum* ist ein in messbare Teilaspekte zerlegtes Individuum: ein Apparat liest messbare Attribute des Individuums, versteht es eben nicht als Ganzes, das in seiner Individualität geachtet werden muss. Der auf Unsichtbarkeit getrimmte Hintergrund an Technologie, der die *„Smart City"* und ähnlich gestrickte Visionen ausmacht, ist ein *Wurzelgeflecht* – ein recht treffendes Bild. *Passworte* sind authentifizierende oder legitimierende Informationen bzw. Artefakte, über die eine Person verfügt: eine PIN, eine Schlüssel- oder Kreditkarte, eventuell auch biometrische Merkmale. Die Kontrolle liegt nicht bei dieser Person: Zugangsberechtigt ist sie von Gnaden des Systems, das ebensogut beschließen kann, sie zu delegitimieren, nicht mehr in ihr eigenes Haus zu lassen. Problematische Aspekte bleiben demnach bei technokratischen Überlegungen zum Aufbau einer *„Smart City"* außer Acht oder werden gleichsam in den AGB versteckt, die es abzunicken gilt.

Klassische Bürokratien dividualisieren gern: Bei Zensus und Mikrozensus wird dem/der Befragten keinesfalls zugestanden, selber zu entscheiden, welche der teils intimen Fragen er/sie beantworten möchte oder für relevant hält.[18] Dabei zwingen genaue Daten offensichtlich nicht zu guter Planung, angebrachter wäre die Klärung der Bedürfnisse mündiger Bürger in einem Dialog. Die *„Smart City"* wiederholt diesen Fehler: eine Gesellschaft als mess- und steuerbares System und ihre Individuen als dividualisierte Datenbündel und nicht als selbstbestimmte Subjekte anzusehen. Das ist schade, da im Volkszählungsurteil das Grundrecht auf informationelle Selbstbestimmung erkannt wurde.[19]

„Smarte" Systeme erkennen Fehlverhalten. *„Smarte"* Infrastruktur kann auf Menschen einwirken: Demonstranten werden über ihre *„Smartphones"* registriert, Anti-Demo-Drohnen sind aus der dystopischen Fiktion auf den realen Markt gewandert (Sadowski und Pasquale, Abschnitt VI). Das Spektrum der Kontrolle ist breit. Durch die digitale Vermittlung von Verrichtungen sowie die Anbindung an Server, die Identität, Legitimation, Vergangenheit prüfen können, weicht der Dialog mit der Umwelt einer strategisch geprägten Beziehung. Wie kann ich das System dazu bringen, nicht gegen mich zu arbeiten? Anders herum: Wie lassen sich vorgegebene Ziele durch Einwirkung auf die Nutzer optimieren? Die automatische Einwirkung durch eine automatisierte Infrastruktur, die das Verhalten der Bewohner im Sinne der Verwaltung und privater Partner steuert (optimiert), ist Kernaspekt der *„Smart City"*.

„Fifth Utilities" und die Selbstverständlichkeit der Überwachung; Eskalation durch Sicherheit; wem gehört die Stadt der Zukunft?

Utilities sind Versorgungsinfrastrukturen: Strom, Wasser, Gas, Telekommunikation. Ironisch werden Kameras (in Sadowski und Pasquale, Abschnitt V) zur *Fifth-Utility* erklärt – wegen der schockierenden Selbstverständlichkeit, mit der Überwachbarkeit als neue Norm etabliert wird, natürlich immer mit den besten Absichten, was aber, wie Sadowski und Pasquale bemerken, Makulatur ist: Niemand hält sich an Absichten.

Was zählt, sind geschaffene Fakten. Die *„Smart City"* wird uns wohl genau zuschauen und -hören. Der Umbau der Stadt in eine private Werbefläche,[20] euphemistisch *Stadtmöblierung*, hat ebenfalls *fifth-utility*-Charakter. Versuche mit Gesichtserkennung laufen auch schon.[21,22] Ein Dialog zwischen Gleichen sieht anders aus. Wem gehört die Stadt der Zukunft?

Nach Sadowski und Pasquale wird in der *„Smart City"* Ungerechtigkeit eher ausgebaut als gemildert. Überwachung wird komplementiert durch *Sicherheit*. Kameras mit *Intentionserkennung* und Taserpistolen – ein Sinnbild für die Implikationen der *„Smart City"* für die innere Sicherheit: Resignation entsteht, *„smarte"* Kontrolltechniken schränken die Handlungsfreiheit derart ein, dass die Frustration in Gewalt umschlagen kann: Friedlicher Protest wird erstickt. Realwelt und Internet konvergieren (*cyborg urbanization*, Sadowski und Pasquale, Abschn. VII): Eine *Infrastruktur der Unfreiheit* wird aufgebaut.[23,24]

Zurück in *die Zukunft*: wer kontrolliert wen? Die Idee des Regelkreises passt, zumal bei *„Smart"* ein naiver Effizienzgedanke im Vordergrund steht, siehe Lanier.[25] Ist die *„smarte"* Zukunft eifrigen Selbstoptimierern vorbehalten, deren Teilhabe am Leben stets über irgendeine kommerzielle Plattform vermittelt ist? Eine traurige Vorstellung. Wer kontrolliert was? Versprechen, dass die Kontrolle über die eigenen Daten beim Kunden bleibt, sind nichts wert: Nur nachprüfbare technische Umsetzungen des Prinzips sind glaubwürdig. Natürlich ist *„Smart City"*-Forschung auch durch Idealismus und Kreativität getrieben. Unterliegt die Entscheidung, was wie zum Einsatz kommt, Betriebswirtschaft und Macht, negieren diese jedoch das emanzipatorische Potenzial nützlicher Technologie. Ein Ausweg kann darin bestehen, die Beziehung zur Technologie neu zu denken: In einem freiwilligen Modell, bei dem die Kontrolle über Programmierung und Betrieb aller Endgeräte beim Nutzer liegt und kein Dienst persönlich identifizierbare Daten sammelt, ließen sich manche Vor-

Nils Erik Flick

Nils Erik Flick ist Doktorand in der Informatik an der Carl von Ossietzky Universität Oldenburg und seit 2011 FIfF-Mitglied. Seine Forschungsschwerpunkte sind Software-Verifikation und formale Sprachen, seine Interessengebiete u. a. Computer-Sicherheit und Kryptologie.
Kontakt: *flick@informatik.uni-oldenburg.de*

teile realisieren. Vernetzung ist gedanklich von allem zu trennen, das lokal realisierbar ist. Zu aggregierende Daten ließen sich dann durch datensparsame Algorithmen verknüpfen[26,27]. Proprietäre Systeme sind ebenfalls kritisch zu sehen. Eine löbliche Ausnahme vom Trend, IT-Riesen zu beauftragen, ist Barcelona:[28] Implementation in freier Software, Messdaten als *Open Data*. Die Verdrängung proprietärer *Lösungen* durch freie, selbstorganisierte Projekte ist ein richtiger Schritt und kann z. B. das Offenhalten von Sicherheitslücken verhindern. Gute Intentionen genügen aber nicht: Auch *Big Other* bedroht die informationelle Selbstbestimung.[29]

Fazit, Konklusion und Ausblick

Im Vortrag *„We lost the war"* von 2006 warnten Frank Rieger und Rop Gonggrijp vor einer bevorstehenden dunklen Zeit des Grundrechteabbaus und gaben zu bedenken, dass den wenigen AktivistInnen nicht genügend Mittel zur Verfügung stünden, um alle Schlachten zu schlagen.[30] Der Trend zum automatischen Polizeistaat hält an. Es zeigt sich, dass die Interessen staatlicher Überwacher und kommerzieller Datensammler miteinander vereinbar sind und sich im *Big Data* treffen. Das Potenzial zum Missbrauch von Scorings oder Rohdaten durch staatliche Stellen ist ein Grund, vernetzte Sensoren abzulehnen. Der Artikel von Sadowski und Pasquale liefert einen Beitrag dazu, den ideologisch verzerrten und von Schönrednerei geprägten Diskurs über *„Smart Cities"* gerade zu rücken und vor Überwachung und Kontrolle zu warnen. Viele der Referenzen, darunter weitere zum Thema *„Smart Cities"*, sind lesenswert. Sadowski und Pasquale helfen, *„Smart City"* Pläne besser einzuordnen.

Ist die Bekämpfung von *PESTs* (*Privatsphäre-erodierende „Smart"-Technologien*, im Englischen auch *Parasiten* …) eine Schlacht, die geschlagen werden muss? Ist eine Eindämmung realistisch oder muss man anders ansetzen? Lanier z. B. scheint in seinem zitierten Essay aufgegeben zu haben und fordert eine faire Vergütung als zweitschlechteste Alternative zum zentralisierten unbezahlten Datenraub. Solange eine starke Gegenbewegung fehlt, bleibt der Unmut über die Usurpation vormals freier Lebensbereiche durch *Big Data* eine müßige, solitäre Beschäftigung. Freiräume werden marginalisiert, bedrängt durch autoritäre Strömungen, die die von Sadowski und Pasquale skizzierte Version der *„Smart City"* wohl begrüßen werden. Es ist daher geboten, überwachungs- und dividualisierungsfreie Zonen zu verteidigen, und in die Offensive zu gehen. Datensparsamkeit muss *cool* werden. Abgesehen von Datenschutzbedenken wäre es auch gar nicht dumm (geradezu *smart*!), die wachsende Abhängigkeit von Computersystemen zu überdenken, nicht zu intensivieren.

Anmerkungen

1 Vorweggenommen von Douglas Adams in „Per Anhalter durch die Galaxis", wo eine solche Funktion ungeahnte Konsequenzen hat. Douglas Adams, „Life, the Universe and Everything" (1982, ISBN 0-345-39182-9).

2 Jathan Sadowski and Frank Pasquale, The spectrum of control: A social theory of the smart city. First Monday Peer-Reviewed Journal on the Internet, http://www.firstmonday.org/ojs/index.php/fm/article/view/5903

3 R. Kitchin, 2014. "The real-time city: Big data and smart urbanism," GeoJournal, vol. 79, no. 1, pp. 1–14.

4 John Bellamy Foster and Robert W. McChesney, Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age. Monthly Review, http://monthlyreview.org/2014/07/01/surveillance-capitalism/

5 Shoshana Zuboff, 2015. „Big Other: Surveillance Capitalism and the Prospects of an Information Civilization". Journal of Information Technology (2015) 30, 75–89. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754

6 Nach zaghaften Modellversuchen in der Branche beschliesst die Telekom 2015, alle Mobilfunkkunden zu tracken und die Erkenntnisse zu verkaufen. https://netzpolitik.org/2015/data-analytics-deutsche-telekom-rastert-mobilfunk-vorratsdaten-zu-kommerziellen-zwecken/

7 Kreditech: „The Kreditech Group uses big data algorithms and automated processes to score everyone worldwide, also the 4bn [4 Milliarden] unbanked that do not have a credit score." https://www.datenschutz.de/news/detail/?nid=5905

8 Mordini, Emilio. „Ethics and Policy of Biometrics." Handbook of Remote Biometrics. Springer London, 2009. 293-309.

9 Wright, David, et al. „Sorting out smart surveillance." Computer Law & Security Review 26.4 (2010): 343-354.

10 Am Datenschutz krankt es schon in den unteren Netzwerkschichten: Der IPv6-Standard [RFC 4862, „stateless autoconfiguration"] sieht auch für mobile Geräte zunächst eine eindeutige und unveränderliche Netzwerkschnittstellen-Kennnummer vor, die in der globalen IPv6-Adresse des Gerätes eingebaut ist. Erweiterungen wie das Würfeln der Geräteadresse [RFC 4941] sind in billigen Chips kaum zu erwarten. Schon heute haben etwa WLAN-Chips in mobilen Geräten die problematische Eigenschaft, eine weitgehend eindeutige Hardware-Adresse (MAC) zu nutzen, die oftmals nur unter Schwierigkeiten temporär geändert werden kann. Damit lassen sich Bewegungsprofile, zunächst der Dinge, davon abgeleitet natürlich auch der Besitzer erstellen. Dies gehört, ebenso wie die Frage, welche Datenverarbeitung lokal geschieht und welche auf den Servern eines „Cloud"-dienstleisters, zu den unsichtbaren Eigenschaften der Technologie, die aber als essenziell zu betrachten sind und nur in einer unehrlichen oder fehlinformierten Abstraktion ignoriert werden können.

11 Z. B. Fitnessmessgeräte von der Firma OMRON, http://www.omron-healthcare.de/. Zum Herunterladen der Daten auf den PC wird offenbar eine Anmeldung nebst Zustimmung zu Datensammel-AGB in einem Online-Portal verlangt. Der Treiber liegt nicht bei, und die Verpackung warnt nicht. Marketing-Claim auf der OMRON-Homepage: „Wir stellen den Mensch vor die Technologie" (sic, mit Deppenbeugung).

12 Meldegesetz: https://www.datenschutzbeauftragter-info.de/neues-meldegesetz-der-staat-als-adresshaendler/

13 Samsung möchte das „Internet of Things" vorantreiben: http://www.technologyreview.com/news/533941/ces-2015-the-internet-of-just-about-everything/; IBM: „Smarter Planet"-Kampagne

14 http://www.zeit.de/digital/datenschutz/2013-11/smart-meter-teuer-daten-vermarkten

15 Siehe Beiträge zur eGK in früheren Ausgaben der FIfF-Kommunikation.

16 Evgeny Morozov, 2014. „To Save Everything, Click Here: The Folly of Technological Solutionism", ISBN 978-1610393706

17 Gilles Deleuze, 1995. „Negotiations, 1972–1990". (Transl.: Martin Joughin), Columbia Univ. Press, ISBN 978-0231075817

18 www.devianzen.de/2014/12/31/das-recht-in-ruhe-gelassen-zu-werden/

19 Volkszählungsurteil von 1987: http://www.servat.unibe.ch/dfr/bv065001.html. Zugleich wurden im Urteil Grenzen für das Recht auf informationelle Selbstbestimmung vorgesehen, falls das „öffentliche Interesse überwiegt".

20 Straßenkunst oder kreative Verfremdungen oder Richtigstellungen der Werbung können als Vandalismus verfolgt werden, während andersherum ziemlich viel Narrenfreiheit herrscht: die Anregung zum Überkonsum hat eine privilegierte Stellung inne. Sieht so Fortschritt aus? Die Stadt als kommunikative Einbahnstraße? Wird sich die „Smart City"-Entwicklung in diese Kette von Entfremdungen einreihen?

21 TESCO-Tankstellen missbrauchten Gesichtserkennung für Werbung, http://www.bbc.co.uk/news/technology-24803378

22 Keine Konzessionen bei kommerzieller Gesichtserkennung: https://firstlook.org/theintercept/2015/06/16/privacy-advocates-resign-protest-u-s-facial-recognition-code-conduct-2 – Es stellt sich ohnehin die Frage, mit welcher Legitimation datensammelnde und -verarbeitende Industrie überhaupt zum *Stakeholder* in der Privatsphäre anderer erklärt wird.

23 Eben Moglen (siehe Endnote 24) – mit dem Unterschied, dass die Datenspuren in der realen Welt sehr viel breiter und sehr viel schlechter zu verschleiern sind, wenn einmal eine ähnliche Überwachungsdichte erreicht wird. Es ist unmöglich, der Überwachung in der realen Welt durch Kryptographie zu entkommen. Daher führt der Ausbau hier in eine noch sehr viel unfairere Lage als theoretisch im *Cyberspace*. Die Konvergenz läuft natürlich auch anders herum, etwa durch realweltliche Verbote sicherer Endgeräte (oder deren pervasive Kompromittierung http://www.ceu.edu/article/2015-01-19/real-world-battles-will-be-won-or-lost-internet-doctorow-says).

24 Eben Moglen, Snowden and the Future, http://snowdenandthefuture.info/ (4 Vorträge)

25 Lanier, Jaron. Who owns the future? Penguin, 2014, ISBN 978-0-241-95721-9 [S. 42 ff.]

26 *Secure Multiparty Computation* erlaubt es, beliebige Funktionen auf Datensätzen zu berechnen, ohne jedoch zusätzliche Information über den Inhalt zu verraten.

27 Yehuda Lindell, Benny Pinkas, 2009. „Secure multiparty computation for privacy-preserving data mining". Journal of Privacy and Confidentiality 1, no. 1, pp. 59–98

28 Open Source, Open Data Barcelona: http://smartcity.bcn.cat/en/sentilo.html; anderes Projekt: https://smartcitizen.me/

29 Shoshana Zuboff, 2015. „Big Other: Surveillance Capitalism and the Prospects of an Information Civilization". Journal of Information Technology (2015) 30, 75–89. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754

30 „We lost the war". Vortrag von Rop Gonggrijp und Frank Rieger (CCC) auf dem 22c3, https://events.ccc.de/congress/2005/fahrplan/events/920.en.html

vor*gänge* – Zeitschrift für Bürgerrechte und Gesellschaftspolitik

Cybersecurity

Der NSA-Überwachungsskandal hat deutlich gemacht, in welchem Umfang und mit welcher Reichweite westliche Geheimdienste die Überwachung der Kommunikationsnetze betreiben. Der damit verbundene finanzielle, technische und personelle Aufwand lässt erahnen, dass es dabei keineswegs nur um die Ausforschung der Privatsphäre mehr oder weniger ahnungsloser Bürger.innen geht. Die Zeiten, in denen der Cyberspace nur dem Gedankenaustausch diente, sind längst vorbei; die Datennetze sind zur zentralen Infrastruktur unserer Gesellschaft geworden. Ihre Überwachung zielt deshalb nicht nur auf jene, die per E-Mail, Chat oder Onlineplattformen kommunizieren, sondern kann buchstäblich jede.n treffen: ob am Bankautomaten, in der Arztpraxis, bei der Arbeit oder im vernetzten Heim. Der „Cyberspace" ist zu einem Ort geworden, an dem sich neue Formen der Kriminalität, des Krieges und der terroristischen Bedrohung entwickeln, aber auch neue Strategien der Sicherheit erprobt werden. Diese Ausgabe der **vor*gänge*** widmet sich dem Thema Cybersecurity, der zunehmenden sicherheitspolitischen Durchdringung des digitalen Raumes.

*aus dem Editorial der **vor**gänge 209 (Heft 1/2015) von Claudia Krieg und Sven Lüders*

Martin Ehrenhauser, Alexander Sander

Politik im Dienst der Sicherheitsindustrie

Politik sollte die unterschiedlichen Einzelinteressen gerecht ausgleichen. Die Praxis sieht jedoch anders aus. Deutsche Europaabgeordnete dienen als Lobbyist.innen der nationalen Sicherheitsindustrie. Ein Fallbeispiel über die fehlende Trennung zwischen Politik und Lobbyismus.

Der europäische Sicherheitsmarkt ist einer der am stärksten wachsenden Wirtschaftsbereiche der Europäischen Union (EU). Laut den aktuellsten Zahlen der Europäischen Kommission, ist das weltweite Marktvolumen innerhalb von zehn Jahren von etwa zehn auf rund 100 Milliarden Euro im Jahr 2011 angewachsen und hat sich damit – trotz der Krise – verzehnfacht. Die europäischen Unternehmen haben mit einem Jahresumsatz von 25 bis 36 Milliarden Euro einen Anteil von etwa 25 Prozent am Weltmarkt. Rund 180.000 Personen arbeiten europaweit in diesem Sektor. Die europäische Sicherheitswirtschaft ist damit ein wichtiger Faktor auf dem globalen Sicherheitsmarkt und ein Schwergewicht der europäischen Wirtschaft.[1]

Zur Unterstützung dieser Industriebranche investiert die EU: knapp 1,7 Milliarden Euro werden bis zum Jahr 2020 in die Sicherheitsforschung fließen.[2] Die Ausgaben sind Teil des EU-Rahmenforschungsprogramms *Horizon 2020*. Das Ziel ist, wie beinahe in jedem EU-Programm erklärt wird, durch Innovationen bei Produkten, Dienstleistungen und Prozessen, die Wettbewerbsfähigkeit der europäischen Unternehmen zu erhöhen und dadurch mehr Wachstum und Arbeitsplätze zu schaffen.[3]

Oder kurz formuliert: *Horizon 2020* ist ein Subventionsprogramm für die europäische Sicherheitsindustrie. Denn Grundlagenforschung, etwa im Bereich Datenschutz, oder sozial- und rechtswissenschaftliche Untersuchungen werden nur in marginalem Ausmaß gefördert. Das zeigt auch eine Analyse des Vorgängerprogramms FP7, dem 7. Rahmenforschungsprogramm der EU. Unter den Top-10-Projektteilnehmern befinden sich vor allem multinationale Unternehmen, etwa EADS oder Thales. Mit rund 43 Prozent ist die Industriebeteiligung an der Sicherheitsforschung im Vergleich zu anderen Forschungsfeldern überdurchschnittlich hoch. Die Erfolgsrate ist jedoch, laut der Europäischen Kommission, mit 16 Prozent äußerst niedrig.[4]

Der Zugang zu den Brüsseler Forschungsgeldern ist hart umkämpft. Unzählige Interessenvertreter.innen versuchen gegenüber der Politik die Höhe der Forschungsgelder, die Ausschreibungskriterien oder den Verwendungszweck zu beeinflussen und begleiten gleichzeitig die Unternehmen während des gesamten Ausschreibungsprozesses. Der direkte Zugang zu den politischen Entscheidungsträger.innen ist dabei eine Grundvoraussetzung für den Erfolg. Die klare Trennung zwischen Lobbyismus und Politik, die es den Amtsträger.innen ermöglichen soll, unabhängig und im Sinne des Gemeinwohls Entscheidungen zu treffen, wird dabei zur ineffizienten Hürde, die es zu überwinden gilt.

Lobbyismus „Made in Germany“

Der Wettbewerb um die EU-Forschungsgelder ist stark von nationalen Konflikten geprägt. Jedes Mitgliedsland versucht das größte Stück vom Förderkuchen für seine heimische Industrie zu generieren. Für die deutsche Sicherheitsindustrie lobbyiert unter anderem die *German European Security Organisation* (GESA). Der in Berlin ansässige, gemeinnützige Verein wurde im Jahr 2006 gegründet und hat sich nach eigenen Angaben zum Ziel gesetzt, Wissenschaft und Forschung zu fördern, insbesondere auf dem Gebiet der zivilen Sicherheit. Dazu gehört „die Entwicklung und Erarbeitung von Forschungszielen auf nationaler und europäischer Ebene“ sowie die „Durchführung eigener Forschungsvorhaben“.[5] Anders formuliert: Der Verein versucht die Vergabe der Forschungsmittel erfolgreich im Sinne seiner Mitglieder zu beeinflussen, etwa als die Gestaltung der Vergaberegeln für *Horizon 2020* im Europäischen Parlament auf der Tagesordnung stand. Für den Parlamentsbericht *Rule for the participation and dissemination in ‚Horizon 2020' (2014-2020)* war Christian Ehler Berichterstatter, der damalige Vorstandsvorsitzende der GESA. Er formuliert somit federführend die neuen Spielregeln. Als Schattenberichterstatter fungiert der deutsche Sozialdemokrat Norbert Glante, ebenfalls GESA-Mitglied. Die Fraktionen, die von den

Martin Ehrenhauser und Alexander Sander

Martin Ehrenhauser war von 2009 bis 2014 Mitglied des Europäischen Parlaments. Im Jahr 2013 veröffentlichte er zusammen mit Alexander Sander die Studie *Lobbyismus der Sicherheitsindustrie in der Europäischen Union*. In einer weiteren Fallstudie analysierte Ehrenhauser, wie Großunternehmen, die regelmäßig gegen Gesetze verstoßen, in den Beratungsgremien der Europäischen Kommission politische Entscheidungen beeinflussen. Ehrenhauser ist u. a. Mitunterzeichner der österreichischen Verfassungsklage gegen die Vorratsdatenspeicherung.

Alexander Sander ist Geschäftsführer des Vereins *Digitale Gesellschaft* in Berlin. Als Mitarbeiter von Martin Ehrenhauser veröffentlichte er zusammen mit ihm im Jahr 2013 die Studie *Lobbyismus der Sicherheitsindustrie in der Europäischen Union.*

beiden Europaabgeordneten im zuständigen Industrie-Ausschuss vertreten wurden, stellten mit 38 von insgesamt 61 stimmberechtigten Abgeordneten die deutliche Mehrheit. Beste Voraussetzungen für die Neugestaltung im Sinne der GESA-Mitglieder.

Christian Ehler, Schattenberichterstatter für den entscheidenden Parlamentsbericht, setzte sich auch erfolgreich dafür ein, als es darum ging, die Fördergeldmenge für die Sicherheitsindustrie auszuweiten: Bis *Horizon 2020* wurden aus dem Forschungsrahmenprogramm lediglich zivile Forschungsprojekte unterstützt, jedoch keine militärischen. Damit war der Zugang zu einem großen Teil der EU-Fördergelder für die Sicherheitsindustrie limitiert. Das musste sich ändern. Durch die Förderung von sogenannten „Dual-Use-Technologien", also Technologien, die sowohl zivil als auch militärisch einsetzbar sind, wurde mit diesem Grundsatz gebrochen.

Herzliche Einigkeit

Gegründet wurde die GESA unter anderem von acht deutschen Europaabgeordneten, darunter Alexander Graf Lambsdorff von der FDP (heute Vizepräsident des EU-Parlaments), Erika Mann von der SPD (derzeit Lobbyistin für Facebook) oder eben Christian Ehler von der CDU. Die Logik des Vereins ist rasch erklärt: Wer zahlt, bekommt exklusiven Zugang zu den politischen Entscheidungsträger.innen und kann seine politischen Interessen effektiver durchsetzen als die Konkurrenz. Vereinsmitglieder, wie etwa der Rüstungskonzern *EADS Deutschland GmbH* oder der Hersteller von Nacktscannern *Smith Heimann GmbH*, müssen jährlich bis zu 5.000 Euro Mitgliedsbeitrag zahlen.

Dass die Tätigkeit als politische.r Amtsträger.in mit der Tätigkeit als Lobbyist.in der deutschen Sicherheitsindustrie für viele Europaabgeordnete Hand in Hand geht, belegen zahlreiche Beispiele. Bereits bei der Gründung hatte die damalige Vize-Vorsitzende Erika Mann in der Presseaussendung ihren parlamentarischen Assistenten für Rückfragen als Kontaktperson angegeben. Ähnliches gilt auch für die parlamentarische Mitarbeiterin von Christian Ehler. Aus ihrem E-Mail-Verkehr wird ersichtlich, dass diese organisatorische Aufgaben für die GESA übernahm. So wurden Vertreter.innen der Europäischen Kommission zu verschiedenen GESA-Veranstaltungen eingeladen.[6] Die Tätigkeit für die GESA ist damit nicht mehr losgelöst vom Mandat zu betrachten. Das Lobbying für die Sicherheitsindustrie übernimmt der/die Politiker.in und sein/ihr Personal persönlich. Die Kosten dafür tragen nicht mehr das Unternehmen oder der Verein, sondern die Steuerzahler.innen.

Allerdings existiert seit 1. Januar 2012 ein Verhaltenskodex für Mitglieder des EU-Parlaments. Darin wurden Leitprinzipien für die Mitglieder definiert. Danach müssen diese bei der Ausübung ihres Mandats nach der Maßgabe von „Uneigennützigkeit, Integrität und Transparenz" handeln. Die Mitglieder handeln „nur im öffentlichen Interesse und erlangen oder erstreben keinerlei unmittelbaren oder mittelbaren finanziellen Nutzen oder eine sonstige Zuwendung." Es wurde festgelegt, dass Mitglieder „keinerlei Vereinbarung" eingehen, um „im Interesse einer anderen juristischen oder natürlichen Person zu handeln oder abzustimmen."[7]

Mit Blick auf die Gesamtkonstruktion der GESA ergeben sich viele Fragwürdigkeiten, denn die Arbeit der GESA ist keine Arbeit im öffentlichen Interesse, sondern im Interesse der zahlenden Unternehmen. Auch dürfen parlamentarische Assistent.innen ausschließlich für Tätigkeiten in Zusammenhang mit der Mandatsausübung eingesetzt werden. Für Christian Ehler war die Arbeit der Assistentin für die GESA ein „Einzelfall" der „nicht beabsichtigt gewesen" wäre. Und überhaupt: „Viele Abgeordnete engagieren sich für gemeinnützige Belange. Wenn Sie das verbieten, müssen Sie alle Abgeordneten rausschmeißen, die ADAC-Mitglied sind." Für ihn, so Ehler, sei die GESA ein „gemeinnütziger Verein wie die Caritas."[8]

Zähe Transparenz

Die enge Verzahnung zwischen Politik und Wirtschaft, die sich in der GESA widerspiegelt, haben die Autoren in einer umfassenden Studie mit dem Titel *Lobbyismus der Sicherheitsindustrie in der Europäischen Union* im Februar 2013 thematisiert. Nach der Veröffentlichung reagierte die GESA zunächst verärgert. Dass die Europaabgeordneten die Interessen der deutschen Sicherheits- und Rüstungsindustrie vertreten sei „wahrheitswidrig", so eine Vertreterin der GESA. Sollte Gegenteiliges behauptet werden, würde man dies als „Verleumdung" auffassen, gegen die juristische Schritte angewendet werden.[9]

Juristische Schritte wurden bisher keine eingeleitet, schließlich wollte man auch nur abschrecken. Echte Transparenz bei der Tätigkeit der GESA war eben nicht erwünscht. Marginale Veränderungen wurden vorgenommen, etwa die Postanschrift. Zuvor war es der Platz der Republik 1, in 11011 Berlin, dort hat der Deutsche Bundestag seinen Sitz und auch Christian Ehler sein CDU-Büro. Dabei diente diese Adresse wohl eher als Briefkasten, denn der eigentliche Sitz der GESA-Geschäftsstelle war im nahegelegenen Potsdam, in der Gregor-Mendel-Straße. Auch dort hat Christian Ehler ein weiteres Büro, sein „Europabüro". Gleichzeitig hat unter dieser Anschrift auch die Landesgeschäftsstelle der CDU Brandenburg und die Junge Union Brandenburg eine Postanschrift. Nach der Veröffentlichung der Fakten ist die GESA umgezogen. Heute residiert der Verein „unabhängig" im Berliner Stadtteil Charlottenburg.

Auch die Struktur der GESA wurde leicht verändert. Sämtliche Vorstandsmitglieder, die gleichzeitig als Abgeordnete tätig waren, sind heute nicht mehr im Vorstand. Scheinbar sollte die zuvor kritisierte enge Verzahnung von Mandat und Vorstandstätigkeit aufgelöst werden. Mit der Neubesetzung des Vorstandes führte die GESA jedoch einen Beirat ein. In der Satzung der GESA heißt es zu den Aufgaben des neuen Gremiums: „Vorstand und Geschäftsführung werden bei ihrer Arbeit von einem Beirat unterstützt und beraten."[10]

Ehemalige Vorstandsmitglieder, die noch immer im EU-Parlament aktiv sind, etwa Monika Hohlmeier[11] und Christian Ehler[12], sind beide nun Mitglieder des Beirates der GESA. Auch der Bundestagsabgeordnete Hans-Peter Uhl, ehemaliges Vorstandmitglieder der GESA, sitzt im Beirat.[13] Die Änderungen sind rein kosmetischer Natur. Eine klare Trennung zwischen Politik und Lobbyismus sieht anders aus. Die GESA veröffentlichte nach der Publikation unserer Studie zwar, wer Mitglied des Vereins ist;

wer jedoch neben den oben Genannten Mitglied des Beirates ist, erfährt man auf der Internetseite der GESA nicht. Mit dem Beirat wurde sogar noch weiter zur Verschleierung der Arbeit des Vereins beigetragen, da nur über Umwege ersichtlich wird, wer Einfluss auf die Arbeit der GESA nimmt. Hinzu kommt, dass die allgemeinen Informationen auf der Internetseite des Vereins deutlich weniger werden. Im Bereich „Rückblick" ist der letzte Beitrag vom Juni 2013, der letzte „Kalendereintrag" vom Oktober 2014, der „Terminplaner" ist gänzlich ohne aktuelle Einträge. Zuvor konnte man an diesen Stellen Informationen über die Tätigkeit der GESA einsehen.

Die Verflechtung der Politik mit den finanzstarken Partikularinteressen, die als Art „fünfte Gewalt im Staat" die politischen Entscheidungen dirigieren, ist ein Teil der politischen Realität. Jeder der dies aus demokratiepolitischen Gründen verurteilt, wird mit Klagen bedroht. Verständnis für die Probleme die dadurch entstehen, existiert nur bei einer Minderheit der Politiker.innen. Denn anstatt die Strukturen ernsthaft zu ändern und Mandatsträger.innen zumindest aus einflussreichen Positionen im Verein zu entfernen, reagiert die GESA mit Intransparenz und versteckten neuen Strukturen, um die Einflussmöglichkeiten der Abgeordneten und damit die Attraktivität des Vereins für Unternehmen nicht zu beschneiden. Die Politiker.innen fühlen sich eben wohl in ihrer Rolle als Erfüllungsgehilfen der Sicherheitsindustrie.

Anmerkungen

1 *Vgl. Europäische Kommission: Eine Industriepolitik für die Sicherheitsbranche; KOM (2012) 417 endgültig; Brüssel, 2012; S. 2, 4.*
2 *http://ec.europa.eu/research/horizon2020/pdf/press/fact_sheet_on_horizon2020_budget.pdf.*
3 *http://www.horizont2020.de/einstieg-programmaufbau.htm.*
4 *Ehrenhauser/Sander: GESA & EOS – Lobbyismus der Sicherheitsindustrie in der Europäischen Union; Seite 13.*
5 *Satzung der GESA in der Fassung vom 18. Juni 2013, § 2.*
6 *Ehrenhauser/Sander: GESA & EOS – Lobbyismus der Sicherheitsindustrie in der Europäischen Union; Seite 12.*
7 *Ebd.; Seite 31.*
8 *Verhaltenskodex der EU-Abgeordneten.*
9 *http://www.taz.de/!5072754/.*
10 *http://www.profil.at/home/eu-lobbying-ruestungsbranche-sichere-stimmen-356960.*
11 *Satzung der GESA in der Fassung vom 18. Juni 2013, §11.*
12 *http://www.europarl.europa.eu/mepdif/96780_DFI_rev0_DE.pdf.*
13 *http://www.europarl.europa.eu/mepdif/28226_DFI_rev1_DE.pdf.*
14 *https://www.bundestag.de/bundestag/abgeordnete18/biografien/U/uhl_hans_peter/259136*

Dieser Artikel wurde zuerst in **vor***gänge* – Zeitschrift für Bürgerrechte und Gesellschaftspolitik *– veröffentlicht. Der Nachdruck erfolgt mit freundlicher Genehmigung der Redaktion.*

Birgit und Michael Ahlmann

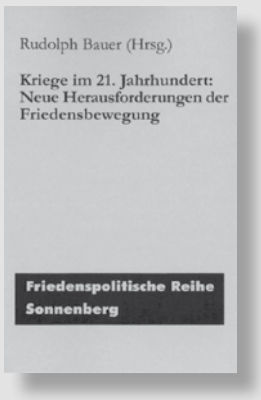
Rudolph Bauer (Hg.): „Kriege im 21. Jahrhundert: Neue Herausforderungen der Friedensbewegung"

Kriege im 21. Jahrhundert *führt vor Augen: die Art der Waffen und der Kriegführung mögen sich im Laufe der Jahrhunderte verändert haben – nicht jedoch die ideologische Mobilmachung und die Propaganda für das Militär. Hat der preußische und russische Offizier und Militärtheoretiker Carl von Clausewitz 1830 noch Regeln aufgestellt für den Einsatz der herkömmlichen Waffen und Truppen und deren taktischer Bereitstellung an der Front zum Feind (siehe* Vom Kriege – hinterlassenes Werk des Generals Carl von Clausewitz*, 1832), so werden heutzutage gerne ferngelenkte unbemannte Flugobjekte über weite Distanzen zur Aufklärung und zum Kampf verwendet.*

Clausewitz ist einer der ersten Militärtheoretiker, der die Theorie und Praxis der Kriegführung mit eigenen Erfahrungen besonders seit der französischen Revolution analysiert hat und unter anderem die *Nichtkalkulierbarkeit* eines Krieges festgestellt hat. Er sagte: „Der Krieg ist also ein Akt der Gewalt, um den Gegner zur Erfüllung unseres Willens zu zwingen." (Clausewitz: Vom Kriege, Buch I, Kap. 1, Abs. 2)

Den Menschen wird vermittelt, dass die eigene Familie, das eigene Land und die eigene Freiheit gegen feindliche Übergriffe verteidigt werden müssen. Auch diesem Phänomen, dass jede Generation wiederum mit den altbekannten Ideologien geködert wird und den Kriegstreibern mehr oder weniger auf den Leim geht, geht das Buch *Kriege im 21. Jahrhundert* nach.

Zum Einstieg verweist ein Vorwort auf die Antikriegskonferenz Berlin 2014. Deren Ziel sei es gewesen, infolge der möglichen Kriegsgefahr Widerstand gegen etwaige Kriegsvorbereitungen zu organisieren und deshalb entsprechende Entwicklungen und Kriegspropaganda aufzuzeigen.



Rudolph Bauer (Hg.) (2015):
Kriege im 21. Jahrhundert:
Neue Herausforderungen der Friedensbewegung,
Annweiler am Trifels: Sonnenberg Verlag,
374 Seiten
Preis € 19,80
ISBN 978-3-933264-77-0

Die Autoren des 2015 in der *Friedenspolitischen Reihe* des Sonnenberg-Verlags erschienenen Buchs berücksichtigen in ihren Beiträgen bereits das Geschehen im Veröffentlichungsjahr. Es ist sowohl von der Themenstellung her sehr aktuell als auch von der Herangehensweise. Die Strukturierung in die drei Bereiche *Militarisierung*, *Mobilmachung* und *Einspruch* sorgt für Übersichtlichkeit und erleichtert Leserinnen und Lesern die Auseinandersetzung mit der zahlreichen Aspekten der vielseitigen Thematik. In jedem der drei Bereiche äußern sich mehrere Autoren jeweils zu speziellen Schwerpunkten, Entwicklungen und Fragestellungen und beleuchten diese aus politischer, finanzpolitischer, sozialer, technologischer, wirtschaftlicher, juristischer, ökologischer, historischer, kommunikativer und informationeller Perspektive mit wissenschaftlicher Methodik. Weil dieses Buch so viele verschiedene kritische Perspektiven und Ansätze bietet, weil historische Hintergründe beleuchtet, Fehlentwicklungen aufgezeigt und nicht zuletzt Deutschlands Rolle im globalen Machtpoker kritisch betrachtet werden, ist es ein sehr fesselndes Buch, das geeignet ist, Augen zu öffnen und persönliche Betroffenheit – vielleicht sogar persönliches Engagement – zu erzeugen.

Die „ideologische Aufrüstung" erfolge in Deutschland (wer hätte das gedacht) bereits in den Schulbüchern. Deren Texte und Illustrationen vermitteln den Schülerinnen und Schülern ein Bild von Menschen und Gesellschaften innerhalb und außerhalb der Bundesrepublik, von Bekanntem und Fremdem, von Gemeinsamem und Trennendem. Gut und sicher ist es demnach *innen*, unsicher und gefährlich *außen*. Die Trennung nach Arm und Reich, Nord und Süd sowie West und Ost erzeuge ein bestimmtes Bild der Welt in den Schulbüchern, das sich gut als Nährboden für eine gezielte Politik eigne, der zufolge die Sicherheit der westlichen Nationen bedroht sei. Dieses hätten bekanntlich diverse Terrorakte bereits gezeigt, und folglich sei es auch Deutschlands Aufgabe, die Sicherheit seiner eigenen und der Bevölkerung seiner Verbündeten zu schützen – zunehmend durch Aufrüstung und Einsatz von Militär vor allem im Verbund der NATO. Es erscheine daher nicht verwunderlich, wenn kritische Stimmen bei dieser Art von Propaganda unter den Tisch fielen und bei etwaigen Schulbuchkontrollen kein Korrekturbedarf an den Inhalten angemahnt werde.

Aufgezeigt wird, dass die Vorbereitung der Bevölkerung auf Militär und Aufrüstung und etwaige Kriegseinsätze ebenso durch kriegerische oder Gewalt verharmlosende Computerspiele gefördert wird wie durch die Vielzahl von Kriegsfilmen in den Medien und in den Kinos – aber auch durch die Unmenge von verfügbarem Kriegsspielzeug für Kinder. Der Leser erfährt, was von den Beteiligten meist nicht kommuniziert wird, dass es nämlich eine fruchtbare Zusammenarbeit zwischen Rüstungsindustrie und Computerspiele-Herstellern gibt. Die Computerspiele liefern häufig bereits bestimmte Feindbilder, die unterschwellig oder offensichtlich bestimmte Ideologien für die militärische Aufrüstung und Kriegspropaganda transportieren.

In *Kriege im 21. Jahrhundert* wird den Lesern vor Augen geführt, dass Deutschland zwar ebenso wie andere westliche und viele weitere Staaten nach den verheerenden Folgen zweier Weltkriege seine innere und äußere Ordnung nach rechtlichen und sozialen Grundsätzen wie demokratische Verfassung, Menschenrechte, Genfer Konvention und weiteren Abkommen gestaltet hat. Sie erfahren jedoch, dass dennoch im Laufe der letzten Jahrzehnte die Politik oft genug versäumt hat, ihre Entscheidungen im Geiste der genannten juristischen, demokratischen und humanitären Grundlagen zu treffen. Wenngleich der *Kalte Krieg* Geschichte sei, so sei der Fortbestand der NATO nie ernsthaft in Frage gestellt worden, heißt es. Deutlich wird die Verflechtung von Finanzen, Politik und Militär mit der Rüstungsindustrie sowie mit den Medien aufgezeigt und aus verschiedenen Blickwinkeln beleuchtet. Eine Ergänzung der Beiträge über die globale Vernetzung und Verflechtung von Rüstungsfirmen und ihre daraus resultierenden Vorteile wäre wünschenswert, ist aber leider im Themenkatalog nicht enthalten.

Mit dem Einsatz von Atombomben und chemischen Kampfmitteln sowie an den Beispielen der Reaktorunglücke in Three Mile Island (1979), Tschernobyl (1986) und Fukushima (2011) hat sich auch das zerstörerische Potenzial der militärischen wie zivilen Nutzung von Forschungsergebnissen (*dual use*) gezeigt. Aus diesen Erfahrungen ergeben sich die Forderung und der Anspruch an Wissenschaft und Forschung und die Institutionen, Forschungsaufträge aus Politik und Industrie ausschließlich für zivile Zwecke zuzulassen.

Dieser Ansatz wird ebenfalls problematisiert – denn der Verzicht auf Forschungsgelder für militärische Zwecke setzt einerseits voraus, alle zukünftigen Anwendungsmöglichkeiten vorauszusehen (und möglichst auszuschließen), und andererseits benötigen die Hochschulen und Universitäten die Forschungsgelder der Industrie zur Aufbesserung ihres knappen Budgets. WeilTransparenz über die Ziele der Militärforschung fehlt, ist es schwer, die Zuteilungsfähigkeit beantragter Forschungsgelder zu beurteilen. Die Autoren fordern deshalb eine Transparenz- und Zivilklausel, deren Umsetzung ein hoffnungsvoller erster Schritt in Richtung zu mehr Durchblick und Beteiligung im Sinne der Demokratie wäre.

In den Beiträgen wird herausgearbeitet, dass die Digitalisierung und der Einsatz der Informationstechnologie die Sammlung und Auswertung aller möglichen Daten gewährleisten und militärische Aktionen über weite Strecken mit präziser Zieldefinition und angeblich hoher Treffsicherheit ermöglichen. Der Kampf Mann gegen Mann oder Heer gegen Heer wird zunehmend ersetzt durch ferngelenktes Gerät, durch die Zerstörung auf Knopfdruck. Die Sicherheitstechnik ist in zunehmendem Maße von der Informations- und Kommunikationstechnik abhängig. Die alltägliche Versorgung der Gesellschaft mit Wasser oder Energie ist ohne digitale Technik nicht mehr vorstellbar. Dadurch sind die zivilen Bereiche angreifbarer geworden. Es wird darauf hingewiesen, dass die mögliche Bedrohung durch einen Cyberkrieg zwar zunimmt, dass jedoch die verstärkte Aufrüstung des Militärs dagegen so gut wie gar nichts nützt.

Für die USA ist die amerikanische Militärbasis in Ramstein beim Einsatz amerikanischer Drohnen gegen Ziele im Nahen Osten von ganz zentraler Bedeutung, und Deutschland spielt in diesem Kontext eine problematische Rolle. Aus Sicht der Länder, die Ziel der amerikanischen Drohnen sind, wird Deutschland folglich als feindliche Nation angesehen, die bekämpft werden muss.

Aufgezeigt wird auch die erneute Ausbreitung des Lobbyismus der Rüstungsindustrie in Politik, Medien und zivilem Tagesgeschehen – trotz zweier Weltkriege – und wie Politik und Polizei ebenso wie Militär aus Einzelaktionen ein breites Bedrohungsszenario durch feindliche Mächte oder Terroristen ableiten. Dies wird wiederum zur Manipulation genutzt: die erzeugte Angst vor Bedrohung von

außen und das erhöhte Sicherheitsbedürfnis der Bevölkerung dienen den Regierenden als Rechtfertigung für die Erweiterung und Vermischung von militärischen und polizeilichen Aufgaben.

Als Bedrohungsargumente werden angeführt: soziale Probleme wie die extrem hohe Jugendarbeitslosigkeit vor allem im Süden Europas, die wachsende Distanz der Einkommen von Arm und Reich sowie die *Flut der Asylanten*. Europa steht vor neuen Aufgaben, doch führen diese nicht dazu, mögliche Lösungen für mehr Gerechtigkeit in der Gesellschaft zu suchen, sondern dienen der Politik der Herrschenden als Begründung für eine weitere Militarisierung. Die gleichzeitige Zunahme nationalstaatlichen Denkens, so ist zu lesen, begünstige Abschottung, Fremdenfeindlichkeit, Aufrüstung und Militarisierung.

Industrialisierung, Imperialismus, Kapitalismus, Kriege und sonstige macht- und gewinnorientierte Unterdrückungsmaßnahmen haben dazu geführt, dass Menschen in anderen Ländern ihrer Lebensgrundlagen beraubt wurden. Die Industriestaaten verklappen ihren Müll in den ärmsten Ländern und verseuchen dort das Trinkwasser. Europäischer Wohlstand wurde und wird mit der Armut der Menschen im Osten und Süden des Kontinents und der Erde bezahlt. Einerseits sind die Folgen hiervon Piraterie, Diebstahl und andere Überfälle bis hin zu Terrorakten, und andererseits resultieren daraus die wachsenden Flüchtlingsströme. Die Menschen aus den Ländern, die durch Imperialismus und Kapitalismus ausgebeutet wurden, stehen nun als Einwanderer vor den Türen der reichen europäischen Länder. Flüchtlinge aus Kriegsgebieten suchen in Europa Asyl. Diese Menschen werden als Bedrohung empfunden, gegen die man sich abschotten, vor denen man die Grenzen schließen muss und derentwegen Polizei und Militär gut (auf)gerüstet sein sollen.

Deutschland hat sich weit von seiner Erklärung „nie wieder Krieg“ entfernt. Ein Beitrag hebt hervor, dass in 2014 die Bundeswehr an 17 verschiedenen Einsätzen weltweit beteiligt war. Es wird bezweifelt, dass diese sämtlich der Sicherung der Landesgrenzen der Bundesrepublik dienen. So erklärt sich, warum der ehemalige Bundespräsident Köhler letztlich von seinem Amt zurücktreten musste: er hatte den *Fauxpas* begangen öffentlich zu bemerken, die Kriegspolitik der Bundesrepublik hänge direkt mit den wirtschaftlichen Interessen der Exportwirtschaft zusammen.

Die westlichen Machthabenden sind bestrebt, das Kriegsgeschehen in der Welt möglichst in entfernten Ländern zu belassen, das geht aus einigen Beiträgen hervor; dennoch wird zugleich im Inneren des eigenen Landes die Aufrüstung vorangetrieben. Das Militär wird inzwischen als Bestandteil der Normalität dargestellt. Der Werbeetat der Bundeswehr für Nachwuchsgewinnung und zur Imagepflege wächst beständig – und neuerdings werden an deutschen Schulen Lehrerinnen und Lehrer sowie Referendare und Referendarinnen eingeladen, an Seminaren über die Bundeswehr teilzunehmen. Ergänzt wird diese Bundeswehrwerbung für Jugendliche durch ein Angebot an Spaß- und Sportveranstaltungen. Dies hat dazu geführt, dass der UN-Ausschuss für die Rechte des Kindes Anfang 2014 empfahl, alle auf Kinder gerichteten Werbemaßnahmen der deutschen Streitkräfte zu verbieten. Dieser Empfehlung will die Bundesregierung jedoch nicht folgen.

Ein Beitrag fordert mehr alternative Medien, um der militärfreundlichen Berichterstattung und der Bauernfängerei von Jugendlichen etwas entgegensetzen zu können: nämlich mehr Transparenz und mehr kritische Beiträge.

Die UN-Charta gibt in Kapitel 6 vor, dass Streitigkeiten zwischen den Mitgliedstaaten friedlich beigelegt werden sollen. Im Zuge des Ukraine-Konfliktes verhängen besonders die USA harte Sanktionen gegen Russland. Die wirtschaftlichen Beziehungen zwischen Russland und Deutschland haben sich bereits spürbar verschlechtert, weil die Bundesregierung die amerikanischen Sanktionen gegen Russland unterstützt. Gemäß der UN-Charta müssten jedoch die kriegstreibenden Sanktionen aufgegeben werden, denn es geht darum, Kriege im 21. Jahrhundert zu verhindern und den Gedanken der *kollektiven Sicherheit* umzusetzen, wie er auch von der OSZE (57 Mitgliedsstaaten) vertreten wird.

Kriege im 21. Jahrhundert zeigt die zunehmende Militarisierung und kriegsfördernde Gefahren auf. Es weist auf Fehler der Vergangenheit sowie der Gegenwart hin. Zugleich erinnert es an vorhandene globale Spielregeln für friedliche Konfliktlösungen zur Verhinderung von Kriegen. Man muss diese Regeln allerdings anerkennen, wiederbeleben, sich für sie einsetzen, sie umsetzen. Weil jeder Einzelne diese Verantwortung trägt, sollte jede/r dieses wichtige Buch lesen und weiterempfehlen: „Give peace a chance!“ (John Lennon)

Birgit und Michael Ahlmann

Nach dem Studium des Informationsdesigns an der FH Kiel arbeitete **Birgit Ahlmann** zunächst als Grafikerin, studierte dann Soziologie und Anglistik/Amerikanistik an der CAU Kiel und arbeitete danach als PR-Managerin und Messespezialistin in der Maschinenbauindustrie. Anschließend war sie elf Jahre Betriebsratsvorsitzende und stellvertretende Gesamtbetriebsratsvorsitzende und leitete die IT-Ausschüsse in Betriebsrat, Gesamtbetriebsrat und Konzernbetriebsrat. Weiterhin gilt ihr aktuelles Interesse der Gestaltung der Zukunft von Arbeit und Umwelt.

Michael Ahlmann studierte an der CAU in Kiel Mathematik und Physik. An der Universität Hannover erwarb er den Diplom-Ingenieur für Allgemeine Elektrotechnik. In einem Elektronikunternehmen in Bremen arbeitete er als Softwareentwickler und Betriebsrat. Neben den Aufgaben eines Betriebsratsvorsitzenden leitete er einen Gesamt- und einen Konzernbetriebsrat und wirkte in zwei großen Konzernen in Deutschland im Konzernbetriebsrat und besonders in den entsprechenden IT-Ausschüssen mit. Seit ca. dreißig Jahren ist er aktives Mitglied im FIfF und im AK RUIN. Seine politischen Interessen liegen in den Themen Cyberpeace und nachhaltigem Leben.

Bernd Meiners

Global denken und lokal handeln

Gesellschaftliche Verantwortung am Beispiel von *Meiners Druck*, der Druckerei der FIfF-Kommunikation

Seit 2001 haben wir mit dem FIfF zu tun und kommen in den Genuss, die vierteljährliche Ausgabe nicht nur zu drucken sondern auch zu lesen. Da gibt es manche Artikel, die einen den Kopf schütteln lassen ob des Blödsinns, der zeitweise veranstaltet wird und andere, die sehr informativ, gut aufbereitet und in der Tiefe recherchiert sind.

Die Zusammenarbeit mit den netten Menschen im Bremer Büro und dem Layouter Herrn Schroeder ist eng und konstruktiv. So kommt man dann auch mal dazu, über den Tellerrand zu schauen und über aktuelle Themen zu sprechen. Da der Inhalt der FIfF-Kommunikation schon seit Jahren auf Recyclingpapier gedruckt wird, freute ich mich sehr darüber, Herrn Schroeder berichten zu können, das wir nun *CO_2-neutral* produzieren würden. Darüber kamen wir ins Gespräch und nach Rücksprache fragte er mich, ob ich nicht mal unsere Lösung vorstellen wolle. Darüber freute ich mich natürlich, denn ein wichtiger Aspekt „unserer Lösung" ist ja die Kopierbarkeit für andere.

Vorarbeiten

Am Anfang (1999) standen wir mit einem Neubau da, der wunschgemäß mit guter Außendämmung ausgeführt wurde. Beim Verlassen des Gebäudes sollten auf Knopfdruck die Lichter ausgehen. Damals wurde das von unserem Elektriker über Stromstoßschalter an einfachen Tastern gelöst. Nachdem wir etwas später eine größere Maschine brauchten, haben wir uns eine Tabelle mit Parametern gemacht, die uns wichtig erschienen. Die Energieaufnahme war ein wesentlicher Punkt auf dieser Liste und deshalb fiel die Entscheidung für ein energiesparendes Modell. Als nach und nach die Fahrzeuge ausgetauscht werden mussten, haben wir uns bewusst für Modelle mit Erdgasantrieb entschieden. Die erreichten zur damaligen Zeit zwar nicht die Reichweite der Dieselfahrzeuge, dafür war aber die Effizienz hoch und die entstehenden Schadstoffe im Vergleich zu Modellen mit Benzin oder Diesel stark reduziert. Ich weiß nicht mehr genau, ob wir dann unsere Photovoltaikanlage zuerst auf das Dach gebracht oder aber auf den Bezug von Ökostrom gesetzt hatten, jedenfalls ist das eine abhängig vom anderen. Wer Ökostrom haben will, sollte auch welchen produzieren bzw. wer Ökostrom produziert, sollte ihn auch abnehmen. Privat hatte ich bereits Erfahrung mit Bussystemen in der Gebäudeautomation (KNX) gemacht und so entschloss ich mich, die Stromstoßschalter gegen Schaltaktoren zu ersetzen. Das Licht wird heute von Präsenzmeldern geschaltet, unsere Server sind virtualisiert. Statt sieben PC laufen nur noch zwei Server. Parallel dazu zogen wir einen externen Berater hinzu, der uns noch einige Maßnahmen zur Effizienz empfahl. Dazu gehörten die regelmäßigere Reinigung von Kühlrippen, der Austausch von Röhren bei Ausfall gegen effizientere Modelle und die Verlagerung der Kühlaggregate in die kühlere Nachbarhalle.

Das Eingemachte

Dann (2012) kam der Geschäftsführer der gemeinnützigen Klimaschutzagentur *energiekonsens* (BEK) auf uns zu und fragte, ob wir denn nicht als nächsten Schritt die CO_2-neutrale Produktion einführen wollten. Nach kurzer Beratung erschien uns das sehr sinnvoll und wir setzten uns mit dem *energiekonsens* und dem Energieberater zusammen und erstellten eine Tabelle mit den notwendig zu ermittelnden Faktoren, um eine CO_2-neutrale Produktion zu ermöglichen.

Projektgebiet Klimamoor „Dorumer Moor", Foto: Henning Kunze

Für die CO_2-Bilanz[1] betrachteten wir die Energieversorgung, Wasser/Abwasser, Transporte, Mitarbeiter An- und Abreise, Hilfsstoffe (Farben, Alkohol, Reinigungsmittel), Druckplatten (Aluminium) und Papier. Am einfachsten konnten die Parameter für Transporte und Mitarbeiter An- und Abreise gewonnen werden, gefolgt von Energieversorgung und Wasser/Abwasser. Die Berechnung der Parameter für Hilfsstoffe und Druckplatten war deutlich schwieriger. Bestimmte allgemein bekannte Werte von Isopropanol wurden angesetzt, bei den Farben haben wir einen Modellansatz des Bundesverbandes Druck zu Grunde gelegt. Beim Papier haben wir zunächst eine Jahresbilanz aufgestellt und uns die größten Posten herausgesucht. Für dieses Papier forderten wir dann Datenblätter zur CO_2-Erzeugung bei der Papierherstellung an. Was einfach schien, war komplizierter als gedacht, denn solche Datenblätter lagen nur vereinzelt vor, und viele unserer Lieferanten bekamen Fragezeichen auf der Stirn, was wir denn wohl damit bezwecken mögen. Kurzum: Einige Papierfabriken hatten das Thema bereits bearbeitet, während andere gänzlich uninformiert waren.

Nach Auswertung der Tabelle ergab sich, dass wir trotz unserer Maßnahmen zur Einsparung noch 41 t CO_2 erzeugt hatten, die wir nun irgendwie ausgleichen mussten. International gibt es den sogenannten Emissionsrechtehandel[2]. Global agierende Unternehmen kaufen an den Energiebörsen sozusagen Verschmutzungserlaubnisse. Für unsere „Kleinigkeit" kam das

aber nicht in Frage und wir machten uns auf die Suche nach einer regionalen Lösung. Im Dorumer Moor[3] südlich von Cuxhaven gibt es große Flächen, die vor langer Zeit zur Torfgewinnung trockengelegt wurden. Der BUND hat mit seinem Projekt *Moorland* auf eine Projektlaufzeit von 20 Jahren ausgerechnet, wie viel CO_2 eingespart werden könnte, wenn das Moor wiedervernässt wird und bietet dafür Klima-Zertifikate für Firmen und Privatpersonen an. Wir haben anfangs 41 Zertifikate erworben. Mit den Mitteln aus dem Verkauf aller Zertifikate konnte am 6. März 2015 die Wiedervernässung umgesetzt werden. Der Zersetzungsprozess des Moores wird nun auf ein naturnahes Maß verlangsamt und ein seltener Lebensraum für Tiere und Pflanzen entsteht.

Das Beste daran: wir können von Bremen aus da hin radeln und uns das ganze konkret ansehen. Für uns war und ist es wichtiger, dass lieber 10.000 kleine Leute ein wenig machen, als 5 große nichts.

Übrigens können auch Privatpersonen Zertifikate erwerben. Was also hindert Sie daran, im Zuge des nächsten Fluges mal ein paar *Moorzertifikate* zu erwerben? Oder schauen Sie mal, was in Ihrer Region an Aktivitäten zum Thema stattfindet. Vielleicht gibt es ja auch bei Ihnen ein tolles regionales Projekt!

Und unsere nächsten Schritte? Wir werden nach und nach die Beleuchtung austauschen, unsere angebaute Halle bekommt eine Photovoltaik-Anlage auf das Dach, die Beleuchtung und Beschattung werden wir weiter automatisieren und ….

Anmerkungen

1 *https://www.prima-klima-weltweit.de/co2/kompens-berechnen.php#rechner*
2 *http://de.wikipedia.org/wiki/Emissionsrechtehandel*
3 *http://www.moor-land.de/index.php?id=67*

Wissenschaft und Frieden 3/2015 – „Friedensverhandlungen“ und Dossier *Kriegführung im Cyberspace*

Im 19. und noch bis ins späte 20. Jahrhundert endeten bewaffnete Auseinandersetzungen überwiegend mit dem Sieg einer Seite, nur 15-20 % durch Friedensverhandlungen. Das hat sich stark verändert. Bei den zwischenstaatlichen Kriegen setzen die Interventionisten zwar nach wie vor auf Sieg. Siege, die in der Regel chaotische Verhältnisses hinterlassen, siehe Irak, Libyen und Afghanistan. Mehr als 50 % aller Bürgerkriege, die häufigste Form gewaltsamer Konflikte, konnten dagegen am Verhandlungstisch beendet werden, allerdings auch nicht immer mit dauerhaften Erfolg.

Die AutorInnen in W&F 3/2015 untersuchen diverse Aspekte von Friedensverhandlungen: Den generellen Trend, Voraussetzungen und Akteure, die Tauglichkeit der OSZE als Schlichterin sowie einige konkrete Fälle in Kolumbien, Mindanao, der DR Kongo und Afghanistan.

Außerhalb des Schwerpunktes geht es um das Iran-Abkommen, die Rüstungspolitik im Ersten Weltkrieg, Frauen in Krieg und Frieden, die Beteiligung Deutchlands am Drohnenkrieg, die Militärpolitik Österreichs und die Terminologie für gewaltfreies Handeln.

Das Dossier 79 befasst sich mit *Kriegführung im Cyberspace*. Während die Medien aufmerksam die ungebremste Ausspähung in den digitalen Netzen verfolgten, wurde der virtuelle Raum weitgehend unbemerkt von der Öffentlichkeit zu einem Operationsraum der Militärs. Militärische Szenarien beziehen Cyberoperationen als entscheidende Elemente der Kriegführung ein – für Spionageaktionen bis hin zum Einsatz von Cyberwaffen. Ihre beabsichtigte Wirkung reicht von Destabilisierung über Sabotage bis zu Eingriffen in digitale Infrastrukturen mit weitreichenden Folgen für die Zivilbevölkerung. In ihrer Unfassbarkeit und Unkontrollierbarkeit stellen die Cyberaktivitäten der Geheimdienste und Militärs eine verschwiegene, aber höchst reale Gefahr für den Frieden dar. Das *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung* (FIfF) setzt diesem Trend das Konzept des Cyberpeace entgegen.

Wissenschaft & Frieden 3/2015 **Friedensverhandlungen**,
€ 7,50 plus Porto.

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

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

FIfF e.V.

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

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

FIfF-Mailinglisten

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

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

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

FIfF online

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

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

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

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

FIfF-Beirat

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

FIfF-Vorstand

Stefan Hügel (Vorsitzender) – Frankfurt am Main
Prof. Dr. **Dietrich Meyer-Ebrecht** (stellv. Vorsitzender) – Aachen
Sylvia Johnigk – München
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Kai Nothdurft – München
Rainer Rehak – Berlin
Jens Rinne – Mannheim
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
Ingrid Schlagheck – Bremen
Prof. Dr. **Werner Winzerling** – Fulda
Prof. Dr. **Eberhard Zehendner** – Jena

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen
Sara Stadler – Bremen
Thomas Reinhold (Campaigning) – Lübeck

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 D-28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1 100 Stück
Heftpreis	7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren.
Hauptredaktion	Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck, Sara Stadler
Schwerpunktredaktion	Dietrich Meyer-Ebrecht
V.i.S.d.P.	Stefan Hügel
FIfF-Überall	Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an *hubert.biskup@gmx.de.* Ansprechpartner für die jeweiligen Regionalgruppen finden Sie im Internet auf unserer Webseite *http://www.fiff.de/regional*
Retrospektive	Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de*
Layout	Berthold Schroeder
Titelbild	Philipp Hayer
Druck	Meiners Druck, Bremen

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

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*)

31. FIfF-Konferenz FIfFKon 2015
6. bis 8. November, Friedrich-Alexander-Universität in Erlangen
„Kommerzialisierung des Sozialen: Markt und Macht im Zeitalter der digitalen Kompletterfassung (Commercialisation of the Soci(et)al – Markets and Power in the Age of Total Datafication)"

FIfF-Vorstandssitzung
24. Oktober 2015, Frankfurt am Main

FIfF-Mitgliederversammlung
8. November, ab 11:00 Uhr, Erlangen,
Medical Valley Center, Henkestraße 91

FIfF-Kommunikation

4/2015 »Cybercrime«
Eberhard Zehendner
Redaktionsschluss: 6. November 2015

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

W&F – Wissenschaft & Frieden
1/15 – Afrika (mit Dossier 77: Rechter Terror in Deutschland)
2/15 – Technikkonflikte (mit Dossier 78: Zivilklauseln)
3/15 – Friedensverhandlungen (mit Dossier 79: Kriegführung im Cyberspace)

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik
#210/211 Gesetzgebung zum Verbot der Suizidbeihilfe
#212 Reflexhaftes Strafrecht

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

Das FIfF-Büro

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

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

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

Schluss FIfF

Johann Wolfgang von Goethe

Der Zauberlehrling

Hat der alte Hexenmeister
Sich doch einmal wegbegeben!
Und nun sollen seine Geister
Auch nach meinem Willen leben.
Seine Wort' und Werke
Merkt' ich, und den Brauch,
Und mit Geistesstärke
Thu' ich Wunder auch.

Walle! walle
Manche Strecke,
Daß, zum Zwecke,
Wasser fließe,
Und mit reichem vollem Schwalle
Zu dem Bade sich ergieße.

Und nun komm, du alter Besen!
Nimm die schlechten Lumpenhüllen;
Bist schon lange Knecht gewesen;
Nun erfülle meinen Willen!
Auf zwey Beinen stehe,
Oben sey ein Kopf,
Eile nun und gehe
Mit dem Wassertopf!

Walle! walle
Manche Strecke,
Daß, zum Zwecke,
Wasser fließe,
Und mit reichem vollem Schwalle
Zu dem Bade sich ergieße.

Seht, er läuft zum Ufer nieder;
Wahrlich! ist schon an dem Flusse,
Und mit Blitzesschnelle wieder
Ist er hier mit raschem Gusse.
Schon zum zweytenmale!
Wie das Becken schwillt!
Wie sich jede Schale
Voll mit Wasser füllt!

Stehe! stehe!
Denn wir haben
Deiner Gaben
Vollgemessen! –
Ach, ich merk' es! Wehe! wehe!
Hab' ich doch das Wort vergessen!

Ach das Wort, worauf am Ende
Er das wird, was er gewesen.
Ach, er läuft und bringt behende!
Wärst du doch der alte Besen!
Immer neue Güsse
Bringt er schnell herein,
Ach! und hundert Flüsse
Stürzen auf mich ein.

Nein, nicht länger
Kann ich's lassen;
Will ihn fassen.
Das ist Tücke!
Ach! nun wird mir immer bänger!
Welche Miene! welche Blicke!

O, du Ausgeburt der Hölle!
Soll das ganze Haus ersaufen?
Seh' ich über jede Schwelle
Doch schon Wasserströme laufen.
Ein verruchter Besen,
Der nicht hören will!
Stock, der du gewesen,
Steh doch wieder still!

Willst's am Ende
Gar nicht lassen?
Will dich fassen,
Will dich halten,
Und das alte Holz behende
Mit dem scharfen Beile spalten.

Seht, da kommt er schleppend wieder!
Wie ich mich nun auf dich werfe,
Gleich, o Kobold, liegst du nieder;
Krachend trifft die glatte Schärfe.
Wahrlich! brav getroffen!
Seht, er ist entzwey!
Und nun kann ich hoffen,
Und ich athme frei!

Wehe! wehe!
Beide Theile
Stehn in Eile
Schon als Knechte
Völlig fertig in die Höhe!
Helft mir, ach! ihr hohen Mächte!

Und sie laufen! Naß und nässer
Wird's im Saal und auf den Stufen.
Welch entsetzliches Gewässer!
Herr und Meister! hör' mich rufen! –
Ach da kommt der Meister!
Herr, die Noth ist groß!
Die ich rief, die Geister,
Werd' ich nun nicht los.

„In die Ecke,
Besen! Besen!
Seyd's gewesen.
Denn als Geister
Ruft euch nur, zu seinem Zwecke,
Erst hervor der alte Meister."

Entstanden 1797, erschienen 1827. Goethe's Werke. Vollständige Ausgabe letzter Hand. Erster Band. S. 217–220.
https://de.wikisource.org/wiki/Der_Zauberlehrling_%281827%29

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