H 7625

FIfF-Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

26. Jahrgang 2009 Einzelpreis: 7 EUR

1/2009 - März 2009

KRIEG & FRIEDEN ···- DIGITAL

ISSN 0938-3476

• Berichte über die Jahrestagung • Krieg und Informatik • Ereignislog

FIfF Kommunikation

Titelbild: Caro von Totth

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

inhalt

Inhalt

Ausgabe 1/2009

Editorial

Das FIfF hat Geburtstag – in diesem Jahr wird das FIfF 25 Jahre alt. Aus diesem Grund hat die Redaktion beschlossen, die kommenden Hefte der FIfF-Kommunikation als einen zusammengehörigen Komplex zu planen, quasi als einen Jahresschwerpunkt »25 Jahre FIfF«.

Den Anfang macht das vorliegende Heft, eine Dokumentation der FIfF Jahrestagung am 7./8.11.2008 in Aachen, durchgeführt in Kooperation mit dem Aachener Friedenspreis e.V. und den Interdisziplinären Foren der RWTH Aachen. Das Tagungsmotto »*Krieg und Frieden – digital*« steht in direktem inhaltlichen Bezug zur den Diskussionen über Informatik und Rüstung, welche vor einem Vierteljahrhundert ein wesentlicher Impuls zur Gründung des FIfF waren und die sich entsprechen auch im Namen des FIfF widerspiegeln. Der Beitrag von Dietrich Meyer-Ebrecht (Seite 11) enthält einen Bericht zum Verlauf der Tagung und ist damit gleichzeitig eine ausführliche Einleitung zu anderen Beiträgen im Schwerpunktteil des vorliegenden Heftes.

Im zweiten Heft dieses Jahres – *Kritische Informatik* – wollen wir den Blick auf einige der vielen Vereinigungen, Initiativen Organisationen und Gruppen richten, die sich kritisch begleitend mit den gesellschaftlichen und politischen Wechselwirkungen sowie mit ethischen und rechtlichen Fragen hinsichtlich Informatik, Informations- und Kommunikationstechnik und digitalen Medien auseinandersetzen.

All den unterschiedlichen Themen, mit denen sich das FIfF seit seiner Gründung beschäftigt, ist eines gemeinsam: Wir wollen die Menschen – und nicht die Technik – ins Zentrum der Diskussion rücken. Das dritte Heft unseres Jahresschwerpunktes »25 Jahre FIfF« soll daher folgerichtig dem Menschen mit all seinen Rollen gewidmet sein: als Entwickler/in, Benutzer/in, Betroffene/r. Das Motto lautet ironisierend: *Der Computer und sein Mensch*.

Neben einer Rückschau und Bestandsaufnahme soll der Blick auch nach vorne in die Zukunft gerichtet sein: Welche gesellschaftlich relevanten Trends in der Informatik können wir ausmachen und welche Perspektiven ergeben sich hieraus für das FIfF und seine Arbeit. Dies wird Thema des vierten Heftes – *Herausforderungen* – sein.

Auch wenn es bereits jenseits des Jubiläumsjahres liegt: Inhaltlich schließt sich Heft 1/2010 dann nahtlos an, da es mit seinem Schwerpunkt *Verantwortung 2.0* – dem Motto der FIfF Jahrestagung 2009 (siehe Ankündigung Seite 10) – den zweiten Schlüsselbegriff aus dem Namen des FIfF aufgreift.

Wir laden herzlich dazu ein, an all diesen Heften aktiv mitzuarbeiten – mit eigenen Beiträgen oder insbesondere auch in den jeweiligen Schwerpunktredaktionen. Entsprechende Angebote erbitten wir an die Redaktionsadresse *redaktion@fiff.de*.

Nochmals zurück zum vorliegenden Heft und zu den Beiträgen jenseits des Schwerpunktes:

In seinem *Brief an das FIfF* thematisiert Hans-Jörg Kreowski einige besondere Aspekte dieses Jahres – auch jenseits des FIfF-Jubiläums. Katastrophal begonnen hat das Jahr jedenfalls aus der Perspektive des Arbeitnehmer-Datenschutzes. So waren die letzten Monate erneut angefüllt mit einer Vielzahl von Meldungen über Arbeitnehmerüberwachung, „Abgleich“ von Mitarbeiterdaten etc. Solche und viele andere Punkte wurden in bewährter Weise von Stefan Hügel in seinem Ereignis-Log festgehalten und zusammengestellt.

Schwerpunktredaktion Heft 1/2009

Dietrich Meyer-Ebrecht, Aachen
Stefan Hügel, München
Hans-Jörg Kreowski, Bremen
Ralf E. Streibl, Bremen

Durchaus inhaltlichen Bezug zum Schwerpunktthema hat unsere „Retrospektive“: Vor 24 Jahren erklärte David L. Parnas nach nur wenigen Tagen seine Rücktritt aus dem SDIO-Ausschuss (Strategic Defense Initiative Organization), in den er berufen worden war und begründete dies eindrucksvoll in einem offenen Brief, den wir in diesem Heft noch einmal abdrucken.

Wir wünschen allen Leserinnen und Lesern dieser FIfF-Kommunikation eine anregende Lektüre dieses Heftes und ein fiffiges Jubiläumsjahr 2009!

Ralf E. Streibl für die Redaktion

Stefan Hügel

Ereignis-Log 1/2009

Seit Oktober 2008 gab es wieder eine Reihe von Ereignissen, Verlautbarungen und Entscheidungen, die im Zusammenhang mit dem fortschreitenden Abbau von Bürgerrechten stehen. Wir dokumentieren hier einige davon. Die Aufzählung kann nicht vollständig sein; die Aufzählung einiger besonders bedeutsamer Ereignisse soll aber auf die weiterhin besorgniserregende Entwicklung hinweisen.

Oktober 2008

27. Oktober 2008: Der Chaos Computer Club (CCC) legt den Abschlussbericht zur Wahlbeobachtung in Brandenburg vor. Der Bericht zieht das Fazit, dass die verwendeten Nedap-Wahlcomputer weder unter Sicherheitsaspekten noch hinsichtlich der Bedienbarkeit eine brauchbare Alternative zur herkömmlichen Wahl darstellen (Quelle: CCC).

29. Oktober 2008: Bei der Suche nach den Dieben der 17 Millionen Kundendatensätze von T-Mobile haben Mitarbeiter der Deutschen Telekom gegen geltendes Recht verstoßen. Sie überprüften Verbindungsdaten von ca. 20-30 Personen; dabei mindestens einmal von einen inländischen Wettbewerber und einem ausländischen Unternehmer. Dies teilte der Datenschutz-Vorstand der Telekom auf einer Pressekonferenz mit (Quelle: Heise).

29. Oktober 2008: In der Türkei wird der Bloghoster *Blogspot* gerichtlich gesperrt. Erwirkt wurde die Sperre durch einen Fernsehanbieter, der das Monopol für Streams von türkischen Fußball-Ligaspielen beansprucht. Einige Blog enthielten Links zu Seiten, die entsprechende Aufnahmen kostenlos angeboten hatten (Quelle: Heise).

November 2008

4. November 2008: Der Demokrat Barack Obama wird zum 44. Präsidenten der Vereinigten Staaten von Amerika gewählt. In einem Papier zu Innovation und Technologie kündigt er Maßnahmen zum Schutz eines offenen Internet und der Privatsphäre an. Obama hatte bereits im Wahlkampf stark auf das Internet gesetzt (Quelle: www.barackobama.com/issues/technology).

8. November 2008: Die Deutsche Polizeigewerkschaft (DPolG) warnt vor dem Beschluss des BKA-Gesetzes. Das Gesetz hat nach dem DPolG-Vorsitzenden Wendt vor dem Bundesverfassungsgericht „keine Chance“. Als Hauptkritikpunkt wird die „Selbstkontrolle“ des BKA beim Eingriff in den absolut geschützten Kernbereich privater Lebensgestaltung genannt (Quelle: Heise).

11. November 2008: Das hessische Innenministerium bestätigt, dass es keine Genehmigung für Nedap-Wahlcomputer für die Landtagswahl im Januar erteilen wird (Quelle: Heise).

12. November 2008: Der Suchmaschinenbetreiber Google gibt bekannt, dass es Suchanfragen auswertet, um Phänomene der realen Welt besser zu erfassen. Beispielsweise wurden Suchanfragen nach Infektionskrankheiten gezielt ausgewertet, um daraus Folgerungen für deren Verbreitung zu ziehen (Quelle: Heise).

12. November 2008: Der Deutsche Bundestag verabschiedet die Novelle des BKA-Gesetzes (Quelle: Heise).

13. November 2008: Die Kassenärztliche Bundesvereinigung der Zahnärzte (KZBV) empfiehlt ihren Mitgliedern, als Konsequenz des neuen BKA-Gesetzes keine Rechner mit Patientendaten mehr an das Internet anzuschließen (Quelle: Heise).

13. November 2008: Die australische Regierung will trotz öffentlicher Kritik Internetprovider verpflichten, für alle Internetnutzer Filter zu installieren (Quelle: Heise).

14. November 2008: In Italien werden die Urteile gegen 29 Polizisten gesprochen, die wegen massiver Übergriffe gegen Demonstranten beim G8-Gipfeltreffen 2001 in Genua angeklagt waren. Lediglich 13 Beamte wurden zu vergleichsweise milden Strafen verurteilt; die verantwortlichen Vorgesetzten wurden freigesprochen. Die Polizisten hatten eine Schule gestürmt, auf die teilweise bereits schlafenden Demonstranten eingeschlagen und diese zum Teil erheblich verletzt (Quelle: taz).

18. November 2008: Der polnische Inlandsgeheimdienst ABW führt einen Versuch durch, bei dem in Posen Absender und Empfänger von Briefen und deren graphologische Merkmale erfasst werden (Quelle: Heise).

19. November 2008: Interpol durchforstet auf der Suche nach Kriminellen verstärkt soziale Netzwerke. Dies erklärten Delegierte einer Interpol-Konferenz in Johannesburg (Quelle: Heise).

21. November 2008: Die EU-Kommission will Ganzkörperscanner („Nackt-Scanner") vorläufig nicht zulassen. Als Grund wird angegeben, dass die entsprechende Verordnung die Neufassung der Kontrollvorgaben für die Luftverkehrssicherheit blokkiert habe. Entsprechende Pläne waren auf heftige öffentliche Kritik gestoßen (Quelle: Heise).

28. November 2008: Die Einführung von Videoüberwachung in Wiener Taxis ist an zu hohen Kosten gescheitert. Für entsprechende Pläne hatte der Chef der Wiener Taxi-Innung, Heinrich Frey, 2007 einen BigBrotherAward erhalten (Quelle: Heise, www.bigbrotherawards.at).

30. November 2008: Die deutsche Bundespolizei will im Dezember mit Labortests von Ganzkörperscannern beginnen. Obwohl die Bundesregierung erklärt hatte, dass die Geräte nicht an deutschen Flughäfen eingesetzt werden sollen, will das Innenministerium die Technologie erproben (Quelle: Heise).

Dezember 2008

3. Dezember 2008: Das Kabinett beschließt, 2011 wieder eine Volkszählung in Deutschland durchzuführen. Bei der Zählung sollen Melde- und Verwaltungsregister ausgewertet und sieben bis acht Prozent der Bürgerinnen und Bürger stichprobenartig befragt werden. Es sollen nur die Merkmale erhoben werden, die durch die EU vorgegeben sind. 1987 hat die damalige Volkszählung zu heftigen Protesten und nach einer Verfassungsklage zur Anerkennung des Rechts auf informationelle Selbstbestimmung durch das Bundesverfassungsgericht geführt (Quelle: Heise).

19. Dezember 2008: Das umstrittene BKA-Gesetz wird im Bundesrat verabschiedet. Zuvor hatte der Bundestag die gegenüber der ursprünglichen Fassung leicht entschärfte Version ohne Aussprache durchgewinkt (Quelle: Heise).

Januar 2009

2. Januar 2009: Die britische Regierung plant, möglicherweise private Firmen mit der Sammlung und Speicherung von Verbindungsdaten zu beauftragen (Quelle: Heise, Guardian).

15. Januar 2009: Nach einem Spitzengespräch mit Internet-Providern plant die Bundesregierung noch in dieser Legislaturperiode die Einführung von Maßnahmen zur gezielten Sperrung des Zugangs zu Internetseiten. Zunächst sollen Seiten mit pornographischen Darstellungen von Kindern gesperrt werden. Erfahrungen aus anderen Ländern zeigen, dass Sperrungen häufig auch auf andere Inhalte ausgedehnt werden. Entsprechende Forderungen – beispielsweise bei Seiten, die Glücksspiel anbieten – sind bereits erhoben worden; Ministerin von der Leyen erklärte, nicht zu wissen, welche „Wünsche und Pläne" künftige Bundesregierungen entwickeln würden (Quelle: netzpolitik.org, Spiegel).

21. Januar 2009: Unbekannte verschaffen sich Zugang zu Kreditkartendaten des US-Kreditkartendienstleisters Heartland Payment Systems. Analysten erklären, dass es sich möglicherweise um einen der größten Fälle von Datendiebstahl überhaupt handle (Quelle: netzpolitik.org, Wall Street Journal).

27. Januar 2009: Bettina Winsemann („Twister") legt Verfassungsbeschwerde gegen das novellierte BKA-Gesetz ein. Vertreten wird sie von Fredrik Roggan (Quelle: Heise).

28. Januar 2009: Bei der Deutschen Bahn wurden 2002 und 2003 ca. 173.000 Mitarbeiter und damit fast die gesamte Belegschaft bei einem Datenabgleich überprüft, um Korruptionsfälle aufzudecken. Gegen die überprüften Mitarbeiter lag kein Anfangsverdacht vor. Der Bundesdatenschutzbeauftragte Schaar bezeichnete das Vorgehen der Bahn als „Rasterfahndung"; die Mitarbeiter und der Betriebsrat wurden nicht von der Maßnahme informiert (Quelle: Stern, Heise, Süddeutsche Zeitung).

30. Januar 2009: Der Deutsche Verkehrsgerichtstag hat sich für einen Test der Geschwindigkeitsüberwachung durch *Section Control* ausgesprochen. Bei dieser Methode, die beispielsweise in Österreich bereits eingesetzt wird, wird die Durchschnittsgeschwindigkeit auf einem Streckenabschnitt anstatt wie bisher die punktuelle Geschwindigkeit gemessen. Das Verfahren stößt auf Datenschutzbedenken, da unabhängig von der Geschwindigkeit alle Fahrzeuge bei der Einfahrt in den Streckenabschnitt erfasst werden müssen (Quelle: Spiegel).

Februar 2009

7. Februar 2009: Der Verfassungsausschuss des britischen Oberhauses veröffentlicht einen Bericht, in dem er vor dem Abgleiten des Landes in einen absoluten, einzig an der technologischen Machbarkeit orientierten Überwachungsstaat warnt. Die stetige Ausweitung der Überwachung repräsentiere die signifikanteste Veränderung seit dem zweiten Weltkrieg, heißt es in dem Bericht (Quelle: Süddeutsche Zeitung).

Stefan Hügel

Stefan Hügel ist stellvertretender Vorsitzender des FIfF. Er arbeitet als IT-Berater und lebt in München.

Hans–Jörg Kreowski

Brief an das FIfF

Liebe Mitglieder des FIfF, liebe Leserinnen und Leser,

das FIfF wurde 1984 gegründet, so dass wir in diesem Jahr ein 25-jähriges Bestehen begehen und vielleicht sogar etwas feiern können. Die diesjährigen Ausgaben der FIfF-Kommunikation sollen das Jubiläum in verschiedener Weise reflektieren. Nachdem die Jahrestagung 2008 mit Krieg und Frieden - digital schon auf den Begriff Frieden im Namen des FIfF eingegangen ist, wird die 25. Jahrestagung mit der gesellschaftlichen Verantwortung den zweiten Teil des Namens in den Mittelpunkt rücken. Ich würde mich freuen, wenn viele FIfF-Mitglieder und am Thema Informatik und Gesellschaft Interessierte zu diesen Jubiläumsaktivitäten beitragen oder sich dadurch anregen lassen und eigene Initiativen entwickeln.

Das Jahr 2009 ist allerdings nicht nur für das FIfF ein Jubiläumsjahr, sondern auch die Gründung der Bundesrepublik Deutschland vor 60 Jahren und der Mauerbau vor 20 Jahren geben Anlass zu Rückschau und Nachdenken. Denn beide Ereignisse sind Startpunkte vieler weiterer Einrichtungen und Begebenheiten, die für unsere gesellschaftliche Entwicklung bestimmend wurden und sind. Ihre Reflexion ist deshalb für sich interessant, aber auch aus Sicht des FIfF, weil es als Teil der Zeitgeschichte davon beeinflusst ist und selbst ein Stück weit Einfluss genommen hat. Das wäre vielleicht sogar einmal eine vertiefte Untersuchung wert.

Und noch ein Jubiläum: 2009 ist das 10. Wissenschaftsjahr, das deshalb nicht wie alle Vorgänger einer einzelnen Disziplin oder einem einzelnen Wissenschaftszweig gewidmet ist. Das Wissenschaftsjahr 2009 steht unter dem Motto *Forschungsexpedition Deutschland* und soll zeigen, „welche Rolle Wissenschaft und Forschung für die Menschen in Deutschland spielen – gestern, heute und in Zukunft." Das gesamte Konzept dieser Kampagne und die bereits geplanten Veranstaltungen, die sich über das ganze Jahr und ganze Land verteilen, zielt auf bewunderndes Staunen und Bejubeln des Erreichten und noch zu Erreichenden ab. Aber für kritische Stimmen ist durchaus Platz. Im Hochschulwettbewerb *„Alltagstauglich?"* wird beispielsweise gefragt: „Welchen Einfluss hat Wissenschaft auf die Gesellschaft? Wie prägen und verändern Entdeckungen, Erfindungen, Deutungen und Denkmodelle unseren Alltag?" Wäre es nicht sehr erstrebenswert, wenn aus dem FIfF heraus im FIfF-Zusammenhang und im Sinne des FIfF an dem einen oder andern Ort Veranstaltungen stattfänden, die auf diese Fragen eingehen?

2009 ist aber nicht nur ein Jahr der Jubiläen, sondern kurz vor Weihnachten hat die deutsche Bundeskanzlerin 2009 zum „Jahr der schlechten Nachrichten" erklärt. Es ist schon sehr verräterisch, welche hohlen Phrasen die politische Kaste von sich gibt, wenn sie ihre Hilf- und Ratlosigkeit angesichts der rücksichtslosen Profitgier und schamlosen Bereicherung in der Finanz- und Wirtschaftswelt kaschieren will.

Was Datensammelwut und Überwachungswahn in Staat und Wirtschaft angeht, war allerdings bereits 2008 (und eigentlich auch die Jahre davor) von schlechten Nachrichten geprägt, so dass eine Steigerung kaum vorstellbar ist. Da wurden schwerwiegende Fälle von Datenmissbrauch im betrieblichen Bereich bei Lidl und der Telecom bekannt, die gegen Beschäftigte gerichtet waren. Und doch hat die Bundesbahn es geschafft, den Skandal zu potenzieren, indem gleich von Hunderttausenden ihrer Mitarbeiterinnen und Mitarbeiter mehrmals widerrechtlich Daten „abgeglichen" wurden. Da trat ein Gesetz zur Vorratsdatenspeicherung in Kraft, das im EU-Kontext dafür sorgt, dass die Telekommunikations-Verbindungsdaten aller Deutschen ein halbes Jahr gespeichert werden, um gegebenenfalls zur Verbrechens- und Terrorismusbekämpfung zur Verfügung zu stehen. Denn wir sind alle verdächtig. Weitere Beispiele waren eine Serie kriminellen Missbrauchs personenbezogener Daten, der millionenfache Diebstahl und „Verlust" solcher Daten auf Grund eklatanter Sicherheitsmängel in verschiedenen Unternehmen und nicht zuletzt die Verankerung der online-Durchsuchungen im BKA-Gesetz. Aber es gab auch gute Nachrichten in dem Zusammenhang. So wurde beim Bundesverfassungsgericht eine Massenklage gegen die Vorratsdatenspeicherung eingereicht, die durchaus auch eine gewisse Chance auf Erfolg hat. So hat dieses Gericht bereits den Ländern Hessen und Schleswig-Holstein untersagt, Autokennzeichen massenhaft zu erfassen. So hat im Oktober in Berlin die Demonstration *Freiheit statt Angst* Zehntausende auf die Straße gelockt und der Politik eindrucksvoll gezeigt, dass viele Bürgerinnen und Bürger überhaupt nicht damit einverstanden sind, wenn Grundrechte unter dem Vorwand der Sicherheit eingeschränkt werden. Ich hoffe, dass in diesem Jahr der Protest noch weiter anschwillt und dass das FIfF als Organisation und viele seiner Mitglieder sich noch stärker in diese Bewegung einbringen.

2009 ist auch das Jahr der Astronomie. Dazu wäre einiges zu sagen, aber das verschiebe ich auf einen späteren Brief. Und nach dem chinesischen Kalender hat gerade das Jahr des Büffels begonnen, was in China ein günstiges Zeichen ist. Der Büffel gilt als geduldig und ruhig, verschwiegen und schwerfällig, zurückhaltend und ausgeglichen, methodisch und genau, originell und intelligent, vertrauenserweckend, ungeheuer fleißig und leistungsfähig. Vielleicht kann das auch für die Arbeit des FIfF als gutes Omen genommen werden, wobei es letztlich wohl darauf ankommt, was im FIfF selbst zu Wege gebracht wird. 2009 wird ein Jahr der guten FIfF-Nachrichten.

Mit fiffigen Grüßen

Hans-Jörg Kreowski

Als "Retrospektive" haben wir für dieses Heft einen Brief gewählt, dem eine besondere Bedeutung zukommt. 1985 verließ David L. Parnas nach nur zwei Monaten den vom damaligen Präsidenten Reagan initiierten SDI-Ausschuss. Er stellte seine Gründe dafür in einem offenen Brief dar, dem acht kurze Artikel beigefügt waren. Frieder Nake schilderte den Hintergrund dieses Briefes und einige Auswirkungen bei der Verleihung des FIfF-Preises an David L. Parnas am 30.9.2001 in seiner Laudatio folgendermaßen:

„(...)

Software Engineering als eine gesellschaftliche Verantwortung

*David Parnas blickt von seinem wissenschaftlichen Standort auch nach *außen* und klagt Verantwortung vor der Gesellschaft ein.*

Sein Austritt aus dem kleinen, hochrangigen Beraterkreis des Präsidenten zur SDI-Entwicklung und seine damit verbundene Stellungnahme setzten ein Fanal. Diese Tat und ihre um den Globus herum reichende Wahrnehmung und Wirkung gehören zu den bemerkenswertesten Auftritten des wissenschaftlichen Gewissens in moderner Zeit. Vermutlich wäre er früher dafür auf den Scheiterhaufen gekommen. Verglichen damit hatte er es leichter als historische Vorbilder. Jedoch - wie selten hören wir Warnungen vor Falschem und Unsinnigen, wie seltener noch zieht jemand persönliche Konsequenzen!

*Die kleine Geschichte jener SDI-Beratertätigkeit ist bemerkenswert. Durch seine Teilnahme an nur zwei Tagen im Kreise der Berater bemerkte Parnas, das das Projekt vor keine klare Aufgabe gestellt war und zu keinem praktikablen Ergebnis führen würde. Er brachte seine Bedenken im Kollegenkreis der Berater vor, die die Einwände durchaus einsahen, sie jedoch angesichts der winkenden Gelder in den Wind schlugen. Besser *wir* nehmen das Geld und machen mit, und die Informatik wird insgesamt sogar einflussreicher, als dass jemand anderes das täte. Klingt uns das nicht vertraut?*

Erst nachdem Parnas seine Bedenken höheren Ortes bei Regierungsstellen vorgetragen hatte und nicht erhört worden war, hatte er nichts dagegen einzuwenden, dass die New York Times die Sache publik machte. Aus irgendeiner Quelle waren sie mit dem Material versorgt worden. Die Tatsache, dass die acht kurzen Essays aus seiner Feder stammten, leugnete er nicht.

*Zuerst erschienen seine Warnungen im *American Scientist* im Sept./Okt. 1985. Die *Communications of the ACM* druckten die Papiere im Dezember 1985 nach und machten sie ungekürzt der wissenschaftlichen Öffentlichkeit der Informatik bekannt. 1986 erschienen dänische, japanische, hebräische, schwedische, deutsche Übersetzungen (die deutsche im Kursbuch 83). Vermutlich gibt es noch mehr, Im Februar 1987 hatte Parnas Gelegenheit, in einem Themenheft des *Informatik Spektrum* erneut zum Thema zu schreiben.*

Die Reaktionen, Fortsetzungen, Publikationen, Vorträge und Diskussionen im weiteren Verlauf waren grandios. Parnas' Einwände trafen so recht auf das, was die damalige Friedensbewegung unmittelbar aus der Höhle des Biestes heraus brauchen konnte.

Die Bemühungen Parnas' trugen sogar zu einem leisen Abrücken Reagans von der grandiosen Ankündigung bei, dass durch das SDI Programm Atomwaffen außer Kraft gesetzt würden, ein Ankündigungsschachzug, der auch Parnas zunächst dafür gewonnen hatte, sich zu beteiligen. Später wurde das ganze Star Wars Konzept allmählich eingemottet - um neuerdings allerdings aus der Mottenkiste geholt und begeistert aufgegriffen zu werden, dieses Mal ohne Rekurs auf die atomare Bedrohung.

(...)"

Der damalige FIfF-Vorsitzende Reinhard Keil-Slawik, David L. Parnas mit dem FIfF-Preis in Händen und Frieder Nake, der die Laudatio auf der FIfF Jahrestagung 2001 hielt.

Angesichts der gegenwärtigen Debatten über einen "Raketenschild" in Europa und auch vor dem Hintergrund der Aachener FIfF-Tagung "Krieg und Frieden – digital", deren Beiträge in dem vorliegen Themenheft der FIfF-Kommunikation dokumentiert werden, entstand der Gedanke, diesen Brief als "Retrospektive" abzudrucken. Wir danken David L. Parnas für die Genehmigung zum Abdruck. Aus Platzgründen können wir hier leider nur den Brief, nicht aber die beigefügten Essays wiedergeben. Interessierte seien auf die frühern Publikationen verwiesen (s.u.). Wir freuen uns ganz besonders, das David L. Parnas aus Anlass dieser "Retrospektive" eigens einen Kommentar geschrieben hat – 24 Jahre später.

(Ralf E. Streibl für die Schwerpunktredaktion)

Zum Weiterlesen:

David Lorge Parnas: Software Aspects of Strategic Defense Systems. Commun. ACM 28 (12): 1326-1335 (1985)

David L. Parnas: Software Wars. Ein offener Brief. In: Michel, K.M.; Spengler, T. (Hrsg.): Kursbuch 83: Krieg und Frieden – Streit um SDI. Berlin: Kursbuch Verlag, S.49-69.

David Lorge Parnas: Warum ich an SDI nicht mitarbeite: Eine Auffassung beruflicher Verantwortung. Informatik Spektrum 10 (1): 3-10 (1987)

Frieder Nake: Im aufrechten Gang. Zu Ehren von Prof. David L. Parnas aus Anlass der zweiten Vergabe des FIfF Preis auf der Jahrestagung am 30.9.2001 in Bremen. In: FIfF Kommunikation 19 (1): 9-12 (2002).

David L. Parnas June 28, 1985

Ein Brief aus dem Jahr 1985

Mr . James H . Offut
Assistant Director, BM/C3
Strategic Defense Initiative Organization
Office of the Secretary of Defense
Washington, D .C .
20301

Dear Mr . Offut:

Thank you for your letter of 5 June 1985 appointing me a member of the SDIO Panel on Computing in Support of Battle Management. I appreciate the recognition implicit in being chosen as one of your expert advisors on computer science.

After attending the first meeting of the panel and giving the problem considerable thought, I am resigning my membership in the panel. I do not believe that further work by the panel will be useful and I cannot, in good conscience, accept further payment for useless effort.

The panel's work will not be useful for two reasons.

1) The goals stated for the Strategic Defense System cannot be attained by the class of systems that you are considering.

2) The SDIO is not the appropriate organization to fund and administer the research it is supporting . Most of the money spent will be wasted. The panel on which you have asked me to serve, is not appropriately constituted, clearly chartered, and adequately informed. There are better ways to select and manage research.

My conclusions are not based on political or policy judgements. Unlike many other academic critics of the SDI effort, I have not, in the past, objected to defense efforts or defense sponsored research. I have been deeply involved in such research and have consulted extensively on defense projects. My conclusions are based on more that 20 years of research on software engineering including more than 8 years of work on real-time software used in military aircraft. They are based on familiarity with both operational military software and computer science research. My conclusions are based on characteristics peculiar to this particular effort, not objections to weapons development in general.

Before making my decision and writing this letter I have carefully reconsidered what I have learned in my own research area and I have reviewed reports of work in related fields. These reviews lead inevitably to the judgements stated above. I am willing to stake my professional reputation on my conclusions.

Enclosed with this letter are brief papers (1-2 pages each) summarizing my observations and substantiating the conclusions stated above. Their purpose is to explain my decision.

These papers explain:

1) The fundamental technological differences between software engineering and other areas of engineering and why software is unreliable,

2) The properties of the proposed SDI software that make it unattainable,

3) Why the techniques commonly used to build military software are inadequate for this job,

4) The nature of research in Software Engineering, and why the improvements that it can effect will not be sufficient to allow construction of a truly reliable strategic defense system,

5) The nature of research in Artificial Intelligence, and why I do not expect it to help in building reliable military software,

6) The history of research in Automatic Programming, and why I do not expect it to bring about the substantial improvements that are needed,

7) Why Program Verification cannot give us a reliable strategic defense battle management software system,

8) My opinions on the management of applied research, why I consider this panel and the SDIO in general to be an inappropriate vehicle for funding research, and what I would do instead.

I am quite certain that you will be able to find software experts who disagree with my conclusions. For many, the project offers a source of funding, funding that will enrich some personally, while offering others new and generous support for their personal research projects. During the first sittings of our panel, I could see the dollar figures dazzling everyone involved. Almost everyone that I know within the military industrial complex sees in the SDI a new „pot of gold“ just waiting to be tapped.

For others, the project offers an unending set of technological puzzles that are fun to work on; such problems are exciting and challenging whether or not the work ever produces useful results. Almost every software expert that I know, entered the field because they enjoy this kind of challenge. Several of the speakers at the first meeting of our panel could not hide their delight at

the unbounded set of technical challenges implicit in the unattainable goals of the project.

I can tell you, as one who likes both money and technical challenges, that these temptations are very hard to resist. You will find it very hard to find unbiased expert opinions on this issue.

In March 1983 the President asked us, as members of the scientific community, to provide the means of rendering nuclear weapons impotent and obsolete . I believe that it is our duty, as scientists and engineers, to reply that we have no technological magic that will accomplish that. The short term applied research and focussed development that SDI is now funding is not going to solve the problem; the President and the public should know that.

Yours truly,

David L . Parnas

Lansdowne Professor

Cc : S . Wilson, panel members

David Parnas

David Parnas, geb. 1941, Professor Emeritus. Studium der Elektrotechnik und Promotion am Carnegie Institute of Technology (heute Carnegie Mellon University), später Lehre und Forschung an verschiedenen Universitäten in den U.S.A., Deutschland, Kanada und Irland. Dr. h.c.: ETH Zürich, Louvain, Lugano. 1987 erhielt er den Norbert Wiener Award der CPSR, 2001 den Preis des FIfF.

David L. Parnas

Ein Kommentar im Jahr 2009

Jüngere Leserinnen und Leser fragen sich möglicherweise, weshalb sie Texte lesen sollen, die 20 Jahre und älter sind. Die Antwort darauf findet sich in einer E-Mail, die ich im Jahr 2003 von einem Angestellten der U.S. BMDO (Ballistic Missile Defence Organisation) erhalten habe. Er schrieb:

"Ich bin als Softwarearchitekt und -entwickler eines Kampfmanagementsystems unseres ballistischen Raketenabwehrsystems angestellt. Ich habe viele Ihrer Texte einschließlich der ihres Buches „Software Fundamentals – Collected Papers by David L. Parnas" gelesen. Ich habe außerordentlich großen Respekt vor Ihrer Arbeit und Ihren Erkenntnissen darüber, was wir bei unseren Softwareentwicklungen machen können und was nicht.

Von besonderem Interesse waren für mich diejenigen Texte, welche Ihre Überlegungen zur SDI Software widerspiegeln. Die Probleme, die Sie Mitte der 80er Jahre identifiziert haben, sind dieselben Probleme, denen wir heute uns gegenüber sehen. Unglücklicherweise haben wir es im Department of Defence (oder wie es scheint auch in der Privatwirtschaft) nicht geschafft, die Art und Weise, wie wir Software entwickeln, zu verbessern. Ich glaube nicht, dass wir so wie bisher weitermachen können und dabei irgendeinen winzigen Erfolg erzielen."

(Übersetzung für die FIfF-Kommunikation; die Redaktion)

Es ist meine Überzeugung, dass der Verfasser dieses Schreibens Recht hat. Die in meinen alten Beiträgen diskutierten Probleme sind noch immer echte Probleme. Sie sind grundlegend und werden daher nie verschwinden.

Der Autor setzte seine E-Mail fort mit Begründungen für die Wichtigkeit einer Raketenabwehr. Er merkte an, dass sich Raketentechnologie weiter verbreitet und forderte – da andere Länder über Raketen verfügen – für die Vereinigten Staaten eine Raketenabwehr. Auch dies ist richtig. Solange einige Länder für sich das Recht in Anspruch nehmen, Atomraketen zu besitzen, werden andere Länder das gleiche für sich einfordern, die Verbreitung dieser Waffen wird weitergehen und die Vereinigten Staaten werden eine Raketenabwehr benötigen. Aufgrund der in meinen damaligen Artikeln geschilderten Probleme können sie jedoch eine derartige Abwehr nicht haben. Der einzige Weg sich von der Bedrohung durch Nuklearwaffen befreien zu können ist zu akzeptieren, dass keiner das Recht hat, solche Waffen zu besitzen.

Es gehört zur Verantwortung derjenigen, die ein Verständnis für die Begrenztheit der Softwaretechnik haben, der Öffentlichkeit verständlich zu machen, was wir nicht tun können und welche Auswirkungen sich aus diesen Grenzen ergeben.

Verantwortung 2.0

25. FIfF-Jahrestagung

vom 13. bis 15. November 2009 in Bremen

Das FIfF wurde 1984 in Bonn gegründet, sein 25-jähriges Bestehen lädt ein zu Rückschau und Neubestimmung. Da die Friedensthematik bereits im vorigen Jahr im Zentrum der Jahrestagung stand, liegt es nahe, in diesen Jahr mehr auf die gesellschaftliche Verantwortung einzugehen. Der Zusatz 2.0, der mit leichter Ironie an entsprechende Begriffsbildungen wie Web 2.0, War 2.0, Stasi 2.0 angelehnt ist, soll andeuten, dass verantwortlicher Umgang mit Informations- und Kommunikationstechnik und allen weiteren Errungenschaften und Hervorbringungen der Informatik durch die erreichte Verbreitung und Durchdringung in allen gesellschaftlichen Bereichen eine wachsende Herausforderung darstellt.

Im nächsten Heft der FIfF-Kommunikation werden Konzeption und Planung detailliert vorgestellt. Anregungen dazu einschließlich thematischer oder personeller Vorschläge für Vorträge, Arbeitsgruppen und sonstige Programmpunkte sind willkommen.

Die Kontaktadressen sind:

FIfF-Geschäftsstelle
Goetheplatz 4
28203 Bremen
Tel.: 0421 - 33 65 92 55
Fax: 0421 - 33 65 92 56
fiff@fiff.de

E-Mail: *2009@fiff.de*

FIfF-Jahrestagung 2009
c/o Hans-Jörg Kreowski
Universität Bremen
Fachbereich Mathematik/Informatik
OAS 3001
Linzer Straße 9a
28359 Bremen
E-Mail: *kreo@fiff.de*

Dietrich Meyer–Ebrecht

Krieg und Frieden ···– digital

Am 7. und 8. November 2008 fand die Jahrestagung des FIfF in Aachen statt. Sie wurde gemeinsam mit dem Aachener Friedenspreis e.V. und den Interdisziplinären Foren der RWTH Aachen ausgerichtet. Leitthema war die Rolle der Informatik und Informationstechnik in Konfliktszenarien und Friedensbemühungen. Der Schwerpunktteil der vorliegenden Ausgabe des FIfF Kommunikation ist den Referaten der Tagung gewidmet[1].

„Krieg und Frieden — digital", ein plakativer Titel. In schwarz und weiß provozieren die grafischen Grundelemente der Poster, Flyer und Internetseiten: Können Wissenschaft, Technologie, Technik in ‚gute' und ‚schlimme' differenziert werden? Vor einem Vierteljahrhundert, zur Gründung des FIfF, war die Situation übersichtlicher. Es ging um punktuelle militärische Anwendungen der Informatik vornehmlich in Waffensystemen, autonome Zielfindung mit Bildanalysemethoden zum Beispiel in Cruise Missiles oder Pershing-II-Raketen. Längst ist unser Arbeits- und Privatleben so vollständig von Informationstechnologie durchdrungen, dass die Übergänge zwischen nützlichen, wünschenswerten Anwendungen zu schädigenden, zerstörenden absolut fließend sind. Informatische Methoden, die im Operationssaal Leben zu retten helfen, werden auf dem Schlachtfeld zum Töten eingesetzt. Informationstechnik, die Menschen über Grenzen und Meere näher zueinander bringt, macht gleichzeitig kriminelle und terroristische Gruppen global aktionsfähig. Von den Medien wenig beachtet, von der Öffentlichkeit kaum wahrgenommen weitet sich die Grauzone der Sowohl-als-auch-Anwendungen neuer Technologien kontinuierlich aus. Wie viel wichtiger ist daher der Dialog über die Janusköpfigkeit unserer Informatik und Informationstechnik geworden! So ist es an der Zeit, dass das FIfF die Diskussion wieder intensiver führt. Anlass genug für eine Jahrestagung zu dieser Thematik – nicht nur in Rückbesinnung auf unsere 25jährigen Wurzeln!

Einmal Aachen als Austragungsort auserkoren, ergab sich der wunderbare Umstand, dass der *Aachener Friedenspreis e.V.* seine Mitarbeit bei der Ausrichtung der Tagung anbot, die wir ohne Zögern annahmen. **Otmar Steinbicker** stellt in seinem Geleitwort zu unserem Schwerpunktteil das Wirken des Vereins dar und sein Motiv für seine Mitarbeit: Wer Frieden schaffen und erhalten will, muss die Mittel kennen, mit denen Kriege vorbereitet und geführt werden oder verhindert werden können — auch die technischen. Informationstechnik hat heute auch hier eine Schlüsselstellung inne. Sie hat mit ihrer stetig zunehmende Leistungsfähigkeit nicht nur zu neuartigen Waffensystemen geführt, sie hat auch neue Formen der Kommunikation der Akteure ermöglicht und Öffentlichkeitsstrukturen verändert. Mit ihr haben Kriege zwischen Staaten, asymmetrische Konflikte und Terrorismus grundlegend ihre Gestalt verändert, und auch Friedensinitiativen stehen heute andere Möglichkeiten offen.

Und ein weiterer wichtiger Partner fand sich in Aachen schnell, die *RWTH*. In der *Rheinisch-Westfälischen Technischen Hochschule* erreichen wir die heranwachsende Generation der für die zukünftigen Entwicklungen Verantwortlichen. Und von ihr kommen wichtige Impulse für unsere Arbeit, nicht nur technische. Welche Spannweite von Themen die RWTH in der Forschung abdeckt, stellt **Armin Heinen** in einem weiteren Geleitwort dar, und dass es gerade bei diesem Thema unverzichtbar ist, die Brücke zwischen den Wissenschaften zu schlagen. Mit ihren *Inter-*

Unsere Tagungsstätte: die Couvenhalle der RWTH
Bildquelle: Jürgen Jansen

disziplinären Foren hat die Aachener Universität erfolgreich einen Weg beschritten, disziplinübergreifende Themen, so auch gesellschaftsrelevante Fragestellungen zu bearbeiten. Für das *Forum Informatik* und insbesondere für des *Forum Technik und Gesellschaft* ist die Teilnahme als Mitveranstalter der Tagung eine willkommene Möglichkeit, die Präsenz der RWTH auch auf diesem Themenfeld zu zeigen.

Wie zu erwarten, ergibt die Zusammenarbeit dieser drei so unterschiedlichen Institutionen erfreuliche Synergieeffekte. Gemeinsam lassen sich die Kosten der Tagung leichter tragen, das gemeinsame Auftreten ist hilfreich für die Einwerbung einer großzügigen finanziellen Unterstützung durch *ProRWTH*, dem Förderverein der RWTH, die repräsentative Couvenhalle der RWTH wird uns als Veranstaltungssaal zur Verfügung gestellt — und Aachener Prominenz ist bei der Eröffnung zugegen: Nach der Begrüßung durch Hans–Jörg Kreowski am Freitag Nachmittag hält Aachens Oberbürgermeister Dr. **Jürgen Linden** eine Ansprache, in der er an die geschichtliche Bedeutung des Tagungsthemas für die Stadt anknüpft und die Verantwortung von Wissenschaft, Politik und Medien für eine Nutzung technischer Innovationen im Dienste der Gesellschaft herausstellt. Prof. **Heather Hofmeister**, Prorektorin der RWTH, nimmt in ihrer anschließenden Ansprache das Thema auf. Sie macht deutlich, dass im Rahmen der Exzellenzinitiative — „meeting global challenges" — zu den vordringlichen Aufgaben der RWTH auch zählt, im Dialog zwischen den Wissenschaften nach Möglichkeiten für die Friedenssicherung zu suchen. Grußworte des Vorsitzenden des Aachener Friedenspreis e.V., Otmar Steinbicker, und des Sprechers des Forums Technik und Gesellschaft , Prof. Armin Heinen, leiten zu den Referaten über, die in den Beiträge des Themenschwerpunktes wiedergegeben werden.

„Kriegstechniken — Techniken des Krieges", unter diesem Leitwort bilden zwei komplementäre Referate den Auftakt. Dahinter steht der Begriff *Revolution of Military Affairs* (RMA), die Bezeichnung für den Prozess einer Veränderung militärischen Denkens und Handelns, der maßgeblich durch das Vordringen neuer Technologien in der Rüstung ausgelöst wurde. RMA steht für die Wechselwirkung zwischen neuen Mitteln der Kriegsführung, den neuen Methoden der Kriegsführung und ihren politischen Konsequenzen. **Jürgen Altmann**, Physiker und Friedensforscher, behandelt die auslösenden Faktoren. Er stellt die Geschichte der auf neuen technologischen Entwicklungen basierenden Waffen dar. Er beschreibt, wie unter zunehmendem Einsatz der Informationstechnologie eine Entwicklung zur Autonomisierung von Waffensystemen eingesetzt hat. Altmann widmet sich aber auch dem Einsatz neuer Technologien für Konfliktlösung und Friedensstabilisierung, so zum Beispiel im Dienste der Abrüstungsbemühungen. Aus der Perspektive der Politikwissenschaft stellt **Ralph Rotte** den fundamentalen Wandel der Kriegsführung seit dem Ende des ‚Kalten Krieges' als Folge der Verfügbarkeit neuartiger Waffensysteme dar. Wenn durch diese der Wirkungsbereich des einzelnen Soldaten dramatisch ausgeweitet und dieser gleichzeitig der direkten Bedrohung entzogen wird, hat dies auch politische Konsequenzen: Die Suggestion eines ‚Menschen schonenden' Krieges könnte die Schwelle zum Kriegseintritt senken. Andererseits bietet Technologiedominanz allein noch keinen verlässlichen Schutz. Sie provoziert Reaktionen, denen auf dem konventionellen Kriegsschauplatz nicht zu begegnen ist. Sie führt zunehmend zu ‚asymmetrischen' Kriegen und schafft damit einen neuen Zustand der permanenten Unsicherheit in der Gesellschaft.

Eine ganz besondere Stellung unter den Waffensystemen, die neueste Informationstechnologie und KI–Methoden einsetzen, nehmen – darauf weist bereits Altmann in seinem Referat hin – autonome Fahrzeuge für den Kampfeinsatz ein. **Noel Sharkey**, KI–Forscher und engagierter Agitator für *public awarenes*, zeichnet ein umfassendes Bild im Einsatz und in der Entwicklung befindlicher fahrender, fliegender und laufender Roboter, zunächst für die Aufklärung geschaffen, inzwischen zunehmend sogar mit Waffen ausgerüstet. *„We are sleepwalking*

Der Vortragssaal in der Couvenhalle
Bildquelle: Jürgen Jansen

into a brave new world where robots decide who, where and when to kill": Sharkey's Kernpunkt ist die ethische Problematik, die Frage, wer übernimmt die Verantwortung für den Einsatz und die Handlungen autonomer Systeme mit letalen Waffen? — Wie die Gesellschaft zur Akzeptanz von Robotern konditioniert wird, vermittelt **Stefan Krebs** in seiner technikhistorischen Bearbeitung des Themas. In der journalistischen Berichterstattung über die Entwicklung und den Einsatz von Militärrobotern werden diese immer wieder mit Robotern aus der Science-Fiction in Bezug gesetzt. Ausgehend von dieser Beobachtung bringt Krebs in seinem Beitrag Beispiele für so genannte *spill-over*-Effekte zwischen den populären Roboter-Geschichten und der aktuellen Militärrobotik.

Der Einsatz der Informationstechnologie für zivile Konfliktbewältigung ist das Thema **von Christopher Kullenberg**. Seit dem Terrorangriff auf das World Trade Center führen gesetzlich geforderte Überwachungstechniken zu einer zunehmenden Aushöhlung der individuellen Freiheit und Persönlichkeitsrechte. Kullenberg argumentiert, dass die parlamentarische Politik allein nicht zu einer offenen und demokratischen Diskussion in der Lage ist. Hier muss die Zivilgesellschaft, oder besser, müssen zivile Gruppen, Vereinigungen, Verbände aktiv werden. Das Internet mit seiner Option zu einer globalen Vernetzung ist dafür ein unverzichtbares Medium. Kullenberg fordert deshalb die Zusammenarbeit von Experten der Informationstechnik auf privater Ebene mit gesellschaftlichen Aktivisten, Menschenrechtsorganisationen und Bürgerjournalismus.

Der Publizist **Berndt Georg Thamm** widmete sich in seinem Vortrag der neuen Gefahr des asymmetrischen Krieges, auf der einen Seite die traditionell hierarchisch organisierten staatlichen Militärs und Ordnungskräfte, auf der Gegenseite hochflexible Terrornetzwerke. Er zeigte am aktuellen Beispiel al–Qaida die entscheidende Rolle moderner digitaler Kommunikationstechniken für die Existenz und das Wirken gegenwärtiger Terrororganisationen. Das Internet wir in zunehmenden Maße für Propagandaverbreitung, Spendensammlung, Rekrutierung und terroristische Ausbildung genutzt. Internet und Mobiltelefonie dienen darüber hinaus auch der Planung und Durchführung terroristischer Operationen. Sie sind wichtige Faktoren für die globale Entwicklung dieser neuen Kriegsform. In unserem Interview mit Thamm vertieften wir gezielt die das Tagungsthema berührenden Fragestellungen.

Die Rolle der Medien in Zeiten des Terrors, zu diesem Thema hatte **Marie-Theres Tinnefeld** eine Arbeitsgruppe anbieten wollen. Leider konnte die Arbeitgruppe nicht stattfinden. Statt dessen erscheint nun ihr Referat zu diesem Thema. Es behandelt die Folgen schwerer Terroranschläge, insbesondere der Anschäge vom 11. September 2001 für die Menschenrechte und befasst sich vor allem auch mit der Rolle der Medien, die eine wichtige Funktion in der Verteidigung der Menschenrechte haben, positiv wie negativ.

Ilona Koglin und **Marek Rohde** zeigen an vielen Beispielen, dass die Möglichkeiten, die die Informationstechnologie bietet, nicht nur fragwürdigen Zwecken dienen. Sie gibt Millionen Menschen weltweit die Möglichkeit, sich für Frieden und Menschenrechte einzusetzen. Obwohl das Internet zunächst für das Militär entwickelt wurde, ist es heute ein regelrechter Humus für Engagierte weltweit. So wird ihr Beitrag zu einer kleinen Reise durch die Kontinente dieser Welt, auf der es zu entdecken gibt, wie viele Menschen unsere modernen Kommunikationstechnologien für eine bessere Welt einsetzen.

Aachens Oberbürgermeister Dr. Jürgen Linden während seiner Begrüßungsansprache
Bildquelle: Jürgen Jansen

Dass die Folge der Referate nach einem Spektrum beunruhigender Szenarien und albtraumhafter Visionen mit einer versöhnlicher Utopie schließt, bricht ein wenig den Pessimismus, der sich beim Planen der Tagung vertiefte. „Krieg *und* Frieden…" war nicht nur als griffige Formel gewählt worden. Zu Beginn hatten wir ganz sicher noch die Vorstellung einer Balance zwischen Missbrauch und Nutzen, zwischen zerstörenden und aufbauenden Wirkungen – schwarz und weiß… Die deprimierende Realität holte uns bei der Planung ein: Das düstere Feld war mit Themen und ReferentInnen schnell zu besetzen, und viele Facetten dieses Feldes blieben unbesetzt, weil unser Zeitbudget eng begrenzt war. Gegengewichte zu finden gestaltete sich dagegen viel schwieriger. Nun, wenigsten eines haben wir gefunden...

FIfF-Tradition: der Tagungsbecher
Bildquelle: Dietrich Meyer–Ebrecht

Anschließend an die Vorträge wurden vier Arbeitsgruppen angeboten. Der Journalist **Detlef Borchers** praktizierte mit den Teilnehmern seiner Arbeitsgruppe, das Internet als Plattform für Friedensaktivitäten und auch für Gewalt provozierende Aktivitäten zu erkunden. In seinem Beitrag stellt er, komplementär zur Thematik der Arbeitsgruppe, den nichtstaatlichen Akteuren die Aktivitäten staatlicher, vornehmlich militärischer Akteure gegenüber.

Science-Fiction-Bezüge gab es nicht nur in mehreren Vorträgen, sondern auch in einer Arbeitsgruppe, welche die Verwendung von Spielfilm-Sequenzen im Lehrkontext zum Gegenstand hatte: Moderiert von **Ralf E. Streibl** wurden anhand einiger ausgewählter Filmausschnitte diesbezügliche Möglichkeiten und methodische Ansätze der Auseinandersetzung mit dem Themenfeld „Informatik und Krieg" sowohl für die akademische Lehre im Fach „Informatik und Gesellschaft" als auch für allgemeinbildende Veranstaltungen aufgezeigt und ausprobiert.

Alex Klein arbeitete gemeinsam mit den Teilnehmerinnen und Teilnehmern seiner Arbeitsgruppe an der Weiterentwicklung des Konzeptes für ein Informationsportal zu Rüstungs– und Militärstandorten in Deutschland.

Michael Ahlmann schließlich diskutierte mit den Teilnehmern seiner Arbeitsgruppe persönliche Konflikte bei der Konfrontation mit Rüstungsaufgaben im Berufsleben.

Das Abendprogramm des ersten Tages bot mit dem Literatur-Kabarett „Krieg und Frieden im Werk von Kurt Tucholsky und Erich Kästner" der beiden Kölner Kabarettisten **Hein & Katzenburg** einen sehr schöner Ausklang der Vorträge. Die beiden Künstler stöberten bei beiden Dichtern und stellten zum Thema der Tagung ein Programm zusammen, das mit scharfsinnigen Pointen, musikalisch untermalt, gleichermaßen unterhielt und berührte.

Wir danken nun nach dem erfolgreichen Abschluss dieser gut besuchten Tagung – knapp hundert TeilnemerInnen – allen, die an Planung, Organisation und Durchführung mitgewirkt und uns mit Ressourcen unterstützt haben. Unter den vielen, die mit Ideen und Beiträgen zur Planung und Gestaltung der Tagung beitrugen, möchte ich **Benedikt Kaleß** aus dem Vorstand des Aachener Friedenspreis e.V., **Vanessa Mai** von den RWTH–Foren und **Joerg Zeltner** aus dem FIfF-Vorstand besonders nennen. Die Organisation, vor allem die nicht unkomplizierte finanzielle Abwicklung oblag vor Ort **Vanessa Mai** und in der FIfF-Geschäftsstelle **Anja Riemer**. Dass die sich hervorragend ergänzende Veranstaltungspartnerschaft zustande kam, verdanken wir **Otmar Steinbicker**, dem Vorstandsvorsitzenden des Aachener Friedenspreis e.V. und **Armin Heinen**, dem Sprecher des Forum Technik und Gesellschaft. Die Zentralstellen der RWTH unterstützen uns bei der Einrichtung des Veranstaltungssaales und mit dem Aufbau der Veranstaltungstechnik, und viele freiwillige Helferinnen und Helfer sorgten für einen reibungslosen Ablauf der Veranstaltung und eine gastfreundliche Betreuung der ReferentInnen und TeilnehmerInnen. Ein herzlicher Dank sei ihnen allen an dieser Stelle noch einmal ausgesprochen!

In meinem persönlichen Resümee bin ich besonders erfreut darüber, dass auf unserer Tagung viele neue persönliche, auch internationale Kontakt geknüpft wurden. Die Tagung selbst gab konkrete Anstöße zu weiteren Veranstaltung in Aachen und außerhalb. So wird es im Juni auf *dem Global Media Forum* der Deutschen Welle zum Thema „Conflict Prevention in the Multimedia Age"[2] unter FIfF-Beteiligung zwei Workshops geben: ein Workshop über Robotics im militärischen Einsatz mit Referenten unserer Tagung, sowie einen vom FIfF zu gestaltenden Workshop mit dem Arbeitstitel „IT to provoke or prevent conflicts". In Planung sind außerdem eine Veranstaltung der Evangelischen Stadtakademie Aachen mit dem Titel „Frieden durch Technik" mit Beteiligung von ReferentInnen unserer Tagung und eine Vortragsveranstaltung des Aachener Friedenspreis e.V. zu diesem Feld. Und vielleicht schaffen wir es sogar zur Einrichtung eines Arbeitskreises in Aachen?

Endnotes

1 *Alle Vorträgen wurden mitgeschnitten. Sie sind als Podcasts aufbereitet von den Internetseiten der Tagung www.kufd.de/programm abrufbar.*

2 *www.dw-gmf.de*

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. Von 1997 bis 2003 war er Sprecher des Forum Informatik der RWTH. (dme@fiff.de).

Armin Heinen

Geleitwort im Namen der Interdisziplinären Foren zur Tagung „Krieg und Frieden – digital“

Als 1989 Mauer und Stacheldraht entlang des Verlaufs der Elbe mit einem Male verschwanden, Ost- und Westeuropa zusammenwuchsen, schien eine neue Zeitepoche anzubrechen. Vom Ende der Geschichte dozierte Francis Fukuyama, was gewiss nicht die schlechteste Zukunftsaussicht war. Denn erstmals einte die Welt eine gemeinsame Wertordnung. Der Sicherheitsrat agierte ungewohnt einvernehmlich, und die USA zeigten als „demokratischer Weltpolizist“ ihre Muskeln.

Aber dann kam doch alles ganz anders. Samuel Huntington diagnostizierte einen Zusammenprall der Kulturen. In Kuweit prüfte der irakische Diktator Sadam Hussein die Festigkeit der neuen Weltordnung und konfrontierte die Öffentlichkeit mit der Realität des Krieges. Der war dann durchaus nicht so septisch und so sauber, wie es die Militärs mit ihren neuen zielgerichteten Waffen versprochen hatten. Noch immer starben Zivilisten, trotz aller Fortschritte der Lenkwaffentechnik, und noch immer starben auch die „eigenen Jungs“, die doch durch die neue Technik geschützt sein sollten. Der Jugoslawienkonflikt erschütterte Europa und bewies wiederum, dass der Waffengang noch längst nicht vorbei war. Und als die Türme des World Trade Centers zusammenkrachten, mehr als 2.600 unschuldige Menschen unter sich begruben, da stand die Welt tatsächlich vor ganz neuen Herausforderungen. Der Glaube an die gemeinsame Weltordnung war sichtbar aufgekündigt, und so wollten die USA nur noch ihrer eigenen Stärke vertrauen. Afghanistan und Irak bildeten die nächsten Etappen in einem Konflikt, der jetzt als „asymmetrischer Krieg“ beschrieben wurde und in den neben Staaten auch militante Gruppen eingriffen. Der Macht der Mächtigen und deren Fähigkeit zur Vernichtung des im offenen Feld agierenden Feindes begegneten sie mit der Aufhebung des Unterschiedes von Militär und Zivilisten. Ihre Waffe war der unvorhersehbare, unberechenbare Mord, die Entgrenzung des Schreckens. Primitiv muteten ihre Tötungsformen im Vergleich zu jenen der Militärs an. Und doch bedienten sie sich der modernsten aller Techniken, zumindest dann, wenn es um das Eigentliche ging, dem Kampf um die Öffentlichkeit. Das Internet wurde so zum Schauplatz gegenseitiger Beschuldigungen und Bedrohungen, freilich auch der Intervention einer kritisch agierenden Gegenöffentlichkeit.

Anders als 1990 noch erwartet, hat die Welt also keinen Frieden gefunden, hat die technische Entwicklung viel eher Kriege in neuer Form möglich gemacht. Die Unterscheidung zwischen den gewaltbelasteten Ländern der Dritten Welt und dem „friedlichen Norden“ ist aufgehoben. Und die Utopie einer durch Technik vereinten, durch intelligente Waffen vor Diktatoren und Terroristen „beschützten Welt“ scheint ausgeträumt.

Aber wie beurteilen Fachleute die Realität heute? Wie stellen sich Militärs Krieg vor? Können „intelligente“ Waffensysteme Soldaten schützen, Zivilisten schonen und Angreifer von ihrem Tun abblocken, wie es Politiker im Westen hoffen und das Völkerrecht es einfordert. Welches Potenzial bietet das Internet, um dessen Missbrauch vor Gewalthandeln zu begegnen. Krieg ist längst „digital“ geworden, die „digitale Gewalt“ zu einer globalen Herausforderung herangewachsen.

Wenn die FIfF-Tagung dieses Jahr an der RWTH Aachen stattfindet, so ist das gewiss kein Zufall, hat sich doch unsere Hochschule zur Aufgabe gemacht, die „Global Challenges“ – also die großen Herausforderungen an unsere Welt – in ihrem Forschungsprogramm systematisch zu thematisieren. Wir sind überzeugt, dass wir hierfür hervorragend aufgestellt sind, weil wir – das hängt mit der Größe der Universität zusammen – parallele Forschungen durchführen, eine Vielzahl alternativer Technologien begleiten und bewerten können. Unsere Hochschule forscht mit einer für Europa besonderen Disziplinenvielfalt und kann dadurch die vorzeitige „Schließung von Technologien“ verhindern und Alternativen sichtbar machen. Zudem ist die RWTH Aachen in der Lage, Aufgaben und Themen in einer besonderen Interdisziplinarität zu verhandeln, die für andere Hochschulen eher ungewöhnlich ist.

Interdisziplinarität wird an der RWTH maßgeblich durch die Interdisziplinären Foren gefördert. Das sind freiwillige Zusammenschlüsse von Professoren in sechs thematisch gegliederten Bereichen, von denen sich insbesondere das Forum Informatik und das Forum Technik und Gesellschaft an der Veranstaltung der Tagung beteiligt haben. Die Interdisziplinären Foren verstehen sich als Gemeinschaft zur Entwicklung von interdisziplinärer For-

Armin Heinen

Univ.-Prof. Dr.phil. Armin Heinen lehrt Neuere und Neueste Geschichte im Historisches Institut der RWTH Aachen. Zugleich ist er Sprecher des Forums Technik und Gesellschaft der RWTH. (armin.heinen@post.rwth-aachen.de).

schung und Stärkung der multidisziplinären Lehre. Sie dienen als Kommunikationsnetzwerk und sind ein Marktplatz für kreative Ideen. Die Perspektive des Forums Technik und Gesellschaft liegt dabei auf der Sichtbarmachung und Reflexion der sozialen, historischen und wirtschaftlichen Dimensionen von Technik und Wissenschaft.

Inhaltlich wird im Rahmen der Tagung ein weites Spektrum abgeschritten. In einem vorgängigen Pressegespräch wurde gefragt: „Sind Sie eigentlich alle Pessimisten?" Die Antwort fiel differenziert aus. Wir leben in einer Gesellschaft, in der nicht mehr klar ist, was Frieden und was Krieg ist. Die Technologiedominanz des Westens und die zunehmende Asymmetrie der Kriegsführung von Staaten und Gruppen auf unterschiedlichem technischem Niveau führen zu einem permanenten Zustand zwischen Krieg und Frieden. Es gibt keine eindeutigen Antworten mehr. Vielmehr bedarf es vielfältiger Lösungsansätze: technischer Herangehensweisen, wie Jürgen Altmann sie in seinem Beitrag schildert, kluger Politik, wie sie Ralf Rotte beschreibt, und der Aufmerksamkeit Einzelner, wie Ilona Koglin und Marek Rode sie eindrucksvoll vorführen. Daher ist ein interdisziplinärer Zugang zur Frage der Tagung, welche Rolle die Informatik und die Informationstechnologie bei der Kriegsführung und Sicherung des Friedens spielen, tatsächlich erforderlich. „Krieg und Frieden", das ist heute gewiss „Krieg und Frieden – digital". Gleichwohl wäre die Informatik allein mit dem Thema überfordert. Deshalb haben die Interdisziplinären Foren ihr Mitwirken gerne zugesagt.

Otmar Steinbicker

Geleitwort des Aachener Friedenspreis e.V. zur Tagung „Krieg und Frieden – digital"

Als vor 20 Jahren, am 7. Mai 1988, der Verein Aachener Friedenspreis von 46 Personen gegründet wurde, da wagte wohl kaum eines der Gründungsmitglieder zu prophezeien, dass dieser Verein heute 400 Mitglieder hat und zu den stärksten lokalen Friedensorganisationen in Deutschland zählt. Mehr als 40 Organisationen und Institutionen, darunter die Stadt Aachen, der DGB, politische Parteien, der Diözesanrat der Katholiken im Bistum Aachen, der Evangelische Kirchenkreis, die katholischen Institutionen Misereor und Missio, zählen dazu sowie mehr als 350 Einzelpersonen.

Seit 1988 wird alljährlich jährlich zum Antikriegstag am 1. September der Aachener Friedenspreis an Frauen, Männer und Gruppen verliehen, die von „unten her" dazu beigetragen haben, der Verständigung der Völker und der Menschen untereinander zu dienen sowie Feindbilder abzubauen und Vertrauen aufzubauen. Die Preisträgerauswahl erfolgt unabhängig von ideologischen, religiösen oder parteipolitischen Kriterien und unabhängig von sozialer oder nationaler Zugehörigkeit der Preisträgerinnen und Preisträger. In der Regel wählt die Mitgliederversammlung einen internationalen und einen nationalen Preisträger. In diesen 20 Jahren ist dem Verein mit seinen Aachener Friedenspreisträgerinnen und Friedenspreisträgern ein Kompetenzteam erwachsen, das wesentlich die Bedeutung und die Ausstrahlungskraft des Aachener Friedenspreises als Preis, aber auch als handelnde Organisation in der deutschen Friedensbewegung bestimmt.

Wir wissen natürlich, dass es sehr viel mehr kompetente Menschen gibt, die sich von unten her für Frieden und Menschenrechte einsetzen, als wir mit dem Aachener Friedenspreis auszeichnen können. Wir möchten mit möglichst vielen von ihnen – auch unabhängig von Preisverleihungen – für die Sache des Friedens zusammenarbeiten. Von daher haben wir im Laufe der Jahre auch unsere Kooperation mit Organisationen und Persönlichkeiten aus der deutschen und Internationalen Friedensbewegung ausgeweitet.

Mit unserer Beteiligung an der Jahrestagung FIfF möchten wir einen weiteren Schritt auf diesem Wege gehen, um Wissenschaftlerinnen und Wissenschaftler der RWTH und auch weit darüber hinaus für eine weitere und weiter gehende Zusammenarbeit zu gewinnen. Schließlich sind Forschung und auch speziell Software für Rüstung und Krieg nicht nur Themen der diesjährigen FIfF-Tagung, sondern auch Realität in unserer Stadt: An der RWTH wird u.a. durch Kooperationsverträge mit Teilinstituten der Forschungsgesellschaft für Angewandte Naturwissenschaften (FGAN) geforscht. In drei Software-Schmieden werden Softwaresysteme auf Fregatten der Bundesmarine betreut, sowie High-level-Sicherheitslösungen für Netzwerke auch im militärischen Bereich und Echtzeitsysteme für die Luftwaffe entwickelt.

Wir sind als Friedensbewegung unserer Stadt gefordert, uns mit diesen Tatsachen auseinanderzusetzen und hoffen dabei auf wertvolle Anregungen.

Otmar Steinbicker

Otmar Steinbicker arbeitet nach abgeschlossenem Studium der Geschichte und Sozialwissenschaften seit 1989 als freier Journalist. Seit November 2003 ist er Vorsitzender des Vereins Aachener Friedenspreis. (steinbicker@aachener-friedenspreis.de)

Jürgen Altmann

Bomben, Chips und Algorithmen – Informationstechnik zwischen Krieg und Frieden

Informationstechnik war seit ihrem Beginn durch Kriegsbedürfnisse geprägt. Das letzte Jahrhundert liefert wichtige Beispiele. Im 2. Weltkrieg gelang es Großbritannien, die mit der Enigma-Maschine verschlüsselten deutschen Funksprüche zu entschlüsseln, was entscheidend für die Schlacht im Atlantik und den Nachschub der Alliierten war. Nach 1945 wurden die ersten Großrechner für ballistische Rechnungen und die Modellierung der Prozesse in Kernwaffen entwickelt. Wie es im Computer-Archiv des US-Army Research Laboratory heißt: „The Purpose of This Archive: To help the public remember that it was the U. S. Army which initiated the computer revolution ... all modern computers are descended from ENIAC, EDVAC, ORDVAC, and BRLESC — all of which were conceived of and built to address pressing Army needs." (ftp.arl.mil/~mike/comphist/)

1. Informationstechnik und Militär/Krieg: Stichworte zur Geschichte

Über Jahrzehnte war dann das Militär der Hauptfinanzier der Entwicklung von Computern, Software, Netzwerken usw. Die jeweils stärksten Supercomputer (in den USA ab 1948 UNIVAC, 1964 CDC 6600, 1977 Cray–1 usw.) wurden für Entwicklung neuer Atomwaffen eingesetzt, für Aerodynamik, Raketen und vieles andere mehr [1]. Kleinere Rechner wurden für die Echtzeitsteuerung von Waffensystemen entwickelt. In den USA wurde Robotikforschung an Universitäten seit etwa 1960 vom Militär finanziert. Das ARPAnet wurde für die sichere Datenübertragung unter Atomkriegsbedingungen entwickelt und wurde dann zum Vorläufer des heutigen Internet. Integrierte Schaltkreise und Mikrocomputer wurden zwar im zivilen Bereich entwickelt, aber auf der Basis von vorangegangener intensiver militärischer Halbleiterforschung. Damit wurde der PC möglich, und ein Massenmarkt für Computer und Informationstechnik entwickelte sich, in dem dann mehr Geld in Forschung und Entwicklung floss, so dass sich nun im zivilen Bereich der technische Fortschritt schneller vollzog als im militärischen.

2. Aktuelle Entwicklungen und Trends

Auch wenn bei den Massenprodukten die technische Dynamik inzwischen vom zivilen Bereich ausgeht (und die Streitkräfte immer mehr zivile IT-Produkte einsetzen müssen), lässt das Militär weiterhin in sehr großem Umfang Forschung und Entwicklung für Aufnahme, Verarbeitung und Übertragung von Informationen betreiben – gegenwärtig heißt eines der zentralen Ziele Informationsdominanz. Da die USA am aktivsten sind, kommen die folgenden Beispiele von dort, aber andere Länder folgen in der Regel zügig nach.

Ein Bereich ist die stetige Erhöhung der *Zielgenauigkeit*. War es mit Hilfe der Trägheitsnavigation gelungen, die mittlere Zielabweichung bei Interkontinentalraketen bei 10.000 km Reichweite auf unter 100 m zu verringern, wurde zur Driftkorrektur bei Marschflugkörpern zunächst der Geländehöhen- und dann der Szenenvergleich entwickelt. Dann kamen die hochgenauen Satellitennavigationssysteme (GPS der USA, GLONASS der Sowjetunion/Russlands). Heute wird an automatischer Zielerkennung gearbeitet. Bei allen diesen Verfahren spielen digitale Daten und mathematische oder Mustererkennungs-Algorithmen eine zentrale Rolle.

Das aktuelle Leitbild moderner Streitkräfte heißt *Netzwerk-zentrierte Kriegführung*. Die eigene Truppe soll so vernetzt werden, dass aufgenommene Informationen breit verteilt werden bzw. abgerufen werden können. Dadurch soll sich ein gemeinsames Lagebewusstsein herausbilden, das durch Selbst-Synchronisierung erheblich stärkere Wirksamkeit im Kampf ergeben soll. Als zentrales System soll das Global Information Grid aufgebaut werden, das Netz, dass alle Waffenplattformen, Sensoren und Führungszentren vereinigt, in gewisser Weise wie das öffentliche Internet. Allerdings ergeben sich hier erhebliche Probleme: Wie kann die notwendige Übertragungsbandbreite – etwa für Echtzeit-Videodaten von Aufklärungsdrohnen – zur Verfügung gestellt werden? Wie lässt sich eine sichere Übertragung gewährleisten, die auch noch gegen feindliches Mitlesen oder Stören geschützt ist? Wie lässt sich vermeiden, dass die beteiligten Menschen und Systeme nicht durch zu viel Information überlastet werden?

Mit der wachsenden Bedeutung von Rechnernetzen steigt das Interesse an *Cyber-Kriegführung*. Man möchte in gegnerischen Netzen spionieren, sie ggf. blockieren und infiltrieren. Dabei lässt sich – anders als bei den meisten Angriffen in der realen Welt – die Herkunft verschleiern, so dass der Verursacher seine Beteiligung abstreiten kann. Das eröffnet viele Möglichkeiten für Manipulation, wenn eine Macht z.B. zwei andere gegeneinander aufhetzen möchte. Weil militärische IT-Systeme erheblich besser gegen Fremdeinwirkung geschützt sind, ist abzusehen, dass Cyber-Kriegführung sich zum großen Teil gegen zivile Netze wenden wird.

Ein ganz anderer Bereich ist *biologisch inspirierte Informationstechnik*. Projekte in den USA widmen sich z.B. dem Nachbilden biologischer Sensoren, der Verarbeitung von Sinnesdaten ähnlich wie in den Nervensystemen von Lebewesen oder dem Lernen aus Erfahrungen

Ein Haupttrend der nächsten Jahrzehnte ist der zu *besatzungslosen* bzw. *robotischen Kampfsystemen*. Schon 2001 hat der US-Kongress beschlossen, die Streitkräfte sollen die Fernsteuerungstechnik so entwickeln, das 2010 ein Drittel der Angriffsflugzeuge und 2015 ein Drittel der Land-Kampffahrzeuge ohne Besatzung fliegen bzw. fahren. Aufbauend auf Jahrzehnte militärischer Roboterforschung und -entwicklung sowie Tausende von Einsätzen von Aufklärungsdrohnen bemüht sich das US-Verteidigungsministerium nun um die Teilstreitkräfte übergreifende Vereinheitlichung; auch für besatzungslose Land-, Über-

Titelseite der UMS Roadmap (US DoD)
Bildquelle: US-Regierung

wasser- und Unterwasserfahrzeuge wird intensiv gearbeitet. Der Fahrplan sieht breite Nutzung vor, mit vielen Stufen wachsender Fähigkeiten [2]. Die kompliziertesten Aufgaben – das verbundene Gefecht auf Land, die U-Boot-Bekämpfung auf und unter Wasser sowie der Luftkampf – sollen ab etwa 2020 möglich werden. Auch kleine Roboter werden erforscht; während sie schon heute zum Entschärfen von Sprengkörpern eingesetzt werden (aus einigen 10 m Abstand ferngesteuert), gibt es auch Ideen, sie große Entfernungen zurücklegen zu lassen, etwa beim US-Scorpion-Projekt, das beim deutschen Fraunhofer-Institut für Autonome Intelligente Systeme bearbeitet wurde. Kleinstflugzeuge sollen unbemerkt aufklären oder Zielpersonen bekämpfen – hier zeigen sich aber auch Grenzen bei der Höchstgeschwindigkeit (einige 10 km/h) und der Betriebsdauer (bisher einige 10 Minuten). Ein Spezialgebiet der Forschung ist die Schwarm-Intelligenz.

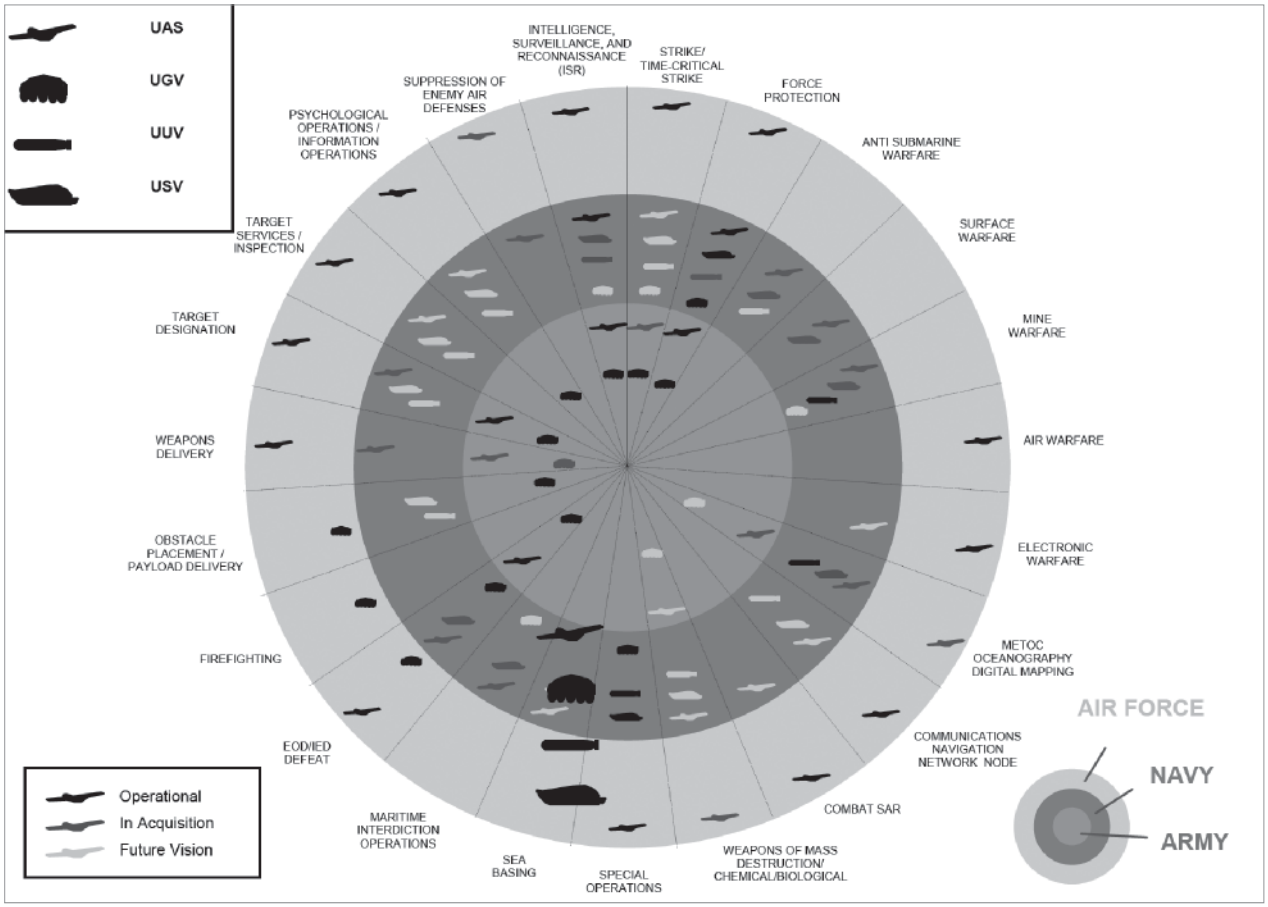
Die USA haben ihr besatzungsloses Aufklärungsflugzeug Predator (Länge 8 m) nachträglich mit Hellfire-Flugkörpern ausgestattet und im sog. Krieg gegen den Terrorismus seit 2002 eingesetzt. Inzwischen gibt es mit dem Reaper (Länge 11 m) ein besonders für den Kampf konstruiertes Flugzeug mit 1100 kg Waffennutzlast. Diese Typen werden von einer Basisstation in den USA aus gesteuert. Insbesondere über den Waffeneinsatz muss immer noch ein menschlicher Bediener entscheiden. Angedacht wird aber auch die *autonome Entscheidung* durch die Computer an Bord; insbesondere wenn es zukünftig auch gegnerische besatzungslose Fahr- und Flugzeuge geben wird, wird es einen Druck geben, schneller zu entscheiden, als die Satellitenverbindung und menschliche Reaktionszeit am anderen Ende der Übertragungsstrecke erlauben. Es gibt in der Robotik Forschungsprojekte zum Töten durch autonome Systeme – ein Forscher argumentiert, man könne robotischen Systemen die Regeln des Kriegsvölkerrechts (z.B. Unterscheidung zwischen Kombattanten und Zivilisten) einprogrammieren, und sie würden sie sogar genauer einhalten, da Überreaktionen wie bei menschlichen Soldaten vermieden würden. Ein Konzept für ein „künstliches Gewissen" sieht sogar die Möglichkeit der Befehlsverweigerung vor, wenn ein dem Völkerrecht widersprechender Auftrag gegeben wird [3]. Ob autonome Kampfsysteme tatsächlich mit dieser Fähigkeit ausgestattet würden, kann man bezweifeln. Wichtiger ist die Frage, ob die absehbare „Intelligenz" von KI-Systemen ausreicht, um eine Situationsbeurteilung und Aktionsentscheidung mindestens auf der Höhe menschlicher Fähigkeiten zu gewährleisten [4].

Wie schwierig die Umsetzung von Konzepten für netzwerkzentrierte Kriegführung mit besatzungslosen Fahrzeugen sein kann, zeigt das *Future Combat System* (FCS) der US Army. Seit 2000 wurde das Konzept entwickelt, 2002 wurden die Firmen Boeing und Sciende Applications International als führende Systemintegratoren verpflichtet, seit 2003 läuft die Systementwicklung. Neben Bodensensoren, einem Flugkörperstartsystem und „intelligenter Munition" sollte das FCS vier Klassen besatzungsloser Flugzeuge und drei Typen besatzungsloser Bodenfahrzeuge umfassen, neben fünf Arten mit Personen besetzter Fahrzeuge. Die 18 verschiedenen Systeme sollten mit einem Netzwerk verbunden werden. 2005 hat der Rechnungshof des US-Kongresses erhebliche Verzögerungen festgestellt, die Kosten waren von 80 auf 108 Milliarden $ gestiegen. Daraufhin verlangt der Kongress seit 2006 jährlich einen Bericht. Im Jahr 2007 wurden drei besatzungslose Systeme gestrichen, dadurch konnten die Kosten auf 161 Milliarden $ begrenzt werden. In seinen Berichten von 2008 stellte der Rechnungshof fest [5]:

- Nach fast fünf Jahren Entwicklung sei unklar, ob das Informationsnetzwerk, der Kern des FCS, entwickelt, gebaut und demonstriert werden kann.

- Die in Entwicklung befindliche Software für Netzwerk und Plattformen umfasse 95 Millionen Kodezeilen, fast dreimal

Predator mit Hellfire-Flugkörpern (US Air Force)
Bildquelle: US-Regierung



UMS Roadmap: besatzungslose Fahrzeuge für alle Medien vorgesehen (US DoD)
Bildquelle: US-Regierung

so viele wie 2003 vorgesehen und viermal so viele wie die nächsten beiden Software-intensiven Militärprogramme.

- Es sein unklar, wann oder wie demonstriert werden könne, dass die FCS-Software funktioniert.
- Die Army werde den Entscheidungsträgern 2013 wahrscheinlich ein teilweise entwickeltes und weitgehend nicht demonstriertes System zur Produktion präsentieren.
- Der Meilenstein 2009 sei entscheidend, er könne die letzte Gelegenheit zur Kursänderung bieten.

Auch das breite Feld von *Nanotechnik* und *konvergenten Techniken* soll intensiv militärisch genutzt werden [6]. Bei Nanotechnik geht es um die Untersuchung und Gestaltung von Systemen auf der Ebene von Nanometern (10^{-9} m), mit Strukturgrößen etwa zwischen 0,1 nm (Atom) and einigen 100 nm (großes Molekül). Auf dieser Ebene verschwimmen die Grenzen zwischen den Disziplinen – Nanotechnik, Biotechnik, Informationstechnik, Kognitionswissenschaft und andere Felder konvergieren. Diese Techniken sollen die nächste industrielle Revolution bringen, mit weit reichenden Konsequenzen in allen Lebensbereichen. In den USA wird von einer „neuen Renaissance" gesprochen, die „Weltfrieden, universellen Wohlstand, ... einen höheren Grad von Mitgefühl und Erfüllung" bringen werde. Im Bereich „nationale Sicherheit" wird jedoch betont, dass „militärische Überlegenheit" der USA unerlässlich sei [7].

Nanotechnik soll dafür sorgen, dass das „Mooresche Gesetz" der exponentiell wachsenden Rechnerleistung auch dann noch weiter gilt, wenn die Lithographie auf Halbleiteroberflächen ihre Grenzen erreicht hat, etwa mittels Kohlenstoff-Nanoröhren oder Molekülen als Speicher- und Schaltelemente. Mutige KI-Forscher extrapolieren, dass 1000-Dollar-Computer in 15 Jahren die rohe Rechenleistung des menschlichen Gehirns erreichen werden. Kleine und kleinste Rechner würden in alle militärischen Systeme integriert. Durch fähigere Steuerungen, festere Materialien usw. wird Nanotechnik neue kleine Waffen ermöglichen, etwa Flugkörper zur Flugabwehr, die vielleicht 30 cm lang sind und 3 kg Masse haben, somit viel leichtere Möglichkeiten für Terrorangriffe bieten als die bisherigen Schulter getragenen Flugabwehrsysteme (MANPADS) mit 1,5 m und 30 kg. Auch kleinste Satelliten zum Andocken und Manipulieren anderer werden möglich werden.

In der medizinischen Nanobiotechnik wird intensiv an Kapseln für den sicheren Einschluss und die verzögerte Abgabe von Agentien gearbeitet, mittels aktiver Gruppen sollen sie sich an spezifische Ziele in Organen und Zellen binden. Erforscht werden Mechanismen zum leichteren Eintritt in Körper oder Zellen, insbesondere durch die Blut-Hirn-Schranke, Mechanismen zur selektiven Reaktion mit speziellen Genmustern oder Eiweißen sowie zur Überwindung der Immunreaktion des Zielorganismus. Alles dies könnte auch für feindliche Zwecke verwendet werden, wobei man das Risiko durch Begrenzung der Haltbarkeit, programmierte Selbstzerstörung, Aktivierung oder Deakti-

vierung durch zweites Agens oder zuverlässige Impfung für die eigene Seite verringern könnte. Somit kann es möglich werden, die Wirkung auf besondere Gruppen oder gar ein einzelnes Individuum einzugrenzen. Nanotechnik wird aber auch schnellere, billigere, empfindlichere und selektivere Sensoren für chemische oder biologische Kampfstoffe erlauben, bessere Filtermaterialien und effektivere Dekontamination.

Damit Nanotechnik schneller in die Armee eingeführt werden kann, finanziert die US Army das Institute for Soldier Nanotechnologies, das 2002 am Massachusetts Institute of Technology gegründet wurde. Hier arbeiten über 170 Personen in fünf multidisziplinären Forschungsfeldern an einem schützenden Kampfanzug, Sensoren für den Körperzustand und medizinischen Techniken. Nach Bedarf sollen Wirkstoffe verabreicht und Wundkompressen gebildet werden.

Im Bereich *Hirn-Maschine-Schnittstelle* gelang es, mit Multielektroden auf der motorischen Hirnrinde eines Affen die Signale für Armbewegungen zu erkennen, so dass schließlich der Affe einen Roboterarm wie seinen eigenen steuern konnte. Andersherum konnte eine Ratte mittels implantierter Hirnelektroden über beliebige Kurse gesteuert werden.

In den USA ist die Defense Advanced Research Projects Agency (DARPA) für weit in die Zukunft reichende Forschung zuständig [8]. Sie hat fünf fachliche Abteilungen; Informationstechnik-Fragen werden vor allem im Information Processing Techniques Office bearbeitet. Dort gibt es sechs Schwerpunktbereiche; Tabelle 1 gibt einen Eindruck von den darin bearbeiteten Programmen.

Die DARPA hat, wie erwähnt, auch das Future Combat System mitkonzipiert, vielleicht wegen des Herangehens: „And please, please tell us that something simply cannot be done – it's science fiction. That is the challenge we cannot resist." [9]

Zwei kurze Schlaglichter auf die EU und Deutschland sollen folgen. Die Europäische Verteidigungsagentur (EDA) der *Europäischen Union* hat ein Defence R&T Joint Investment Programme on Innovative Concepts and Emerging Technologies. Dort spielen Informationstechnik und Nanotechnik eine herausragende Rolle; Tabelle 2 zeigt die Themenbereiche der ersten beiden Ausschreibungen.

Für *Deutschland* wird zunächst auf das European Land-Robot Trial (ELROB) verwiesen, einen Wettbewerb für besatzungslose Landfahrzeuge, den die Bundeswehr – nach dem Muster der DARPA Grand Challenges – seit 2006 jährlich durchführt, im Wechsel militärisch und zivil. Von den 14 deutschen Teams, die am militärischen ELROB 2008 teilnahmen, kamen 4 aus Informatik-/Robotik-Gruppen deutscher ziviler Universitäten [10].

Das zweite Beispiel betrifft die Entwicklung besatzungsloser Kampfflugzeuge (unmanned combat air vehicle, UCAV). EADS entwickelt das Barracuda mit 8 m Länge, über 7 m Spannweite und etwa 3 t Startmasse. Es flog im April 2006 zum ersten Mal, stürzte dann aber weniger Monate später ins Meer.

Das Deutsche Zentrum für Luft- und Raumfahrt untersucht Technologien für die Entwicklung von besatzungslosen Kampfflugzeugen, für die ab 2020 ein möglicher Bedarf zur Bekämpfung mobiler Ziele zu Lande, in der Luft gesehen wird.

3. Probleme und Auswege

Beim Nachdenken über Frieden und internationale Sicherheit muss ein Grundproblem berücksichtigt werden. Im gegenwärtigen internationalen System gibt es – anders als im Inneren von Staaten – keine übergeordnete Autorität mit einem Monopol legitimer Gewalt, die die Einhaltung von Regeln durchsetzen und vor allem Staaten vor Angriffen schützen kann. Jeder Staat versucht, die eigene Sicherheit durch die Drohung mit seinen Streitkräften zu gewährleisten. Dabei erhöht er aber gerade auch die Bedrohung für andere, so dass sich in der Summe die Sicherheit aller verringert.

Ein Ausweg aus diesem so genannten Sicherheitsdilemma ist die freiwillige wechselseitige Begrenzung der Streitkräfte, also *Rüstungskontrolle* oder gar Abrüstung (allerdings gibt es Widersprüche mit dem Ziel des Sieges, sollte dennoch Krieg ausbrechen). Rüstungsbegrenzung ist nur verlässlich, wenn die Staaten überprüfen können, ob die Vertragspartner die Vereinbarungen auch einhalten. Diese *Verifikation* braucht eine ausgewogene Mischung zwischen Offenheit und Geheimhaltung und wird umso schwieriger, je kleiner, billiger oder häufiger die nachzuweisende Objekte werden.

Für neue militärische Technologien ist präventive Rüstungskontrolle relevant – also ein Verbot oder eine Beschränkung einer militärisch nutzbaren Technologie oder von Waffensystemen, die wirken, bevor die neuen Systeme beschafft werden. Für solche vorbeugenden Beschränkungen gibt es eine Reihe von Präze-

Schwerpunktbereich	Anzahl Programme	Beispielprogramm
Cognitive Systems	15	Learning Applied to Ground Robots
Command & Control	8	Urban Leader Tactical Response, Awareness & Visualization
High Productivity Computing	3	Disruptive Manufacturing Technology, Software Producibility
Language Processing	3	Spoken Language Communication and Translation System for Tactical Use
Sensors & Processing	14	Camouflaged Long Endurance Nano Sensors
Emerging Technologies	3	Information Theory for Mobile Ad-Hoc Networks

Tabelle 1
Schwerpunktbereiche des Information Processing Techniques Office der US-DARPA mit je einem willkürlich ausgewählten Programm (Quelle: www.darpa.mil/ipto/thrust_areas/thrust_areas.asp)

denzfällen. Die Teststoppverträge (partiell 1963, vollständig 1996) verbieten nukleare Testexplosionen. Der Raketenabwehrvertrag (1972-2002) verbot Abwehrsysteme, die luft-, see- und beweglich landgestützt sind. Sowohl das Biologische-Waffen-Übereinkommen (1972) als auch das Chemiewaffen-Übereinkommen (1993) verbieten nicht nur die Herstellung, sondern schon Entwicklung und Erprobung solcher Waffen.

First Call	Second Call
Non Linear Control Design	Remote Detection of Hidden Items
Integrated Navigation Architecture	Nanostructures – Electro-Optical and Other
Nanotechnologies	Radar Technologies – Processing
Structural Health Monitoring	Radar Technologies – Components

Tabelle 2
Themenbereiche der ersten zwei Projektausschreibungen der Europäischen Verteidigungsagentur für innovative Konzepte und aufkommende Technologien (Quelle: www.eda.europa.eu/genericitem.aspx?id=368)

Präventive Rüstungskontrolle braucht die folgenden Schritte: Zunächst müssen die technischen Eigenschaften und die mögliche militärische Nutzung vorausschauend analysiert werden. Die Ergebnisse müssen dann unter Kriterien bewertet werden. Schließlich sind dann mögliche Beschränkungen und Verifikationsmethoden zu entwerfen. Die Kriterien lassen sich in drei Gruppen einteilen. Bei der ersten geht es um die Einhaltung und Weiterentwicklung von Rüstungskontrolle, Abrüstung und Völkerrecht. Die zweite betrachtet die militärische Stabilität einschließlich der Weiterverbreitung. Die dritte Gruppe hat den Schutz von Mensch, Umwelt und Gesellschaft zum Inhalt.

Am Beispiel der Nanotechnik hat sich gezeigt, dass von 21 möglichen militärischen Anwendungen 8 besonders gefährlich sind und präventiv verboten werden sollten, darunter metallfreie Schusswaffen, kleine Flugkörper und kleine Roboter. U.a. damit die Verifikation nicht zu aufdringlich wird, sollten die Verbote nicht an der Verwendung von Nanotechnik festgemacht werden, sondern an militärischen Systemen oder Aufgaben, unabhängig von der im Innern verwendeten Technik. Die Regelungen sollten in die allgemeine Rüstungsbegrenzung und Abrüstung integriert werden, z.B. sollten kleine Satelliten als Antisatellitenwaffe im Rahmen eines allgemeinen Verbots von Weltraumwaffen erfasst werden. Neue biologisch-chemische Waffen sind schon verboten, aber das Biologische-Waffen-Übereinkommen sollte durch ein System für Einhaltung und Verifikation ergänzt werden, wie es beim Chemiewaffen-Übereinkommen schon existiert.

4. Informationswissenschaft und -technik für Abrüstung und Frieden

Informationswissenschaft und –technik kann auf verschiedene Weise direkt für Abrüstung und Frieden eingesetzt werden. Eine Art ist die kritische Begleitung militärischer Forschung und Entwicklung. Können große militärische Softwaresysteme funktionieren, oder sind sie zu komplex, nicht durchschaubar, nicht verifizierbar und nicht validierbar? Zum Beispiel ist der Softwaretechnik-Pionier David Parnas 1985 aus dem Panel on Computing in Support of Battle Management des US-Raketenabwehrprogramms "Strategic Defense Initiative" ausgetreten, weil die Aufgaben der Gefechtsmanagement-Software nicht erfüllbar waren: Sie sollte feindliche Raketen erkennen ohne Wissen über deren genaue Eigenschaften. Sie werde – als auf viele Satelliten und andere Knoten verteiltes System – unzuverlässig arbeiten und könne die Echtzeitanforderungen nicht erfüllen (D. Parnas erhielt dafür 2001 den FIfF-Preis).

Für die in Entwicklung befindlichen ferngesteuerten Waffensysteme sind folgende Fragen zu bearbeiten: Kann eine sichere Datenverbindung – auch unter Feindeinwirkung – gewährleistet werden? Ist die per Videokamera verfügbare Information ausreichend, um kriegsrechtskonforme Entscheidungen zu treffen, ob ein bestimmtes Ziel angegriffen werden darf? Ist die Bedienerschnittstelle für die tödliche Entscheidung angemessen gestaltet? Gibt es bei Fernsteuerung eine größere Enthemmung durch die extreme Trennung vom Ort des Kampfes, die Ähnlichkeit mit einem Videospiel?

Weitere wichtige Forschungsfragen sind [11]:

- Kann künstliche Intelligenz gewährleisten, dass autonome Kampfsysteme das Kriegsvölkerrecht einhalten?
- Wenn Krieg immer mehr automatische Entscheidungen umfasst – welche Folgen wird das für den Frieden oder für die militärische Stabilität zwischen potentiellen Gegnern haben?
- Welche Wechselwirkungen können sich ergeben zwischen Cyber-Angriffen durch Hacker und militärischen Aktionen und Reaktionen?
- Kann man einen Schutz für kritische Informationsinfrastrukt ur im Kriegsvölkerrecht verankern?
- Ist es möglich, Vorbereitungen auf den Cyber-Krieg durch Rüstungskontrolle zu beschränken?
- Kann man die Informationstechnik, die für legitime UN-Einsätze gebraucht wird, von der für einen großen Krieg trennen?

Im Bereich Verifikation ist Forschung nötig für die automatisierte Verarbeitung von Satelliten- oder Luftbildern sowie von Daten von Vor-Ort-Sensoren.

Ein wenig problematisch und ambivalent ist die Frage, ob man mittels *data mining* Indikatoren für heimliche bzw. illegale Aktivitäten finden kann, etwa in Bezug auf die Weiterverbreitung beschränkter Technologien.

5. Verantwortung für Frieden in der Informationstechnik

Es gibt verschiedene Arten, wie man die Verantwortung, die man für die friedliche Nutzung der eigenen Wissenschaft/Technik hat, wahrnehmen kann. Einige wenige können die eigene Forschung oder Entwicklung direkt der Abrüstung widmen. Die vielen anderen, die „normale" zivile Forschungs- oder Softwareprojekte bearbeiten, können wachsam sein und militärische Forschung und Entwicklung im eigenen Feld verfolgen. Insbesondere in den USA, wo die Militärförderung von Universitäten eine starke Tradition hat, können die Computerwissenschaftler/innen überlegen, ob sie solche Finanzierung annehmen wollen.

Ein Beispiel für die bewusste Ablehnung gibt Benjamin Kuipers von der University of Texas, Austin [12]. Problematische militärische Anwendungen können in der Fachgemeinschaft zur Diskussion und in Frage gestellt werden, wie es Noel Sharkey macht [13].

Ich denke, dass zur Wahrnehmung der Verantwortung für den Frieden auch Grundkenntnisse in Abrüstung gehören, einschließlich der entsprechenden Verträge sowie der Methoden, wie die Einhaltung überprüft wird. Auch elementares Wissen über das Völkerrecht sollte vorhanden sein.

Verantwortung beginnt in der Lehre: Dort sollten Abrüstungsthemen mit Bezug zu Informationstechnik und Informatik einbezogen werden, z.B. bei Lehrveranstaltungen zu "Informatik und Gesellschaft". Sehr hilfreich wäre die Entwicklung entsprechender Lehreinheiten, auch für die Schule. Zur Information der Öffentlichkeit kann man Vorträge halten oder Gespräche mit Medienvertretern führen.

Das Forum Informatiker/innen für Frieden und gesellschaftliche Verantwortung spielt für Initiativen in diese Richtung eine wichtige Rolle, daher sollte es gestärkt werden.

Quellen und Anmerkungen

1 *S. z.B. Computer History Museum, www.computerhistory.org*

2 *UMS Roadmap 2007-2032, Washington DC: US Department of Defense, 2007.*

3 *Arkin, R. C., Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture, Technical Report GIT-GVU-07-11, College of Computing, Georgia Institute of Technology, 2007, www.cc.gatech.edu/ai/robot-lab/online-publications/formalizationv35.pdf*

4 *Siehe dazu den Artikel von Noel Sharkey in diesem Heft.*

5 *Government Accountability Office, 2009 Is a Critical Juncture for the Army's Future Combat System, GAO-08-408, Washington DC: U.S. Government Printing Office, 2008, www.gao.gov/new.items/d08408.pdf; 2008: Defense Acquisitions – Significant Challenges Ahead in Developing and Demonstrating Future Combat System's Network and Software, GAO-08-409, 2008, www.gao.gov/new.items/d08409.pdf*

6 *J. Altmann, Military Nanotechnology: Potential Applications and Preventive Arms Control, Abingdon/New York: Routledge, 2006; s. auch www.bundesstiftung-friedensforschung.de/pdf-docs/berichtaltmann.pdf.*

7 *M. C. Roco, W. S. Bainbridge, (eds.), Converging Technologies for Improving Human Performance – Nanotechnology, Biotechnology, Information Technology and Cognitive Science, Boston MA: Kluwer, 2003 (auch in: www.wtec.org/ConvergingTechnologies/1/NBIC_report.pdf); das europäische Konzept für konvergierende Techniken ist deutlich anders, High Level Expert Group Foresighting the New Technology Wave, Converging Technologies – Shaping the Future of European Societies, A. Nordmann (Rapporteur), Brussels: European Communities, 2004.*

8 *www.darpa.mil*

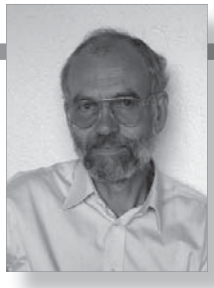
9 *B. Giroir, Ideas Begin Here, Teleprompter Script, presented at DARPATech, DARPA's 25th Systems and Technology Symposium, August 7, 2007, Anaheim CA, www.darpa.mil/DARPATech2007/proceedings/dt07-dso-giroir-ideas.pdf*

10 *Institute for Systems Engineering (ISE) Leibniz-Universität Hannover; FB 12, Universität Siegen; FB Informatik, Univ. Kaiserslautern; Jacobs University Bremen, www.elrob.org/Teams_Exhibitors.38.0.html*

11 *Wer interessiert ist, solche Forschung zu beginnen, kann sich gern an den Autor wenden.*

12 *B. Kuipers, Why don't I take military funding?, www.cs.utexas.edu/~kuipers/opinions/no-military-funding.html*

13 *Siehe den Artikel von Noel Sharkey in diesem Heft.*



Jürgen Altmann

PD Dr. Jürgen Altmann ist Physiker und Friedensforscher. Er hat Rechner betreut und Computer-Mustererkennung (an Bildern, an akustischen und seismischen Signalen) betrieben. Seit 1985 macht er Abrüstungs-orientierte Forschung. Schwerpunkte sind kooperative Verifikation von Abrüstungs- und Friedensabkommen mit akustischen, seismischen und magnetischen Sensoren sowie Militär-Technikfolgenabschätzung und präventive Rüstungskontrolle. Im letzteren Bereich hat er u.a. geforscht über „nicht tödliche" Waffen, Nanotechnik und besatzungslose militärische Systeme. Er ist Mitgründer des Forschungsverbundes Naturwissenschaft, Abrüstung und internationale Sicherheit FONAS und ein stellvertretender Sprecher des Arbeitskreises Physik und Abrüstung der Deutschen Physikalischen Gesellschaft DPG. (altmann@e3.physik.tu-dortmund.der.

Ralph Rotte

Kriegsbilder Im Wandel:

Gesellschaftliche und politische Herausforderungen

Die technologischen Innovationen der letzten zwei Jahrzehnte haben zu einem differenzierten Wandel des Kriegsbildes geführt, das in der Politikwissenschaft und in den Internationalen Beziehungen unter Stichworten wie „Revolution in Military Affairs" (RMA) oder „Neue Kriege" diskutiert wird. Im folgenden Essay werden einige exemplarische Aspekte und Perspektiven der politik- und sozialwissenschaftlichen Diskussion über das Phänomen des Krieges und seiner aktuellen Entwicklungen aufgezeigt, die gerade für den interdisziplinären Dialog von Interesse sind.

Drei exemplarische Ansätze und Diskussionsstränge

(1) Die Debatte um RMA und NCW

Die Diskussion um eine neue, in erster Linie technologiebedingte „Revolution in Military Affairs" (RMA) als "rapid and radical increase in the effectiveness of military units that alters the nature of warfare and changes the strategic environment" (Metz, 1997: 185) wurde Mitte der 1990er Jahre unter dem Eindruck der konzeptionellen Umsetzung in der von den USA vorangetriebenen „Network Centric Warfare" (NCW) in einer breiteren sozialwissenschaftlichen Öffentlichkeit angestoßen. Die Konzeption der NCW zielt darauf ab, die neuesten Informations- und Sensortechnologien zu nutzen, um ein integriertes „system of systems" aufzubauen, in dem drei interagierende Netzwerke – das *sensor grid*, das *information grid* und das *engagement grid* - eine teilweise dezentralisierte, völlige Informations- und damit militärische Handlungsdominanz gegenüber jedem Gegner gewährleisten sollen. Auf der Basis von *information superiority*, *speed of command* und *self-synchronization* soll den (U.S.-) Streitkräften eine überwältigende konventionelle Überlegenheit verschafft werden (*full spectrum dominance*) (Cebrowski 1998).

Wie die Erfahrungen in Afghanistan seit 2002 und im Irak seit 2003 gezeigt haben, funktioniert diese neue Art der Kriegführung jedoch bislang keineswegs so reibungslos wie vorgesehen (Gray 2004). Besondere Probleme in der Praxis bestehen dabei insbesondere in der Unfähigkeit, Formen asymmetrischer Kriegführung zu bewältigen, die nicht zuletzt auf die Unterschätzung der notwendigen Zahl von „boots on the ground" und die ignorierte „relevance of close combat" (Leonhard 2004) zurückzuführen ist. Hinzu kommen Aspekte wie die Unmöglichkeit einer politischen Stabilisierung eines besetzten Landes mit ausschließlich militärischen Mitteln und die wachsende Last der horrend steigenden Kosten für die Entwicklung und Beschaffung von NCW-Systemen.

(2) Die „neuen" Kriege

Der Begriff der „neuen Kriege" wurde unter dem Eindruck der Balkankriege der 1990er Jahre in die politikwissenschaftliche Debatte eingebracht (Münkler 2001; Kaldor 2007). Im wesentlichen behauptet dieser Ansatz, dass sich das gegenwärtige Kriegsbild durch eine Reihe fundamentaler Neuerungen auszeichnet:

- die typischerweise asymmetrische Kriegführung,
- die Dominanz innerstaatlicher Kriege,
- die völlige Nichtbeachtung und Entwertung des humanitären Völkerrechts, sowie
- die Eigendynamik und Persistenz des Krieges durch die Entstehung von Kriegsökonomien.

Als unmittelbare Folge des Phänomens der „neuen Kriege" wird dann die erhebliche Erschwernis einer Auflösung von Konfliktsituationen, insbesondere von außen, gesehen. Trotz der Popularität des Begriffs im sozialwissenschaftlichen Diskurs bleibt das Konzept der „neuen Kriege" mit einigen Problemen behaftet (z.B. Schlichte 2006), die insgesamt zu wenig berücksichtigt werden:

- einem ausgeprägten historischen Eurozentrismus, der die Kriegserfahrung auf anderen Kontinenten weitgehend ignoriert,
- der historisch zweifelhaften Idealisierung des europäischen Krieges seit dem 17. Jahrhundert, sowie
- der Unterschätzung der empirischen Bedeutung zwischenstaatlicher Konflikte.

(3) „Postheroismus" westlicher Gesellschaften

Der Begriff des Postheroismus wird seit Mitte der 1990er Jahre unter dem Eindruck der RMA und des Endes des Ost-West-Konfliktes diskutiert (z.B. Luttwak 1995). Grundsätzlich bezeichnet das von seinen Vertretern behauptete Phänomen den wachsenden Unwillen der etablierten Demokratien, Menschenverluste zu tragen (loss aversion). Ursachen hierfür werden beispielsweise in einem quasi-pazifistischen gesellschaftlichen Wertewandel oder im demographischen Wandel mit den sinkenden Geburtenraten in (post-) industrialisierten Ländern gesehen.

Als Ausweg aus dem resultierenden Dilemma zwischen mangelnder Opferbereitschaft und außenpolitischen Ansprüchen bzw. sicherheitspolitischer Gefahrenabwehr bietet sich der Rückgriff auf neue Technologien an. Durch den Einsatz von präzisen Distanzwaffen soll eine militärische Durchsetzungsfähigkeit ohne das Risiko eigener Verluste gewährleistet werden. Damit ist aber paradoxerweise eine potenzielle Erhöhung des Kriegsrisikos verbunden: Denn die Scheu vor dem Krieg kann durch seine scheinbare neue Risikolosigkeit quasi überkompensiert werden.

Auch die postheroische Interpretation des Konfliktverhaltens westlicher politischer Systeme weist eine Reihe gravierender Probleme auf, die von ihren Vertretern nicht konsequent gesehen werden (z.B. Rotte/Schwarz 2008):

- die nicht immer ausreichende Differenzierung unter den westlichen Demokratien,
- die unterschätzte Bedeutung der strategischen Zielsetzung eines Krieges für die Überzeugung der Bevölkerung, sowie
- die empirisch nachgewiesene weiter bestehende Fähigkeit von Demokratien zum „Durchhalten" eines Krieges bei als fundamental wahrgenommenen Sicherheitsbedrohungen.

Komplexität und Unschärfe des neuen Kriegbilds

Fasst man vor diesem gesellschaftlichen Hintergrund die wesentlichen Aspekte des aktuellen Kriegsbildes und seiner technologischen Bedingungen zusammen, so ergibt sich der Befund eines hochkomplexen, keineswegs konsistenten Phänomens (z.B. Gray 2005). Auf der einen Seite wird dieses neue Kriegsbild im westlichen Kontext dominiert von technologischer Innovation. Auf der anderen Seite stehen die Reaktionen der rüstungstechnologisch und ökonomisch unterlegenen tatsächlichen und potenziellen Gegner:

(1) Asymmetrische Kriegführung

Die taktisch-operative Reaktion auf die klare Überlegenheit eines Gegners besteht seit jeher im Anstreben solcher Gefechtskonstellationen, in denen er seine Überlegenheit am besten ausspielen kann, z.B. im Rückgriff auf traditionelle Guerilla-Taktiken. Ein weiteres Instrument asymmetrischer Kriegführung, wie sie in Afghanistan seit 2002 und im Irak seit 2003 zu beobachten ist, ist der Einsatz von Selbstmordattentätern. Dabei richtet sich diese Art der Kriegführung nicht nur gegen reguläre Streitkräfte, sondern nicht zuletzt im Rahmen einer auf politische und gesellschaftliche Destabilisierung ausgerichteten Strategie gegen einheimische Zivilisten.

(2) Eigene Nutzung moderner Informationstechnologien

Die zweite Antwort auf den „western way of war" besteht paradoxerweise im Rückgriff auf moderne Technologien auch durch die schwächere Konfliktpartei, vor allem auf prinzipiell allgemein zugängliche und vor allem billige Kommunikations- und Informationstechnologien. Im Rahmen der sogenannten *4th generation warfare* geht es dabei um die Nutzung aller verfügbaren Möglichkeiten, den Gegner von der Unmöglichkeit eines Sieges zu überzeugen (Echevarria 2005). Dies geschieht vor allem durch die Beeinflussung der öffentlichen Meinung mit Hilfe des Internets. So stellt die antiisraelische Propaganda im Internet während des Libanonkrieges 2006 mit den entsprechenden Folgen für die öffentliche Meinung in der Welt und in Israel selbst ein Paradebeispiel für eine Kriegführung dar, in der die Nutzung moderner, auch eigentlich nichtmilitärischer Technologien zum Erfolg der militärisch schwächeren Seite führt (Kreps 2007).

Ein anderer Ansatz, moderne Informationstechnologien zu kriegerischen Zwecken zu nutzen, ist der *cyberwar*. Hier wird versucht, durch die Beeinträchtigung der IT-Infrastruktur des Gegners möglichst große sozioökonomische Schäden anzurichten, um seine politische Ordnung und gesellschaftliche Funktionsfähigkeit zu beeinträchtigen oder die Basis seiner Verteidigungsfähigkeit i.e.S. zu unterminieren. Dies geschieht in erster Linie durch den Einsatz verhältnismäßig billiger Hardware und das Know-how von Informatik-Spezialisten, die quasi als Hacker im Regierungsauftrag handeln. Beispiele für *cyberwarfare* finden sich im behaupteten russischen Vorgehen gegen Estland 2007 und Georgien 2008 (Stratfor 2008). Besonders zu unterstreichen ist in diesem Zusammenhang der potenziell „totale" Charakter des *cyberwar*, der sich angesichts der typischerweise guten Sicherung militärischer IT-Netze notwendigerweise in erster Linie gegen eigentlich zivile Ziele wendet.

Zentrale Herausforderungen

Welche politischen und gesellschaftlichen Herausforderungen ergeben sich nun aus diesem komplexen, technologielastigen und zugleich höchst ambivalenten neuen Kriegsbild für die westlichen Demokratien? Zur Beantwortung dieser Frage seien vier exemplarische, zentrale Dimensionen und sozialwissenschaftliche Diskussionsthemen angeführt:

(1) Militarisierung der Außenpolitik?

Aus theoretischer und empirischer politikwissenschaftlicher Sicht ist weitgehend unbestritten, dass die Verfügung über „a very sharp sword" (Fordham 2004) auch eine erhöhte Wahrscheinlichkeit ihres Einsatzes in sich birgt. Technologisch bedingter militärischer Fortschritt impliziert daher die Gefahr vermehrten unilateralen Handelns der stärkeren Staaten, auch unter Nichtbeachtung des Völkerrechts sowie die wachsende Attraktivität von Präemptionsdoktrinen. Klare Hinweise in dieser Richtung finden sich vor allem in der Strategieentwicklung der Vereinigten Staaten seit dem 11. September 2001.

(2) Professionalisierung und Digitalisierung als Entpolitisierung?

Mit der Fokussierung auf die technologische Transformation von Streitkräften und einer vor allem technologieorientierten Wahrnehmung des Krieges ist die Gefahr des Verlusts genuin strategischen Denkens verbunden, welches sich durch eine rationale Verbindung von (politischem) Zweck und (militärischem) Ziel und Mittel der Anwendung militärischer Gewalt auszeichnet. Technologie wird mehr und mehr zum Strategieersatz, mit dem Ergebnis, dass politische Diskurse über Sicherheit und *grand strategies* kaum mehr geführt werden.

(3) Militarisierung der Gesellschaft?

Im innerstaatlichen Bereich kann die Technologisierung von Streitkräften und Kriegsbildern gravierende Änderungen in den *civil-to-military relations* nach sich ziehen. Die vermeintlich ver-

lustfreie und sichere Kriegführung kann dazu führen, dass vermehrt „zivile Militaristen“ (Johnson 2003) ohne militärischen Hintergrund zur treibenden Kraft der Anwendung militärischer Gewalt werden. Im Endeffekt resultiert daraus möglicherweise die Verstrickung in strategisch dilettantisch geplante, sich lang hinziehende und politisch kontraproduktive militärische Engagements. Die Militarisierung des Zivilen wird zudem dadurch verstärkt, dass angesichts der im Bereich der militärischen Hochtechnologie investierten Mittel für Forschung, Entwicklung und Beschaffung der seit den 1950er Jahren thematisierte „Militärisch-Industrielle Komplex“ durch die vermehrte Einbeziehung von Verwaltungen und Universitäten an Umfang und Reichweite gewinnt. Dabei kommt dem Verschwimmen der Grenzen zwischen dem Militär- und dem Zivilbereich auch zupass, dass im Zuge der Ökonomisierung als gemeinsamem Nenner und gesellschaftlichem Prinzip militärische F&E oft zivile Anwendungen impliziert und umgekehrt.

(4) Destabilisierung des internationalen Systems?

Fehleinschätzungen der eigenen Fähigkeiten führen von Seiten des Westens möglicherweise zu einem „demokratischen Interventionismus“ (Rotte 2008), der in lang andauernde kriegerische Verwicklungen asymmetrischer Art mündet. Demgegenüber sehen sich andere regionale und im globalen Kontext ambitionierte Mächte zu Gegenmaßnahmen genötigt, um nicht auch irgendwann als „Opfer“ des Westens in Frage zu kommen. Das Resultat ist u.a. ein neues Wettrüsten, einerseits bei neuen technologischen Möglichkeiten der Kriegführung (*cyber warfare*), andererseits bei Nuklearwaffen als „Versicherung“ gegen mögliche Interventionen. In diesem Sinne trägt das neue technologiebasierte Kriegsbild des Westens zur Intensivierung des Problems der Weiterverbreitung von Massenvernichtungswaffen bei.

Fazit

Die Konsequenz, die aus diesen skizzierten Facetten eines neuen Kriegsbildes und seiner Folgen zu ziehen ist, erscheint mir offensichtlich: Es ist höchste Zeit für eine neue, öffentliche Diskussion über das Phänomen Krieg, die Frage von Sicherheit im 21. Jahrhundert, die Rolle des Militärs als Instrument der Politik usw. Dabei sind nicht zuletzt traditionelle Begrifflichkeiten zu überdenken, denn möglicherweise macht es angesichts eines neuer Arten von Bedrohungen und Kriegführungsmöglichkeiten sowie einem Verschwimmen der Grenze zwischen dem Zivilen und dem Militärischen nur noch beschränkt Sinn, von einer strikten Trennung von Krieg und Frieden als alternativen politischen und gesellschaftlichen Zuständen zu sprechen. Wenn dies der Fall ist, sind aber auch die gewohnten Konzepte zur Einhegung oder Beseitigung des Krieges vielleicht nicht mehr adäquat.

Konkrete Ansatzpunkte für einen solchen gesamtgesellschaftlichen Diskurs über Krieg und Frieden ergeben sich in einer Intensivierung der strategischen Forschung im interdisziplinären Dialog sowie in einer verstärkten Öffentlichkeit von Forschung. Zentrale Voraussetzung bleibt dabei stets die Bereitschaft zu Tabubrüchen. Dies gilt nicht zuletzt für die Technikwissenschaften selbst: „We need to break the mental chains that bind us to a technology-*über-alles* dream of warfare – a fantasy as absurd and dated as the Marxist dreams of Europe's intellectuals“ (Peters 2006).

Literatur:

Cebrowski, Arthur K. (1998): Network-Centric Warfare: Its Origins and Future. U.S. Naval Institute Proceedings, 1/1998 (www.usni.org/Proceedings/Articles98/PROcebrowski.htm, 11/07/2005).

Echevarria, Antulio J. (2005): The Problem with 4th Generation Warfare. Strategic Studies Institute (www.strategicstudiesinstitute.army.mil/newsletter/opeds/2005feb.pdf, 20/02/2008).

Fordham, Benjamin O. (2004): A Very Sharp Sword. The Influence of Military Capabilities on American Decisions to Use Force. Journal of Conflict Resolution 48 (5): 632–56.

Gray, Colin S. (2004): Grand Strategy for Chaos. RMA and the Evidence of History. London.

Gray, Colin S. (2005): How has war changed since the end of the Cold War? Parameters 35 (1): 14–26.

Johnson, Chalmers (2003): Der Selbstmord der amerikanischen Demokratie. München.

Kaldor, Mary (2007): Neue und alte Kriege. Frankfurt/M.

Kreps, Sarah E. (2007): The 2006 Lebanon War: Lessons Learned. Parameters 37 (1): 72–84.

Leonhard, Robert R. (2004): Let's get closer: Remembering the relevance of close combat. Army Magazine 9/2004 (www.jhuapl.edu/areas/warfare/papers/getcloser.asp, 06/12/2008).

Luttwak, Edward (1995): Towards Post-Heroic Warfare. Foreign Affairs 74 (3): 109-122.

Metz, Steven (1997): Racing toward the future: The Revolution in Military Affairs. Current History 96 (609): 184—188.

Ralph Rotte

Univ.-Prof. Dr. Ralph Rotte lehrt Politische Wissenschaft/Internationale Beziehungen an der RWTH Aachen. Seine Forschungsschwerpunkte sind strategic studies, internationale politische Ökonomie und empirische Konfliktforschung. (*rotte@ipw.rwth-aachen.de*)

Münkler, Herfried (2001): *Die neuen Kriege*. Frankfurt/M.

Peters, Ralph (2006): The Counterrevolution in Military Affairs. *The Weekly Standard* **11** (20), 2.6.2006 (www.weeklystandard.com, 03/11/2008).

Rotte, Ralph (2008): „... a general loosing of the ties of civilized society..." – *Democratic Interventionism* als legales oder legitimes außenpolitisches Instrument im 21. Jahrhundert? In: Biegi, M. et al. (Hg.), *Demokratie, Recht und Legitimität im 21. Jahrhundert*, Wiesbaden: 247—267.

Rotte, Ralph und Schwarz, Christoph (2008): Aeneas statt Achill. Anmerkungen zum Postheroismus westlicher Gesellschaften. *Merkur* 62 (704): 86—90.

Schlichte, Klaus (2006): Neue Kriege oder alte Thesen? Wirklichkeit und Repräsentation kriegerischer Gewalt in der Politikwissenschaft. In: Geis, Anna (Hg.), *Den Krieg überdenken. Kriegsbegriffe und Kriegstheorien in der Kontroverse*, Baden-Baden: 111—132.

Stratfor (Strategic Forecasting, Hg.) (2008): *Cyberwarfare 101: Case Study of a Textbook Attack*, 18.4.2008. (www.stratfor.com/analysis/cyberwarfare_101_case_study_textbook_attack, 26/10/2008).

Noel Sharkey

Weapons of Indiscriminate Lethality

The development of autonomous robot weapons is well underway for use in a new style of hi-tech warfare. This will lead to less physical risk to the combatants deploying them but greater moral risk. There has been insufficient consideration of how these new weapons will impact on innocents. Two of the most serious ethical concerns discussed here are: (i) the inability of robot weapons to discriminate between combatants and non-combatants and (ii) the inability of such robots to ensure a proportionate response in which the military advantage will outweigh civilian casualties.

War is a very odd human endeavour. In normal life, humans are not permitted to murder one another without facing severe penalties. In many civilised countries, even the state is not allowed the right to execute for serious crimes. Yet in war it is acceptable for one large group of humans to kill humans from another large group without moral sanction or guilt. But there is a simple proviso for civilised countries that those killed must be from amongst those who are killing back or are contributing to it. In other words, the ideal is that combatants only kill other combatants. This is one of the cornerstones of the Laws of War.

The Geneva and Hague conventions as well as the various treaties and the laws of armed conflict strictly specify that innocents must be protected from harm. This is part of the justice in the conduct of a war, jus in bello, and is often expressed as the principle of discrimination – only combatants/warriors are legitimate targets of attack. All others, including children, civilians, service workers and retirees, should be immune from attack. In fact the laws of protection even extend to combatants that are wounded, have surrendered or are mentally ill.[1]

These protections have been in place for many centuries. Thomas Aquinas, in the 13th Century, developed the doctrine of Double Effect. Essentially there is no moral penalty for killing innocents during a conflict providing that (i) you did not intend to do so, or (ii) that killing the innocents was not a means to winning, or (iii) the importance to the defence of your nation is proportionally greater than the number of civilian deaths.

There are many circumstances in a modern war where it is extremely difficult, if not impossible, to fully protect non-combatants. For example, in attacking a warship, some non-combatants such as chaplains and medical staff may be unavoidably killed. Similarly, but less ethically secure, it is difficult to protect the innocent when large explosives are used near civilian populations, or when missiles get misdirected. In modern warfare, the equivalent of the doctrine of Double Effect is the Principle of Proportionality which, "… requires that the anticipated loss of life and damage to property incidental to attacks must not be excessive in relation to the concrete and direct military advantage expected to be gained."[2]

In warfare both the principles of discrimination and proportionality can be problematic although their violation requires accountability and can lead to war crimes tribunals. But now it looks as though we may be about to unleash new weapons that could violate both of these principles.[3] These are the proposed autonomous weapons such as unmanned combat vehicles. These will be able to make decisions about who to kill and when to kill them and yet cannot be accountable in themselves.

Lethal Autonomous robots and the problem of discrimination

There are between four and six thousand robots currently operating on the ground in Iraq and Afghanistan. These are mainly deployed in dull, dirty or dangerous tasks such as disrupting or exploding improvised explosive devices and surveillance in dangerous areas such as caves. There are only three armed Talon SWORDS robots made by Foster-Miller although more are expected soon. Most of the armed robots are in the sky; semi-autonomous Unmanned Combat Air Vehicles such as the MQ1-Predator that flew some 400,000 mission hours up to the end of 2006 and have flown significantly more since, and the more powerful MQ-9 Reapers with a payload of 14 Hellfire missiles— the RAF have two MQ-9s operating in Iraq. These can navigate and search out targets but, like the ground robots, it is a remote operator, this time thousands of miles away in the Nevada desert, who makes the final decision about when to apply lethal force.

There is now massive spending and plans are well underway to take the human out of the loop so that robots can operate autonomously to locate their own targets and destroy them without human intervention [4]: This is high on the military agenda of all the US forces: "The Navy and Marine Corps should aggressively exploit the considerable warfighting benefits offered by autonomous vehicles (AVs) by acquiring operational experience with current systems and using lessons learned from that experience to develop future AV technologies, operational requirements, and systems concepts."[5] There are now a number of autonomous ground vehicles such as DARPA's "Unmanned Ground Combat Vehicle and Perceptor Integration System" otherwise known as the Crusher.[6] And BAE systems, recently reported that they have "… completed a flying trial which, for the first time, demonstrated the coordinated control of multiple UAVs autonomously completing a series of tasks".[7]

The move to autonomy is clearly required to fulfil the current US military plans. Tele-operated systems are more expensive to manufacture and require many support personnel to run them. One of the main goals of the Future Combat Systems project is to use robots as a force multiplier so that one soldier on the battlefield can be a nexus for initiating a large scale robot attack from the ground and the air. Clearly one soldier cannot remotely operate several robots alone and it takes the solder away from operational duties.

The ethical problem is that no autonomous robots or artificial intelligence systems have the necessary sensing properties to allow for discrimination between combatants and innocents. Allowing them to make decisions about who to kill would fall foul of the fundamental ethical precepts of a just war under jus in bello as enshrined in the Geneva and Hague conventions and the various protocols set up to protect civilians, wounded soldiers, the sick, the mentally ill, and captives. There are no visual or sensing systems up to that challenge.

The problem is exacerbated further by not having a specification of "civilianess". A computer can compute any given procedure that can be written down in a programming language. We could, for example, give the computer on a robot an instruction such as, "if civilian, do not shoot". This would be fine if and only if there was some way to give the computer a clear definition of what a civilian is. We certainly cannot get one from the Laws of War that could provide a machine with the necessary information. The 1944 Geneva Convention requires the use of common sense while the 1977 Protocol 1 essentially defines a civilian in the negative sense as someone who is not a combatant:

1. A civilian is any person who does not belong to one of the categories of persons referred to in Article 4 A (1), (2), (3) and (6) of the Third Convention and in Article 43 of this Protocol. In case of doubt whether a person is a civilian, that person shall be considered to be a civilian.

2. The civilian population comprises all persons who are civilians.

3. The presence within the civilian population of individuals who do not come within the definition of civilians does not deprive the population of its civilian character. [8]

And even if there was a clear computational definition of civilian, we would still need all of the relevant information to be made available from the sensing apparatus. All that is available to robots are sensors such as cameras, infrared sensors, sonars, lasers, temperature sensors and ladars etc. These may be able to tell us that something is a human, but they could not tell us much else. In the labs there are systems that can tell someone's facial expression or that can recognize faces but they do not work on real time moving people. And even if they did, how useful could they be in the fog of war. British teenagers beat the surveillance cameras by wearing hooded jackets.

In a conventional war where all of the combatants wore the same clearly marked uniforms (or better yet, radio frequency tags) the problems might not be much different from those faced for conventional methods of bombardment. But the whole point of using robot weapons is to help in warfare against insurgents and in these cases sensors would not help in discrimination. This would have to be based on situational awareness and of having a theory of mind, i.e. understanding someone else's intentions and predicting their likely behaviour in a particular situation. Humans understand one another in a way that machines cannot and we don't fully understand how. Cues can be very subtle and there are an infinite number of circumstances where lethal force is inappropriate. Just think of a children being forced to carry empty rifles or insurgents burying their dead.

The problem of proportionality

According to the Laws of War, a robot could potentially be allowed to make lethal errors providing that the non-combatant casualties were proportional to the military advantage gained. But how is a robot supposed to calculate what is a proportionate response. There is no sensing or computational capability that would allow a robot such a determination. As mentioned for the discrimination problem above, computer systems need clear specifications in order to operate effectively. There is no known metric to objectively measure needless, superfluous or disproportionate suffering[9]. It requires human judgment.

No clear objective means are given in any of the Laws of War for how to calculate what is proportionate.[10] The phrase "excessive in relation to the concrete and direct military advantage expected to be gained" is not a specification. How can such values be assigned and how can such calculations be made? What could the metric be for assigning value to killing an insurgent relative to the value of non-combatants, particularly children who could not be accused of willingly contributing to insurgency activity? The military say that it is one of the most difficult decisions that a commander has to make; but that acknowledgement does not answer the question of what metrics should be applied. It is left up to a military force to argue as to whether or not it has made a proportionate response as has been evidenced in the recent Israeli-Gaza conflict.

Uncertainty needs to be a factor in any proportionality calculus. Is the intelligence correct and is there really a genuine target in the kill zone? The target value must be weighted by a probability of presence/absence. This is an impossible calculation unless the target is visually indentified at the onset of the attack. Even

then errors can be made. The investigative journalist, Seymour Hersh, gives the example of a man in Afghanistan being mistaken for bin Laden by CIA Predator operators in 2002. A Hellfire was launched killing three people who were later reported to be three local men scavenging in the woods for scrap metal.[11] And this error was made using a robot plane with a human in the loop. There is also the problem of relying on informants. The reliability of the informant needs to be taken into account and so does the reliability of each link in the chain of information reaching the informant before being passed onto the commander/operator/pilot. There can be deliberate deception anywhere along the information chain as was revealed in investigations of Operation Phoenix—the US assignation programme—after the Vietnam War. It turned out that many of the thousands on the assignation list had been put there by South Vietnamese officials for personal reasons such as erasing gambling debts or resolving family quarrels.[12]

It is also often practically impossible to calculate a value for the actual military advantage. This is not necessarily the same as the political advantage of creating a sense of military success by putting a face to the enemy to rally public support at home and to boost the morale of the troops. Obviously there are gross calculations that work in the extreme such as a military force carrying weapons sufficient to kill the population of a large city. Then it could be possible to balance the number of civilians killed against the number saved. Military advantage at best results in deterrence of the enemy from acting in a particular way, disruption of the social, political, economic, and/or military functions and destruction of the social, political, economic, and/or military functions.[13] Proportionality calculations should be based on the likely differences in military outcome if the military action killing innocents had not been taken.[14]

Despite the impossibility of proportionality calculations, military commanders at war have a political mandate to make such decisions on an almost daily basis. Commanders have to weigh the circumstances before making a decision but ultimately it will be a subjective metric. Clearly the extremes of wiping out a whole city to eliminate even the highest value target, say Osama bin Laden, is out of the question. So there must be some subjective estimates about just how many innocent people equal the military value of the successful completion of a given mission.

Yes, humans do make errors and can behave unethically but they can be held accountable. Who is to be held responsible for the lethal mishaps of a robot? Certainly not the machine itself. There is no way to punish a robot. We could just switch it off but it would not care anymore about that than my washing machine would care. Imagine telling your washing machine that if it does not remove stains properly you will break its door off. Would you expect that to have any impact? There is a long causal chain associated with robots: the manufacturer, the programmer, the designer, the department of defence, the generals or admirals in charge of the operation and the operator. It is thus difficult to allocate responsibility for deliberate war crimes or even mishaps.

Conclusions

There are some weapons that can be entirely be excessive in relation to the concrete and direct military advantage to be gained and that are, by their very nature, indiscriminate. Their lethal application can be decided by factors outside of decisions made by military commanders. For example, many civilised countries have signed treaties to ban landmines and cluster bombs because of their impact on the innocent population outside of their military application. But the military and the weapons manufactures continually exploit new technology to develop new weapons.

There are no current international guidelines or even discussions about the uses of autonomous robots in warfare. These are needed urgently. If there was a political will to use them then legal arguments could be constructed that leave no room for complaints[15]. This is especially the case if they could be released somewhere where there is a fairly high probability that they will kill a considerable greater number of enemy combatants (uniformed and non-uniformed) than innocents i.e. the civilian death toll was not disproportionate to the military advantage. Or if they could be restricted to a "kill box"—to use the US military term—they could be treated legally in the same way as a bombing mission.

Armed autonomous robots could also be treated in a legally way similar to submunitions such as the BLU-108 developed by Textron Defense Systems[16]. The BLU-108 parachutes to near the

Noel Sharkey

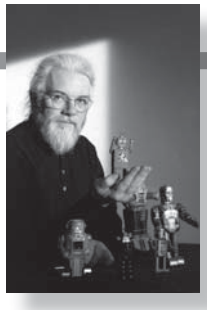


Foto: Bocking

Noel Sharkey BA PhD FIET, FBCS CITP FRIN FRSA is a Professor of AI and Robotics and Professor of Public Engagement at the University of Sheffield (Department of Computer Science) and EPSRC Senior Media Fellow (2004-2009). His main research interests are now in Biologically Inspired Robotics, Cognitive Processes, history of automata (from ancient times to present), Human-Robot interaction and communication, Representations of Emotion and Machine learning. He is currently involved in initiating public discussion about the ethical use of robots and the implications for public safety and human rights. *(noel@dcs.shef.ac.uk)*

ground where an altitude sensor triggers a rocket that spins it upwards. It then releases four Skeet warheads at right angles to one another. Each has a dual-mode active and passive sensor system: the passive infrared sensor detects hot targets such as vehicles while the active laser sensor provides target profiling. They can hit hard targets with penetrators or destroy soft targets by fragmentation.

But the BLU-108 is not like other bombs because it has a method of target discrimination. If it had been developed in the 1940s or 1950s there is no doubt that it would have been classified as a robot and even now it is debatably a form of robot. The Skeet warheads have autonomous operation and use sensors to target their weapons. The sensors provide discrimination between hot and cold bodies of a certain height but, like autonomous robots, they cannot discriminate between legitimate targets and civilians. If BLU-108s were dropped on a civilian area they would destroy buses, cars and lorries. Like conventional bombs, discrimination between innocents and combatants requires accurate human targeting judgements. It is this and only this that keeps the BLU-108 within humanitarian law.[17]

To use robot technology over the next 25 years in warfare would at best be like using the BLU-108 submunition, i.e. can sense a target but cannot discriminate innocent from combatant.[18] But the big difference with the types of autonomous robots currently being planned and developed for aerial and ground warfare is that they are not perimeter limited like the Skeet. The BLU-108 has a footprint of 820ft all around. By way of contrast, mobile autonomous robots are limited only by the amount of fuel or battery power that they can carry. They can potentially travel long distances and move out of line of sight communication.

In a recent sign of these future weapons the US Air Force sent out a call for proposals for Guided Smart Submunitions: "This concept requires a CBU (Cluster Bomb Unit) munition or UAV capable of deploying guided smart submunitions that have the ability to engage and neutralize any targets of interest. The goals for the submunitions is (sic) very challenging, when considering the mission of addressing mobile and fixed targets of interest. The submunition has to be able to reacquire the target of interest it is intended to engage." [19] This could be very like an extended version of the BLU-108 that could pursue hot bodied targets. It is the words "reacquire the target of interest" that is most worrying. If a targeted truck were to, for example, overtake a school bus, the weapons may acquire the bus as a target rather than the truck.

The only humane course of action is to severely restrict or ban the deployment of these new weapons until there have been international discussions about how they might pass an "innocents discrimination test". At the very least there should be discussion about how to limit the range and action of autonomous robot weapons before the inevitable proliferation. Although all of the elements discussed here can be accommodated within the existing Laws of War, autonomous robot weapons could change the nature of war considerably. This needs to be thought through properly and specific new laws should be implemented to not just accommodate but to constrain.

Endnotes

1 *But see also Ford, John S. (1944) The Morality of Obliteration Bombing, Theological Studies,261-309.*
2 *Petraeus D.H. and Amos, J.F. Counterinsurgency, Headquarters of the Army, Field Manual FM 3-24 MCWP 3-33.5, Section 7-30*
3 *Sharkey, N.E. (2008**)** The Ethical Frontiers of Robotics, Science, 322. 1800-1801*
4 *Sharkey, N.E. (2008) Cassandra or the false prophet of doom: AI robots and war, IEEE Intelligent Systems, vol. 23, no, 4, 14-17, JulyAugust Issue*
5 *Committee on Autonomous Vehicles in Support of Naval Operations National Research Council (2005) Autonomous Vehicles in Support of Naval Operations, WashingtonDC: The National Academies Press*
6 *Fox News (2008) Pentagon's 'Crusher' Robot Vehicle Nearly Ready to Go, Feb. 27, 2008*
7 *United Press International (2008) BAE Systems tech boosts robot UAVs IQ, Industry Briefing, Feb. 26.*
8 *Protocol 1 Additional to the Geneva Conventions, 1977 (Article 50)*
9 *Bugsplat software and its successors have been used to help calculate the correct bomb to use to destroy a target and calculate the impact. A human is there to decide and it is unclear how successful this approach has been in limiting civilian casualties.*
10 *Sharkey, N. (in press for 2009) Death Strikes from the Sky: The calculus of proportionality, IEEE Science and Society.*
11 *Hersh, S.M. (2002)"Manhunt: The Bush administration's new strategy in the war against terrorism," New Yorker, p. 66, Dec. 2002.*
12 *Hersh ibid*
13 *Hyder, V. D. (2004) Decapitation Operations: Criteria for Targeting Enemy Leadership, Monograph/report approved for publication. School of Advanced Military Studies United Sates Army Command and General Staff College, Fort Leavenworth, Kansas. p5*
14 *Chakwin, B., Voelkel, D. and Enright S. (2002) Leaders as Targets, Joint Forces Staff College, Seminar # 08*
15 *But it seems that, regardless of treaties and agreements, any weapon that has been developed may be used if the survival of a state is in question. The International Court of Justice (IJC (1996) Nuclear Weapons Advisory Opinion decided that it could not definitively conclude that in every circumstance the threat or use of nuclear weapons was axiomatically contrary to international law, see Stephens, D. and Lewis, M.W. (2005) The law of armed conflict – a contemporary critique. Melbourne J. International Law.**6***
16 *Thanks to Richard Moyes of Landmine Action for pointing me to the BLU-108 and to Marian Westerberg and Robert Buckley from Textron Defense Systems for their careful reading and comments on my description.*
17 *A key feature of the BLU-108 is that it has built-in redundant self-destruct logic modes that largely leave battlefields clean of unexploded warheads and thus keeps the it out of the 2008 treaty banning cluster munitions.*
18 *Sharkey, N.E. (2008) Grounds for Discrimination: Autonomous Robot Weapons, RUSI Defence Systems, 11 (2), 86-89*
19 *USAF call for proposals (2008) Guided Smart Munitions, Topic Number: AF083-093, August, 25*

Stefan Krebs

Über die (Co-)Konstruktion der Militärrobotik aus Wissenschaft und Fiktion

In der Berichterstattung über aktuelle Entwicklungen in der Robotik werden gerne rhetorische Anleihen an die Roboter aus der Science-Fiction gemacht. So lautet der Aufmacher eines Berichts in den VDI nachrichten vom 21. Juli 2006: „Aus Science-Fiction wird immer wieder Wirklichkeit: Exoskelette als Kraftverstärker können Menschen beim Gehen unterstützen oder Lagerarbeitern zu mehr Kraft und Ausdauer verhelfen [...]. Aber auch die Militärforschung setzt auf Exoskelette, weil Soldaten damit viel leistungsfähiger werden – US-Superman lässt grüßen." (VDI 2006) Ein anderes Beispiel ist ein Bericht über Außenskelette in der deutschsprachigen Technology Review, dort heißt es: „Von Atlas bis Zeus, von Superman bis Schwarzenegger – Geschichten übermenschlicher Kräfte durchziehen Mythologie wie Pop-Kultur. Jetzt aber kommen sie in der wirklichen Welt an [...]." (Huang 2004: 100) Auch in der englischsprachigen Presse finden sich entsprechende Formulierungen. Im Juli 2005 betitelt die Fachzeitschrift Assembly einen Artikel über die neuesten Entwicklungen der humanoiden Robotik: „Humanoid Robots are no longer Science Fiction." (Weber 2005: 70) Vergleichbare Beispiele ließen sich anführen.

Ein weiterer Fall mag verdeutlichen, dass die angenommene Verbindung zwischen den fantastischen Robotern und den Prototypen aus den Forschungslaboratorien weiter reicht, als es die These von der Popularisierung wissenschaftlicher Ergebnisse nahe legt. Ein geradezu paradigmatisches Beispiel findet sich in der diesjährigen Mai-Ausgabe des US-amerikanischen Popular Science Magazine. Darin wird ebenfalls über die Entwicklung von Roboteranzügen berichtet. Als Aufhänger der Story dient der zur gleichen Zeit in den Kinos anlaufende Film Iron Man. Der Aufmacher lautet: „While audiences flood theaters this month to see the comic-book-inspired Iron Man, a real-life mad genius toils in a secret mountain lab to make the mechanical superhuman more than just a fantasy." (Mone 2008: 44) Der zehnseitige Artikel stellt detailliert den XOS robot-suit der US-amerikanischen Rüstungsschmiede Raytheon vor und verfolgt die Entwicklung dieses Anzugs zurück in die Studios des Comic-Giganten Marvel. Hier werden also die technologischen Ursprünge, die Konstruktionspläne heutiger Entwicklungen, in der Fantasiewelt von Comic-Heften gesucht. Zur Veranschaulichung dieser entangled history[1] dient eine illustrierte Zeitleiste der Geschichte des Roboteranzugs, in der fiktive und reale Entwicklungsschritte gleichberechtigt nebeneinander stehen: Angefangen beim Hardiman von General Electric aus dem Jahre 1966 geht es über den bereits in den VDI nachrichten zitierten Film Aliens und eine Performance des australischen Künstlers Stelarc hin zum Bleex-Anzug der University of California – um schließlich beim Film Iron Man im Jahr 2008 vorläufig zu enden (ebd.: 50–52).

Das in dieser Zeitleiste präsentierte seamless web aus fantastischer, künstlerischer und wissenschaftlicher Technikgenese kann als ein Geflecht von Übersetzungen unterschiedlicher Konzepte aus einem Feld in ein anderes – und vice versa – gelesen werden. Im Folgenden möchte ich die komplexe Wechselwirkung zwischen Wissenschaft und Fiktion eingehender beschreiben und die zu beobachtenden Übersetzungsarbeiten mit dem Konzept der Co-Konstruktion von Technik erklären helfen.

Science Fiction und Robotik

Für die Verbindung von Science Fiction und Robotik sind zunächst die Erzählungen von Ingenieuren und Wissenschaftlern Legion, die ihr Interesse an der Robotik auf ihre Kindheit und besonders den damaligen Konsum von entsprechenden Comics und Zeichentrickserien zurückführen. Vor allem die japanischen Robotiker verweisen in Interviews immer wieder darauf, dass ihre Berufswahl von der wohl einflussreichsten japanischen Comicfigur Tetsuwan Atomu – Astroboy – beeinflusst worden sei (Wagner 2007: 34–54).

Umetani Yôji, emeritierter Professor für Weltraumtechnik und Maschinenbau am Tokyo Institute of Technology, schreibt programmatisch: „Die japanische Robotik ist vom ‚Tetsuwan

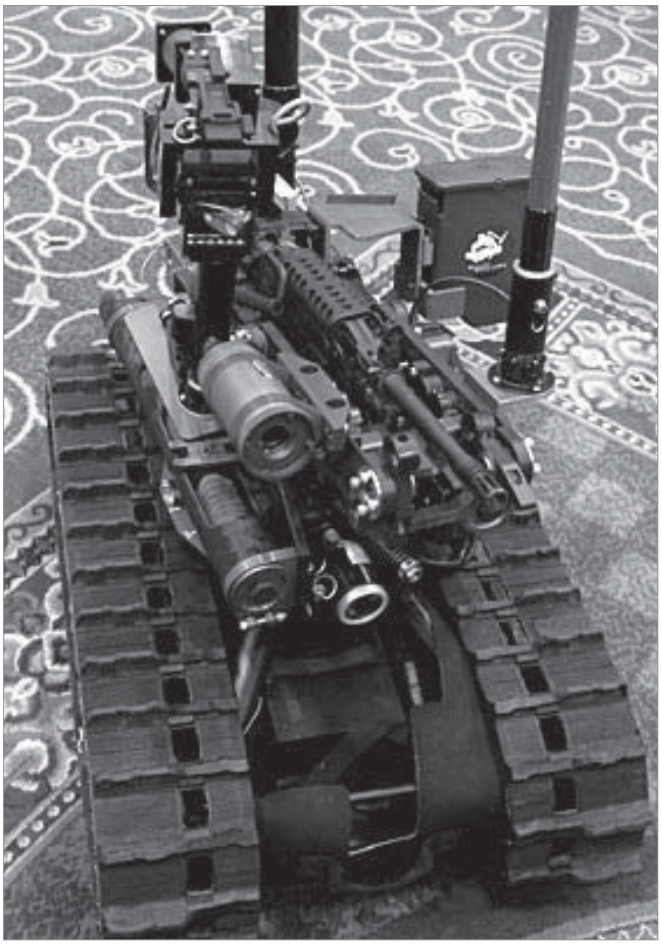
Johnny5_03.jpg
Creative Commons Lizenz Attribution ShareAlike 1.0

Atomu-Traum' beseelt und wird durch ihn gelenkt. Wenn es keine Geschichten und Romane gäbe, gäbe es auch keine Robotik, davon sind die führenden Roboter-Forscher und Entwickler fest überzeugt." (ebd.: 34) Auch die bekannten US-amerikanischen Robotiker werden nicht müde, in Interviews darauf zu verweisen, dass ihre Leidenschaft bis in die Grundschule zurückreiche. (Heuer 2003: 56) Der Berliner Soziologe Werner Rammert kommt zu dem Schluss: „Viele Visionen der heutigen Computerwissenschaftler und Roboterkonstrukteure stammen aus den Science-Fiction-Welten [...] – als Erwachsene versuchen sie in den Labors zu realisieren, wovon sie als Kinder geträumt haben." Auch er geht von einer Übersetzung fiktionaler Konzepte in Wissenschaft aus: „Man könnte die fantastischen Bilder mit ihren technischen Visionen als ein ‚hidden curriculum', gleichsam ein verdeckter Lehrplan, entschlüsseln [...]." (Rammert 2001: 22)

Der Transfer zwischen Fiktion und Wissenschaft verläuft aber auch in die umgekehrte Richtung: So wirken Ingenieure und Wissenschaftler unter anderem als Berater bei der Produktion von Science-Fiction Filmen mit. Ein bekannter Fall ist 2001: Odyssee im Weltraum von Stanley Kubrick aus dem Jahr 1968: Der Bordcomputer HAL 9000 wurde von dem US-amerikanischen Computerspezialisten Marvin Minsky mit konzipiert. Minsky sah in seiner Mitarbeit die Gelegenheit, seine eigene Forschungsarbeit weiter zu denken: „I thought that science fiction was a good venue for exploring the implications of AI [artificial intelligence]. It helps you to be clearer about the implications of your work." (Kirby 2003: 249) Ein Beispiel für die Robotik wäre der Physiker Andre Bormanis, der als wissenschaftlicher Berater für die Fernsehserie Raumschiff Enterprise – Das nächste Jahrhundert arbeitet (Bormanis 2000). Bormanis geht soweit die Serie als ‚science think tank' zu bezeichnen, der es erlauben würde, 10, 20 oder 30 Jahre in die Zukunft zu schauen – ein Luxus, den echte Wissenschaftler in ihrem Tagesgeschäft nicht besäßen (BBC).

Der Wissenschaftssoziologe David Kirby schlägt den Begriff des diegetic prototypes vor, um diese Art der Konstruktion fiktionaler Technik mithilfe wissenschaftlicher Beratung zu fassen. Das heißt, die Science-Fiction bietet unter diesen Umständen den beteiligten Wissenschaftlern einen Möglichkeitsraum an, in dem wissenschaftlich-technische Ideen bis in ihre letzte Konsequenz durchgespielt werden können – ohne unmittelbare Folgen für die ‚reale Welt' (Kirby 2008).

Noch einen Schritt weiter gehen die sogenannten ‚The Real Science of'-Artikel: Hier nehmen Wissenschaftler in Filmbesprechungen Stellung zu den dargestellten technisch-wissenschaftlichen Konzepten (Kirby 2003: 252). In Deutschland war dies besonders zum Kinostart des Films I, Robot zu beobachten. Hans-Dieter Burkhard und Raúl Rojas kommentieren und kritisieren in den VDI nachrichten das zu eindimensionale Roboterkonzept des Films. So fehlen ihnen u. a. spezialisierte Roboter: Es sei unrealistisch, dass es in der Zukunft nur humanoide Allzweckroboter gäbe, dagegen sei das dargestellte Konzept der Robotermuskeln durchaus nah an der Realität (Marsiske 2004). Die Experten verleihen dem Film einerseits Glaubwürdigkeit, da sie viele Darstellungen loben und als realistisch werten. Mit der Kritik an den fiktionalen Robotern übertreten die Rezensenten aber zugleich die Grenze zurück in ihr eigenes Feld, die Wissenschaft – begeben sie sich doch anscheinend auf die Ebene einer fachlichen Auseinandersetzung. Damit wirken die Science-Fiction Filme also zugleich in die Wissenschaftsdiskurse zurück.



SWORDS_robot.jpg
PD-USGov-Military

Science-Fiction und Militärroboter

Als nächstes wende ich mich der Militärrobotik zu: Eine zunächst äußere Ähnlichkeit weisen zahlreiche EOD-Roboter mit ihren fantastischen Vorbildern auf. EOD-Roboter dienen derzeit in erster Linie zur Bombenräumung und werden bereits in größeren Stückzahlen in Afghanistan und im Irak eingesetzt. Die Plattformen SUGV von irobot oder Talon von Foster-Miller erinnern mit ihren Kettenantrieben und binokularen Kameras stark an den Kampfroboter Nummer 5 – im Original Johnny 5 – aus dem gleichnamigen Science-Fiction Film. Diese Assoziation haben zumindest auch die Soldaten, die diese Roboter einsetzen und ihnen Spitznamen wie eben Johnny 5 geben (Garreau 2007).

Die Entsprechungen gehen jedoch über das rein Äußere hinaus. Der Journalist Joel Garreau lässt in einem Artikel in der Washington Post einen Unteroffizier zu Wort kommen, der im Irak mehrfach einen EOD-Roboter eingesetzt hat: „We always wanted him as our main robot. Every time he was working, nothing bad ever happened. He always got the job done. He took a couple of detonations in front of his face and didn't stop working. One time, he actually did break down in a mission, and we sent another robot in and it got blown to pieces. It's like he shut down

Small_Unmanned_Ground_Vehicle_May_2007.jpg
PD-USGov

because he knew something bad would happen." (Ebd.) Der Roboter entwickelt also ein Eigenleben – gerade so wie Johnny 5 im Film. Zumindest erlangen die Roboter in den Erzählungen der Soldaten einen Status jenseits bloß passiver technischer Artefakte. Garreau wartet in seinem Bericht mit einer ganzen Reihe ähnlicher Geschichten auf, in denen die Soldaten ihre Roboter nach erfolgreichen Einsätzen sogar befördern oder ihnen Tapferkeitsmedaillen verleihen (ebd.). Auch wenn die Anthropomorphisierung technischer Artefakte kein genuines Phänomen der Militärrobotik ist und der fetischisierte Umgang der Soldaten mit ihren Robotern dem Stressabbau dienlich sein mag, verwischen hierin dennoch die Grenzen zwischen der realen Welt des Krieges und den auf diese Weise rezipierten fantastischen Welten der Science-Fiction Filme.

Als letztes Beispiel möchte ich ein Memorandum des US-Verteidigungsministeriums anführen, das unter dem unspektakulären Titel „Unmanned Systems Roadmap 2007–2032" die Roboterkriege der Zukunft plant. Lakonisch heißt es in der Einleitung: „This Unmanned Systems Roadmap is focused on the future." (USR 2007: 1) Ein großer Teil der in dieser Studie vorgestellten unbemannten Luft-, Land- und Seesysteme befindet sich heute bereits im Prototypen-Stadium oder sogar schon im Kriegseinsatz. Interessant ist daher in erster Linie die in den Einführungskapiteln beschriebene Vision zukünftiger unbenannter Plattformen sowie deren Rolle bei der Kriegsführung: Dazu zählen beispielsweise Mikro Autonome Systeme und Technologien, die vom Army Research Laboratory entwickelt, ein wichtiger Baustein des network centric warfare werden sollen. Die dazu gehörigen Visualisierungen solcher Systeme erinnern in ihrer Ästhetik und Bildsprache an klassische Superman Comics bzw. aktuelle Computerspiele (ebd.: 33).

Noch etwas fantastischer als diese zeichnerischen Anleihen aus der Comicwelt ist die in dem Kapitel Push Factors gezeigte Vorstellung, dass künstliche Intelligenz nur mehr eine Frage der vorhersehbaren Computerentwicklung sei (ebd.: 46). Der Kurzschluss, dass intelligentes Handeln lediglich eines gewissen Maßes an Rechen- und Speicherressourcen bedürfe, mag dem eindimensionalen Menschenbild des Militärs und der binären Logik von Befehl und Gehorsam entgegen kommen, verweist hier aber darauf, dass die Roadmap des US-Verteidigungsministeriums einen Überschuss an Science-Fiction enthält.[2] Dies mag auch dem Umstand geschuldet sein, dass die Roadmap einen gewissen Zukunftsoptimismus verbreiten und zudem die Idee der unbemannten Kriegsführung popularisieren möchte. Dennoch trägt sie ihren Teil dazu bei, wissenschaftlich-technische Diskurse und populäre Science-Fiction miteinander zu verweben.

Zur (Co–)Konstruktion der Militärrobotik

Abschließend möchte ich einige Überlegungen anstellen, wie das beschriebene Geflecht aus fiktionaler und realer (Militär-)Robotik mithilfe des Ansatzes der Co-Konstruktion von Technik erklärt werden kann. In die Technikgeschichte fand der Begriff der Co-Konstruktion im Rahmen sozialkonstruktivistischer Theorieansätze zur Technikgenese Eingang. Kernthese ist die Annahme, dass technische Artefakte nicht einseitig durch die Produzenten konstruiert werden, sondern dass gerade auch die Benutzer diese mitkonstruieren.

Im vorliegenden Fall tritt die Science-Fiction an die Stelle der Konsumenten: Dies bedeutet, dass sie als Akteur an der Konstruktion realer Roboter beteiligt ist. Wie gesehen interagieren Techniker und Wissenschaftler auf vielfältige Weisen mit der Science-Fiction: Manche von ihnen werden selber zu Autoren fiktionaler Geschichten, andere übernehmen die Rolle wissenschaftlicher Berater für große Film- und Fernsehproduktionen oder reagieren wiederum als Rezensenten und Interviewpartner auf diese. Die Science-Fiction ist in diesem Sinne eine diskursive Arena, in der über die Form und technische Funktion von Robotern zwischen wissenschaftlichen und nicht-wissenschaftlichen Akteuren verhandelt wird. Die Grenzen zwischen Fiktion und Wissenschaft sind dabei nicht stabil, vielmehr kommt es zu Grenzüberschreitungen und -verschiebungen. In den science and technology studies hat sich hierfür der Begriff der boundary-work, der Arbeit an den Grenzen, etabliert.[3]

Dabei lassen sich aus Sicht der beteiligten Wissenschaftler eine Reihe von Gründen für die Infragestellung, Verschiebung oder auch Stärkung der Grenze zwischen Wissenschaft und wissenschaftlicher Fiktion erkennen. Zunächst ist da die öffentliche Aufmerksamkeit, die Wissenschaftler erhalten können, wenn sie sich auf das Feld der Science-Fiction begeben und mit entsprechend spektakulären Thesen aufhorchen lassen: Aufmerksamkeit, die selbst wieder eine Ressource bei der Akquisition von Ressourcen für die eigene Forschung sein kann. Zudem animiert das derzeitige System der Forschungsförderung Wissenschaftler

dazu, Innovationsversprechen zu machen, die weit jenseits des derzeit Realisierbaren liegen (Becker et al. 1997: 181). Eng damit verknüpft dienen solche (Technik-)Fiktionen in hybriden Teams aus anwendungs- und grundlagenorientierten Wissenschaftlern als Forschungsstrategie: Sinkt doch auf diese Weise der Druck, unmittelbar industrieverwertbare Prototypen zu bauen (ebd.). Die Science-Fiction ist ferner ein von gesellschaftlichen und technischen Zwängen entlasteter Raum des Möglichen, ein Raum in dem Technologien und ihr Einsatz bis in ihre letzten Konsequenzen durchdekliniert werden können. Dabei lassen sich auch zugleich die Reaktionen von Politik, Industrie und Zivilgesellschaft erkunden.

Die Science-Fiction ist insofern ein Ermöglichungsraum, in dem ganz im Sinne von Bormanis think tank neue Eigenschaften und Aneignungspraktiken von Militärtechnologien vorgedacht werden können. Auch kann die Öffentlichkeit hier an diese gewöhnt werden – noch vor dem ersten realen Kriegseinsatz (Bürger 2007). Dabei sollte auf keinen Fall die Wirkungsmächtigkeit dieser popkulturellen (Vor-)Bilder unterschätzt werden. George Basalla verweist mit Recht auf die enorme Breitenwirkung von Comics, Zeichentrick- und Spielfilmen (Basalla 1976). Hinzu kommt, dass die US-Armee seit Jahren massiv von den Möglichkeiten der Videospiel- und Filmindustrie Gebrauch macht, um neue Soldaten zu rekrutieren, diese dann zu trainieren sowie für ihre Visionen zukünftiger Kriege zu werben. Der Wissenschaftshistoriker Tim Lenoir spricht treffend vom ‚military entertainment complex', der den klassischen Militärisch-Industriellen-Komplex zwar nicht abgelöst hat, ihm aber aufgrund seiner propagandistischen Schlagkraft[4] gleichbedeutend zur Seite steht (Lenoir 2000). Dieser ‚military entertainment complex' sollte in seiner Funktion, militärische ‚Zukunftspolitik' zu gestalten sowie ihre gesellschaftliche Akzeptanz propagandistisch zu fördern, unbedingt ernst genommen werden: Eine sozialwissenschaftliche Analyse der ihn tragenden popkulturellen Medien erscheint daher umso dringender geboten.

Referenzen

George Basalla (1976): Pop Science: The Depiction of Science in Popular Culture, in: G. Holion/ W. A. Blanpied: Science and its Public, Dordrecht, S. 261–278.

BBC: Interview mit Andre Bormanis, http://www.bbc.co.uk/cult/st/interviews/bormanis/printpage.html, 29.10.2008.

Egon Becker et al. (1997): Out of control. Biorobotik: Science Fiction als wissenschaftlich-technische Innovation, in: Werner Rammert (Hg.): Innovationen – Prozesse, Produkte, Politik, Frankfurt a. M., S. 175–193.

Andre Bormanis (2000): Data, der kluge Androide. Der Roboter im Raumschiff, Enterprise', in NZZ Folio 6/2000.

Peter Bürger (2007): Bildermaschine für den Krieg. Das Kino und die Militarisierung der Weltgesellschaft, Hannover.

Joel Garreau (2007): Bots on The Ground. In the Field of Battle (Or Even Above It), Robots Are a Soldier's Best Friend, in: Washington Post, 6.5.2007, S. D01.

Thomas F. Gieryn (1983): Boundary-work and the demarcation of science from non-science: strains and interests in professional ideologies of scientists, in: American Sociological Review 48 (1983), S. 781–795.

Günther Görz/ Bernhard Nebel (2003): Künstliche Intelligenz, Frankfurt a. M.

Steffan Heuer (2003): Herr und Knecht, in: Technology Review 12/2003, S. 56–59.

Gregory T. Hunag (2004): Roboter zum Anziehen, in Technology Review 9/2004, S. 100–103.

Hartmut Kaelble (2005): Die Debatte über Vergleich und Transfer und was jetzt?, in: H-Soz-u-Kult, 08.02.2005, http://hsozkult.geschichte.hu-berlin.de/forum/2005-02-002.

David Kirby (2003): Science Consultants, Fictional Films, and Scientific Practice, in: Social Studies of Science 33 (2003), S. 231–268.

David Kirby (2008): Screening Technology: Technical Advisors, Diegetic Prototypes, and the Cinematic Creation of the Future, Vortrag SHOT-Tagung Lissabon, 12.10.2008.

Tim Lenoir (2000): All but War is Simulation: The Military-Entertainment Complex, in: Configurations 8 (2000), S. 289–335.

Hans-Arthur Marsiske (2004): Humanoide Roboter erfolgreich im Film, in: VDI nachrichten, 6.8.2004, S. 10.

Gregory Mone (2008): Man of Steel, in: Popular Science Magazine 5/2008, S. 44–54 u. 96–97.

Werner Rammert: Nicht nur natur- und technikwissenschaftliche Experten sind bei Wissenschaftsdebatten gefragt, in: Das Magazin, hg. Wissenschafts zentrum Berlin 1/2001, S. 22–23.

USR (2007): Office of the Secretary of Defense Unmanned Systems Roadmap (2007–2032), 10.12.2007, URL: http://www.acq.osd.mil/usd/Unmanned%20Systems%20Roadmap.2007-2032.pdf.

VDI (2006): Exoskelette als Kraftverstärker, in: VDI nachrichten, 21.7.2006, S. 12.

Cosima Wagner (2007): Robotopia Nipponica, Manuskript, Diss. Goethe-Universität Frankfurt.

Austin Weber (2005): Humanoid Robots Are No Longer Science Fiction, in: Assembly 7/2005, S. 70–78.

Endnoten

1 *Das methodische Konzept der entangled history verweist darauf, dass auch die Geschichte weit entfernter Länder miteinander verknüpft ist. In diesem Sinne könnten auch Wissenschaft und Fiktion als von-*

Stefan Krebs

Dr. Stefan Krebs forscht an der School of Innovation Sciences der TU Eindhoven (NL). Er studierte Geschichte, Philosophie und Politische Wissenschaft an der RWTH Aachen und der Universität Aix-Marseille (F). Nach seinem Magisterabschluss arbeitete er als Wissenschaftlicher Mitarbeiter am Lehrstuhl für Geschichte der Technik an der RWTH Aachen. Dort promovierte er 2007 im Fach Technikgeschichte.

einander weit entfernte und dennoch miteinander verbundene Felder verstanden werden (Kaelble 2005).

2 *Selbst wenn man den Prämissen der harten KI folgte, läge die Realisierung entsprechender intelligenter Artefakte weit jenseits der derzeitigen technologischen Möglichkeiten – entsprechende Extrapolationen sind demnach reine Fiktion.*

3 *In den science studies wird der Begriff boundary-work zur Beschreibung von Vorgängen benutzt, bei denen Grenzen, Demarkationslinien, Teilungen zwischen wissenschaftlichen Feldern errichtet, in Frage gestellt, angegriffen oder verstärkt werden (Gieryn 1983).*

4 *Ein wichtiger Punkt ist sicherlich, dass die militärische Propaganda besonders für die jugendlichen Konsumenten dieser Spiele kaum mehr als solche zu erkennen ist.*

Bildquellen:

http://commons.wikimedia.org/wiki/File:Johnny5_03.jpg.
This file is licensed under Creative Commons Attribution ShareAlike 1.0 License

http://commons.wikimedia.org/wiki/File:SWORDS_robot.jpg
This image is a work of a U.S. Army soldier or employee, taken or made during the course of the person's official duties. As a work of the U.S. federal government, the image is in the public domain.

http://commons.wikimedia.org/wiki/File:Small_Unmanned_Ground_Vehicle_May_2007.jpg
This work is in the public domain in the United States because it is a work of the United States Federal Government under the terms of Title 17, Chapter 1, Section 105 of the US Code. See Copyright.

Ralf E. Streibl

»Krieg und Informatik« im Spielfilm

Perspektiven für Lehre und Bildung im Bereich »Informatik und Gesellschaft«

»Wer aber Frieden will, der rede vom Krieg.«
(Walter Benjamin)

In einigen Vorträgen auf der FIfF-Jahrestagung 2009 in Aachen waren Bezüge zwischen Informationstechnik in militärischen Kontexten und Science Fiction hergestellt worden (vgl. z.B. Krebs 2009). In der hier kurz skizzierten Arbeitsgruppe ging es mir darum, anhand theoretischer Vorüberlegungen und anschließender praktischer Beispiele zu zeigen, warum m.E. Spielfilme bzw. Ausschnitte daraus ein hilfreiches und anregendes Material zur Gestaltung von Lehr- oder Vermittlungssituationen im Bereich Informatik und Gesellschaft sein können.

Informatik und Gesellschaft war für einige Jahre ein Lehrgebiet innerhalb der Informatik, das an manchen Universitäten sogar zum Pflichtkanon gehörte. Derzeit sieht es aber danach aus, als ob solche Lehrinhalte immer mehr verschwinden. Auch personell werden Einschnitte vorgenommen. Der gegenwärtig stärker werdende Fokus auf eine eng verstande »Nützlichkeit« und die technokratische »Verwertbarkeit« von Lerninhalten bei gleichzeitiger Verkürzung der Studiendauer drängt reflektierende Momente im Informatikstudium mehr und mehr an den Rand. Gleichzeitig fällt jedoch auf, dass an anderer Stelle schon seit langem Diskussionen über Anwendungen und Auswirkungen der Informatik geführt werden, die ein kritisches Potential enthalten. Allerdings fehlt es dabei häufiger an einer hinreichenden Tiefe. Gemeint ist die Auseinandersetzung mit Science Fiction und hier insb. mit Filmen, da durch das oft gemeinsame Seherlebnis im Kino, Fernsehen oder auf DVD zeitnahe Diskussionen angeregt werden. Gleichzeitig – dies kann und soll an dieser Stelle nur erwähnt, aber nicht weiter ausgeführt werden – stellen Spielfilme auch ein kulturelles Medium dar, welches vor dem Hintergrund der jeweiligen Produktionsgegenwart Kommentare, Szenarien, Projektionen von Hoffnungen und Ängsten bezogen auf gesellschaftliche und eben auch technische Entwicklungen beinhalten und transportieren kann. Im Bezug auf Informations- und Kommunikationstechnik sind besonders (aber nicht nur!) Science Fiction Filme interessant, die Ideen aus der aktuellen Forschung und Entwicklung aufgreifen und weiterspinnen. Dabei geht es in der Regel nicht um eine fantastische Projektion technologischer Trends, sondern um soziotechnische Szenarien sowie gesellschaftliche Auswirkungen und Reaktionen. Natürlich gibt es Filme, die sich sehr bewusst dieser Thematik annähern, vielleicht auch eine direkte Botschaft vermitteln wollen, während in anderen »Action«, »Thrill« und oder »Fun« dominieren. Dennoch – so zeigt sich bei näherer Betrachtung – können auch solche Filme durchaus als Material für eine intensivere Auseinandersetzung geeignet sein. Im Blick halten sollte man dabei immer, dass die meisten Filme als industrielle Produkte anzusehen sind, die im Produktionsprozess vielen Einflüssen unterliegen. Gerade bei Filmen mit Militärbezug kann es beispielsweise auch vorkommen, dass das Militär Drehbuchänderungen durchsetzt (vgl. z.B. Bürger 2005, S.55ff).

Im Mittelpunkt der Tagung stand die Beziehung von Informatik und Krieg. Ein kleines Brainstorming zu Beginn der Arbeitsgruppe brachte eine beträchtliche Anzahl von Spielfilmen aus ganz unterschiedlichen Zeiten zum Vorschein, in denen dieses Verhältnis zumindest eine bedeutsame Rolle spielt oder gar ein zentrales Element darstellt.

Solche Spielfilme beinhalten weit mehr als die Wertungen und Zuschreibungen, die man aus dem Material und aus Hintergrundinformationen herauszudestillieren versuchen kann. Sie wirken – wie alle Filme – anregend auf die Zuschauer, die beim Betrachten der Filme oder einzelner Sequenzen jeweils ihre Vorerfahrungen, Kenntnisse, Assoziationen und Emotionen mitbrin-

gen. Ganz im konstruktivistischen Sinne hat die Filmbetrachtung also immer einen sehr persönlichen, biographischen und situativen Charakter, dazu kommt ergänzend in einem kommunikativen Kontext die Konfrontation und Auseinandersetzung mit den Sichten, Assoziationen und Interpretationen anderer.

Filme im Bildungskontext einzusetzen ist nichts grundlegend Neues (vgl. z.B. Bergala 2006). Man kann dies auf vielerlei Weise tun, z.B. einfach nur zur Motivation oder zur Illustration eines Themas, man kann inhaltsanalytisch vorgehen, man kann einen Film strukturell analysieren und sich auf filmische Indikatoren beziehen, man kann auch historisch vorgehen und versuchen mehr über die Entstehung des Filmes und seinen Produktions- und Wirkungskontext zu erfahren. All diese Ansätze können auf ihre Weise zu einem Erkenntnisgewinn beitragen. Speziell im Kontext von *Informatik und Gesellschaft* bietet es sich an, einen möglichst kommunikativen Zugang zu wählen.

In der Arbeitsgruppe sind wir hierzu exemplarisch vorzugsweise in einer vorstrukturierten assoziativ-analytischen Weise vorgegangen: Kurze, von mir als Moderator im Vorfeld gezielt ausgewählte Filmsequenzen wurden gezeigt und danach tauschten die Arbeitsgruppenteilnehmerinnen und –teilnehmer ihre subjektiven Beobachtungen, Assoziationen, Gedanken und Gefühle aus. Es zeigte sich, dass teilweise ganz unterschiedliche Aspekte wahrgenommen wurden. Eine nochmalige Betrachtung der gleichen Sequenz nach Abschluss der Diskussionsrunde erlaubte dann, die Beiträge der anderen Personen anhand der Filmsequenz nochmals zu reflektieren. Steht mehr Zeit zur Verfügung, können – je nach Vorkenntnissen – natürlich auch stärker systematischere Analysemethoden zur Anwendung kommen.

Die Beispiele:

Kurz seien hier die in der Arbeitsgruppe verwendeten Filmbeispiele vorgestellt, ohne dass hier im Detail darauf eingegangen werden kann. Angesprochen wurden darüber hinaus zahlreiche weitere Filme. Ziel der Arbeitsgruppe war nicht, ein Teilthema intensiv zu behandeln, sondern anhand durchaus unterschiedlicher Beispiele exemplarisch methodische Vorgehensweisen zu demonstrieren.

Stealth
(USA 2005, R: Rob Cohan)

Eine Bomberstaffel erhält einen neuen »Wingman«, ein von einer Künstlichen Intelligenz gesteuertes UCAV (Unmanned Combat Aerial Vehicle). In der ersten gezeigten Sequenz wird dieses unbemannte Waffensystem den Piloten vorgestellt, wobei die Technik sowohl verherrlicht wird und Faszination erzeugt („… eine Wundertüte – voll mit Elektronik!") als auch diffus bedrohlich erscheint („… wird uns allesamt ersetzen"). Eine weitere Sequenz zeigt das UCAV in einem Kampfeinsatz, wo es sowohl intensivste Aufklärungsdaten in kürzester Zeit sammelt als auch selbständig eine Angriffsstrategie plant. Im weiteren Verlauf des Filmes wird – aufgrund einer Störung des Systems – das Vertrauen in derart autonome Systeme hinterfragt.

A Town called Eureka - Episode 1.11: »H.O.U.S.E. Rules«
(USA 2006, R: Jeff Woolnough):

Ein Beispiel dafür, dass auch Sequenzen aus Fernsehserien durchaus gut eingesetzt werden können. Die Hauptprotagonisten werden vom intelligenten Haus S.A.R.A.H. (= Self Activated Residential Automated Habitat) festgehalten. Ein Versuch, S.A.R.A.H. durch einen Kurzschluss lahmzulegen lässt Brad, ein zugrundeliegendes militärisches KI-System zu Tage treten („You built S.A.R.A.H. on top of Brad?" – „A.I.'s are often built on top of the programming of older generation A.I.'s"…) – ausgehend von dieser kleinen Sequenz lassen sich einige Brücken schlagen, z.B. zu zivil-militärischen Verflechtungen, Dual Use, Sicherheit, etc. entwickeln.

Wag the dog
(USA 1998, R: Barry Levinson):

Um eine Sexaffäre des im Wahlkampf steckenden US-Präsidenten zu vertuschen, wird ein Hollywood-Produzent beauftragt, einen »Trailer« für einen fiktiven Krieg gegen Albanien zu entwickeln. Die erste gezeigte Sequenz zeigt die Entwicklung der grundlegenden Ideen. Der zynische »Spin-Doctor« verdeutlicht dem Produzenten, dass Wahrheit keine Rolle spielt, sondern einzig was Menschen glauben – Information bzw. Desinformation dient als Propagandainstrument, das skrupellos eingesetzt wird. In einem zweiten Ausschnitt wird die Produktion eines gefälschten Nachrichtenclips gezeigt, wobei die Filmsequenz im Studio mit IT-Mitteln beliebig kreiiert und manipuliert wird („It's the same process with the last Schwarzenegger movie…").

Filmemacher sollten bedenken, dass man ihnen am Tag des Jüngsten Gerichts all ihre Filme wieder vorspielen wird.
(Ch. Chaplin)

Zum Abschluss sei hier die der Arbeitsgruppe zugrundeliegende Herangehensweise noch einmal in einem Überblicksschema skizziert: Abbildung 1 zeigt, wie der Inhaltsbereich »Informa-

Ralf E. Streibl

Ralf E. Streibl, Diplom-Psychologe, Mitglied der Redaktion der FIfF-Kommunikation, hauptberuflich an der Universität Bremen im Studienzentrum Informatik, Schwerpunkt in der Lehre: Informatik und Gesellschaft, bekennend filmbegeistert

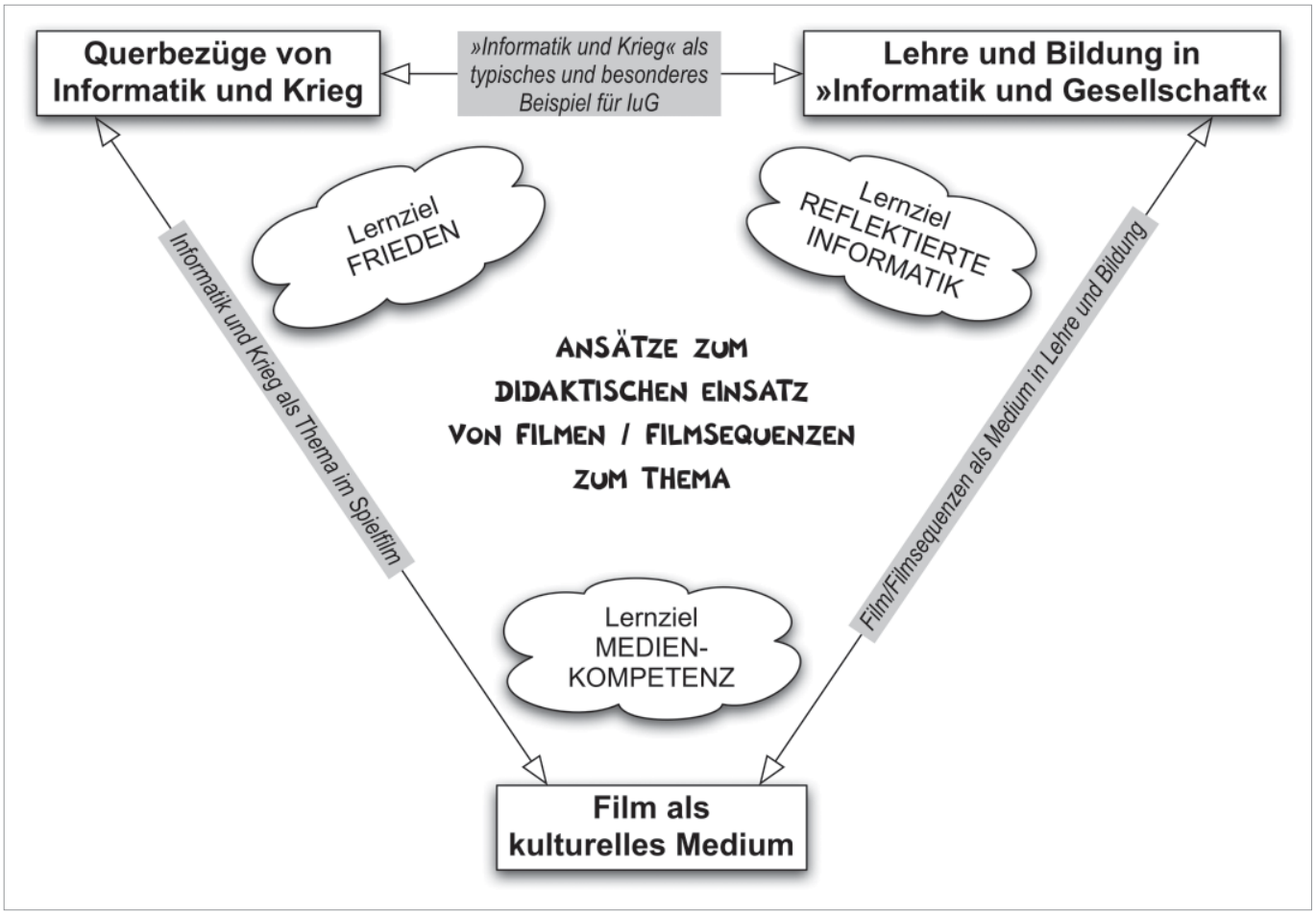


Abb.1: Grundlegende Zusammenhänge und Lernzielbereiche

tik und Krieg«, das eingesetzte Medium »Film« und die jeweils spezifische Lehr-/Lernsituation in »Informatik und Gesellschaft« zueinander in Verbindung stehen. Ich sehe es durch einen variationsreichen und methodisch durchdachten Einsatz von Filmsequenzen zur Ergänzung traditioneller Vermittlungsmethoden als sehr gut möglich an, mehrere unterschiedliche Lernziele zu verbinden:

Klar im Vordergrund steht das große Ziel aus *Informatik und Gesellschaft*, einen reflektierten, fragenden und hinterfragenden Umgang mit Anwendungen und Auswirkungen der Informatik anzuregen und auszubauen. Dies soll auf möglichst konkrete Weise geschehen. Sicherlich sind hier Filmsequenzen kein Allzweckmittel. Doch ich bin durch eine ganze Reihe von Erfahrungen davon überzeugt, dass sie in vielfältiger Weise hilfreich und wirksam eingesetzt werden können.

Ein bewußter Umgang mit dem Medium Film, der immer wieder auch auf einer Metaebene selbst thematisiert wird, erhöht die Medienkompetenz und führt zu anderen Seh-Gewohnheiten.

Die inhaltliche Auseinandersetzung mit der politischen Seite von Krieg und Frieden schließlich kann, darf und soll dazu beitragen, dass auch auf Ebene grundlegender Werthaltungen eine Abwägung und Weiterentwicklung stattfindet, die hoffentlich dazu führt, Frieden, Gerechtigkeit, Humanität etc. nachhaltig ins Zentrum der eigenen Aufmerksamkeit zu nehmen und dafür einzutreten.

Ich danke den Teilnehmerinnen und Teilnehmern dieser Arbeitsgruppe für ihr engagiertes Mitwirken und die auch für mich sehr anregende Diskussion.

Literatur:

Bergala, A. (2006): Kino als Kunst. Filmvermittlung an der Schule und anderswo. Bonn: Bundeszentrale für politische Bildung.

Bürger, P. (2005): Kino der Angst. Terror, Krieg und Staatskunst aus Hollywood. Stuttgart: Schmetterling.

Krebs, S. (2009): Über die (Co-)Konstruktion der Militärrobotik aus Wissenschaft und Fiktion. In: FIfF-Kommunikation, 26 (1).

Christopher Kullenberg

The social impact of IT:
Surveillance and resistance in present day conflicts

How can activists and engineers work together?

Since the 9/11 attacks the world has been challenged with intrusive legislation upon civil liberties and increased use of surveillance technologies. As this development is proceeding rapidly, both from a legal point of view and a technological side, it takes more than parliamentary politics to pursue a democratic and open discussion about these matters. This is where the civil society, or rather the civil societies, need to collaborate. Thus, I will propose that engineers, software-programmers and people in the private sector of Information Technology could co-operate with activists, human-rights organisations and citizen-journalists in a very productive manner. I will also give concrete examples on how such activities have been pursued in Sweden during a controversy on the role of signals intelligence.

Surveillance and War

Issues that keep arising in the backwaters of the "wars" on terrorism, drugs, and trafficking are often complex and require technical and legal expertise, not only to be understood, but more importantly, to be taken seriously in the public debate and by the media. In order to avoid that laws are passed without a proper debate or that technologies are implemented as merely technical solutions, I will propose that criticism could have a positive task in building a collaborative informational infrastructure, an effective media strategy, and other innovations.

Let me give an example from Sweden. During 2008 a law was passed, which allowed the government to pursue extensive signals intelligence on the Internet. It was termed the "FRA-law" in the press, since the authority responsible for signals intelligence is called Försvarets Radioanstalt [1], which is the equivalent to the NSA in the United States, or the BND in Germany.

The FRA was previously only allowed to search and intercept radio traffic, but this new law would allow the authority to intercept all Internet traffic, by monitoring so called "co-operation points" at the Internet Service Providers. By copying all the information passing through the cables, the FRA will be able to extract traffic-data from the multitude of data, both domestic and international. Consequently, a mode of operation which was developed in the context of the post-war arms race, will be transferred to the Internet as this law is effectuated during 2009. However, the Internet is largely used by private and corporate communication, rather than military information, a fact that arises questions concerning privacy, integrity and the rights to private communication.

I will argue that if it were not for the active formation of a public, this law would have been passed without resistance or criticism. In order to understand how this works, the notion of a "public" is borrowed from the philosopher John Dewey, where he explicitly stresses the importance of communication: "But participation in activities and sharing in results are additive concerns. They demand communication as a prerequisite. /…/ Communication of the results of social inquiry is the same thing as the formation of public opinion." [2]

Crucial to the formation of a participatory public issue, and to allow it to build political pressure, is the free flow of information in the sense that it operates without restrictions, something which is very different compared to traditional theories of mass-communication. This is where the Internet has a very interesting potential since its architecture, at least ideally, promotes participation, sharing and communication, which is precisely what Dewey is asking for. However, it seems that this free flow can not be guaranteed by the Internet alone, since the same abilities can be used for intrusive surveillance.

Panspectric surveillance

How are we then to conceive of contemporary technologies of surveillance? One way is to ask how technologies are used throughout society, by analysing their performances and abilities in socio-technical assemblages.

Digital technologies, besides sharing certain properties in hardware such as microprocessors, electricity-based operations and abilities to process instructions and algorithms, usually share many networked, or social effects. The Internet as an assemblage of computers, routers, switches and all kinds of IP-based technologies, such as mobile devices and satellites, shapes emergent forms of effectuation. For example file-sharing, voice-transmission, e-mails etc. are all dependent on interconnectivity. Also, they operate on the potentiality of decentralisation and read-write capacities, and to be able to transfer the analogue world to a digital realm, which we see in the digitalisation of images, sounds, and even in the keystrokes of a keyboard.

There is however a critical paradox built into our mundane technologies. We may use digital cameras on our holiday trips and post the images on a blog, but we may also use the same capacities for an IP-based surveillance camera. The present day technologies are thus at the same time what may liberate sounds, texts, images and videos from their "material imprisonment" and geographical spatiality, while they simultaneously make possible for what is called panspectric surveillance [3].

The concept of panspectrocism comes from philosopher Manuel DeLanda, who situates the origin of these technologies in war. It is worthwhile to quote from his work War in The Age of Intelligent Machines (1991) in length: "There are many differences between the Panopticon and the Panspectron /…/ Instead of positioning some human bodies around a central sensor, a multiplicity of sensors is deployed around all bodies: its antenna farms, spy satellites and cable-traffic intercepts feed into its computers all the information that can be gathered. This is then processed through a series of "filters" or key-word watch lists. The Panspectron does not merely select certain bodies and certain (visual) data about them. Rather, it compiles information about all at the same time, using computers to select the segments of data relevant to its surveillance tasks [4]."

DeLanda thus argues that the technologies we face in contemporary debates on Internet surveillance, originate in a post-war setting which culminated during the cold war. Signals intelligence was born in a combination of radio interception, transferring analogue signals to digital information, and computers which calculated patterns, attached meta-data, and filtered out only the relevant pieces of information in a multiplicity of signals.

The birth of the panspectric technological framework, at least in an abstract sense, thus came from warfare. However, it was developed and refined during times when consumer technologies were not yet digital, and usually not even made for two-way communication (TV, press, radio).

What we see today is a complete change of orders. Signals intelligence performed by governments, such as the NSA, the FRA or the BND have entered a territory populated by ordinary citizens, rather than tanks, spy-satellites and nuclear weapons.

Contemporary panspectric surveillance depends on the interconnectedness of sensors and computational methods such as data mining, sociograms and databases. Sensors include RFID-chips, digital CCTV-cameras, credit cards, mobile phones, internet surveillance etc., and they all have the ability to record an ever increasing part of our everyday lives. This is where we get close to the etymology of the words pan-, which means everything, and spectrum which is the entire range of detectable traces. The radical digitalisation of our societal functions and everyday lives, reconfigure and prolong the range of surveillance. However, to make sense of this enormous abundance of data, methods of reducing complexity and finding relevant traces are needed. This is where the other pole of panspectrocism emerges; the need for super-computers and advanced software and statistics.

The FRA has bought one of the fastest super-computers in the world, and it is plugged directly into the central fibre-cables of the Swedish Internet Service Providers. They will consequently receive a copy of all traffic-data, and then process it in several steps in order to find patterns. The problem is however, that traffic-data (which contains information about with whom, at what time, how frequently etc. that we communicate) can say a great deal about you and your life. If we make social network analyses of the meta-data you give off during a normal day, the surveyor can probably find out who most of your friends are, and where you are most likely to be located. With more and more data, the surveyor is able to tell your religion, sexuality, political affiliation and consumer behaviour.

Citizen journalism, pirate parties and activists

We can make a tripartite division of activities that may challenge the increasing use of legal and technological means of mass surveillance; citizen journalism, pirate parties and activism. They may sometimes resonate in the same direction, towards a clear goal, but their basic properties and relations are essentially heterogeneous.

Issues, such as the FRA-law, can only stir up reactions and become "issues proper" if, following Dewey, there is communication between actors allowing them to react to what is imposed on them. It has been said that the case of the FRA-law was the first time in Swedish history that traditional newspapers lagged the blogosphere, and for the centre-conservative government the force of citizen journalism came as quite a surprise.

The blogosphere displayed a few interesting abilities by co-operating and sharing knowledge. One important aspect of raising issues, needed to be accounted for in this case, is speed. Paul Virilio argues in his book Speed and Politics, that: "If speed thus appears as the essential fall out of styles of conflicts and cataclysms, the current 'arms race' is in fact only 'the arming of the race' toward the end of the world as a distance, in other words as a field of action." [5]

Speed turns distance into action, and the speed of citizen journalism has a higher velocity than the traditional media, being dependent on printing presses, paid and professional journalists, or hierarchical organisations. During the passing of the FRA-law, the only ones being able to read legal documents, do proper research, and have a constructive discussion, were bloggers. In this case (and I do not want to generalise this observation to be valid for „the media" in general) we may say that the allocation of resources were much more efficient than those of large media corporations.

The critical task for the blogosphere in making a successful attempt at stopping this law is knowledge production. Surveillance technologies and intrusive legislations are complex matters which are often secretive in character. Signals intelligence is maybe an extreme case, since details about methods and search criteria is necessarily kept away from the public.

The first step in the case of the FRA was ontopolitical, in the sense that there was (and still is) a struggle to define whether signals intelligence is mass-surveillance, which would be a disaster for integrity, or simply a means to target very few „enemies of society" (terrorists). Bloggers analysed legal documents and government white papers, as a kind of swarm intelligence, and could argue convincingly that entailed many legal exceptions for the FRA in registering political opinions, sexual orientation or religious background. The counter-argument from advocates of the law did not convince the bloggers, and the traditional media started covering the issue extensively. During the summer of 2008 there were articles in the newspaper almost every day for months and many bloggers wrote extensively in both arenas.

From a technical point of view, the struggle was indeed one of definitions. It can be summarised in the question „How does the Internet really work?". I may sound simple, but the understanding of the nature of technologies, may be perceived of in many different ways. The legal documents in many ways still regard data transfers in cables as if they were basically the same as the aether waves that once gave birth to signals intelligence. Also, the advocates of the law stated that the FRA would not read the e-mails of ordinary citizens, and that it would be impossible to store all information that passed the fibre cables on the net. This may be true or not, but it displaces the question of mass-surveillance by only considering content-data, rather than the more intrusive kind of traffic-data [6], which the FRA has unlimited access to in practice [7].

Thus, in order to arrive at a citizen journalism which is able to form a strong public around an issue, both legal and technical expertise is needed, alongside social scientific and historical insights. If this is conveyed in a medium that is faster than traditional media, there is a chance of converting distance into action and make politics. Its effects on parliamentary legislation is however yet to be evaluated.

How an engineer can be an activist, and activist can be technical?

In digital rights there is a special dilemma in the relationship between legislation and technological systems. As technological innovations carry with them new social relations, make new communicational flows possible, and sometimes disrupt legislation [8] forcefully, I would argue that we need more than a "legalist approach" in understanding our contemporary situation.

The legalist approach to technological regulation may be understood as an idealist position, where we grant the rights and obligations to certain actors. For example file-sharing of copyrighted material is illegal in most countries, and we usually try to prevent the police, the homeland security agencies and several other governmental bodies to take away or override civil liberties. The legalist approach is thus a vision of rules that need to be obeyed. However, this approach is very limited in scope, and may work in a faulty manner as we try to open up the conflicts and constellations inherent to surveillance.

The other position we may call a performative approach, or along the reasoning of Rasmus Fleischer [9], a materialist way of understanding what technologies do in our everyday lives. Instead of asking what you are allowed to do with technologies, the performative perspective asks for what human-technologial assemblages are able to do. You are not allowed to share copyrighted material, but a computer and an internet connection makes you able to do it, and this is why a substantive amount of the national internet traffic in Sweden consists of precisely these kind of files.

Anti-surveillance demonstration, 2008
(Photo by Andreas Käiväräinen)

With surveillance, we are running the risk that the surveyor may actually be doing what the harmless "pirate" is doing to copyrighted music or video. If there are systems enabling mass surveillance, we may similarly replace the violation of copyright into the violation of human rights. As mentioned earlier, we give the FRA the technological abilities to record all traffic data on the Internet, but not necessarily the legal means to use them freely.

No matter what you views are on file-sharing, we may still conclude that the Internet is changing the way we consume, share and even produce music. The disruption comes from technology, rather than a legalist process constructed in alignment with certain rights and duties. The materialist approach instructs us to regard such phenomenon from parameters of technological analysis; The increase in bandwidth, storage capacity and the interconnected structure of the Internet enables simultaneously the massive flows of information and the tremendous, and necessary, generation of traffic-data. This data is however the core of panspectric surveillance.

Christopher Kullenberg

Christopher Kullenberg is a PhD-candidate in Theory of Science at University of Gothenburg. His main research concerns the co-production of the social sciences and social change. He is also writing frequently on the role of surveillance and social order, and is the editor of the Resistance Studies Magazine, rsmag.org. (christopher.kullenberg@gmail.com)

To conclude, we may say that securing legal rights does not suffice, but digital activism must necessarily be technical in character. It must affirm a materialist vision, which follows the flows of technologically enabled potentialities throughout society, and thus pushes the traditional front line of the legalist approach even further forwards, to where it hinges on the same level as the innovation, implementation and development of technological systems.

Engineers posses a certain kind of expertise, not only in their particular field, but in a more general way as it comes to understanding technological systems and their potentialities. French sociologist Michel Callon proposed in a 1986 article [10] that engineers were actually better sociologists than sociologists themselves, since the constructions and inventions of technological systems required a social analysis equal to the technical. Without knowing how to analyse social relations, you can not change them and configure them according to you innovations.

However, there is a common view among certain engineers that their tasks do not stretch beyond finding mere technical solutions to particular problems. They distinguish between a technical problem and a social or legal one, and I must thus argue that such a conception is counter-productive.

Let me summarise the consequences in a few general sentences:

1. Activism and public debate must take place at the deployment of technological systems before they become mundane or their social disruption is forgotten in history.

2. Engineers, lawyers, activists and users can contribute to an open and critical debate if they co-operate, and may resolve issues on integrity on a practical level (e.g. encryption software, routing of messages et. cetera) when forming heterogeneous constellations.

3. A performative approach may ensure civil liberties in a more rigorous fashion than a legalist understanding.

The Internet(s) – democratic spaces or mine fields for panspectric surveillance?

As there seems to be a general tendency towards more surveillance, not only in the EU member states but globally, it is easy to become absorbed with pessimism. Shaping publics does not seem to be enough, and turns into a democratic dilemma, especially in places where civil society is less likely to assemble. Technological activism, such as encryption and routing, may be effective, but could also be accused of denying the idea of a collective social and legal project.

I have argued not only that such an opposition is unproductive, but also that it is analytically false in its division of social and technological phenomenon. An issue may be formed around rights and parliamentary processes in the same fashion as it takes an encryption protocol or a piece of hardware as its object. This "hacker attitude" [11] towards the politics of emerging technologies is maybe best expressed in the works of the French activist group *La Quadrature du Net*, who argue [12] that law is code, and if there are errors in it, activists should start "patching" them, instead of merely protesting towards them.

As all of these processes more or less take place on the Internet, simultaneously as they are *about* the Internet, the expression of "reclaiming the streets" seems quite obsolete. Instead we should maybe say that reclaiming the cables, routers and lines of code would be the crucial task for a vibrant politics of the Internet(s).

References

1 The official name in English is the National Defence Radio Establishment (see www.fra.se).

2 Dewey, John (1998) The Essential Dewey: Volume 1: Pragmatism, Education, Democracy, Indiana University Press, p. 296, 304

3 See www.panspectrocism.org

4 DeLanda, Manuel (1991) War in the Age of Intelligent Machines, New York: Zone, p. 206

5 Virilio, Paul (2006) Speed and politics. Los Angeles; Semiotext(e), 152, italics in original.

6 This was uncovered in the largest Swedish daily Dagens Nyheter on September 3rd 2008. An English translation is availible at: klamberg.blogspot.com/2008/10/fra-law-sleepwalking-into-surveillance.html

7 As of early 2009 the original law which was passed in June 2008 is effective. However, there is currently a proposal to add special courts to increase control on the FRA. The role of the traffic-data is still not altered, and the FRA will start connecting physically to the Internet Service Providers in October 2009.

8 Klang, Mathias (2006) Disruptive Technology: Effects of Technology Regulation on Democracy, Doctoral Dissertation, University of Göteborg.

9 Fleischer, Rasmus (2008) "En lektion i nätpolitik", Svenska Dagbladet, 2008-09-16.

10 Callon, Michel (1987) „Society in the Making: The Study of Technology as a Tool for Sociological Analysis." Pp. 83-103 in The Social Construction of Technical Systems: New Directions in the Sociology and History of Technology, edited by W. E. Bijker et. al. London: MIT Press.

11 See also: Palmås, Karl & von Busch, Otto (2006) Abstract Hacktivism – The Making of a Hacker Culture, London: Mute Publishing Ltd.

12 Zimmermann, Jérémy (2008) Presentation at the 25C3 congress in Berlin, 2008-12-30.

Marie–Theres Tinnefeld

9/11 – ein schwarzer Tag für die Menschenrechte?

Gedanken über die Rolle der Medien in Zeiten des Terrors

Die Terroranschläge vom 11. September 2001 haben die Welt verändert. Sie haben Kriege ausgelöst und zu Antiterrorgesetzen geführt, die schwere Menschenrechtsverletzungen zur Folge haben. Rechtsstaaten mutieren zu Präventionsstaaten und betreiben die Zerstörung dessen, was sie ausmachen. Der Beitrag befasst sich vor allem auch mit der Rolle der Medien, wie sie in Zeiten des Terrors Menschenrechte verteidigen, aber auch „verderben".

I.

Der 11. September 2001 war ein schwarzer Tag für die Menschenrechte. Die verheerenden Terroranschläge an diesem Tag haben bis heute nicht nur eine Gewaltwelle ausgelöst, die weltweit zu Krieg und Folter führten und führen. Die Gesetzgeber in den USA und in Europa haben seitdem Antiterrorgesetze und sicherheitspolitische Aktionen beschlossen, wonach Menschenwürde und Freiheitsrechte, Datenschutz und Unschuldsvermutung ihren hohen Rang mehr und mehr einbüßen. Seitdem herrscht Angst unter den Bürgern. Auf der Suche nach mehr Sicherheit mutiert die Zivilgesellschaft zu einer Überwachungsgesellschaft. „Post 9/11, everyone watches and is being watched…" (Jonathan Raban: 2008). Menschenrechte stehen im Verdacht, der Sicherheit vor dem Terror im Wege zu stehen. Das politische Klima hat sich grundlegend geändert und mit ihm die Berichterstattung in den Medien.

II.

Medien und damit auch Medienmacher haben die Ereignisse von am 11. September und weitere Terroranschläge immer wieder in Endlosschleifen im Fernsehen gezeigt. Welchen Effekt hat die Dauerwiederholung der Bilder auf die Zuschauer? Werden dadurch die schrecklichen Ereignisse besser verarbeitet oder eskaliert die Angst der Bürgerinnen und Bürger vor einer permanenten Terrorgefahr? Helfen digitale Medien der Politik, alle Freiheitsrechte zugunsten einer vermeintlichen Sicherheit zu dominieren? Sind sie mitverantwortlich für den „war on terror"?

Der Architekt und Designer Stefan Doesinger (Virtual Home, 2008) zeigt, was Computerspiele im Second Life bewirken können, nämlich einen schleichenden Umkehrprozess. Er lässt sich auf digitale Medienbilder in Zeiten des Terrors übertragen: Die Zuschauer sind permanent konfrontiert mit der Realität und ihren endlosen medialen Abbildern, die sich wechselseitig rückspiegeln. Der Vorgang erinnert an einen Kommentar von Walter Benjamin aus dem Jahr 1929:

„Blicken zwei Spiegel einander an, dann spielt der Satan sein liebstes Spiel und öffnet die Perspektive ins Unendliche."

Im Spannungsfeld zwischen den beiden Spiegeln entsteht ein neues Bewusstsein: hier die hilflose Ausgeliefertheit der Bürgerinnen und Bürger an Terrorakte nach 9/11. Sicherheit bedeutet nicht länger eine ausbalancierte Freiheit aller. Die Abwesenheit garantierter Freiheitsrechte ist zur Anwesenheit, zur Normalität geworden. Die USA und europäische Staaten haben begonnen, sich auf den Bewusstseinswandel einzustellen, insbesondere durch eine Hinwendung zum präventiven Handeln. Prävention als vorherrschende Logik öffnet der Sicherheitspolitik alle Tore, um verfassungsrechtlich bedenkliche Antiterrorgesetze und Maßnahmen zu verabschieden. Dazu gehören Gesetze zur Vorratssammlung von TK-Verkehrsdaten, das PNR-Abkommen zur Vorratssammlung von Flugpassagierdaten, die Erlaubnis zur präventiven Rasterfahndung, die heimliche Durchsuchung privater Computer vor Begehung einer Straftat durch das BKA und vieles mehr. Dazu gehören auch jene automatisierten Datenabgleichverfahren, die zu einer ungerechtfertigten Verdächtigung unbescholtener Personen führen können – wobei sich die rechtsstaatliche Unschuldvermutung derart in eine Schuldvermutung verkehrt, dass nun die Ausgefilterten sich gegenüber den Ermittlungsbehörden rechtfertigen müssen.

Die präventiven Eingriffe haben nicht zuletzt auch gravierende Auswirkungen auf die Medienfreiheit, vor allem durch die Gefährdung des Informantenschutzes. Besondere Vorkehrungen

Marie–Theres Tinnefeld

Prof. Dr. Marie-Theres Tinnefeld ist Juristin und Publizistin mit Schwerpunkt Datenschutz- und Wirtschaftsrecht. Sie ist Mitglied im wissenschaftlichen Beirat des FIfF.

zum Schutz der Pressefreiheit sind in den Gesetzen nicht vorgesehen, obwohl die Geheimhaltung aller Informationsquellen und das Vertrauensverhältnis zwischen den Medien und ihren Informanten grundlegend für die Medienfreiheit sind.

III.

Die Medien sind Teil der Antiterrormaßnahmen und des „war on terror" und als solche sowohl Täter als auch Opfer. Nach 9/11 wurde etwa in den USA ein ungeheuerer Konformitätsdruck aufgebaut, den unangepasste Journalisten besonders zu spüren bekamen (Neuber, 2002).In der Folge verloren diejenigen ihren Job, die sich nicht beugten und dem Mechanismus moderner Kriegspropaganda nicht folgten. Die wachsende Zensur zeigte sich unter anderem bereits bei der „Operation Wüstensturm" im ersten Golfkrieg, wo nur die vom Militär zugelassene Sichtweise in der Öffentlichkeitsarbeit erlaubt war, mithin auch der Versuch unternommen wurde, Medien konform zu schalten und zu zensieren. Erst kürzlich hat der israelische Schriftsteller Tom Segev das halbwahre Bild kritisiert, dass die Medien zu Beginn des Krieges über das Ausmaß der Attacken der terroristischen Hamas auf Israel zeichneten (Jediot Achronot: Eine halbe Million Israelis unter Feuer, SZ. v. 31.12.08, 2).

Medien werden sowohl von Regierenden als auch von den Drahtziehern der Terrornetzwerke als Mittel der Kriegsführung betrachtet. Nicht nur der satirische Film „Wag the Dog" gibt eine Vorstellung von den Potenzialen mediengesteuerter Politik. Auch die Form der Berichterstattung nach 9/11 gibt Auskunft darüber, wie der „war on terror" etwa im Irak medial (mit)inszeniert wurde.

Mit geschönten Nachrichten haben Regierungen schon immer für die Unterstützung ihrer Feldzüge geworben. Aus diesem Grund verabschiedeten die Vereinten Nationen 1948 die Allgemeine Erklärung der Menschenrechte, die die Freiheit der Medien und das Recht des freien Zugriffs auf Informationen (Informationsfreiheit) absichert (vgl. auch die Europäische Konvention der Menschenrechte und die fast wortgleiche EU-Grundrechte-Charta).

Art. 19 Abs. 2 UNO-Pakt II lautet: "(...) Jedermann hat das Recht auf freie Meinungsäußerung; dieses Recht schließt die Freiheit ein, ohne Rücksicht auf Staatsgrenzen Informationen und Gedankengut jeder Art in Wort, Schrift oder Druck, durch Kunstwerke oder andere Mittel eigner Wahl sich zu beschaffen, zu empfangen und weiterzugeben. (...)"

IV.

Wo Meinungen unterbunden werden, gibt es keine sachlichen, wahrheitsgemäßen Informationen mehr, sondern nur noch Propaganda. Wo Prävention zur vorherrschenden Logik wird, sind die Menschenrechte, vor allem Informationsfreiheit und Datenschutz in Gefahr. Die Mitverantwortung und Mitgestaltung des Bürgers am politischen Geschehen versandet.

Wenn die Entblößung des Menschlichen, der Privatheit im Interesse einer vermeintlichen Sicherheit auch rechtlich zulässig wird, dann schwindet der Persönlichkeitsschutz. Wenn Menschen außerdem befürchten müssen, dass ihnen aus ihrer Meinungsäußerung Nachteile erwachsen können, selbst wenn es sich nur um die Notwendigkeit ihrer Rechtfertigung handelt, dann werden sie die Äußerungen häufig unterlassen. In einem Klima mit derartigen Befürchtungen, wird eine beschränkende Wirkung auf die Meinungsfreiheit ausgeübt. Sie wird in der amerikanischen Verfassungsrechtsprechung zutreffend als „chilling effect", als vereisende Wirkung bezeichnet.

Die Demokratie ist auf Meinungsfreiheit, verlässliche Informationen bzw. publizistische Leistungen angewiesen. Die Medien üben als *public watchdog* eine Funktion aus, die eine ausreichende Distanz zu den Kräften und Mächten voraussetzt, die sie kontrollieren sollen. Eine wirksame Medien-Selbstkontrolle ist allerdings auf Standesregeln angewiesen, welche die wirklichen Konflikte aufgreifen, die in der Routine der journalistischen Arbeit beachtet werden müssen: Zum Pflichtenkatalog gehören u.a. Wahrhaftigkeit und Aktualität, Unbestechlichkeit, Respektierung der Intimsphäre. Der Deutsche Presserat erinnert immer wieder an die „Einhaltung der publizistischen Grundsätze", wie sie etwa im Pressekodex festgehalten sind. Trotz der „verständlichen emotionalen Betroffenheit dürfe die Berichterstattung in Wort und Bild ihre professionelle kritische Distanz nicht verlieren". Das heißt vor dem Hintergrund grundrechtlich garantierten Meinungs- und Informationsfreiheit, dass die Medien Feindbildern keinen Vorschub leisten dürfen. Ein, wie es scheint, klarer Satz. Und doch ist er nur Druckerschwärze, wenn er nicht angewendet wird.

V.

Der Science-Fiction-Film *Minority Report* zeigt den anscheinend perfekten präventiven Sicherheitsstaat in Verbindung mit einer propagandageladenen, manipulierten Öffentlichkeitsarbeit. Washington D.C., wo das Szenario im Jahre 2054 spielt, ist zwar fern, aber auch wieder nah: In der Stadt finden sich an allen öffentlichen Plätzen Überwachungskameras, die jede Person per Augen-Scan für die Sicherheitsbehörden identifizieren. Mobile Überwachungsdrohnen, sogenannte *Spyder* (ein Neologismus, der sich aus *spy* und *spider* zusammensetzt) werden bei der Verbrechensbekämpfung eingesetzt. Jeder, der sich ihrem Netzhaut-Scan entzieht, wird durch Elektroschock gelähmt und verhaftet. Die Gedanken- bzw. Sicherheitspolizei (*pre-crime*) handelt nach dem Profiling, der Verbrechensvorhersage von sogenannten *pre-cogs*. Sie unterbindet nicht konkrete, sondern sich abstrakt abzeichnende Gewalttaten; sie verhaftet potentielle Täter und sperrt sie auf immer weg.

Das trostlose, technisch abgesicherte Präventionskonzept vernichtet private Freiräume; es gibt kein verantwortliches Handeln des Einzelnen mehr. Klassische Rechtskategorien wie die Unschuldsvermutung sind ohne Belang. Die Berichterstattung ist manipuliert: Der Sicherheitschef bedient sich eines *Office for Strategic Influence*, das gezielt falsche Informationen in Umlauf bringt und abweichende Voraussagen der Hauptseherin (*minority report*) verheimlicht. Die Präventionsparanoia ist maßlos. Nachdem die Ursache des Übels, ein Mord und die falschen Informationen des Sicherheitschefs durch das Auffinden des Minoritätsberichts aufgedeckt worden sind, ist die Präventivdiktatur und die nationale Infrastruktur der Überwachung erledigt.

VI.

Der „Ewige Friede“, den Immanuel Kant entworfen hat, ist nicht der Frieden auf dem „Kirchhof der Freiheit“. Präventions-, Kriegskonzepte sowie Massenmedien, die den Terror dramatisieren, schaffen unkontrollierbare Risiken (Beck, 2007). Sie unterstützen die politischen Drahtzieher des Terrors und gefährden den freiheitlichen Rechtsstaat (Tinnefeld/Knieper , 2008). Bereits in „Jenseits von Gut und Böse“, dem Vorspiel einer Philosophie der Zukunft, warnt Friedrich Wilhelm Nietzsche vor den Gefahren sich verselbständigender Bilder: „Wer mit Ungeheuern kämpft, mag zusehen, dass er nicht dabei zum Ungeheuer wird. Wenn du lange in einen Abgrund blickst, blickt der Abgrund auch in dich hinein.“

Literatur:

Beck, Ullrich (2007): Weltrisikogesellschaft.

Benjamin, Walter (1989): Pariser Passagen, 1929. In: Rolf Tiedemann (hrsg.): Gesammelte Schriften, Suhrkamp, Bd. 5.

Doesinger, Stephan (2007): Learning from Sim City.

Doesinger, Stephan (2008): Virtually Home.

Raban, Jonathan (2007): Surveillance. London.

Neuber, Harald (2002): Erstes Opfer: Pressefreiheit. In: Palm, Goedart und Rötzer, Florian (hrsg.): Medien Terror Krieg. Telepolis 125—139.

Tinnefeld, Marie-Theres und Knieper, Thomas (2008): Menschenrechte im Spiegel des Präventionsstaates. In: Schweighofer, Erich et al. (hrsg.): Tagungsband des 11. Internationalen Rechtsinformatik Symposions Iris. 557-565.

Ilona Koglin und Marek Rohde

Net Activism

Neue IT-Entwicklungen dienen nicht nur fragwürdigen Zwecken, beispielsweise militärische Anwendungen. Sie geben Millionen Menschen weltweit die Möglichkeit, sich für Frieden und Menschenrechte einzusetzen. Das beste Beispiel ist das Internet: Zunächst für das Militär entwickelt, ist es heute ein regelrechter Humus für Engagierte weltweit. Unternehmen Sie mit uns eine kleine Reise durch die Kontinente dieser Welt und entdecken Sie, wie viele Menschen neue Kommunikationstechnologien für eine bessere Welt einsetzen.

Ein Blick in die Zeitung, das Fernsehen oder das Internet mag einen verzweifeln lassen: Fast 1,34 Billionen US Dollar – also rund 860 Milliarden Euro – wurden 2007 weltweit für Waffen und Millitär ausgegeben. Das sind etwa 3,4 Prozent mehr als noch in 2006. Die USA führen diese Liste der Millitär-Investoren bekanntermaßen an, und zwar mit zirka 547 Mrd. US Dollar (rund 351 Mrd. Euro) in 2007.

Wie viel könnte gewonnen werden, würde man dieses Geld den Armen dieser Welt geben? Dann bekäme jeder der geschätzten eine Milliarden Menschen, die derzeit in unserer Welt hungern und unterernährt sind, in etwa 860 Euro. Wie viel Frieden und Gerechtigkeit sich damit wohl erreichen ließe?

Doch derlei Überlegungen scheinen müßig. Wer ein bisschen Erfahrung im Einsatz für Frieden und Gerechtigkeit hat, der weiß: Jede Errungenschaft muss mühsam erfochten werden. Dabei gleicht der Weg nicht selten einem Wettlauf. Neue Entwicklungen – etwa die in den Bereichen der IT, der Gen- oder Nanotechnologie – sorgen für neue Fragen. Wie werden sie sich auf unsere Umwelt auswirken? Und wie auf unsere Gesellschaft – Stichwort Datenschutz und digitale Überwachung? Dass der Weg mühsam und langwierig ist, sollte uns jedoch nicht verzagen oder gar verzweifeln lassen. Denn neue Technologien mögen zwar auf der einen Seite bedrohlich erscheinen – sie bieten aber auf der anderen Seite oft auch neue Möglichkeiten und Chancen für eine bessere Welt.

Eine militärische Innovation für mehr Demokratie

Das Internet ist wohl eines der Paradebeispiele, wenn es darum geht, die positiven Auswirkungen einer ursprünglich für das Militär entwickelten Technologie zu zeigen. Mit einer Geschwindigkeit, die noch vor zehn Jahren wohl viele nicht für möglich gehalten hätten, hat das digitale Netzwerk Menschen rund um die Erde miteinander verbunden. Sicher, das World Wide Web hat eine Reihe von negativen Auswirkungen mit sich gebracht:

Medien bedienen sich bei Netzaktivisten

“[…] Israel hat ausländischen Journalisten den Zugang zum Gaza-Streifen verboten. Die Quellenlage werde immer schwieriger, […] In dieser Situation gehen aber auch die Sender auf Quellensuche im Internet. Und da werden sie auch fündig: Die „Tagesthemen“ brachten am Sonntag einen Bericht über die zunehmende Bedeutung der Blogs. Diese Darstellungen des Kriegsgeschehens sind selbstredend total subjektiv – aber sie bieten allemal eine andere Sicht auf das Grauen als die „sauberen“, von Opfern als „Casualties“ redenden Berichte der Militärs.”

Quelle: Daland Segler, “Mit Fernsteuerung — Israel lässt keine Journalisten nach Gaza: Wie TV-Sender mit ihren Quellen umgehen”. Frankfurter Rundschau, Nr. 4, 06.01.2009, S. 33

www.tagesschau.de/multimedia/sendung/tt1068.html (06.01.2009)
blog.tagesschau.de/?p=4733 (06.01.2009)

Die internationale Finanzkrise hätte ohne das Internet wohl nicht das derzeitige Ausmaß erreicht, der internationale Terrorismus vielleicht auch nicht.

Doch nur durch das Internet haben es die Menschen beispielsweise geschafft, dass nicht mehr nur einige wenige, klassische Medien die alleinige Meinungshoheit haben. Vielmehr können nun politische Fragen im Internet von vielen Menschen diskutiert werden. Eine Demokratisierung, die es ohne das weltweite Datennetz nicht gäbe.

Das derzeit sicherlich populärste Beispiel dafür ist der Wahlkampf von Barack Obama. Kein Politiker hat das so genannte Web 2.0 mit all seinen sozialen Plattformen – wie flickr, MySpace, Youtube oder twitter – so gekonnt für seine Kampagnen genutzt wie er. Eine Strategie, die ihm ein sagenhaftes Wahlkampfbudget von 600 Millionen US-Dollar einbrachte. Manch einer feiert daher schon die Demokratisierung des US-amerikanischen Präsidentschaftswahlkampfes.

Doch natürlich nutzen nicht nur Profis, wie die Wahlkampfstrategen Obamas, das Internet. Auch Aktivisten oder Bewegungen schaffen sich und ihren Anliegen mit Hilfe des Web ein Forum – und damit Wirkung. Die Facetten, Ausrichtungen und Spielarten sind mannigfach. Doch gibt es einige zentrale Aspekte, die das Internet – und vor allem das seit einigen Jahren wachsende Web 2.0 mit seinen sozialen Vernetzungen – zum Humus für ein neues, weltweites, soziales und politisches Engagement macht.

Das Internet – Geburtshelfer von Bewegungen

Kaum eine Bewegung ist so mit dem Internet verbunden, wie die der Kritiker einer neoliberalen Globalisierung. Eines ihrer wesentlichsten Kennzeichnen ist – neben der inhaltlichen Kritik – ihre Struktur- und Hierarchielosigkeit. Möglich macht dies das Internet, denn es bietet als wirkungsvolle Alternative netzartige Kooperation, Mobilisierung und Organisation. Gruppen, Organisationen und Aktivisten mit zum Teil recht unterschiedlichen Zielen, Vorstellungen und Aktionsformen können sich punktuell und spontan zusammen finden.

Dabei können sie dezentral so „organisiert" sein, dass sich die Mitglieder teilweise gar nicht unter einander kennen. Ein Beispiel dafür ist die internationale Bewegung des Pyings: „Wer eine Torte hat und eine Vision von einer besseren Welt, der ist Mitglied der *Biotic Baking Brigade*", meinte beispielsweise eine anonyme Aktivistin in einem Video-Interview. Die Biotic Baking Brigade ist eine der Pying-Gruppen, die hochrangigen Vertretern aus Politik und Wirtschaft zu offiziellen Anlässen Torten ins Gesicht wirft. Ihre Botschaft: Diese Vertreter sind auch nur Menschen. Menschen, die lächerlich gemacht werden können, gegen die irgend jemand etwas hat und deren Wirken deshalb hinterfragt werden sollte. Dass die Bewegung wieder „zu geschlagen" hat, erfahren die Mitglieder oft erst über das Internet – nämlich immer dann, wenn wieder eine neue Dokumentation des letzten „Anschlags" in Video-Portalen auftaucht.

So genannte virale Effekte sorgen dafür, dass die internationale Web-Community von solchen und anderen Aktionen erfährt: Schnell spricht sich dies über Blogs, Foren, Emails und andere Kommunikationswege herum. Jüngstes Beispiel dafür ist die gefakte New York Times des globalisierungskritischen Duos „The Yes Men": Kurz nach Obamas Sieg verteilten sie in Manhattan eine „Sonderausgabe" der renomierten Zeitung – allein, es handelte sich um eine täuschend echte Nachahmung. Ein Blick in die Zeitung selbst verriet, dass etwas nicht stimmen konnte: Da wurde das Ende des Irak-Kriegs verkündet, Exxon entschuldigte sich in einer fiktiven Anzeige für den Krieg um's Öl und ein anderer Artikel befasste sich mit einer Anklage Bushs wegen Hochverrats… Eine Aktion, die sich binnen Stunden per Web weltweit verbreitete.

Die Grundpfeiler des Net Activism

Bereits diese Beispiele zeigen eine weitere, entscheidende Chance, die das Web 2.0 bietet: die neue Generation des Mitmach-Nets liefert eine Fülle von in der Regel kostenlosen Instrumenten, mit denen jeder relativ einfach und ohne umfangreiche Kenntnisse Texte, Bilder und Filme – kurz Informationen – veröffentlichen kann. Das ist natürlich vor allem für die Länder von Bedeutung, in denen es keine freie Meinungsäußerung gibt: Die Opposition in Malaysia nutzte etwa den kostenlosen Web-Hosting-Service Tripod, um eine Gegenöffentlichkeit aufzubauen und so den unter zweifelhaften Bedingungen verurteilten, ehemaligen Premierminister Anwar Ibrahim zu befreien.

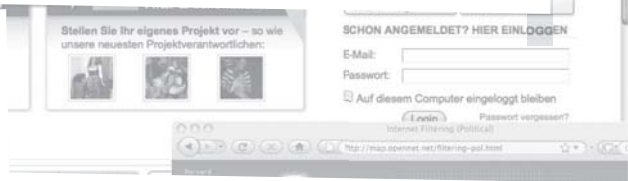
Das Web ist jedoch nicht nur ein Technik-, sondern ebenso ein Material- und Ideenpool. Dazu gehört auch die Kultur der Re-

Ilona Koglin und Marek Rohde

… arbeiten seit Jahren als freie Fachjournalisten für Print- und Online-Artikel rund um die Themenbereiche Gesellschaft, Kommunikation, Medien und Umwelt. Gemeinsam haben sie das Non-Profit-Project „Für eine bessere Welt" ins Leben gerufen, zu dem unter anderem der Weblog www.fuereinebesserewelt.info gehört. Mit diesem möchten sie Aktionen, Initiativen, Bewegungen und gemeinnützigen Organisationen ein Forum bieten und zeigen: Die Welt ist nicht so negativ, wie wir es in den klassischen Medien oft sehen oder hören. (ikoglin@grauwerte.com)

www.theyesmen.org: Kurz nach der Wahl Barak Obamas gab es kostenlose Ausgaben der New York Times. Erst ein Blick auf die Titelseite zeigte, dass hier etwas nicht stimmen kann – denn die erklärte den Irak-Krieg für beendet... Wie sich herausstellte, handelte es sich um eine täuschend echt gemachte Persiflage der renommierten Zeitung, initiiert von dem globalisierungskritischen Duo The Yes Men. Eine Nachricht, die sich im Internet innerhalb von Stunden rund um die Welt verbreitete.

www.opennet.net: Die Open Net Initiative dokumentiert Internet-Zensuren rund um die Erde. Hier zu sehen ist eine interaktive Karte der Staaten und Länder, die das Internet zensieren sowie weitere Zusatzinformationen.



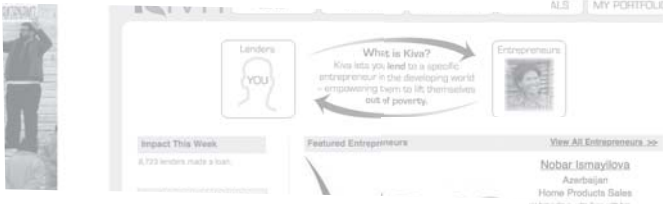
www.ushahidi.com: „Ushuahidi" ist Kisuaheli und bedeutet „Zeuge" – und genau darum ging es auf der gleichnamigen Plattform. Anfang 2008 konnten hier Kenianer Gewaltübergriffe im Anschluss an die Wahlen per SMS melden, die dann im Internet veröffentlicht wurden.

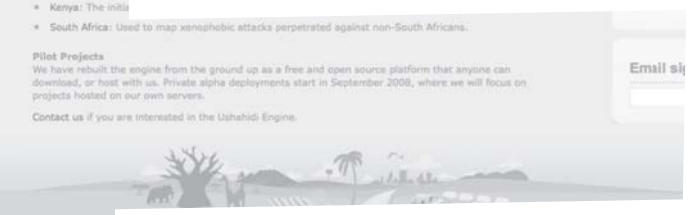
www.frontlinesms.com: FrontlineSMS ist ein Micro-Blogging-System spezielle für NGOs und Aktivisten: Diese können SMS-Nachrichten in Blogs veröffentlichen sowie an angeschlossene Mitglieder versenden.

www.kiva.org: Kiva ist eine internationale Mikro-Kredit-Plattform: Menschen können hier Kleinstkredite – meist an Frauen in so genannten Entwicklungsländern – vergeben und ihnen damit die Existenzgründung ermöglichen. Ein Beispiel dafür, wie das Internet Solidarität ohne Bürokratie ermöglicht.

de.betterplace.org: Die Plattform betterplace verbindet Engagierte weltweit. Mehr als 250 Projekte aus über 60 Ländern haben hierüber bereits Sach-, Geld- und Zeitspender aus Deutschland gefunden. Mitmachen kann jeder, derzeit sind bereits über Tausend Mitglieder registriert.

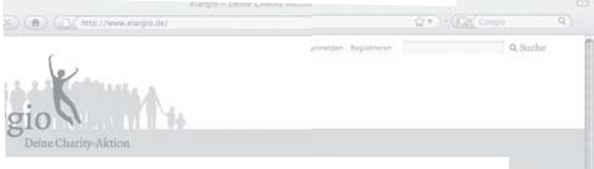
www.campact.de: Der Name der Aktionsplattform Campact setzt sich auch „Campaign" und „Action" zusammen und ist Programm: Über die Plattform werden nicht nur Themen und Argumentationen entwickelt, sie dient auch als Basis für Online- und Offline-Aktionen zu allen möglichen Themen von Umweltschutz bis soziale Gerechtigkeit.





www.elagio.de: Über die Plattform elargio kann jeder zum Fundraiser werden. Ob Geburtstagsparty, Marathonlauf oder Bücherflohmarkt – wer eine besondere Aktion startet, kann sie hier veröffentlichen. Besucher der Site können dann online spenden. Das Geld leitet elargio an die angeschlossenen, gemeinnützigen Vereine weiter.

www.ideenzutaten.org: „Ideen zu Taten" ist eine Community für Engagierte und Social Entrepreneurs. Hier kann man Ideen zu Projekten, Unternehmungen und Aktionen ausschreiben und Mitstreiter suchen – oder sich von Projektausschreibungen zu einem eigenen Engagement inspirieren lassen.



www.netzwirken.net: Wie bringt man engagierte Projekte und spendenwillige Unternehmen zusammen und sorgt dabei auch gleich noch für eine demokratische Verteilung des Budgets? Indem man die Ausschreibung öffentlich macht, wie Netzwirken dies tut. Immer zwei Initiativen treten gegen einander an, die Community stimmt über die Aufteilung ab, nach der eine von einem Unternehmen bereit gestellte Summe verteilt werden soll.

mixes: Tunesische Oppositionelle genauso wie amerikanische Obama-Anhänger verfremdeten beispielsweise einen Werbespot des Computerherstellers Apple. Er zeigt eine Szene aus „1984" – zu sehen war hier jedoch nicht der „große Bruder", sondern einerseits der tunesische Präsident Ben Ali und andererseits die damalige Obama-Konkurrentin Hillary Clinton. Auch wenn sich über den Geschmack des Vergleichs streiten lässt – mit derlei „professionellen" Spots bekommen „unprofessionelle" Aktivisten vollkommen neue Möglichkeiten. Lawrence Lessig – ehemaliger Autor des renommierten Magazins „Wired" und Mitbegründer der Creativ Commons-Bewegung für ein neues Urheberrecht – meinte anlässlich dieser Spots: „Der Remix … markiert einen Wendepunkt im politischen Diskurs, an dem Open Culture und Open Politics die Zentralisierung und Kontrolle der Medien und der Politik beenden".

Ein Video des tunesischen Aktivisten Sami zeigt zudem geradezu exemplarisch, dass das Internet auch neue Recherche-Möglichkeiten eröffnet: Über Plattformen von Hobby-Flugzeugbeobachtern, wie Airliners.net oder Planepictures.net, verfolgte er die Flugrouten des Präsidenten-Flugzeugs, fasste seine Ergebnisse in Form von Screenshots in einer Google Earth-Animationen zusammen und veröffentlichte sie über die Video-Plattform Daily-Motion. Das Brisante daran: Der Präsident Ben Ali ist eigentlich dafür bekannt, Tunesien so gut wie nie zu verlassen. Aufgrund der Ziele des Flugzeugs – nämlich Mode-Metropolen in ganz Europa – gab es für die Aktivisten deshalb nur eine Erklärung: Die Präsidenten-Gattin nutzte das mit Steuergeldern bezahlte Flugzeug für private Shopping-Touren.

Das sorgte in Tunesien für erhebliche Aufregung und so sah sich die Regierung gezwungen, die Video-Plattform kurzerhand zu schließen. Ähnliches geschah auch in Bahrain: Nachdem Google Earth relativ hoch aufgelöste Bilder des kleinen Inselstaates lieferte, wurde es zu einem wahren Volkssport, die Residenzen und Luxusyachten der herrschenden Aristokratenfamilie al-Khalifa zu beobachten. Findige Aktivisten kamen schnell auf die Idee, deren Grundbesitz mit den Landflächen zu vergleichen, die der Bevölkerung zur Verfügung steht und dies in Google Earth einzuzeichnen. Ihr bemerkenswertes Fazit: Rund 80 Prozent des Landes sollen in Privatbesitz sein. Auch hier zensierte die Regierung Google Earth schließlich – allerdings mit, aus ihrer Sicht, verheerenden Folgen. Denn aufgrund erheblicher öffentlicher Proteste, musste die Plattform nach einigen Tagen wieder freigeschaltet werden – die Zugriffe auf die von den Aktivisten eingezeichneten Bereiche sollen sich danach verdreifacht haben.

Zensur und internationaler Personenschutz

Die Kosten für Zensuren steigen damit erheblich. Einzelne Blogs etc. lassen sich schnell abschalten. Doch bei öffentlichen Plattformen erregt dies nicht nur die Aufmerksamkeit einzelner Aktivisten, sondern die weiter Bevölkerungsteile – oder gar die von Engagierten im Ausland sowie der Plattform-Betreiber (die allerdings bedauerlicherweise nicht selten mit diesen Regierungen kooperieren). Oft lenkt somit gerade die Zensur die Aufmerksamkeit auf ein Problem.

Dennoch steigt die Zahl der Internet-Zensuren. Die Open Net Initiative – ein internationaler Zusammenschluss politischer Blogger – dokumentiert seit fünf Jahren alle ihr bekannten Zensuren. Ihr Ergebnis: Waren es anfangs „nur" Saudi Arabien und China, die zensierten, so sollen dies heute über zwei Dutzend Regierungen tun.

Die sicherlich effektivste Zensur ist es daher, unliebsame Blogger so einzuschüchtern, dass sie freiwillig den Mund halten – oder sie gar zu inhaftieren. Doch auch hier hat sich gezeigt, dass moderne Kommunikationstechnologie ein regelrechtes Schutzschild sein kann: Die Mitglieder der „Truth-rising"-Bewegung, die nach dem 11. September in den USA entstand, schützen sich nach eigenen Angaben etwa erfolgreich vor Verhaftungen und Gewaltübergriffen, in dem sie während ihrer Demonstrationen Video-Kameras laufen lassen. In Asien und Afrika sind es vorwiegend Mobil-Telefone, die Aktivisten schützen können: So genannte Micro-Blogging-Dienste, wie Twitter, ermöglichen es, per Handy kurze Textbotschaften in einem Blog zu veröffentlichen und per SMS an die Community zu schicken. So sollen bereits etliche Menschenrechtskämpfer in der Lage gewesen sein, während ihrer Verhaftung ihre Mitstreiter darüber zu informieren. Manchen soll es überdies auch gelungen sein, aus dem Gefängnis heraus weiter zu bloggen und über ihre Haftbedingungen zu berichten.

Ähnliche Micro-Blogging-Systeme entwickeln sich auch gezielt für Aktivisten. Die kenianische Organisation Ushuahidi realisierte etwa ein vergleichbares System, um im Nachgang der Wahl Anfang 2008 Gewaltübergriffe dokumentieren zu können. Dieses stellt sie nun Engagierten weltweit gratis zur Verfügung. Ein anderer, kostenloser Micro-Blogging-Dienst für NGOs ist FrontLineSMS.

Soziale Bewegungen 2.0

Doch nicht nur in Amerika, Asien und Afrika entwickeln sich Alternativen – auch in Europa und in Deutschland wächst seit zwei bis drei Jahren eine neue Generation der sozialen Web-2.0-Plattformen heran: Plattformen, die inhaltlich nicht neutral sind – wie etwa MySpace, YouTube oder flickr –, sondern sich der Vernetzung, Mobilisierung und Kommunikation von Aktivisten verschrieben haben. Die Liste dieser Plattformen ist lang, ihre Anliegen und Tools vielfältig. Doch welche Kraft und welches Potential in ihnen schlummert, mögen ein paar Zahlen verdeutlichen: Seit etwa drei Jahren gibt es die internationale Mikro-Kredit-Plattform Kiva.org. Über sie können Menschen Kleinstkredite vergeben, um Existenzgründungen zu ermöglichen. Allein in diesen drei Jahren verliehen über Kiva.org 340.000 Geldgeber rund 90.000 Kredite im Wert von etwa 45 Millionen US-Dollar.

Schön und gut, werden Sie vielleicht sagen. Aber mit einem Rüstungs-Budget von etwa 1,34 Billionen US-Dollar lässt sich das nun wirklich nicht vergleichen. Das stimmt natürlich. Doch Kiva.org ist schließlich auch nur ein kleines Mosaiksteinchen in einem riesigen Netzwerk von Menschen. Menschen, die erst durch das Internet zu einer Gemeinschaft geworden sind, in der Erfahrungen, Informationen und Unterstützung ausgetauscht werden können – quer über alle Kontinente hinweg. Es ist nur ein Beispiel, das zeigt, dass es in Zeiten der digitalen Vernetzung nicht so sehr darauf ankommt, wie viel ein Einzelner bewegt – oder bewegen kann. Es kommt vielmehr darauf an, dass

alle (kleinen) Aktivitäten zusammen ein großes Ganzes ergeben. Darum sollte uns ein Blick ins Internet auch durchaus ermutigen, Teil dieses weltweiten Engagements zu werden – und sei es nur mit einer ganz kleinen Spende, mit einem kurzen Artikel oder mit einer helfenden Geste. Denn ein Blick in das globale Datennetz zeigt uns: Die Welt besteht nicht nur aus Negativ-Meldungen und Medien-Skandalen. Sie besteht aus unzähligen Menschen, die sich alle eine Zukunft voller Frieden, Freiheit und Gerechtigkeit wünschen – so wie wir. Das Internet bietet uns die bisher einmalige Chance, diese Menschen zu finden, uns mit Ihnen zu verbünden, ihnen zu helfen oder uns helfen zu lassen. Fangen wir an!

Detlef Borchers

Krieg und Frieden: Nicht-staatliche Akteure im Internet

Vorbemerkung: Als die Veranstalter der FIfF-Jahrestagung mich als Moderator dieser Arbeitsgruppe einluden, hatte ich es so verstanden, dass es einen Computer-Raum gibt, wie ich ihn von Vorträgen in Volkshochschulen her kenne, wo alle am Computer sitzen und jeder Schirm variabel auf den Beamer geschaltet werden kann, womit alle über bestimmte Websites diskutieren können. Das war in Aachen nun aufgrund eines Organisationsproblems nicht gegeben. Anstelle gemeinsam Websites zu betrachten, zogen wir mit einer Kiste Laptops durch die Universität in einen Raum, in dem ein paar Laptops angeschlossen wurden, am Ende aber frei diskutiert wurde. Im Kern ging es dabei um die Frage, wie sich nicht-staatliche Akteure via Netz überhaupt zusammenfinden können. Relativ schnell wurde das Modell der AK Vorratsdatenspeicherung diskutiert, einer lockeren Gruppierung, die ohne formales Organisationsgerippe als Paradeorganisation des Web 2.0 gleich 3 Demonstrationen in Berlin und zwei bundesweite Demonstrationen organisieren konnte. Die Diskussion profitierte davon, dass mehrere Mitglieder des AK Vorratsdatenspeicherung von ihren positiven wie negativen Erfahrungen berichten konnten. Die Beteiligten betonten, dass es wichtig ist, nicht nur die virtuelle Komponente zu berücksichtigen, wenn man sich engagieren möchte. „Der AK Vorrat ist dort, wo das FIfF hin möchte", so ein Zitat, dass ich mir extra notiert habe.

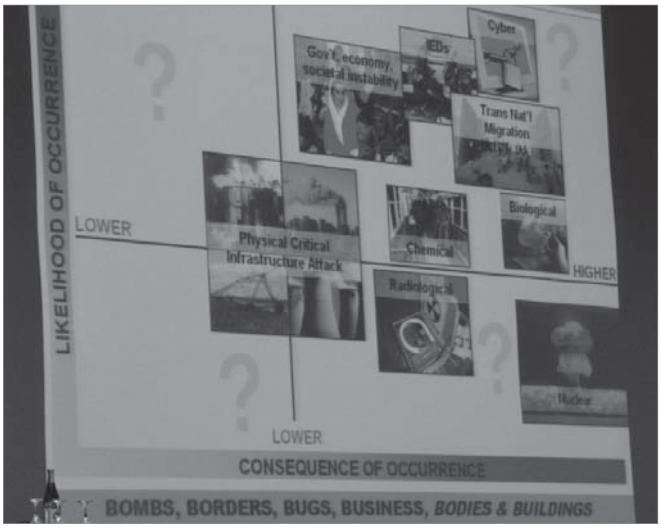
1. Der militärische Bezugsrahmen

Wenn die Rolle von nicht-staatlichen Akteuren im Internet debattiert wird, geht dies nicht ohne Blick auf die staatlichen Akteure. Unter dem Eindruck der asymmetrischen Kriegsführung verändert sich derzeit Theorie und Praxis der Militärs in einem atemberaubenden Maße. Schlagworte wie NetOpFü (vernetzte Operationsführung) bzw. EBAO in NATO-Sprech (Effects Based Approach to Operations) beherrschen die Debatte und künden von der zentralen Rolle der Informationstechnologie in den militärischen Auseinandersetzungen. Klassische Begriffe der Militärs werden dabei obsolet, aber auch die klassische Einteilung in staatliche und nicht-staatliche Akteure. Aus militärischer Perspektive sind nicht-staatliche Gruppen schlicht weitere Informationsangebote, die es abzuschöpfen und verdichten gilt.

Die vernetzte Operationsführung wird in der FüInfoSys-Richtlinie als „Anpassung an die Entwicklung zur Informationsgesellschaft" bezeichnet und so definiert: „Aus der Datenüberlegenheit entsteht die Informationsüberlegenheit, daraus die Führungsüberlegenheit und schließlich die Entscheidungs- und Wirkungsüberlegenheit". In den einschlägigen Schaubildern der Militärführung wird die zentrale These so illustriert:

Information wird zu einem zentralen Baustein der neuen Kriegsführung im asymmetrischen Krieg, wie es diese längere Beschreibung eines Einsatzes deutlich macht:

> *„Die Information hat die größte Hebelwirkung und besitzt das größte Potenzial, um die Kampfkraft der Streitkräfte effizient zu steigern. Dies bedeutet auch, dass jeder Einzelaspekt, ob Force-Protection, Mobilität oder Waffenwirkung durch den Faktor Leadership einen hochwertigen Multiplikator findet, Information aber noch stärker, potenzierender wirken kann. Beispiel Force-Protection: werden eingehende Lageinformationen schnell verfügbar gemacht, bewertet und darüber hinaus mit aktuellen Einsatzplänen korreliert, kann z.B. eine eigene Patrouille früher über drohende Gefahren wie eine Road-Side-Bomb durch terroristische Kräfte*



Quelle: Verteidigungsministerium, Presseinformation „Vernetzte Operationsführung"

informiert werden. Die Route kann daraufhin verzugslos angepasst oder rechtzeitig Unterstützungskräfte eingesetzt werden. Der Anschlag wird hierdurch schnell und effizient verhindert, die Bedrohung eigener Kräfte abgewendet und zivile Opfer vermieden. Darüber hinaus wurden die mit dem Anschlag verbundenen Ziele der Terroristen nicht erreicht. Ggf. können Täter dingfest gemacht werden und zusätzliche Erkenntnis über Strukturen, Hintergründe und Methoden der Terroristen gewonnen werden. Dieses einfache Beispiel zeigt, dass Investitionen in den Faktor Information um ein Vielfaches stärker wirken als z.B. ein paar Zentimeter mehr an Fahrzeugpanzerung."

(Axel Weber, Quo Vadis, Führungsinformationssysteme? Wehrtechnik III/2008, S. 100)

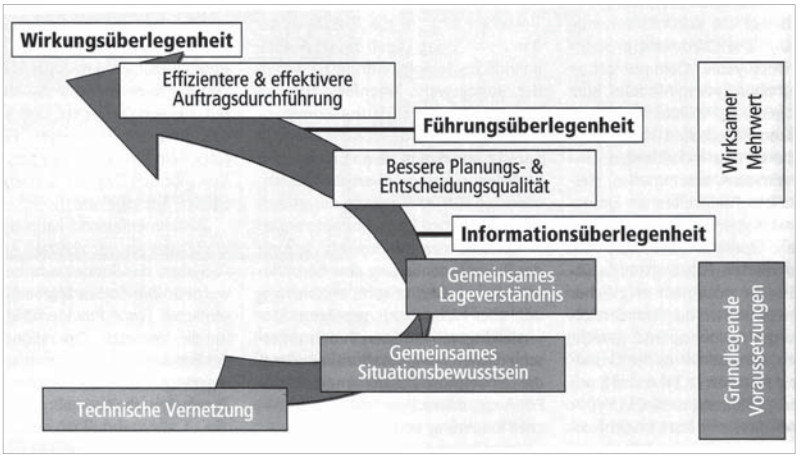
Wesentlich für die Informationsgewinnung ist hierbei die Komponente VeNaGUA (Verbund Nachrichtengewinnung und Aufklärung), die die grundlegenden Voraussetzungen für die Informationsüberlegenheit sicherstellen soll.

„Ähnlich wie Bin Laden nur die allgemeine Richtung vorgibt, wird es bei der Bundeswehr nur die ‚Absicht der Führung' geben, die von autonomen, selbst organisierten und sich selbst synchronisierenden Kampfeinheiten, die – mit der Pflicht zur eigenständigen Informationsbeschaffung al-Qaida-Kommandos ähnlich -- sich ihre Informationen aus dem Internet holen."

Das so bezeichnete Internet ist allerdings nicht das Netz, das wir kennen, sondern ein Intranet, in dem eine eigene VeNaGUA-Suchmaschine Informationen der Sensoren (klassische Aufklärung und vor allem Aufklärung durch Drohnen und Sensoren plus nachrichtendienstliche Informationen und OpInt) gewichtet und verknüpft. Auf diese Informationen greift der „Infanterist der Zukunft" (IdZ) zu, der sich in kleinen Verbänden autonom im asymmetrischen Krieg bewegt. Vorbild sind die fliegenden Verbände: in 97 Prozent aller Einsatzfälle wissen die Piloten nichts von ihrem Auftrag, den sie ausführen sollen, wenn sie starten. Diese Informationen werden nachgeführt. Der IdZ mit mobiler Führungsanbindung über PDA und Mobiltelefon bekommt mit GREL (Gemeinsames Rollenbasiertes Einsatzlagebild) ein Bündel an Informationen, die er im Kampfverbund mit Drohnen und anderen UAVs zu einem Einsatzziel kondensieren kann. (Für Informatiker vielleicht nicht uninteressant, wie die Programmierung von VeNaGUA gesehen wird: „Deshalb wirken sich zukunftsfähige Systemarchitekturen, offene Standards und Ansätze wie Service Oriented Architectures (SOA) besonders positiv aus. Die Bindung an einen einzigen Auftragnehmer oder Hersteller werden zurückgehen." Weber, a.a.O.)

2. Ziviler Bezugsrahmen

Die hauseigene Suchmaschine mit ihrer Datenbank, die GREL speist, kennt eine Cyber-Komponente. „Lageinformationen werden nicht nur aus den IT-Systemen der Bundeswehr, sondern auch aus Informationssystemen von Partner-Streitkräften, anderen Ressorts wie Auswärtiges Amt, Zoll, InterPol und allgemein zugänglichen Informationsquellen beschafft, erfasst, bewertet, korreliert und vernetzt." In dieser Sichtweise bekommt der Cyberwar eine eigene Bedeutung, als Gefahrenquelle der Informationsverschmutzung oder des Einspeisens falscher Informationen. Im Schaubild des US-amerikanischen Department of Defense sieht das so aus:



Quelle: Foto Detlef Borchers, Future Security 08, Konferenz für Sicherheitsforschung Karlsruhe

Cyber-Aktionen und die mit ihnen verwandten IEDs (Inexpensive Explosive Devices = z.B. Selbstmordattentäter) stellen die höchste Gefahr dar. In diesem Rahmen ist es nicht unwichtig, dass sich militärische, geheimdienstliche und polizeiliche Gruppen ebenfalls im Cyber-Raum bewegen. Der asynchrone Krieg ist gewissermaßen doppelt asynchron, wenn (ein aktuelles Beispiel) der Kontaktmann der „Sauerland-Gruppe", der die Sprengsätze besorgte, sich als Mitarbeiter der CIA und MIT (türkischer Geheimdienst) entpuppt. Das gilt auch für andere, gut dokumentierte Fälle:

Detlef Borchers

Detlef Borchers, Jahrgang 55, hat einen Studienabschluss in Medienwissenschaften und ist seit 25 Jahren "EDV-Journalist", er schreibt über große IT-Projekte wie LKW-Maut, elektronische Gesundheitskarte, digitaler Polizeifunk, VeNaGUA usw.

„There are links between UK intelligence and terrorists based in Britain. Britain and the US continue to co-operate with Islamist groups."

(Nafeez Mosaddeq Ahmed, The London Bombings)

„Al Qaida und die CIA bilden ein Joint Venture. Bei allen Anschlagsversuchen und Anschlägen in Europa spielten V-Leute eine unverzichtbare Rolle."

(Jürgen Elsässer, Terrorziel Europa)

In diesem Gemengelage spielen nicht-staatliche Akteure wie Global Voices, das Project Censored, Euro Police, die Informationsstelle Militarisierung oder das Netzwerk Krisen-Kommunikation die Rolle von Informationsvermittlern, die früher einmal dem Journalismus zu eigen war. Das gilt auch für Blogger, wenn sie sich dem Thema Cyberwar oder aber der Überwachungsgesellschaft widmen (Beispiel Ravenhorst) oder aber sogar für die Bundeswehr schreiben (Beispiel Bendler-Blog).

All diese „neuen" Quellen kompensieren mit Informationsangeboten den Ausfall des klassischen Journalismus, der an diese Leistungen wieder Anschluss suchen muss und über den „networked journalism" zur Berichterstattung zurückfinden muss.

„It appears that the media failed to expose the failings of the intelligence that supported the Bush/Blair case for war in Iraq. Was this because they were impotent, incompetent , or deceived?"

(Charlie Beckett, SuperMedia. Saving Journalism So It Can Save the World)

Michael Ahlmann

Als InformatikerIn in der Rüstungsindustrie – wie gehe ich damit um?

... dies war das Thema „meiner" Arbeitsgruppe. Sie war klein, so haben wir in einem Arbeitszimmer eines Dozenten ein schönes Ambiente für unsere Runde vorgefunden. In einer Vorstellrunde haben wir uns miteinander vertraut gemacht, das Spektrum ging über soziale, industrielle und ehrenamtliche Aufgabengebiete und Interessen. Die folgende Zusammenfassung trägt autobiographische Züge.

Ich habe neben Mathematik und Physik allgemeine Elektrotechnik studiert. Seit 1980 arbeite ich als Software-Entwickler in der damaligen Krupp Atlas Elektronik, heute ATLAS ELEKTRONIK, in Bremen. Schon bei der Begrüßung wurde ich gefragt, ob ich programmieren könnte, solche Leute waren damals gesucht und gefragt. Ich hatte neben FORTRAN IV / FORTRAN 77 und ALGOL 60 auch Erfahrung mit dem Intel Prozessor 8085 A 2 auf Assembler-Level; und somit war die Feststellung meines damaligen Abteilungsleiters: Sie sind jetzt unser Software-Entwickler. Damit waren wir zwei Software-Entwickler unter 20 Entwicklungsingenieuren, einer für Sonar und Fishfinder (ich) und mein Kollege für Radar-Systeme. Die Arbeitsbedingungen unterschieden sich sehr deutlich von der Uni-Situation – ich hatte bei ATLAS ein eigenes Intel-Entwicklungssystem mit zwei 8-Zoll-Floppies und Zugriff auf einen Banddrucker, während ich an der Universität vorher schon an einem Monitor arbeiten durfte und keine Kästen mit Lochkarten mehr mit mir herumschleppen musste -, aber noch drastischer von der heute typischen Situation eines Software-Entwicklers: zwei bis drei Arbeitsplatzsysteme, ebenso viele Monitore, eigener Drucker und Scanner, vernetzt im Unternehmen und weltweit. Ich hatte also auch nur einen gleichwertigen Gesprächspartner in der Schiffselektronik. Die Vorgesetzten betraten mit uns Neuland – weg von der analogen Darstellung auf Papier oder Grenzwertanzeigen zur digital berechneten und präsentierten Bildschirm-Technik. Die Technik erlebte einen strukturellen Umbruch, und ich war sehr früh dabei. Fast alle waren begeistert, nur einige stöhnten wegen der neuen Anforderungen und der neuartigen Störungsquellen. Die analoge Welt war vertraut und erprobt, die digitale Welt forderte eine andere Herangehensweise, andere Entwicklungs- und Test-Strukturen – und Kunden, die bereit waren, dafür mehr zu zahlen, um etwas „Neues" einsetzen zu können.

Mein erstes Arbeitsfeld war sehr bewusst in der zivilen Schiffselektronik ausgewählt, in einem bundesdeutschen Projekt „Schiff der Zukunft". Optimismus und Euphorie beflügelten mich – für etwa sechs Monate. Leider wurde dieses Projekt nach wenigen Monaten in Bonn gestoppt, ich hatte Glück und bekam in dem Umfeld Fishfinder und Fishsonar eine neue Aufgabe statt der Kündigung am Ende der Probezeit. Meine in diesen Monaten auf fünf Personen angewachsene Familie hatte also noch einen Ernährer, meine damalige Frau war als Lehrerin in Elternzeit, wie wir es heute benennen.

Nach zwei Jahren und erfolgreich abgeschlossenen Projekten wechselte ich von der reinen zivilen Technik in die allgemeine Softwaretechnik, Betriebssysteme und Programmiersprachen, Treiber und Anwendungsprogramme für alle möglichen bei ATLAS eingesetzten Rechnersysteme. Dies war ein Schritt aus der reinen zivilen Welt näher an die militärischen Systeme, die damals etwa 50% ausmachten. Gleichzeitig war dies aber auch ein Schritt zu höheren Sprach- und Systemebenen, realzeitfähigen Bitslice-Maschinen für Multiuser und Multioperations. Auf einem Anwendungsrechner haben wir die Programme entwickelt und getestet – mit selbstgeschriebener Software und selbstentwickeltem System, ursprünglich einer PDP 11 nachempfunden.

An dieser Stelle mache ich mal einen Schnitt. Seit 1980/1981 gibt es innerhalb der IG Metall Auseinandersetzungen und Konflikte um den Erhalt von Arbeitsplätzen, auf nationaler und internationaler Ebene eine tiefgehende Diskussion um Nachrüstungsbeschlüsse, Veränderungen in der Nato, partielle Beteiligung der Bundeswehr an nuklearen Themen – die Friedensbewegung entwickelt sich. Innerhalb der IG Metall entstehen in einigen süddeutschen Betrieben, vor allem aber auf den Werften an der Küste und bei den Vorgängerbetrieben der Airbus Arbeitskreise für alternative Produkte, für Konversion. Ein Entzündungspunkt dafür ist eine Demonstration in Kiel auf der HDW-Werft, als gut 1.000 Werftarbeiter für die Produktion und das Ausliefern von U-Booten für das damalige faschistische Pinochet-Regime demonstrierten. Es geht bei allen Auseinandersetzungen in diesen Arbeitskreisen vorrangig um den Erhalt und zukunftsfähigen Ausbau von Arbeitsplätzen. Daneben ist auch die soziale Verantwortung für die Produkte und ihre Umweltverträglichkeit zentrales Thema. Logischerweise finde ich bei diesen Diskussionen auch Kontakt zu den Aktivisten des FIfF und arbeite mit im Arbeitskreis „Rüstung und Informatik – RUIN". Seit dieser Zeit bin ich also eines der Bindeglieder zwischen gewerkschaftlicher Diskussion um den Sinn von Arbeit in Betrieben, die sich teilweise oder überwiegend mit Rüstungsgütern beschäftigen, und dem FIfF als politisch auftretende InformatikerInnen-Organisation.

Ich leite heute einen der letzten verbliebenen Arbeitskreise zur Alternativen Produktion, den der IG Metall in Bremen. Bis 2007 haben wir jährlich ein Wochenseminar veranstaltet, heute fehlen dafür leider die Mittel und die Unterstützung. Diesen Niedergang müssen wir als politische Niederlage verstehen. Die Suche nach sinnvollen Energieformen, die Abkehr von Nuklearenergie sind aber massiv beeinflusst durch das Zusammenwirken vieler Kräfte, zu denen ich auch die Arbeitskreise Alternative Produktion zähle, ein noch lange nicht abgeschlossener Prozess – ein Erfolg, der durch die aktuellen politischen Mehrheiten leicht zerdeppert werden kann.

Persönlich habe ich es immer als große Herausforderung gesehen, in einem industrie- und technologiepolitisch hochinteressanten Umfeld eine eigene Meinung zu vertreten, die sehr oft von den Vorständen als Nestbeschmutzung und feindlich diskreditiert wurde und wird. Wichtiger als die Meinung der Vorstände ist für mich allerdings die Verständnisbrücke zu den Kolleginnen und Kollegen. Als Betriebsrat muss ich selbstverständlich Belegschaftsinteressen vertreten, aber ich muss auch Widersprüche und unterschiedliche Meinungen aushalten und bewegen. Die Diskussion um Konversion im Unternehmen ist in den Jahren, in denen das Land Bremen und die Europäische Union Fördermittel angeboten haben – hauptsächlich zwischen 1986 und 1998 –, auch eine offene und kontroverse Diskussion mit Geschäftsführungen und politischen Akteuren gewesen; die Belegschaften haben sich typisch neutral-interessiert verhalten, wenige, vor allem Vertrauensleute der IG Metall und neugierige Ingenieure, TechnikerInnen und PhysikerInnen, haben aktiv in den Arbeitskreisen mitgearbeitet und viele Produktideen generiert. Diese Phase ist in den Betrieben spätestens 2002 wieder eingeschlafen, die Aktivitäten finden eigentlich nur noch in der Freizeit mit sinkender Beteiligung statt.

Seit 1983 bin ich im Betriebsrat, bis 1987 als Nachrücker. Daraus entstanden zwei parallele Arbeitsfelder, als Software-Entwickler und aktiver IG Metaller im Betriebsrat. Gleichzeitig war ich bis 1996 stellvertretender Leiter des Vertrauenskörpers der IG Metall, die damals noch sehr viel deutlicher als heute von und für Lohnempfänger – Arbeiter – ausgerichtet war. Als Akademiker, als Angestellter und Software-Entwickler waren wir nur wenige Ingenieure, Physiker und Informatiker, wir waren eher aus einer anderen und fremden Welt. Von 1987 bis 1998 habe ich mich selbst zu über 80% von der Arbeit freigestellt, ein heftiger Spagat zwischen Beruf und Interessenvertretung. 1998 bis 2002 – die IG Metall hat bei den Betriebsratswahlen die Mehrheit verloren – erlebte ich die zeitweilig schwierige Situation, mich auf der einen Seite wieder als Software-Entwickler in die Fachabteilung integrieren zu müssen, auf der anderen Seite Arbeitgeber und die Betriebsratsmehrheit massiv als Gegner zu erfahren. Dieses Risiko jeden Ehrenamtes, zurück an die Basis zu müssen, empfand und empfinde ich als klärend und positiv, den koordinierten Druck des Arbeitgebers und des damaligen Betriebsratsvorsitzenden gegen mich als Person, als kritischen Geist mit Friedens- und Freiheitsgedanken hingegen als existenzgefährdend. In dieser Zeit ging meine Ehe in die Brüche.

Zum Ende dieser Phase ging das Unternehmen – Hand in Hand mit der damaligen Angestelltengewerkschaft DAG – aus dem Flächentarif heraus und beglückte die Belegschaft mit einer besonderen Form der Arbeitszeitgestaltung, der sogenannten Vertrauensarbeitszeit. Faktisch heißt das, dass die Verantwortung für das Einhalten des Arbeitszeitgesetzes auf den Arbeitnehmer übertragen wird, dieser gleichzeitig kein Geld für einen Großteil der bisherigen Überstunden erhält – natürlich auch keine Zuschläge dafür, weil dies ja nur im Tarifvertrag gilt. Tatsächlich wird die freiwillige Selbstausbeutung normal, keiner und keine will auffallen, eine Aufgabe nicht in der vorgegebenen Zeit zu schaffen. Also spendieren sehr viele KollegInnen sehr viele Stunden als Geschenk an das Unternehmen und riskieren aus Angst um den Arbeitsplatz ein gutes Stück Privatleben.

Michael Ahlmann

Michael Ahlmann ist Betriebsrat im Unternehmen ATLAS ELEKTRONIK in Bremen. Er ist Sprecher des Referentenarbeitskreises und Sprecher des Arbeitskreises Alternative Produktion bei der IG Metall in Bremen. Seit 1996 ist er wissenschaftlicher Beirat des FIfF. (*michael.ahlmann@fiff.de*)

Seit 2002 bin ich ein offiziell freigestellter Betriebsrat, wir haben eine klare IG Metall Mehrheit. Seit 2003 ist das Unternehmen STN ATLAS in zwei Teile zerlegt worden, die damalige Shareholderstruktur – 51% Rheinmetall und 49% British Aerospace Systems (BAE) zerbricht. BAE übernimmt alle maritimen Aktivitäten und führt über drei Jahre die neue ATLAS ELEKTRONIK. 2006 richtet sich BAE fast ausschließlich auf den US-amerikanischen und nicht-europäische Märkte aus und verkauft in Konsequenz fast alle europäischen Beteiligungen und Töchter.

Seit 2003 bin ich BR-Vorsitzender dieser neuen ATLAS ELEKTRONIK, seit 2006, mit einer stabilen IG Metall Mehrheit im Gremium, auch GBR- und KBR-Vorsitzender.

Mittlerweilen sind die Elektronikbetriebe in Bremen, die aus der STN ATLAS hervorgegangen sind, bis zu 90% und mehr internationale Produzenten von Gütern, die als Sensoren, Systeme oder Waffen auf verschiedenen Plattformen zu Lande, auf dem Wasser und in der Luft eingesetzt werden. Die zivilen Unternehmensbereiche wie Schiffselektronik und Hydrographie sind verkauft oder verselbständigt, andere werden gerade dafür vorbereitet. Negativ daran ist aus meiner Sicht, dass sowohl die Sicherheit der Arbeitsplätze wegen fehlender Alternativen im Unternehmen geringer ist, die Betriebsgrößen massiv schrumpfen und damit bei geringen Deckungsspannen auch die Existenz der Unternehmen leichter gefährdet ist.

Dies ist sicherlich ein Teil meiner eigenen Lebensgeschichte, die Arbeitsgruppe in Aachen hat diesen Bericht durch viele Nachfragen nach Strukturen und Motiven sehr lebendig entgegengenommen und gesteuert. Ich danke auch auf diesem Wege den TeilnehmerInnen der Arbeitsgruppe für Ihre Aufmerksamkeit und Neugier.

Interview mit Berndt G. Thamm

Von al-Qaida zu @Qaida – IT: Motor der Globalisierung des Djihad

... so lautete provozierend der Titel des Vortrags von Berndt Georg Thamm, Berlin *auf unserer Jahrestagung. Mit zahlreichen Veröffentlichungen zum Thema Terrorismus und organisiertes Verbrechen hat sich der Publizist Thamm einen Namen gemacht und referiert zu diesen Themen regelmäßig bei Weiterbildungen u.a. in Landespolizeischulen und bei der Bundeswehr. In seinem Vortrag wie auch schon in einem früheren Interview mit der ZEIT* [1] *vertritt Thamm die These, dass terroristische Organisationen – er bezieht sich speziell auf al-Qaida – das Internet zunehmend für ein effizienteres und ortsungebundeneres Agitieren und Operieren nutzen. Wir fragten nach.*

FIfF: Ihr Vortrag auf der Aachener Tagung war plakativ betitelt „Von al-Qaida zu @Qaida". Sie bezeichneten darin Informationstechnik als „Motor der Globalisierung des Djihad". Können Sie zunächst umreißen, was genau Sie damit meinen?

Berndt G. Thamm: Die zum Ende des ersten großen Heiligen Krieges (Djihad) am Hindukusch 1988 in Afghanistan gegründete al-Qaida verstand sich vom Selbstbild her über ein Jahrzehnt als Militärorganisation, die ihre wichtigste Mission im „Sturz der gottlosen Regime und ihre Ersetzung durch ein islamisches Regime" sah (Handbuch „Militärische Studien des Djihad im Kampf gegen die Tyrannen" der al-Qaida). Geographische Basis der al-Qaida war ab 1996/97 das Emirat Afghanistan der Taliban. In ihrer Medienarbeit nutzte die islamistische Militärorganisation in der zweiten Hälfte der 1990er Jahre noch kaum das Internet. Ihr wichtiges „Manifest der internationalen islamischen Front für einen Djihad gegen die Juden und Kreuzfahrer", vom al-Qaida-Führer Osama Bin Laden und Führern der Djihad-Gruppen in Ägypten, Pakistan und Bangladesch verfasst, wurde seinerzeit nicht ins Netz gestellt, sondern noch per Fax der arabisch-sprachigen Tageszeitung ‚Al-Quds Al-Arabi' (London) zugestellt, die den Text in voller Lange am 23. Februar 1998 druckte. Erst nach der Zerschlagung der Qaida als Militärorganisation (nach den 9/11-Anschlägen) 2001/2002 erfolgte eine stärkere Hinwendung zum Netz. Ab 2002/03 wurde aus der zuvor in Afghanistan lokalisierbaren Militärorganisation durch zunehmende Netz-Nutzung der überlebten Rumpf-Qaida eine islamistische – mehr virtuelle – Bewegung. Die zunehmende Netz-Präsenz ging einher mit der Globalisierung des Djihad. Militärische Lehrbücher, deren Inhalte zuvor nur in den Camps durch Unterweiser face-to-face weitergegeben wurden, waren nun über das Netz für jeden Djihad-Interessierten zugänglich. Den virtuellen Djihad-Terrorismus brachte der Führer der al-Qaida in Saudi Arabien, Abd al-Aziz al-Muqrin, im Januar 2004 auf den Punkt: „Mit Hilfe Gottes wird es dir nun möglich sein, für dich allein, in deinem Zuhause, oder gemeinsam mit deinen Geschwistern [im Glauben (A.d.V.)] mit der Durchführung des Programms [= Terrorismus-Kurse (A.d.V.)] zu beginnen".

FIfF: Ihrer Ansicht nach kommt dem Internet in diesem Zusammenhang eine besondere Bedeutung als Informationsmedium zu. In welcher Weise und in welchem Umfang wird das Internet ihrer Kenntnis nach als Kommunikationsmedium im Kontext terroristischer Aktivitäten genutzt?

Berndt G. Thamm: Den Erfordernissen des globalen Djihad angepasst dient das Internet heute der offenen und verdeckten Kommunikation, der Verbreitung zielgruppenspezifischer Botschaften, der Informationssammlung, der Radikalisierung (der Gesinnung), der Rekrutierung von jungen Männern, aber auch von Frauen und selbst von Kindern, weiterhin der Bildung (virtuelle Djihad-Universität), und Ausbildung (Online-Universität

für Djihadisten), der Öffentlichkeitsarbeit und Propaganda, der Spendensammlung, der Netzwerkarbeit, der Mobilisierung und der Planung von Operationen sowie der psychologischen Kriegführung. Für den letzten Anwendungsbereich steht beispielhaft die Medienoffensive verschiedener Djihadisten gegen Deutschland im ersten Monat des Wahljahres 2009. Innerhalb von nur drei Wochen nutzten Djihad-Terroristen das Internet wie nie zuvor für massive Drohungen gegen Deutschland und gegen Deutsche im Ausland:

- Anfang Januar tauchte eine Botschaft der Islamischen Bewegung Usbekistan (IBU) auf. In einem 30-minütigen Videofilm forderte in fast akzentfreiem Deutsch ein Mann mit dem Kampfnamen ‚Abu Adam aus Deutschland' die deutschen „Geschwister" auf, sich dem Djihad anzuschließen.

- Am 17. Januar tauchte ein – offenbar schon im Oktober 2008 direkt von der al-Qaida-Medienabteilung ‚As Sahab' produziertes – Drohvideo mit dem Titel „Das Rettungspaket für Deutschland" im Internet auf. In diesem drohte der deutsch-marokkanische Djihadist Bekkay Harrach Deutschland in fast akzentfreiem Deutsch eine halbe Stunde lang Anschläge an: „Sollten die Deutschen leichtgläubig und naiv meinen, als drittgrößter Truppensteller [in Afghanistan (A.d.V.)] ungeschoren davonzukommen, dann sind deutsche Politiker im Bundestag fehl am Platz".

- Zum Wochenende des 24./25. Januar wurde bekannt, dass die islamistische Propagandaoffensive im Internet mit einem dritten Drohvideo verstärkt worden war. Auf YouTube (das Video war hier am 12. Januar gelöscht worden) behaupteten islamistische Terrorsymphatisanten – mutmaßlich Djihad-terroristische Trittbrettfahrer – "wir werden eine Armee senden mitten in eure Stadt, besonders Berlin, Köln und Bremen".

- Am 27. Januar fand sich ein weiteres Islamisten-Video mit Passagen auf Deutsch im Internet. In dem 26-minütigen Drohvideo kündigten vermummte Kämpfer der Islamic Jihad Union (IJU) unter Verweis auf den Krieg im Gazastreifen Anschläge an: „In diesem Jahr haben wir ein paar Überraschungspakete an die Besatzungsmächte vorbereitet. Denn der Verbündete der Besatzungsmächte muss immer mit unseren Angriffen rechnen" ...

FIfF: Welche Konsequenzen sollten Ihrer Meinung nach aus dieser Entwicklung gezogen werden?

Berndt G. Thamm: Ich teile die Meinung des Bundesinnenministers Wolfgang Schäuble, dass das Internet sich zu einer „universellen Plattform des Djihad" gegen den „Internationalen Unglauben, insbesondere gegen die westliche Welt" entwickelt hat: „In diesem virtuellen Raum versammeln und bündeln Islamisten ihre Ressourcen weitgehend ungehindert und unkontrolliert". Vor diesem Hintergrund ist über kurz oder lang eine sicherheitspolitische Güterabwägung zu treffen. Auf der einen Seite steht die Aufrechterhaltung der „absoluten Offenheit des virtuellen Raumes". Auf der anderen Seite könnte eben diese „zur Gefahr für die Offenheit der demokratischen Gesellschaft mit seiner Werteordnung" werden. Die Terrorismusfahnder im Gemeinsamen Internetzentrum (GIZ) in Berlin-Treptow machten schon vor einem Jahr – Anfang Februar 2008 – auf eine neue Qualität der islamistischen Propaganda aufmerksam. Neben den Hetzbotschaften gegen den Westen wurden zunehmend „Bombenbastelanleitungen in deutscher Sprache" ins Netz gestellt. Diese Ausweitung der schon ab 2007 feststellbaren Internet-Offensive der al-Qaida-Bewegung spiele, so die GIZ-Fahnder, „eine große Rolle bei der Radikalisierung von jungen Muslimen, die in Deutschland leben". Wer vor dem Hintergrund dieser Entwicklung die Aufrechterhaltung der absoluten Offenheit des virtuellen Raumes fordert, nimmt die genannten Gefahren billigend in Kauf.

Auf die Antworten auf unsere ersten drei Fragen fragten wir in einer zweiten Interviewetappe zu einigen Punkten detaillierter nach:

FIfF: In Ihrer Antwort auf unserer Frage nach der Nutzung des Internet für terroristische Aktivitäten gingen sie vorwiegend auf Propaganda-Aktivitäten ein. In Ihrem Interview mit der ZEIT [1] betonten sie aber auch, dass viele terroristische Aktivitäten „heute über's Internet regelrecht gesteuert" würden. Können Sie das konkretisieren?

Berndt G. Thamm: „Der Heilige Krieg ist mittlerweile Internet-gesteuert", wurde Dennis Pluchinsky vom US-Außenministerium schon im Spätsommer 2005 zitiert. Der religiös motivierte Terrorismus der Djihadisten liegt in einer einzigartigen Kombination von Alt und Neu – von Elementen einer Stammesreligion des 7. Jahrhunderts mit der technischen Intelligenz des 21. Jahrhunderts. Al-Qaida ist es – wie keiner anderen islamistischen Organisation zuvor – gelungen, diese bizarre Kombination zu verwirklichen. In einem Zeitraum von nicht einmal 20 Jahren ist aus einer ursprünglich geographisch lokalisierbaren, islamistischen Militärorganisation eine globale Bewegung des Djihad geworden, eine Bewegung (movement), die auf dem wahhabitischen

Berndt G. Thamm

Berndt Georg Thamm, Berlin, Fachpublizist: 1974 bis 1988 soziale Tätigkeiten in der Drogenarbeit im In- und Ausland, seit 1988 freiberufliche Tätigkeiten in den Themenbereichen Rauschgift (RG), organisierte Kriminalität (OK) und Terrorismus (TE), insbesondere als Fachpublizist (über 200 Veröffentlichungen, darunter 18 Bücher), Referent für Schutzorgane (vornehmlich Strafverfolgungsbehörden) und Advisor/Berater für Print- und AV-Medien; Kontaktarbeit mit und für ausländische Diplomaten.

Islamismus aufbaut und zugleich als modernes, weltweit virtuelles Netzwerk organisiert ist. Unterschiedlichste islamistische Gruppen und Grüppchen sehen sich unter einem gemeinsamen Dach – dem finalen Djihadziel der Errichtung eines Gottesstaates mit religiöser Rechtsordnung – verbunden, nennen sich dementsprechend al-Qaida in Indien, al-Qaida im Irak, Al-Qaida in Saudi Arabien, al-Qaida in Nordafrika. Das Internet bot und bietet in einer riesigen islamischen Weltgemeinschaft (virtuelle) Zugehörigkeit zu einer kleinen, aber wichtigen „Rettergeneration", die dazu „auserwählt" ist, dass sie die „anderen" aus der Dekadenz der sie umgebenden „Unreinheit" führen kann und soll. Jeder einzelne „Retter" ist wichtig, ist er doch als „Soldat Allahs" zum Djihad bereit. Das Internet bringt so „Retter" zusammen, die sich sonst wohl nie kennen gelernt hätten. Es hat zugleich die ursprüngliche al-Qaida selbst geändert. Der SPIEGEL-ONLINE-Redakteur Yassin Musharbash beschrieb diese Änderung auf der BKA-Herbsttagung im November 2007: Das Internet hat einen neuen Aktivistentyp hervorgebracht, den „Terror-Ehrenamtlichen", al-Qaida sei damit im virtuellen Raum „auf dem Weg zu einer Art Wiki-Qaida: einem Internet-basierten Djihad-Projekt, an dem jeder mitschreiben und mitwirken darf".

FIfF: Sie erwähnten eine „virtuelle Djihad-Universität" sowie eine „Online-Universität für Djihadisten". Was muss man sich darunter jeweils konkret vorstellen? Was gibt es dort für Angebote und an wen richten sie sich?

Berndt G. Thamm: Als das wichtigste Propagandainstrument von al-Qaida, so der Islamwissenschaftler Rainer Hermann, gilt das „Zentrum für islamische Studien und Forschungen" (Markaz al-Dirasat wa-l-Buhuth al-Islamiya), das im Internet lange eine Zeitschrift herausgeben konnte, deren Artikel (in der Regel) nicht namentlich gezeichnet waren. In einem solchen Beitrag, der am 17. März 2003 im islamistischen Internetforum Sada al-Jihad verbreitet worden war, hatte es unter der Überschrift „Die Kultur des Djihad" geheißen: „Der Scheich [Osama Bin Laden, (A.d.V.)] hat uns gezeigt, dass, solange wir danach streben, Allah uns helfen wird, dem Islam durch den Djihad das zu geben, was wir sollen. Auch mit dem Ende des Scheichs sollen wir nicht stehen bleiben". Noch lebt der Scheich. Sein einflussreicher Interpret in der im Internet entstandenen offenen Djihad-Universität war der Palästinenser Maqdisi. Für diesen geistlichen Führer der Terrorgruppe Biat al-Imam galt die Demokratie als Herrschaft des Heidentums und Erfindung, die den Werten des Islam widerspricht. Maqdisi betrieb eine eigene Website „Die Einheit Gottes und der Djihad". Auf ihr hatte er geschrieben, Bin Laden sei der „Imam des Jahrhunderts", und nur ein Ungläubiger könne dies bestreiten. Der Online-Aufruf zum Djihad ist mittlerweile fester Bestandteil der Medienstrategie islamistischer Terroristen. Wichtiges Anliegen der offenen Djihad-Universitat ist die theologische Rechtfertigung des Djihad als „Gipfel des Glaubens".

Ende 2001 verlor al-Qaida ihre paramilitärischen Camps im untergegangenen Emirat Afghanistan der Taliban, in denen zuvor über ein halbes Jahrzehnt mindestens 20.000 zur Gewalt bereite Islamisten „beschult" wurden. Die al-Qaida-Bewegung bot in der Folge über das Internet zunehmend virtuelle Trainingscamps unter dem Motto „kannst du nicht zur Ausbildung kommen, kommt die Ausbildung zu dir" an. In den neuen, in den Cyberspace verlagerten Ausbildungscamps konnten die „Auserwählten" (islamistischer Rettungsideologien) schon vor Jahren auf Websites lernen, wie man hochgiftiges Rizin mischt (im Netz gab es das „Mudjaheddin-Gift-Handbuch"), Bomben baut und per Handy zur Explosion bringt (im Netz gab es ein „Mudjaheddin-Sprengstoff-Handbuch"), wie man unbemerkt von A (z.B. Syrien) nach B (z.B. Irak) kommt, wie man schultergestützte SA-7-Raketen bedient u.a.m. Schon 2005 wurden derartige „Lehrgänge" auf Arabisch, Urdu, Paschtu und anderen Sprachen angeboten. Tauchten beim Bombenbau oder bei der Geiselnahme Probleme auf, beantworteten erfahrene „Brüder des Djihad" Fragen im Chatroom. Im März 2008 berichtete Bayerns Innenminister Joachim Herrmann, dass der Verfassungsschutz des Freistaates erstmals eine Art „Online-Universität" für Djihadisten im Internet entdeckt hatte. „Lehrer" und „Schüler" würden dort einschlägiges Fachwissen und Daten über Waffenkunde, Bombenbau, Guerillakampf und konspirative Kommunikation austauschen. Diese virtuelle „Ausbildung mittels Fernstudiums" ergänzt zunehmend die Ausbildungslager, die von einer reorganisierten Rumpf-Qaida, Taliban, turkestanischen Djihadisten der Islamic Jihad Union (IJU) im afghanisch-pakistanischen Grenzraum unterhalten werden.

FIfF: §130a StGB verbietet die Verbreitung von Anleitungen für Straftaten. Dies gilt laut Bundesjustizministerium auch für Bombenbauanleitungen im Internet. Konkret lassen sich damit entsprechende Angebote aus Deutschland strafrechtlich verfolgen. Für Angebote aus anderen Ländern, in denen keine entsprechenden Regelungen bestehen, gilt dies nicht. Hier wird als Konsequenz bspw. von Bert Weingart, Vorstand der Firma PAN AMP, eine umfassende Filterung von Internet-Inhalten vorgeschlagen. Wäre dies Ihrer Ansicht nach eine wünschenswerte und geeignete Lösung oder haben Sie andere Vorschläge?

Berndt G. Thamm: Die al-Qaida-Bewegung versteht sich als globale Bewegung, die der Völkergemeinschaft des internationalen Unglaubens den Heiligen Krieg (Djihad) erklärt hat. Dieses Djihad-terroristische Gegenüber, dem das Netz als Kommunikationsmedium, Werbeträger, Fernuniversität, Trainingscamp und Think-Tank dient, lässt sich nachhaltig nur global, nicht nationalstaatlich bekämpfen. Der Vorschlag von Herrn Weingart, Internet-Inhalte umfassend zu filtern, ist im Rahmen eines globalen Terrorbekämpfungsansatzes nur zu begrüßen.

FIfF: Sie stellen mit Blick auf den Sicherheitsaspekt die Aufrechterhaltung der Offenheit des Internets in Frage. Gehen wir damit im Vergleich zum westlichen Ausland nicht einen Schritt zu weit, siehe z.B. die sehr sicherheitsbewussten USA: „Protect the Openness of the Internet" und „Safeguard our Right to Privacy" [2]? Und sind über eine intendierte Kontrolle der im Internet verbreiteten Inhalte hinaus die noch drastischeren Maßnahmen des Bundesinnenministers zur Kontrolle privater Nutzerdaten vertretbar, womit auch alle unbescholtenen Bürger unter einen Generalverdacht gestellt werden? Entspricht das – in Abwägung mit den damit erzielbaren Fahndungsergebnissen – noch dem Grundsatz der Verhältnismäßigkeit?

Berndt G. Thamm: Ich bin kein Jurist, teile aber die Besorgnis des BKA-Präsidenten Jörg Ziercke, für den das Internet „zum Leitmedium für Terroristen und Pädophile geworden" ist (Wiesbaden, November 2007). Die Verbreitung von Kinderpornographie und die Verbreitung des „Djihad gegen den internationa-

len Unglauben“ ist der Internet-„Wachstumsmarkt“ schlechthin. Ich bin der festen Überzeugung, dass Menschenverachtung nicht zur freiheitlichen Meinungsäußerung von Menschen gehört bzw. gehören darf. Im Kampf dagegen müssen wohl auch neue Wege beschritten werden. Der Einsatz von Filtersystemen, die entsprechende Seiten blockieren, ist technisch bestimmt möglich. Um eine Güterabwägung wird nationale und internationale Politik nicht herumkommen. Mit einer Einschränkung der jetzigen Offenheit des Internets würde ich mich als unbescholtener Bürger nicht unter Generalverdacht gestellt sehen, wenn diese dem Schutz des Gemeinwohls dient.

FIfF: Herr Thamm, wir danken Ihnen für das Interview!

Quellen

1 Jochen Bittner: Die virtuelle Terror–Uni, Terrorismus–Experte Berndt Georg Thamm über das Internet als Propagandainstrument, Kollektivhirn und Schulungsraum von al–Qaida (Interview). DIE ZEIT, 08.05.2008 Nr. 20

2 www.barackobama.com/issues/technology/

Das Interview führten Dietrich Meyer–Ebrecht und Ralf E. Streibl. In zwei Etappen stellten wir Berndt G. Thamm schriftlich Fragen und erhielten die Antworten ebenfalls schriftlich.

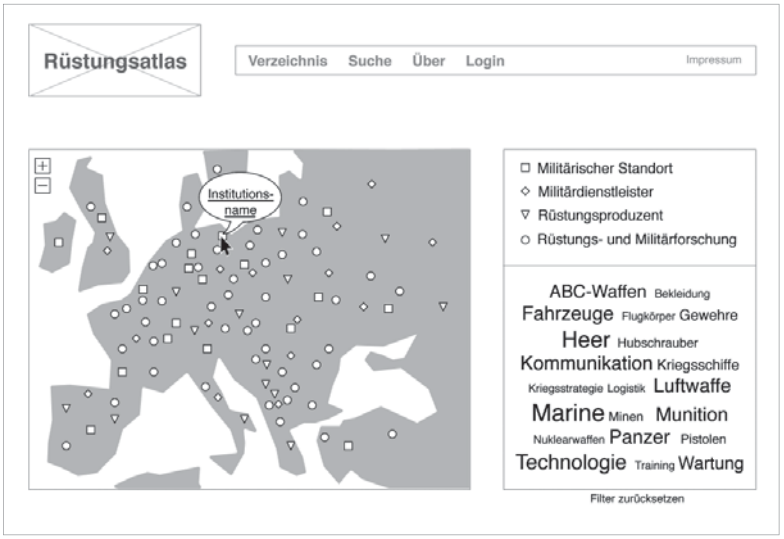
Eine der Arbeitsgruppen auf der Tagung wurde im Zusammenhang mit einer bereits bestehenden Projektidee angeboten: Alex Klein hatte einige Monate zuvor ein Konzept für einen „Rüstungsatlas“ entwickelt und grundlegende konzeptuelle Vorarbeiten dafür geleistet. Doch um solch ein Projekt zu realisieren sind weitere Ideen und Diskussionsbeiträge hilfreich und vereinte Kräfte für eine konkrete Umsetzung notwendig. In diesem Sinne – das zeigt der nachstehende Kurzbericht – war die Arbeitsgruppe auf der Jahrestagung ein Schritt voran und weitere werden folgen.

Alex Klein

Der Rüstungsatlas

Schritte zur Umsetzung

Bereits im Sommer 2007 ist die Idee eines Rüstungsatlanten entstanden. Der Rüstungsatlas sollte eine offene und interaktive Internetplattform werden, auf der Informationen zu Rüstungs- und Militärstandorten zentral gesammelt, aktualisiert und vernetzt werden. Praktisch eine Art Wikipedia zu Rüstungs- und Militärstandorten mit einer geografischen Zuordnung auf einer Karte. Schnell war zu dieser Idee ein umfassender Konzeptentwurf verfasst, der bereits in gekürzter Form in der FIfF-Kommunikation 3/2007 („Visionen“) erschien[1].



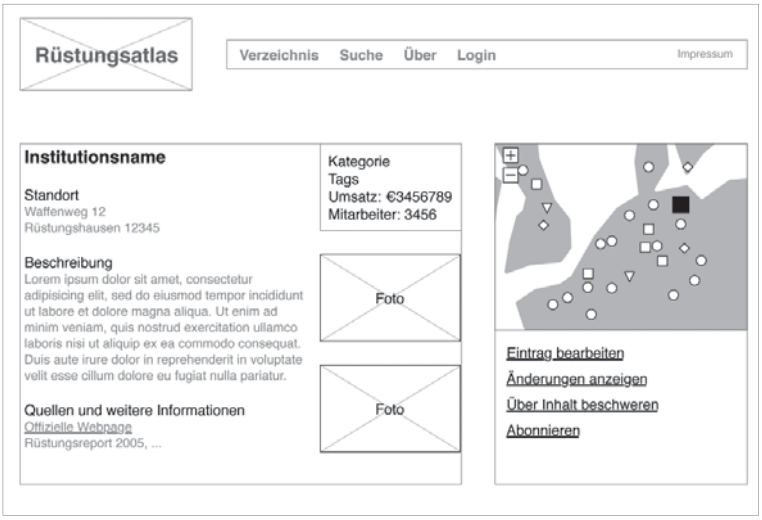
Leider ist danach sehr wenig passiert. Auf der letzten Jahrestagung in Aachen hat sich nun allerdings eine kleine Arbeitsgruppe zusammengefunden, die sich mit der praktischen Umsetzung des Rüstungsatlanten auseinandersetzt. Ein Projektwiki und eine Mailingliste zur Koordination der Projektmitglieder wurden etabliert, auf denen nun über die weitere Umsetzung beraten wird. Dabei haben sich zwei Arbeitsschwerpunkte herauskristallisiert: Die technische Um-

Alex Klein

Alex Klein, Diplomstudium der Wirtschaftsinformatik an der FHW Berlin, Berufsakademiestudium bei IBM. Anschließend Masterstudium Friedens- und Konfliktforschung an der Otto-von-Guericke-Universität in Magdeburg.

setzung sowie die öffentlichkeitswirksame „Vermarktung“ des Rüstungsatlanten. Schließlich lebt die Idee des Rüstungsatlanten von der Partizipation vieler, die durch die Bereitstellung, Erweiterung und Korrektur von Informationen dieses Projekt erst zum Leben erwecken. Daher erscheint es den Projektmitgliedern sehr wichtig, viele und möglichst auch gewichtige PartnerInnen zu finden, die den Rüstungsatlas aktiv, mit Daten, oder passiv, durch Unterstützung in der Öffentlichkeitsarbeit unterstützen.

Viele der am Projekt beteiligten sind naturgemäß stark in Beruf oder Studium eingebunden. Wir freuen uns daher sehr über weitere InteressentInnen und MitstreiterInnen, die den Erfolg des Rüstungsatlanten mit vorantreiben wollen – völlig egal ob technisch oder anderweitig. Wir freuen uns auf Kontaktaufnahmen unter *ruestungsatlas@fiff.de*



Endenote: 1 Klein, A. (2007): Der Rüstungsatlas. Ein basisdemokratisches Informationsportal. In: FIfF-Kommunikation 24 (3), S.21-25.

Was tut sich bei...

DVD – Deutsche Vereinigung für Datenschutz

Die DVD gab im Dezember eine Presseerklärung zum 25-jährigen Jubiläum des Volkszählungsurteils heraus. Darin heißt es u.a.:

> *„Der Datenschutz ist im Jubiläumsjahr aus dem öffentlichen Bewusstsein nicht mehr wegzudenken. Skandalöse Datenmissbrauchsfälle in der privaten Wirtschaft und spektakuläre Gesetzgebungsprojekte im Sicherheitsbereich haben die Öffentlichkeit nachhaltig beeindruckt und zuletzt im Oktober 2008 Tausende zu öffentlichen Demonstrationen mobilisiert. Datenschutz ist endgültig zu einem Qualitätsmerkmal, Standortfaktor und Zeichen einer demokratische Gesellschaft geworden. Der Wille, sich nicht ungefragt erfassen und speichern zu lassen, ist 25 Jahre nach dem Volkszählungsurteil weiter verbreitet denn je.“*

Die DANA 01/09 (Schwerpunkt „Bundesgesetzgebung Datenschutz“) fasst Informationen, Hintergrund und Stellungnahmen zu aktuellen Gesetzgebungsvorhaben des Bundes zusammen und geht insbesondere auf die Stärkung der Verbraucherrechte und das Datenschutzaudit ein.

Humanistische Union

Das aktuelle Heft der Zeitschrift für Bürgerrechte und Gesellschaftspolitik *vorgänge Nr. 184* (Heft 4/2008) hat den Schwerpunkt „Der gläserne Mensch“.

BigBrotherAwards

10. Verleihung der BigBrotherAwards 2009: Die »Oscars für Überwachung« (Le Monde) werden im Rahmen einer großen Gala am Freitag, 16. Oktober 2009 von 18 bis 20 Uhr im „Historischen Saal“ der Ravensberger Spinnerei in Bielefeld verliehen.

Nominierungen für die Awards 2009 werden noch bis zum 15. Juli 2009 entgegengenommen: *http://www.bigbrotherawards.de/nominate*

AK Vorratsdatenspeicherung

Obwohl der Europäische Gerichtshof die von schwarz-rot beschlossene EG-Richtlinie zur verdachtslosen Sammlung der Verbindungs- und Standortdaten der gesamten Bevölkerung (Vorratsdatenspeicherung) vorerst nicht für nichtig erklärt hat, bleibt der Arbeitskreis Vorratsdatenspeicherung als Initiator der Verfassungsbeschwerde optimistisch.

> *„Die Entscheidung betrifft nur die formale Frage der einschlägigen Rechtsgrundlage und hat die Verletzung der Grundrechte durch die anlasslose Erfassung des Telekommunikations- und Bewegungsverhaltens der gesamten Bevölkerung nicht zum Gegenstand“, sagt Werner Hülsmann FIfF-Vorstandsmitglied und aktiv im Arbeitskreis Vorratsdatenspeicherung. „Die 34.000 deutschen Beschwerdeführer/innen haben bereits beantragt, dass das Bundesverfassungsgericht den Europäischen Gerichtshof in einem zweiten Verfahren über die Vereinbarkeit der verdachtslosen Vorratsdatenspeicherung mit unseren Grundrechten entscheiden lässt.“*

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.

Das FIfF-Büro

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

Die aktuellen Bürozeiten entnehmen Sie bitte unseren Webseiten.

Bankverbindung:
Sparda Bank Hannover eG
Kontoverbindung: 92 79 29
BLZ 250 905 00
IBAN: DE05 2509 0500 0000 9279 29
BIC: GENODEF1S09

FIfF im Netz

Das ganze FIfF:
www.fiff.de

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 Abmeldung unter
http://lists.fiff.de/mailman/listinfo/cctv-L
Beiträge an: *cctv-L@lists.fiff.de*

Beirat

Michael Ahlmann (Bremen); **Peter Bittner** (Köln); **Dagmar Boedicker** (München)**; Prof. Dr. Wolfgang Coy** (Berlin); **Prof. Dr. Wolfgang Däubler** (Bremen); **Prof. Dr. Christiane Floyd** (Hamburg); **Prof. Dr. Klaus Fuchs-Kittowski** (Berlin); **Prof. Dr. Thomas Herrmann** (Dortmund); **Prof. Dr. Wolfgang Hesse** (Marburg); **Dr. Eva Hornecker** (Milton Keynes; UK); **Prof. Dr. Michael Grütz** (Konstanz); **Ulrich Klotz** (Frankfurt); **Prof. Dr. Klaus Köhler** (München); **Prof. Dr. Herbert Kubicek** (Bremen); **Prof. Dr. Klaus-Peter Löhr** (Berlin); **Dipl.-Ing. Werner Mühlmann** (Oppburg); **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. Dirk Siefkes** (Berlin); **Prof. Dr. Marie-Theres Tinnefeld** (München); **Dr. Gerhard Wohland** (Waldorfhäslach)

FIfF-Vorstand

- **Prof. Dr. Hans-Jörg Kreowski (Vorsitzender)** – Bremen
- **Stefan Hügel (stellv. Vorsitzender)** – München
- **Carsten Büttemeier** – Münster
- **Werner Hülsmann** – Konstanz
- **Prof. Dr. Dietrich Meyer-Ebrecht** – Aachen
- **Michael Riemer** – Memmelsdorf
- **Jens Rinne** – Kaiserslautern
- **Prof. Dr. Britta Schinzel** – Freiburg
- **Jakob Schröter** – Bremen
- **Prof. Dr. Joseph Weizenbaum †**
- **Joerg Zeltner** – Köln

Überregionale Arbeitskreise des FIfF

AK »Videoüberwachung und Bürgerrechte«
Peter Bittner,
peter@pbittner.de

AK »RUIN« (Rüstung und Informatik)
Kontakt über das FIfF-Büro Bremen

AK »Kampagne gegen Datensammelwut«
Werner Hülsmann,
werner@fiff.de

Regionalgruppen und regionale Ansprechpartner

Aachen
Prof. Dr.-Ing.
Dietrich Meyer-Ebrecht
Tel.: (0241) 8949 8959
dme@fiff.de

Berlin
Skander Morgenthaler
Richard-Sorge-Str.63
10249 Berlin
smorg@gmx.de

Bremen
Prof. Dr. Hans-Jörg Kreowski
Universität Bremen
FB Informatik/Mathematik
Postfach 330 440
28334 Bremen
Tel.: (0421) 218-2956
http://fiff.informatik.uni-bremen.de
fiff@informatik.uni-bremen.de

Darmstadt
Julia Stoll
Heinheimer Str. 29-31
64289 Darmstadt
Tel.: (06151) 71 21 81
julias@acm.org

Erlangen/Fürth/Nürnberg
Klaus Thielking-Riechert
Am Dummetsweiher 9
91056 Erlangen
klaus.thielking-riechert@nefkom.net

Freiburg
Prof. Dr. Britta Schinzel
Universität Freiburg
Institut für Informatik und Gesellschaft
Friedrichstr. 50
79098 Freiburg im Breisgau
Tel.: (0761) 203-4953
Fax: (0761) 203-4960
schinzel@modell.iig.uni-freiburg.de

Hamburg
Sebastian Jekutsch
22083 Hamburg
fiff-hh@fiff.de
Mailing-Liste: http://lists.fiff.de/mailman/listinfo/fiff-hh

Heilbronn
Michael Müller
Hochschule Heilbronn
Fakultät W1
Max-Planck-Straße 39
74081 Heilbronn
Tel.: (07131) 50 43 64
michael.mueller@hs-heilbronn.de

Jena
Prof. Dr. Eberhard Zehendner
Institut für Informatik
Friedrich-Schiller-Universität
07737 Jena
Tel.: (03641) 9463-85
Fax: (03641) 9463-72
nez@uni-jena.de

Kaiserslautern
Jens Rinne
67655 Kaiserslautern
rinne@fiff.de

Karlsruhe
Prof. Dr. Thomas Freytag
Paul-Ehrlich-Str. 24
76133 Karlsruhe
Tel.: (0721) 81 54 16 (p)
fiff@thomas-freytag.de

Koblenz
Dr. Michael Möhring
Uni Koblenz-Landau
Campus Koblenz
FB Informatik
Universitätsstraße 1
56070 Koblenz
Tel.: (0261) 287 2668
Fax: (0261) 287 100 2668
moeh@uni-koblenz.de

Konstanz
Werner Hülsmann
Obere Laube 48
78462 Konstanz
Tel.: (07531) 365 90 56
werner@fiff.de
Mailing-Liste: http://lists.fiff.de/mailman/listinfo/bodensee

Köln
Peter Bittner
Moltkestr. 49
50674 Köln
peter@pbittner.de

München
Bernd Rendenbach
Leerbichlallee 19
82031 Grünwald
Tel.: (089) 641 05 47
Bernd.Rendenbach@web.de
Mailing-Liste: majordomo@lists.lrz-muenchen.de

Münster
Carsten Büttemeier
Mindener Str. 22
48145 Münster
fiff@buettemeier.de

Paderborn
Harald Selke
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn
hase@uni-paderborn.de

Stuttgart
Kurt Jaeger
Mezgerstraße 34
70563 Stuttgart
Tel.: (0711) 870 13 09
0171 3101372
Fax: (0711) 5406 5984
pi@c0mplx.org

Ulm
Bernhard C. Witt
Reuttier Str. 15
89231 Neu-Ulm
bcw@bc-witt.de

Kopieren, ausfüllen und einsenden an:
FIFF e.V.
Goetheplatz 4
D-28203 Bremen
Fax: (0421) 33 65 92 56

Vielzweckschnipsel

Das möchte ich:

- ❑ aktives Mitglied des FIfF werden.
  Normale Mitgliedschaft mit Stimmrecht und Bezug der FIfF-Kommunikation. Der Mindestbeitrag ist für Verdienende **60 Euro** und für Studierende und Menschen in vergleichbarer Situation **15 Euro**. (Für Studierende ist das erste Jahr kostenlos.)
- ❑ förderndes Mitglied des FIfF werden.
  Mitgliedschaft ohne Stimmrecht, z.B. für Institutionen. Der Mindestjahresbeitrag beträgt **60 Euro**.
- ❑ die FIfF-Kommunikation zum Preis von **20 Euro** jährlich frei Haus abonnieren.
- ❑ dem FIfF etwas spenden.
- ❑ Ich überweise den Betrag auf das **Konto 92 79 29** bei der Sparda Bank Hannover eG, BLZ **250 905 00** oder nutze die internationale Kontonummer **IBAN: DE05 2509 0500 0000 9279 29** , **BIC: GENODEF1S09.**
- ❑ Der Mitglieds- bzw. Abobeitrag soll per Lastschriftverfahren von meinem Konto abgebucht werden.

Datum _____ Unterschrift _____

Einzugsermächtigung

Hiermit ermächtige ich das FIfF widerruflich, meinen Mitgliedsbeitrag durch Lastschrift einzuziehen. Wenn das Konto keine Deckung aufweist, besteht keine Verpflichtung des Geldinstituts, die Lastschrift auszuführen.

Name: _____

Jahresbeitrag: _____ EUR, erstmals: _____

Konto-Nr.: _____ BLZ: _____

Geldinstitut: _____

Datum _____ Unterschrift _____

Wir werden ihre Daten nach §28 BDSG nur für eigene Zwecke verarbeiten und keinem Dritten zugänglich machen.

Die/der bin ich:

Name: _____

Straße: _____

Wohnort: _____

ggf. Mitgliedsnummer: _____

Telefon (privat): _____ (Arbeit): _____

Ich möchte als Mitglied per E-Mail über Aktionen, Beschlüsse u.ä. informiert werden; meine E-Mail:

_____

Was sonst noch so geht:

- ❑ Ich möchte mehr über das FIfF wissen, bitte schickt mir:

  _____
- ❑ Ich möchte gegen Rechnung und zuzüglich Portokosten bestellen:

  _____

  _____
- ❑ Ich möchte das FIfF über einen Artikel oder ein Buch informieren: _____

  _____
- ❑ Ich möchte zur FIfF-Kommunikation beitragen mit
  - ❑ einem Manuskript zur Veröffentlichung
  - ❑ einer Anregung (siehe unten)

  _____

  _____
- ❑ Der Vielzweckschnipsel ist nichts für mich. Ich möchte einen richtigen Brief schreiben.

Die FIfF-Kommunikation bittet um Beiträge!

Die FIfF-Kommunikation lebt von der aktiven Mitarbeit ihrer Leserinnen und Leser! Interessante Artikel sowie Fotos und Zeichnungen zur Illustration (mit Quellenangaben und Nachdruckgenehmigung) sind immer herzlich willkommen. Die Bearbeitung wird erleichtert, wenn Beiträge elektronisch und zusätzlich auf Papier der Redaktion zugehen. Die Redaktion behält sich Kürzungen und Titeländerungen vor.

Geplante Themenschwerpunkte der nächsten Hefte:

Heft 2/2009
„Kritische Informatik"
Carsten Büttemeier, Stefan Hügel, Ralf E. Streibl u.a.
Redaktionsschluss: 4.5.2009

Heft 3/2009
„Der Computer und sein Mensch"
Maike Hecht, Jens-Holger Streck, Ralf E. Streibl u.a.
Redaktionsschluss: 4.8.2009

Heft 4/2009
„Herausforderungen"
H.-J. Kreowski, R. E. Streibl u.a.
Redaktionsschluss: 4.11.2009

Die Termine für den Redaktionsschluss gelten für aktuelle Beiträge. Schwerpunktartikel haben einen früheren Termin

Artikel zu aktuellen Themen sind immer willkommen.
Bitte setzen Sie sich mit der Redaktion in Verbindung:

redaktion@fiff.de oder über die Geschäftsstelle des FIfF e.V.

Das FIfF-Büro

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

Bürozeiten:
Bitte entnehmen Sie diese unserer Webseite *http://www.fiff.de.*

Wichtiger Hinweis:

Postvertriebsstücke wie die FIfF-Kommunikation werden von der Post auch auf Antrag nicht nachgesandt; daher bitten wir alle Mitglieder und Abonnenten, dem FIfF-Büro jede Adressänderung rechtzeitig bekannt zu geben!

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	Carsten Büttemeier (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Jens-Holger Streck, Ralf E. Streibl
Schwerpunktredaktion	Dietrich Meyer-Ebrecht, Stefan Hügel, Hans-Jörg Kreowski, Ralf E. Streibl
V.i.S.d.P.	Ralf E. Streibl
FIfF-Überall	Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an *hubert@mtsf.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 *sj@fiff.de*
Lesen, SchlussFIfF	Beiträge für diese Rubriken bitte per E-Mail an *res@fiff.de*
Fachschaften	Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de*
Layout	Berthold Schroeder
Titelbild	Caro von Totth
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.

Schluss FIfF

Kurt Tucholsky

Wofür?

Gleich Kindern laßt ihr euch betrügen,
Bis ihr zu spät erkennt, o weh! –
Die Wacht am Rhein wird nicht genügen,
Der schlimmste Feind steht an der Spree.
Georg Herwegh

Am 1. August habe ich hier auseinandergesetzt, wofür zwölf Millionen Menschen in vier Blutjahren ihr Leben gelassen haben. Die wenigen Zeilen haben genügt, auf einer Tagung des Reichsbanners einen Teil seiner Führer zu einer feierlichen Bannbulle gegen ›*Das Andere Deutschland*‹ zu veranlassen. Nachdem der Streit nun eine Weile hin- und hergegangen ist, scheint es mir, als seinem Veranlasser, richtig, ein paar Worte dazu zu sagen.

Der moderne Krieg hat wirtschaftliche Ursachen. Die Möglichkeit, ihn vorzubereiten und auf ein Signal Ackergräben mit Schlachtopfern zu füllen, ist nur gegeben, wenn diese Tätigkeit des Mordens vorher durch beharrliche Bearbeitung der Massen als etwas Sittliches hingestellt wird. Der Krieg ist aber unter allen Umständen tief unsittlich. Es ist nicht wahr, daß in unsrer Epoche und insbesondere in der Schande von 1914 irgend ein Volk Haus und Hof gegen fremde Angreifer verteidigt hat. Zum Überfall gehört einer, der überfällt, und tatsächlich ist dieses aus dem Leben des Individuums entliehene Bild für den Zusammenprall der Staaten vollkommen unzutreffend.

Wer Zeit und Lust hat, mag einmal einen gebundenen Jahrgang seines Morgenblattes aus dem Jahr 1914 durchblättern. Im April, im Mai, Anfang Juni wußte auf allen Seiten kein Redakteur und kein Leser, was zwei Monate später geschehen würde; präpariert war nur die Massenbereitschaft, sofort anzutreten, wenns klingelte. Sie sind angetreten, ohne mehr von den Ursachen des Alarms zu wissen, als was ihnen die Telegrafenagenturen der Regierungen vorzusetzen beliebten. Wir wissen heute, daß damals auf allen Seiten schändlich gelogen worden ist.

Um eine Wiederholung zu vermeiden, gilt es also, den sittlichen Unterbau einer unsittlichen Idee zu zerstören. Dieser Unterbau heißt: Es ist süß und ehrenvoll fürs Vaterland zu sterben.

Was die Süße anbetrifft, so wird ja auch der verlogenste Kriegshetzer nicht mehr wagen (wenn es nicht gerade ein Militärpfarrer ist), von diesem Bonbon des Patriotismus zu sprechen. Wer ihn einmal geschmeckt hat, wer am nebelgrauen Wintermorgen Verwundete mit blutdurchtränkten Verbänden aus einem Wäldchen hat hinken sehen, wer den Zerschossenen, dem die Eingeweide heraushingen, hat brüllen hören: »Schießt mich tot, schießt mich tot!« – wer das gesehen und gehört hat, der weiß, wie süß es ist.

Ist es ehrenvoll? Nein.

Die Ehre wohnt einer Sache nicht inne, sie wird ihr erst beigelegt. Wenn die überwiegende Mehrheit eines Staates soweit aufgeklärt und erzogen ist, daß sie den Massenmord von Einzelmord nicht mehr unterscheidet, so ist es mit der Ehrung des Soldaten vorbei. Es bleibt das tiefe Bedauern für die Gefallenen, Mitleid mit den Hinterbliebenen, Pflicht, für diese Hinterbliebenen zu sorgen (dieser Pflicht kommt der kriegerische moderne Staat nicht nach –), und es bleibt die tiefste Verachtung für einen wirtschaftlichen Vorgang, der sich mit den Zutaten des Films behängt, um sich populär zu machen, und der seine Bilanz im stillen zieht. Sie ist nicht mit roter Tinte geschrieben.

aus: Ignaz Wrobel (Kurt Tucholsky), Das Andere Deutschland, 24.12.1925

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