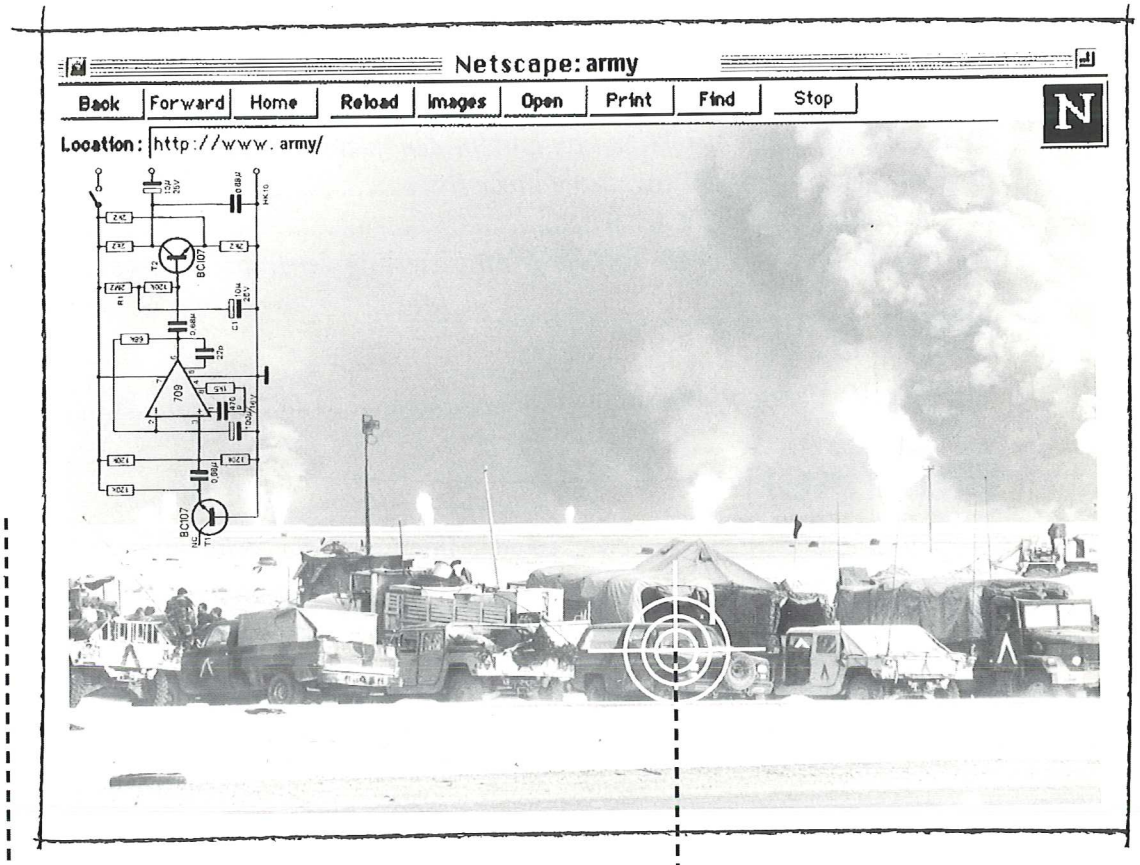
F.J.F.Kommunikation
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.
16. Jahrgang 1999 • Einzelpreis: 6 DM
G 7625
4/99
Dezember 1999

HIGH TECH, KRIEG UND FRIEDEN



ISSN 0938-3476

Inhalt

Editorial

Aktuell

Schwerpunkt »High-Tech, Krieg und Frieden«

FIfF e.V.

Rubriken

High-Tech, Krieg und Frieden

Die militärische Bedeutung der Informationstechnik hat eine neue Dimension erreicht. In den 50er Jahren hatte der Computer Funktionen der strategischen Kontrolle. Ende der 60er Jahre erwuchsen daraus erste Einsätze von Informationstechnik auf dem Schlachtfeld. Mit dem Rüstungsschub der 80er Jahre wurde Informationstechnik endgültig zum integralen Bestandteil von Waffensystemen. Der Golfkrieg machte diese hohe Bedeutung der Informationstechnik für High-Tech-Kriege der breiten Öffentlichkeit ebenso bewußt wie der Fachdisziplin. Der Computer in der »intelligenten« · Waffe wurde zum Medienspektakel, Informationstechnik zum Publicity-Vehikel, mit dem sich blutiges Kriegsgemetzel auf ein visuelles Schauspiel reduzieren ließ.

In kriegerischen Konflikten unter Beteiligung von Hochtechnologie-Nationen – andere Staaten eifern dem mittlerweile nach – hat die Informationstechnik heute eine Doppelfunktion. Informationstechnologisch gestützte Waffensysteme erlauben Kriegshandlungen in bislang unbekannter Intensität und Zerstörungswirkung. Zugleich dient die Präzision der Waffensysteme dazu, Begriffe wie »Präzisionsbombardements« und »chirurgische Schläge« glaubhaft zu machen. Die durch Informationstechnik mögliche massive Kampfwertsteigerung bei gleichzeitig verbesserter medialer Aussenwirkung wird unter dem Begriff Information Warfare von den Militärs konzeptionell gebündelt und ausgebaut.

Dieses Paradoxon eines durch Informationstechnik gleichzeitig tödlicheren, aber unblutigeren Krieges konnten die Militärs weitgehend ungestört entwikkeln, sieht man einmal von Arbeiten vor allem aus dem Kontext des FIfF ab[1]. Unabhängig von ihrer realen Bedeutung wurde auch im Kosovo-Krieg der Informationstechnikeinsatz zu einem dominanten Thema. Dies war der Anlass für das FIfF, erneut ein Schwerpunktheft dem militärischen Einsatz der Informationstechnik zu widmen.

Der Kosovo-Krieg als Anlass macht eine Auseinandersetzung mit der Funktion von Information Warfare einerseits und den politischen Hintergründen andererseits erforderlich. Von unterschiedlichen Ausgangspunkten her analysieren Ralf Bendrath und Ingo Ruhmann in ihren Beiträgen den Einsatz von Information Warfare-Elementen im Kosovo, aber auch zugleich deren dabei sichtbar gewordenen Grenzen. Fazit beider ist, dass die mediale Darstellung des Informationstechnikeinsatzes ein weit erfolgreiches Bild gezeichnet hat, als die Analyse der Kriegshandlungen zeigt.

Medien als Werkzeug von Information Warfare werden dann zu wirkungsvollen Mitteln im Krieg, wenn das Wissen um die Konfliktursachen und –hintergründe nicht allzu weit verbreitet ist. Diese Hintergründe trägt der umfangreiche Beitrag von Hans-Georg Ehrhart und Matthias Z. Karádi vom Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg zusammen. Aufgezeigt werden darin auch die Optionen einer politischen Konfliktbewältigung.

Eine nüchterne Sachdarstellung dient der Analyse, sie gibt jedoch selten etwas von der emotionsgeladenen Auseinandersetzung wieder, die dieser Krieg ausgelöst hat und die auch im FIfF geführt wurde. Einen Kontrapunkt stellt deshalb der Beitrag von Eckard Spoo dar, der die subjektiven Reiseeindrücke aus einigen Städten Jugoslawiens während des Krieges und die unmittelbaren Kriegsfolgen für die Zivilbevölkerung schildert.

Abhängig von den jeweiligen Eigeninteressen lassen sich verschiedenartige Schlussfolgerungen ziehen. Aus der von den USA vorgeführten militärischen Schlagkraft folgte in Europa die Debatte, neue Rüstungsvorhaben anzustoßen. Karen Jaehrling untersucht die Maßnahmen, die die Bundesregierung zur konzeptionellen Begleitung der Umgestaltung der Bundeswehr ergriffen hat.

Auch jenseits von Kriegshandlungen wird Information Warfare zu einem Gefährungsszenario der zivilen Informationsgesellschaft, das unterschiedliche Reaktionen hervorruft. In einem Beitrag zu Cyberterrorismus geht es um die Frage der zivilen oder militärischen Antwort auf die technisch verursachten Risiken der Informationsgesellschaft.

Am Beispiel der »Künstlichen Intelligenz« lässt sich aufzeigen, in welchem Umfang Informatik als Wissenschaft für Militärs von Interesse ist. Gleichzeitig macht diese Disziplin auch deutlich, in welcher Weise die Informatik auch zu friedlichen Zwecken genutzt werden kann. Die Beiträge von Leonie Dreschler-Fischer und Marc Hermann stellen die Probleme der Minenräumung vor und beschreiben ein KI-gestütztes Verfahren zur Bekämpfung der Landminenplage.

Ute Bernhardt
Leonie Dreschler-Fischer
Ingo Ruhmann

1 J. Bickenbach; R. Keil-Slawik; M. Löwe; R. Wilhelm (Hg.): Militarisierte Informatik. Schriftenreihe Wissenschaft und Frieden 5, Marburg, 1985; Ute Bernhardt, Ingo Ruhmann: Ein sauberer Tod. Informatik und Krieg; Marburg, 1991; Ralf Klischewski, Ingo Ruhmann: Ansatzpunkte zur Entwicklung von Methoden für die Analyse und Bewertung militärisch relevanter Forschung und Entwicklung im Bereich Informations- und Kommunikationstechnologie; Gutachten für das Büro für Technikfolgenabschätzung des Deutschen Bundestages, Bonn, März, 1995; Ute Bernhardt; Ingo Ruhmann: Der digitale Feldherrnhügel. Military Systems: Informationstechnik für Führung und Kontrolle. in: Wissenschaft und Frieden, Heft 1/97, Dossier Nr. 24, S. 1-16

Aktuell

Halbgares Fertigmenü

Aktionsplan der Bundesregierung Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts

Mitte September legte die rot-grüne Bundesregierung mit dem Aktionsprogramm Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts (http://www.iid.de/aktionen/aktionsprogramm/deckblatt.html) einen Plan vor, der Deutschland in eine europaweite Spitzenposition in der Informationsgesellschaft bringen soll. Erklärtes Ziel von Bundesforschungsministerin Edelgard Bulmahn und dem Parlamentarischen Staatssekretär im Bundeswirtschaftsministerium Siegmar Mosdorf ist es, damit nachhaltig neue Beschäftigungspotentiale zu erschließen. Vollmundig priesen die beiden den übergreifenden Gesamtentwurf ihrer Politik, der die Aktivitäten der Bundesregierung für den Aufbruch in das Informationszeitalter bündele.

Bereits in seiner Regierungserklärung hatte Bundeskanzler Schröder vor knapp einem Jahr die Neuen Medien und die IT-Wirtschaft als zentrales Politikfeld bezeichnet – immerhin gehen Schätzungen davon aus, daß die Informations- und Kommunikationsbranche mit einem Umsatz von 206 Milliarden Mark in diesem Jahr erstmals den Automobilmarkt übertrifft. Ein Jahr lang ließen sich Bundeswirtschafts- und Bundesforschungsministerium Zeit, bis sie den Aktionsplan jetzt vorstellten. Im wesentlichen flossen in die Vorgabe des Ministeriums, dem von Siegmar Mosdorf noch zu Oppositionszeiten bei der Friedrich-Ebert-Stiftung vorgelegten Masterplan die Vorstellungen des Zentralverbandes Elektroindustrie (ZVEI) sowie des DGB ein.

Der Plan nennt einige Erfolgskennzahlen, an denen er sich messen lassen will. So geht er von zusätzlichen 250.000 Arbeitsplätzen allein in der Multimedia-Branche bis zum Jahr 2001 aus. Die Zahl, die auf einer Studie des Beratungsunternehmens Booz, Allen & Hamilton aus dem Jahr 1998 beruht, ist jedoch mit Vorsicht zu genießen. Der Schwerpunkt der Studie lag nicht auf Beschäftigungseffekten, sondern auf der wirtschaftlichen Entwicklung in der Informationstechnik. Die Zahlenbasis, auf der die Schätzungen beruhen, stammt aus den Jahren 1995 und 1996. Angesichts der schnellwachsenden Internetwirtschaft kann dies keine Basis für Prognosen darstellen. Gegenprognosen lassen sich schnell finden: Eine aktuelle Studie des Bonner Forschungsinstitutes Empirica rechnet gar mit einem Verlust von über 100.000 Arbeitsplätzen in Deutschland durch die Einsparpotentiale im elektronischen Geschäftsverkehr in den nächsten zwei Jahren.

Nach einem Jahr gespickt mit politischen Enttäuschungen will Rot-Grün jetzt unbedingt Positives präsentieren. Dabei hat sie ein Dilemma: Die Schaffung von Arbeitsplätzen steht an oberster Stelle der Regierungspolitik. Mit ihr positive Schlagzeilen zu erreichen, ist jedoch fast ein Ding der Unmöglichkeit. Bereits die Enquete-Komission Zukunft der Medien ging mit Prognosen vorsichtiger um. In ihrem Schlußbericht stellte sie fest, dass die Frage nach den Beschäftigungseffekten die am schwierigsten zu beantwortende und zugleich brisanteste ist. In einem Vergleich mehrerer Studien stellte die Komission fest, dass sich positive Arbeitsplatzeffekte herauslesen lassen. Diese greifen jedoch erst mittelfristig und reichen nicht aus um den rückläufigen gesamtwirtschaftlichen Beschäftigungstrend zu kompensieren.

Reinhard Keil-Slawik vom Forum Informatikerinnen für Frieden und gesellschaftliche Verantwortung (FIfF) kritisiert, dass die IT im Aktionsprogramm als arbeitsplätzeschaffender Wohlstandsmotor verkauft wird. Er fordert, dass die Bundesregierung jetzt hingegen den Dialog über die Ziele der Informationsgesellschaft beginnen solle. So mache beispielsweise Open-Source deutlich, dass auch die Fördermethoden auf dem Prüfstand stehen müssen. Keil-Slawik: Das Umdenkungsvermögen der rot-grünen Bundesregierung wird sich daran ablesen lassen, ob und wie sie auf neue Ansätze wie Open-Source eingeht. Tatsächlich können es sich freie Entwickler kaum leisten, zu Besprechungen in Fördergremien anreisen zu müssen. Für die entstehenden Reisekosten könnten sie hingegen locker ihren PC mit einer 10 GB-Festplatte aufrüsten. Zudem arbeiten freie Entwickler in einem Organisationsumfeld, das nicht zum herkömmlichen Förderinstrumentarium passt. Allein die Suche nach einem geeigneten Projektträger kann daher unverhältnismäßig viel Zeit beanspruchen.

In Bonn-Berliner Ministerialkreisen kursiert derzeit eine interne Stellungnahme des SPD-Abgeordneten Jörg Tauss zum Aktionsplan. Darin bemängelt Tauss, dass der Plan keine profunde Schwachstellenanalyse enthalte. Das größte Defizit sei die fehlende Internet-Politik von deutscher Seite. So spielen deutsche Vorstellungen bei der Formulierung von Standards in der Regel keine Rolle. Wie auch? Deutsche Firmen scheuen Reisekosten und Personalauf-

wand – und sind in den internationalen Internetstandardisierungsgremien W3C und IETF kaum vertreten. Auch, so Tauss, sei die Dominanz der Hard- und Softwarehersteller kein Thema – als hätte die deutsche Politik vor US-amerikanischen Herstellermonopolen bereits kapituliert.

Dabei hätte es durchaus anders kommen können, doch Erkenntnisse der bündnisgrünen Bundestagsfraktion, wie sie in einem Sondervotum zum Schlußbericht der Enquete-Kommission Zukunft der Medien 1998 festgehalten wurden, wurden im Aktionsplan nicht berücksichtigt: So hatte die bündnisgrüne Arbeitsgruppe unter dem Punkt Standards und Marktmacht die Empfehlung ausgesprochen, dass Fördermittel auch dazu genutzt werden sollten, offene Standards weiterzuentwickeln und deren Einsatz im Datenaustausch zwischen Behörden sowie zwischen Behörden und Unternehmen zu verstärken. Angesichts der marktbeherrschenden Stellung von Microsoft forderten die Bündnisgrünen damals, wirksame Maßnahmen gegen Monopolbildungen zu ergreifen. Beim Datenaustausch sollten beispielsweise Behörden die Nutzung proprietärer Formate vermindern und bei der Beschaffung zur Erhaltung von Anbietervielfalt alternative Anbieter berücksichtigen. Nicht nur dass der Aktionsplan keine kritischen Anmerkungen zu Monopolen in der IT-Wirtschaft findet, er selbst ist auf der BMWI-Homepage nur im Word- bzw. PDF-Format (http://www.iid.de/aktionen/aktionsprogramm/deckblatt.html) zu erhalten.

Für den CSU-Mann Martin Mayer ist das völlig unverständlich: Der Bundestagsabgeordnete forderte in einem Beitrag der VDI-Nachrichten ein europäisches Gegengewicht gegen die Quasi-Monopolstellungen amerikanischer Unternehmen. Richtungsweisende Startprojekte im IT-Bereich müßten ähnlich wie bereits in der Luftfahrtindustrie die Abhängigkeit von weltweiten Monopolisten außerhalb Europas brechen. Mayer kann sich vorstellen, dass durch staatliche Beschaffungsmaßnah-

Kommentar des FifF zum Aktionsprogramm der Bundesregierung

Das Aktionsprogramm kann nicht für sich in Anspruch nehmen, ein besonders inspiriertes Programm zu sein. Die Bundesregierung hat sich weitgehend an den aus Kohl-Zeiten stammenden langfristigen Haushaltsfestlegungen orientiert. Das Aktionsprogramm ist damit in weiten Teilen nicht mehr als eine Bestandsaufnahme statt einer Zukunftsaussage.

Ein wenig Spielraum für die Bundesregierung sollte durch die »Zukunftsmilliarde« geschaffen werden – eine Milliarde für innovative Ideen und rot-grüne Akzente jenseits eingefahrener Denk- und Fördermuster. Wo in anderen Bereichen noch zaghafte Ansätze erkennbar sind, herrscht in der IT jedoch offenbar weitgehende Innovationsmüdigkeit. Neue Ansätze der IT-Förderung sind kaum erkennbar.

Wie die alte Bundesregierung oder die Bundestagsenquete »Zukunft der Medien in Deutschland – Deutschlands Weg in die Informationsgesellschaft« der letzten Legislaturperiode, deren Vorsitzender Mosdorf sich heute als parlamentarischer Staatssekretär im Wirtschaftministerium um das Internet kümmert, wird die IT im Aktionsprogramm als Arbeitsplätze schaffender Wohlstandsmotor verkauft. Der Unterschied zur alten Bundesregierung schimmert leider nur am Rande durch, wo die rot-grüne Bundesregierung ihr Interesse bekundet »Internet Politik«, aktiv zu gestalten.

Solche zaghaften Ansätze zu neuen Zielen bei der Gestaltung der Informationsgesellschaft können nicht überzeugen. Damit bleibt als Chance nur der Ablauf des vom früheren Forschungsminister Rüttgers aufgelegten IT-Förderprogramms , das 2001 ausläuft. Dies ist für die rot-grüne Bundesregierung die letzen Chance für einen großen gestalterischen Neuanfang. Die Weichen für ein neues IT-Forschungskonzept müssen jetzt gestellt werden.

Die Bundesregierung muss jetzt ernst machen und den Dialog über die Ziele der Informationsgesellschaft beginnen. Neue tragfähige Förderziele entstehen nur, wenn unterschiedliche gesellschaftliche Gruppen in den Dialog einbezogen werden, neben der Wirtschaft eben auch die wissenschaftliche Community, Verbände und Initativen.

Neben den Zielen macht das Beispiel »Open Source« deutlich, daß auch die Fördermethoden auf dem Prüfstand stehen müssen, die hier nicht mehr greifen. Neben den etablierten Förderschienen hat sich mit Open Source ein neuer Ansatz erfolgreich etabliert, der der europäischen Softwarebranche eine neue Perspektive eröffnet. Das Umdenkungsvermögen der rot-grünen Bundesregierung wird sich daran ablesen lassen, ob und wie sie auf neue Ansätze wie diese eingeht.

Reinhard Keil-Slawik

men positive Entwicklungen wie Linux unterstützt werden könnten. Für die effektivste finanzielle Förderung hält Mayer die spürbare Senkung von Steuersätzen. So könne Unternehmen flexibles Kapital an die Hand gegeben werden. Doch das ist eine vergleichsweise unpräzise Forderung, die sich kaum in eine zielgerichtete Förderung umwandeln lassen könnte. In den USA kündigte Al Gore bereits im Januar an, dass die US-Regierung Unternehmen, die verstärkt in Forschung und Entwicklung investieren, einen 20 prozentigen Steuernachlaß in der Höhe von 2,5 Milliarden US-Dollar im Zeitraum vom 30. Juni 1999 bis zum 30. Juni 2000 gewährt. Ziel: Der Nachlaß soll forschungsintensiven Industrien in der Informations-, Kommunikations- und Elektronikbranche unterstützen. Der große Anteil der Entwicklungsgelder wird direkt in die Gehälter der Angestellten investiert. Zugleich setzt die US-Regierung darauf, dass durch das Investment in Forschung und Entwicklung Telekommunikationsinfrastrukturen weiterentwickelt werden.

Anstatt zwischen kurzfristigen Aktionen zur Beseitigung der Defizite, mittelfristigen Zielmarken und langfristigen Visionen zu unterscheiden, stehen im Entwurf die Aktionen mehr oder minder unabhängig hintereinander. Der Aktionsplan ist ein Copy&Paste-Konglomerat aus dem jährlich veröffentlichten Faktenbericht des BMBF, den Dossiers einzelner Ministeriumsreferate sowie Quartalsberichten verschiedener Verbände zu verschiedenen IT-Themen. Zum einen werden darin zahlreiche Förderprogramme beschrieben, die bereits seit Jahren laufen. Auch werden Preise wie der Internetpreis, der im nächsten Jahr anläßlich der Cebit erstmals verliehen werden soll oder Wettbewerbe wie der des Bundeswirtschaftsministeriums namens FABNET für Telekooperationskonzepte von virtuellen mittelständigen Unternehmen, sowie große Förderprogramme des Bundesforschungsministeriums beispielsweise zur Entwicklung von neuartigen breitbandigen Mobilkommunikationsthemen in dem Bericht vorgestellt. Zum anderen werden rechtliche Weichenstellungen in den Bereichen Urheberrecht oder Arbeits-Sozialrecht angekündigt, die inhaltlich wenig Konkretes liefern. Interessant ist, daß trotz proklamierter Nähe zum Bündnis für Bildung ein eindeutiger Schwerpunkt der Fördermittel im Hard- und Softwarebereich liegt –vergleichsweise wenig wird in Qualifizierungsmaßnahmen investiert.

Trotz Eichelscher Sparpläne hatte sich das Forschungsministerium allerdings eine Zukunftsmilliarde gesichert, mit der innovative Ideen und rot-grüne Akzente jenseits eingefahrener Denk- und Fördermuster verwirklicht werden sollten. Doch im wesentlichen wird die IT-Politik der alten Bundesregierung fortgeführt. Nicht einmal das noch in der Koalitionsvereinbarung angekündigte Informationsfreiheitsgesetz findet mit einem einzigen Wort Erwähnung. Ganz anders im Ausland: In den USA beispielsweise rief Al Gore kurz nach der Machtübernahme 1993 eine Agenda für die sogenannte National Information Infrastructure (http://nii.nist.gov/) auf den Plan. Dabei handelte es sich um ein integriertes Gesamtkonzept unter anderem für verstärkten Wettbewerb auf dem Telekommunikationsmarkt, einen erweiterten Zugang zu Regierungsinformationen und das Bildungssystem. In Großbritannien stellte das Blair-Kabinett jetzt einen Aktionsplan E-Commerce

(http://www.cabinet-office.gov.uk/innovation/1999/ecommerce/ec_body.pdf), vor,

der anders als das deutsche Papier eine Zeitleiste mit konkreten Zielvorgaben, Verantwortlichkeiten und Terminen bietet. Neue Ansätze der IT-Förderung sind kaum erkennbar, konstatiert Reinhard Keil-Slawik. Aus Ministerialkreisen ist entschuldigend zu hören, dass dies am engen Zeitplan liege, den Siegmar Mosdorf vorgegeben hatte. Mosdorf hatte kurzfristig die Verabschiedung des Plans um einen Monat vorverschoben – damit seine Präsentation auf den 50. Geburtstag der Bundesrepublik fällt. Ein Umstand, den die im allgemeinen sehr wohlgesonnene Presse aber schlicht ignorierte.

Seit Jahren fordern Verbände und Fachleute aus den Bundestagsfraktionen einen Koordinator für die Rahmenbedingungen der Informationsgesellschaft. Er sollte im Kanzleramt sitzen und auch als deutscher Ansprechpartner für die EU-Kommission fungieren. Zwar präsentierte sich Siegmar Mosdorf jüngst gegenüber Focus als Internetbeauftragter der Bundesregierung und damit einflussreichster Politiker in Berlin, was das neue Medium angeht. Er hat jedoch im Bundeswirtschaftsministerium nur Zugriff auf zehn Prozent der einschlägigen Fördermittel. Denn noch immer bestimmt das Bundesforschungsministerium in Bonn, was mit dem Löwenanteil der Haushaltsmittel geschieht. Die persönlichen Interessen von Bundesforschungsministerin Edelgard Bulmahn und ihrem parlamentarischen Staatssekretär Catenhusen liegen jedoch auf Bildung sowie der Gen- und Biotechnologie.

Jörg Tauss hat Anfang September über die AG Kultur und Medien einen Antrag eingebracht, der die Einrichtung einer Internet-Agentur vorsieht, die mit erheblichem wissenschaftlichen Sachverstand einschließlich administrativer Möglichkeiten ausgestattet sein soll. Sie soll wissenschaftliche Studien vergeben und einen internationalen Kongress zu Standards im Internet im Jahre 2001 vorbereiten. Es ist der Bundesrepublik Deutschland bisher nicht gelungen, auch nur eine dieser bedeutenden Veranstaltungen der Internet-Society nach Deutschland zu bekommen und entsprechende Impulse im nationalen Interesse zu setzen, begründet Tauss seine Forderung, die einhellig von der SPD- und Grünen-Bundestagsfraktion unterstützt wird. In einem ersten Vorgespräch bügelten Mosdorf und Catenhusen den Plan allerdings ab. Kein Wort davon steht im Aktionsprogramm.

Zeitleiste für's Politik-Benchmarking

Auf 150 Seiten listet der Aktionsplan der rot-grünen Bundesregierung teilweise minutiös auf, welche Ziele wann erreicht werden sollen – allerdings ohne chronologische Übersicht. Doch wenn Projekte und Zielvorgaben des deutschen Aktionsplanes mit einer konkreten Zeitnennung auf eine Zeitleiste gesetzt werden, passiert vor den nächsten Bundestagswahlen im Jahr 2002 wenig. Konkrete Versprechungen wie die Schaffung von 350.000 neuen Arbeitsplätzen sowie 40.000 Ausbildungsplätzen in den neuen IT-Berufen sind erst für das Jahr 2003 terminiert. Vor den Bundestagswahlen gibt es allein einen Benchmark: Die Anzahl der Multimediafirmen soll sich von heute 1.500 auf 3.000 im Jahr 2001 verdoppeln. Unglaublich, aber wahr: Die IT-Verbände ließen sich nur unwillig auf die Nennung konkreter Zahlen ein. Selbst zu so einem lächerlichen Betrag wie den 40.000 Ausbildungsplätzen wollte sich

die Branche anfangs nicht bekennen, weiß Thomas Michel, Geschäftsführer der Dienstleistungsgesellschaft für Informatik im Wissenschaftszentrum Bonn, der unter anderem den Europäischen Internetführerschein betreut. Michel: Ich bin mir sicher, daß in der Branche weitaus mehr Ausbildungsplätze geschaffen werden.

Vorhaben ohne konkrete Nennung des Zeitrahmens – wie zum Beispiel in den nächsten Jahren – beziehungsweise bereits in diesem Jahr abgelaufene Projekte wurden in der Zeitleiste nicht berücksichtigt.

Stand 1999

- 9 Prozent Internetnutzer
- 800.000 Telearbeitsplätze
- 1500 Multimedia-Firmen
- bei Unternehmensgründungen liegt der Frauenanteil bei 30 Prozent
- Höchstleistungrechner am Leibniz-Rechenzentrum in München mit einer Leistung über 1 TeraFlop eingerichtet – 60 Millionen Mark
- Oktober: Start der Aktion Frauen ans Netz (http://frauen-ans-netz.de)
- Oktober: Start der Aktion zur Erhöhung des Frauananteils an ingenieurwissenschaftlichen und Informatikstudiengängen, z.B. Ada Lovelace
- Oktober: Zwischenbericht Projekt Familienbezogene Gestaltung von Telearbeit
- Dezember: Anpassen der Kernvorschriften der Vergaberegeln an die neue Möglichkeiten elektronischer Vergabe, damit öffentliche Auftraggber elektronische Ausschreibungsverfahren nutzen können.
- Dezember: Sensibilisierungsbericht zu kritischen Infrastrukturen liegt vor
- Dezember: unbefristete Verlängerung des WTO-Moratoriums für die (Nicht-)Erhebung von Zöllen für auf elektronischem Weg erbrachte Leistungen

2000

- Januar: elektronische Einkommenssteuererklärung wird im Bereich der Finanzverwaltung breit eingeführt; sukzessive Ausdehnung auf Umsatzsteuervoranmeldung und Lohnsteueranmeldung
- Januar: Regulierungsbehörde für Telekommunikation und Post vergibt Lizenzen für UMTS (Universal Mobile Telecommunication System)
- Internet-Preis von Bundeswirtschaftsministerium und Wirtschaft wird anläßlich der Cebit erstmals verliehen
- März: Abschlußbericht Projekt Familienbezogene Gestaltung von Telearbeit
- Frühjahr: Deutsches Forschungsnetz (DFN) erreicht Geschwindigkeiten im Gigabitbereich
- bis Juli: Erste Ergebnisse des Lenkungsausschusses der Initiative Digitaler Rundfunk
- Sommer: Bundesregierung legt IT-Strategie für die Informationsdienstleistungen der Bundesverwaltung vor; IuK-Technologien werden breitenwirksam in der öffentlichen Verwaltung eingesetzt
- Angebote und Vertragsabschlüsse können im öffentlichen Auftragswesen elektronisch abgewickelt werden; Ergebnisse von Pilotprojekten liegen im 1. Halbjahr vor
- Herbst: IT-Verfahren der Bundesanstalt für Arbeit für die Geschäftsprozesse Arbeitsvermittlung und Arbeitslosengeld bzw. Arbeitslosenhilfe ist einsatzbereit
- BMWi-Ausschreibung Sichere und verläßliche Transaktionen in offenen Kommunikationsnetzen (VERNET) - die 10 besten Projektideen werden gefördert

2001

- Alle Schulen, Aus- und Weiterbildungsstätten sind mit multimediafähigem PC und Internetanschlüssen ausgestattet
- 3000 Multimedia-Firmen
- Start des BMWi-Wettbewerbs FAB-NET für Telekooperationskonzepte von virtuellen mittelständischen Unternehmen
- Sommer: Fördermittel für die 24 regionalen Kompetenzzentren für den elektronischen Geschäftsverkehr laufen aus (seit 1998)
- Großbritannien: Auch hier Verdoppelung der Anzahl von KMUs im IuK-Bereich

2002

Bundestagswahlen

- drahtloser Internetzugang
- 1,6 Millionen Telearbeitsplätze
- letztmalige Förderung des Gründerwettbewerbs Multimedia mit 2 Millionen Mark
- Großbritannien: 25 Prozent aller staatlichen Dienstleistungen elektronisch verfügbar

2003

- 350.000 neue Arbeitsplätze
- 40.000 Ausbildungsplätze in neuen IT-Berufen
- Digitale Bibliothek (www.subito-doc.de) und elektronische Dokumentenlieferdienste (SUBITO) sind aufgebaut – 115 Millionen Mark
- Förderung von Telematiksystemen läuft aus – 187 Millionen Mark
- Aufbau und Ausbau eines flächendeckenden Gigabitnetzes für die Wissenschaft mit neuen netznahen Diensten beendet – 160 Millionen Mark
- BMBF-Förderungsprogramm zur Entwicklung neuer Hochtechnologien der Mikroelektronik läuft aus – 350 Millionen Mark

2005

- weitere 250.000 Fachkräfte stehen für qualifizierte IT-Aufgaben zur Verfügung
- bei Unternehmensgründungen liegt der Frauenanteil bei 40 Prozent
- bei IT-Berufsausbildungen liegt der Frauenanteil bei 40 Prozent
- bei Informatikstudiengängen liegt der Anteil von Studienanfängerinnen bei 40 Prozent
- weltweite Spitzenposition bei Bildungssoftware – seit 2000 durch den Einsatz von 100 Mio. Mark BMBF-Fördermittel erreicht nationaler Bildungsserver
- internetbasierte Informationsstruktur von Fachinformationszentren, Bibliotheken und anderen Dienstleistungsanbietern
- 40 Prozent Internetnutzer
- flächendeckende Nutzung vernetzter Computer an Hochschulen in Präsenzlehre und Selbstudium – seit 1999 wurden 454 Millionen Mark Bund-Länder-Fördergelder investiert
- rein optische Netzwerke im Terabit-Bereich sind entwickelt
- neuartige breitbandige Mobilkommunikationssysteme mit Zugriffsmöglichkeit auf multimediale Dienste zu jeder Zeit an jedem Ort – für optische und Funknetze zusammen 400 Millionen Mark
- BMBF-Förderungsprogramm von neuen, spezifischen Internettechnologien zur Verbesserung der Informationssuche und zur Erhöhung der Dienstequalität läuft aus – 100 Millionen Mark
- BMBF-Förderungsprogramme Grundlagenforschung Software und Mensch-Technik-Interaktion laufen aus – 500 Millionen Mark

2006

- USA: fast die Hälfte der US-Arbeitnehmer arbeiten in Industrien, die entweder Hersteller oder intensiver Nutzer von IT-Produkten und Dienstleistungen sind

2008

- Europäisches Satellitennavigationssystem Galileo (Konkurrenz zu GPS) ist einschließlich terrestrischer Infrastruktur betriebsbereit (deutscher Beitrag 1997-2002 insgesamt 75 Millionen Mark)
- 100.000 Arbeitsplätze europaweit im Bereich von Galileo-Anwendungen, 2000 Arbeitsplätze für Betrieb

2010

- flächendeckend Glasfaser bis zum Hausanschluß
- Ende der analogen TV-Übertragungen

Tagung Grundrechte in der Informationsgesellschaft

- Zwischenbilanz rot-grüner IT-Politik –

Veranstalter: Berliner Datenschutzbeauftragter (BlnDSB)
Technische Universität Berlin, Institut für Angewandte Informatik – Informatik und Gesellschaft (TU Berlin)
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF)
Bürgerrechte & Polizei (CILIP)
Deutsche Vereinigung für Datenschutz (DVD)
am Freitag/Samstag, den 18./19. Februar 2000
Technische Universität Berlin, Straße des 17. Juni 135, 10623 Berlin, Räume MA 004, 309, 371, 366, 367.

Die rot-grüne Bundesregierung ist angetreten, die bundesdeutsche Gesellschaft zu modernisieren. Sie wollte die richtigen Weichen stellen für die Verwirklichung von Bürgerrechten, Demokratie und Sozialstaatlichkeit in einer zukunftsorientierten Informationsgesellschaft. Nach mehr als einem Jahr ist es Zeit zu prüfen, welche Initiativen von ihr gestartet wurden, welche geplant sind und welche noch ausstehen, um dieses Ziel zu erreichen.

Erste Signale deuten in die richtige Richtung: der Verzicht auf die Regulierung von Kryptografie, ernsthafte Planungen zur umfassenden Modernisierung des Datenschutzrechts, auch der Schaffung eines Arbeitnehmerdatenschutzgesetzes, Pläne für ein Informationsfreiheitsgesetz, eine Initiative »Schulen ans Netz«... Es gibt aber auch Signale, die Widerspruch provozieren: umfassende Pläne zur Telekommunikationsüberwachung, Verpflichtung der Privatwirtschaft, sich durch die Bereitstellung teurer Infrastruktur hieran zu beteiligen, Fortschreibung der Kontrollbefugnisse der Sicherheitsbehörden, Ausweitung der Kontrollen im Gesundheitsbereich; konkrete Datenschutzinitiativen sind verzagt und halbherzig.

Längst ist die unkritische Technikbegeisterung der Einsicht gewichen, die Informationsgesellschaft politisch gestalten zu müssen, um nicht bürgerrechtliche, demokratische und soziale Errungenschaften auf´s Spiel zu setzen. Die demokratische Gestaltung der informationstechnischen Rahmenbedingungen setzt eine breite öffentliche Diskussion voraus. Diese wollen wir auf der Tagung führen.

Die Veranstaltung soll über die aktuellen politischen Planungen und Kontroversen informieren und die Diskussion hierüber vorantreiben.
Anmeldung bei:

Deutsche Vereinigung für Datenschutz e.V. (DVD), Bonner Talweg 33-35, 53113 Bonn, Tel.: 0228/222498 (außerhalb Bürostunden: Anrufaufzeichner), Email: dvd@aktiv.org oder

Technische Universität Berlin – Institut für Angewandte Informatik, Franklinstr. 28/29, 10587 Berlin, Tel.: 030/314-73420 Fax: 314-24891, Email: sekr@ig.cs.tu-berlin.de

Rückfragen möglich auch bei: Thilo Weichert: 0431/9719742 (p) 9881205 (d).
Tagungsgebühr: 100 DM pro Person, reduziert 50 DM für Studierende/Arbeitslose/Rentner,
Überweisung des Tagungsbeitrags bitte an DVD, Kto.Nr. 59459-502 Postgiroamt Köln, Blz. 37010050 mit dem Stichwort »Tagung«. Der Tagungsbeitrag kann bei der Anmeldung per Überweisung oder zu Tagungsbeginn bar entrichtet werden.

Übernachtungsmöglichkeiten zu reduzierten Preisen können an den o.g. Anmeldeadressen erfragt werden.

Ablauf

Freitag, den 18.02.2000

19.00 bis 21.30 (MA 004)

Erwartungen an die Politik in der Informationsgesellschaft aus der Sicht eines Datenschutzbeauftragten
Prof. Jürgen Garstka, Berliner Datenschutzbeauftragter
aus wissenschaftlicher Sicht
Prof. Bernd Lutterbeck, Technische Universität Berlin
aus Arbeitnehmersicht
Prof. Wolfgang Däubler, Universität Bremen
aus der Sicht der Wirtschaft
Prof. Alfred Büllesbach, Daimler Chrysler AG

Samstag, den 19.02.2000

9.00 – 12.00 (MA 004)

Vorstellung der Informationstechnikpolitik der Bundesregierung
Neue Impulse beim Datenschutz
Claus-Henning Schapper, Staatssekretär im Bundesministerium des Innern
Rechtsstaatlichkeit, Sicherheit und Informationstechnik
Dr. Hans-Jörg Geiger, Staatssekretär im Bundesministerium der Justiz
Neue Impulse für Wissenschaft, Bildung und Wirtschaft
Edelgard Bulmahn, Ministerin für Bildung und Forschung
mit Diskussion

14.00 bis 15.30 (Arbeitsgruppen mit Vertretern aus Ministerien und Organisationen)

1. Die Novellierung des Bundesdatenschutzgesetzes
   Dr. Martina Weber, Bundesministerium des Innern
   Dr. Thilo Weichert, Deutsche Vereinigung für Datenschutz
2. Arbeitnehmerdatenschutz
   Prof. Wolfgang Däubler, Universität Bremen
   Hans Peter Viethen, Bundesministerium für Arbeit und Sozialordnung
3. Telekommunikationsüberwachung
   Christiane Schulzki-Haddouti, Journalistin bei Spiegel-Online
   Josef Brink, Bundesministerium der Justiz
4. Grenzüberschreitender Datenverkehr in Europa, mit den USA, in der Welt
   Dr. Stefan Walz, Landesbeauftragter für den Datenschutz Bremen
   Harald Eul, HEC Consulting u. externer Datenschutzbeauftragter

16.00 bis 17.30 (Arbeitsgruppen mit Vertretern aus Ministerien und Organisationen)

5. Sicherheitspolitik – neue technische Ermittlungsmethoden, neue Befugnisse, Strafverfahrensänderungsgesetz
   Prof. Felix Herzog, Humbold-Universität Berlin
   Lutz Diwell, Senatsverwaltung für Justiz Berlin
6. Informationsfreiheit
   Rolf Breidenbach, Ministerium des Innern Brandenburg
   Dr. Alexander Dix, Landesbeauftragter für Datenschutz u. Akteneinsicht Brandenburg
7. Datenschutz und Verbraucherschutz als Wirtschaftsfaktor
   Michael Wachs, Verbraucherzentrale Niedersachsen
   Harald Summa, electronic commerce forum (eco) e.V.
   Ute Bernhardt, Forum InformatikerInnen für Frieden und gesellsch. Verantwortung
8. Sind wir gegen den Information Warfare gerüstet?
   Marit Blattner-Zimmermann, Bundesamt für die Sicherheit in der Informationstechnik
   Ralf Bendrath, FU Berlin
   Ingo Ruhmann, Forum InformatikerInnen für Frieden und gesellsch. Verantwortung

18.00-19.30 (MA 004)

Öffentliche Podiumsdiskussion mit Abgeordneten aus den im Bundestag vertretenen Fraktionen.

FIfF-Mitglieder-versammlung 1999

Ort: **Heinz Nixdorf Institut, Universität Paderborn**
Zeit: **9.10.99, 15.45 bis 19.00 Uhr**
Leitung: **Reinhard Keil-Slawik, Protokoll Dagmar Boedicker**

Tagesordnung

1.) Wahl der Versammlungsleitung und der Protokollführung

2.) Beschlussfassung über die Tagesordnung

3.) Bericht des Vorstandes (Reinhard Keil-Slawik) einschliefflich des Kassenberichts (Werner oder Ute)

4.) Bericht der Kassenprüfer (schriftlich von Manfred Keul)

5.) Diskussion des Vorstandsberichts und der Kassenprüfung

6.) Entlastung des Vorstandes und der Kassenprüfer

7.) Neuwahl des Vorstands Wahl der Wahlleiter/-in Wahl einer Wahlkommission Vorstellung der Kandidaten, Diskussion Wahl der/des Vorsitzenden Wahl der Beisitzer/-innen

8.) Neuwahl der Kassenprüfer

–) Satzungsänderung (entfällt)

9.) Beitragsänderung (u.a. Anpassung an den Euro)

10.) Diskussion aktueller Themen, Verabschiedung von Stellungnahmen, Berichte aus den Regionalgruppen

11.) Verschiedenes

TOP 1

Die Vorschläge (Sitzungsleitung Reinhard Keil-Slawik, Protokoll Dagmar Boedicker) wurden von der Mitgliederversammlung per Akklamation akzeptiert.

Top 2

Der Vorstand hatte vorsorglich eine Satzungsänderung auf die Tagesordnung gesetzt, für den Fall, dass der Sitz des Vereins hätte geändert werden müssen, weil die Geschäftsstelle umgezogen ist. Da aber weiterhin Treffen des Vorstands und andere Aktivitäten des Vereins in Bonn stattfinden werden, ist das nicht nötig. Eine Satzungsänderung erübrigt sich, die geänderte Tagesordnung wird per Akklamation akzeptiert.

TOP 3

Vorbemerkung: Da die Kooperationspartner für die geplante Jahrestagung in Berlin den Termin sehr plötzlich auf nächsten Februar verschieben mussten, wir aber durch unsere Satzung zu einer Mitgliederversammlung noch in diesem Jahr verpflichtet sind, mussten wir Termin und Ort sehr kurzfristig festlegen. Es war zwar möglich, den satzungsgemäflen Termin für die Einladung einzuhalten, der Geschäftsführer, die Kassenprüfer und einige Mitglieder des Vorstands hatten aber diesen Termin nicht mehr frei, so dass Ute Bernhardt sowohl den Kassenbericht als auch der Bericht der Kassenprüfer stellvertretend halten muss. Auch einige Beisitzer-Kandidaten für den Vorstand konnten nicht selbst erscheinen. Sie haben sich aber bereit erklärt, das Amt zu übernehmen, wenn sie gewählt würden.

Reinhard Keil-Slawik berichtet über die kontinuierliche Arbeit, auch wenn das FIfF nicht so viel Präsenz zeigen konnte und sich nicht zu allen wesentlichen Themen äuflern konnte, wie es wünschenswert gewesen wäre. Einige Brüche in der Kontinuität dieser Arbeit gab es leider:

Geschäftsstelle: Weil die Geschäftsführerin Ute Bernhardt und die zweite Seele des Geschäfts, Ingo Ruhmann, beide beruflich in eine andere Stadt umziehen mussten, konnten sie die Arbeit in der Geschäftsstelle nicht fortführen. Andere FIfF-Mitglieder in Bonn, die sich dazu bereitgefunden hätten, gab es nicht. Glücklicherweise konnte Werner Hülsmann die Räumlichkeiten in Medemstade und Ingrid Engelkes Mitarbeit organisieren. Einmal haben wir einen groflen Teil der Vorstandssitzung für den Umzug gebraucht. Die Arbeit im Büro klappt trotz des Umzugs und der nötigen Einarbeitung schon erstaunlich gut und reibungslos. Dank an Ingrid und Werner für ihren Einsatz für eine rasche Umstellung, Dank an Ute und Ingo für ihre langjährige Arbeit im Büro.

FIfF-Kommunikation: Hier ist über lange Zeit gute kontinuierliche Arbeit geleistet worden, Dank an Harald Selke und Markus Hoff-Holtmanns dafür. Die FIfF-Kommunikation wird viel gelesen (auch in Ministerien), unter anderem deshalb, weil es sonst keine Publikation dieser Art gibt. Vor allem die Schwerpunktredaktionen bringen sehr viel Kompetenz auch von auflen, weil dort gelegentlich Experten schreiben, die nicht im FIfF sind. Ca. 1000 Hefte gehen in den Versand an Mitglieder und Abonnenten.

Markus wird noch für einige weitere Hefte die Vorlagenproduktion in Paderborn weitermachen. Schwierig ist nach wie vor die Koordination: das Büro liefert zu, es gibt eine Schwerpunktredaktion für jedes Heft, die Abstimmung der Inhalte und Prozesse liegt weiterhin vorwiegend in Paderborn und ist nicht ganz einfach. Deshalb die Bitte an die Schwerpunktredaktionen, sehr diszipliniert zu arbeiten und Termine einzuhalten.

Web-Server mit FIfF Seiten: Hierfür wird weiterhin ein Kümmerer gesucht. Die Bitte geht an die Mitglieder.

Allgemeines: Die Mitgliederzahl liegt bei etwa 880, Ein- und Austritte halten sich in etwa die Waage. Die Tendenz zur Überalterung ist bedenklich, und wir sollten sie im FIfF diskutieren. Ein Grund für den nicht sehr zahlreichen Nachwuchs könnte es sein, dass Standesorganisationen bei InformatikerInnen möglicherweise weniger akzeptiert sind als in anderen Berufen.

Die Position des FIfF zur Kosovo-Frage: Einerseits ist das FIfF Teil der Friedensbewegung, in deren Schofl es 1983 geboren ist, andererseits hat zu seiner Entstehung als soziale Bewegung auch die Debatte um die informationelle Selbstbestimmung anlässlich der Volkszählung beigetragen. Die Stellungnahmer zum Kosovo-Krieg in der FIfF-Kommunikation war Ergebnis eines ausführlichen Diskussionsprozesses im Vorstand und eines weniger ausführlichen Diskussionsprozesses in der Mailing-Liste. Die UnterzeichnerInnen haben ausdrücklich als einzelne Vorstandsmitglieder unterschrieben, weil selbst im Vorstand keine einheitliche Meinung herrschte und alle eine ausführlichere Auseinandersetzung innerhalb des FIfF für notwendig hielten. Es ist also weder eine Stellungnahme des FIfF noch des Vorstands herausgegangen. Trotzdem hat dieser Beitrag zu vier Austritten bei langjährigen, verdienten Mitgliedern geführt, die dazu allerdings auch keine weitere Diskussion angeboten hatten. Über diese vier Mitglieder hinaus hat der Vorstand keine weiteren »offiziellen« Rückmeldung erhalten.

Die derzeitigen Formen der Kriegsführung und der Kosovo-Krieg werden Schwerpunktthema der nächsten FIfF-Kommunikation sein, im FIfF geht die Diskussion selbstverständlich weiter. Sie ist weder im Vorstand noch im FIfF abgeschlossen. Über die Mailing-Liste ist kaum diskutiert worden, allerdings gingen etliche Mails direkt an Ralf Streibl. Im Austausch bewegt sich allerhand, auch im Umgang mit der eigenen Hilflosigkeit.

Das FIfF ist als Berufsverband zur Behandlung spezieller Probleme entstanden, die u.a. mit Rüstung zusammenhängen. Dieser Anspruch und die politische Haltung lassen sich nicht immer ad hoc kompetent darstellen, manchmal müssen wir uns im FIfF dieses Wissen erst gemeinsam erarbeiten. - Wenn andere Verbände (eine Bürgerinitiative, Gewerkschaft, ...) an uns herantreten, kann das zu einem Dilemma werden. Erstaunlich wenige sind bereit und in der Lage, als Experten aufzutreten. Immer dieselben Namen unter den qualifizierten Stellungnahmen.

Der FIfF-Beirat: Reinhard erläutert noch einmal seine Funktion, nämlich

Information und Erfahrung aus den jeweiligen Tätigkeitsfeldern der Mitglieder ins FIfF zu tragen. Beim letzten Treffen haben die eingeladenen Politikvertreter dringend nach Beratungskompetenz gefragt. Es geht ein Appell an die Mitglieder, sich anzubieten, wenn sie spezielle Kenntnisse mitbringen.

Tagungen:

18./19.2.2000 in Berlin Tagung mit DVD, CILIP, Humanistische Union, Lutterbeck, und Garstka (LfD Berlin) zum Thema »Grundrechte in der Informationsgesellschaft«.

Die Jahrestagung 2000 macht die Regionalgruppe Hamburg zum Thema »Frieden mit der Natur und der Welt«.

Die Jahrestagung 2001 findet als internationale Tagung in Bremen statt.

Die Jahrestagung 2002 findet zum Thema »Frauen in der Informationsgesellschaft« in Freiburg statt.

Ute Bernhardt legt den Kassenbericht (siehe Anlage) vor und erläutert ihn. Von Bedeutung sind die Haushaltsjahre 98/99. Die Finanzlage ist zwar in Ordnung, lässt aber kaum Spielraum. Auch wurden in diesem Jahr keine Studien o.ä. an das FIfF vergeben. Für 1999 wäre es nach der Finanzlage nicht möglich gewesen, einen Tagungsband herauszugeben, wenn die Tagung planmäflig in Berlin stattgefunden hätte.

TOP 4

Ute trägt auch diesen (schriftlichen) Bericht vor (siehe Anlage). Manfred Domke hat sein Amt wegen der Kosovo-Differenzen niedergelegt und nicht mitgearbeitet. Manfred Keul hat die Arbeit aber gemacht. Satzungsmäflig genügt ein Kassenprüfer.

Der Vorstand hat die Empfehlung von Manfred umgesetzt. Der Kassenprüfer hatte keine schwerwiegenden Beanstandungen, stellte aber fest, dass in einem Fall aufgrund einer zu hohen Kilometerpauschale 2,66 DM zuviel erstattet worden sind. Dies wurde korrigiert.

TOP 5

Für das FIfF stellt sich auch die Frage: Wie kommen wir aus der reaktiven Rolle? Es sollten möglichst viele ihr Wissen einbringen, regelmäflige Treffen mit zahlreicher Beteiligung heben die inhaltliche Arbeit auch auf die überregionale Ebene.

Reinhard fordert die anwesenden Mitglieder auf, möglichst zahlreich für den Vorstand zu kandidieren.

TOP 6

Der Vorstand wird mit 6 Enthaltungen ohne Gegenstimmen, die Kassenprüfer einstimmig entlastet. (Kassenstand vom 2.9.99)

TOP 7

Als Wahlleiter bestimmen die Mitglieder per Akklamation : Lothar Sowada
Die Kandidaten stellen sich vor und nach einer kurzen Aussprache findet die Wahl mit folgendem Ergebnis statt:

Vorsitz Reinhard Keil-Slawik (23 Stimmen abgegeben, 20 Ja, 1 Enthaltung, 2 ungültig)

Stellvertretende Vorsitzende Ute Bernhardt (21 Stimmen abgegeben, 19 Ja, 1 Enthaltung, 1 ungültig)

Wahl der BeisitzerInnen:
Die Kandidaten stellen sich vor.

Bittner, Peter
Boedicker, Dagmar
Dreschler-Fischler, Leonie
Hornecker, Eva
Hülsmann, Werner
Ruhmann, Ingo
Schinzel, Britta
Streibl, Ralf

Laut Wahl- und Geschäftsordnung sind die Beisitzer zum Vorstand en bloc zu wählen. Ralf Streibl stellt den Antrag zur Geschäftsordnung, einzelne Namen auf den Wahlzettel zu schreiben, statt einer einer En-Bloc-Wahl.

Gegenrede von Werner Winzerling: Er sieht keinen Dissenz in der Aufstellung der KandidatInnen, und die Zeit für Formalia sollten wir kurz halten.

Über den Antrag von Ralf wird abgestimmt: 2 dafür, 11 dagegen, 8 Enthaltungen

Ergebnis der BeisitzerInnenwahl: 22 abgegebene Stimmen, 20 Ja, 1 Nein, 1 Enthaltung

TOP 8

Neuwahl der KassenprüferThorsten Reinsch und Friedrich Holl werden vorgeschlagen und einstimmig per Akklamation gewählt.

TOP 9

Angesichts der nicht erfreulichen Finanzsituation und der Tatsache, dass die Mitgliedsbeiträge seit 1992 unverändert geblieben sind und der Euro Anlass zur Neubetrachtung der Finanzlage gegeben hat, schlägt der Vorstand vor, den Beitrag für verdienende Mitglieder auf 60 Euro (117,35 DM) und für nicht Verdienende auf 15 Euro (29,34 DM) zu erhöhen und die reduzierten Beiträge für die neuen Bundesländer wegfallen zu lassen. Für Fördermitgliedschaften sind die Beiträge nach Studierenden (auch beispielsweise Fachschaften) und Verdienenden unterteilt und unterscheiden sich nicht von denen für aktive Mitglieder.

Den neuen Abonnementpreis hat der Vorstand bereits auf 20 Euro (39,15 DM) erhöht, denn vor allem mit der FIfF-Kommunikation entstehen Kosten, die sich auch weiterhin tragen müssen.

Die Versammlung diskutiert die Höhe des neuen Beitrags, und versucht die Mehreinnahmen durch die Erhöhung abzuschätzen. Die vorgeschlagene Beitragserhöhung wird bei 2 Enhaltungen angenommen.

TOP 10

Diskussion über zukünftige Themen für die FIfF-Arbeit. Gefragt wurde, wofür das FIfF steht und nach der Sinnhaftigkeit von Kampagnen. Ein Vorschlag ist es, wie CPSR Leitthemen zu definieren. Eine Selbstverständnisdiskussion wird nach einiger Diskussion abgelehnt, da das FIfF eine Vielfalt von Themen bearbeitet, eine Selbstverständnisdiskussion aber kein Weg sei, diese Vielfalt zu strukturieren. Kampagnen eignen sich dafür dagegen schon. Der Vorstand wird darüber beraten.

Für das Schwerpunktheft »Informatik und Behinderung« werden noch Ansprechpartner und Beiträge gesucht.

TOP 11 (entfiel)

Paderborn, 10.10.99
D. Boedicker

Schwerpunkt

Ralf Bendrath[5]

Der Kosovo-Krieg im Cyberspace

Elektronische Belagerung der NATO aus Jugoslawien

Im Mai dieses Jahres schreckte das US-Nachrichtenmagazin Newsweek die Öffentlichkeit mit einer nach Science-Fiction klingenden Meldung auf: Hacker des US-Geheimdienstes CIA seien dabei, in die Computer ausländischer Banken einzubrechen und Milosevics Konten zu löschen. Autorisiert sei dieser Plan von US-Präsident Bill Clinton selber.[1] Sind damit die in Schundromanen[2] und Hollywoodproduktionen[3] schon seit einigen Jahren verbreiteten Visionen vom virtuellen Krieg Wirklichkeit geworden? In der Tat beschäftigen sich die US-Streitkräfte und Geheimdienste seit mehr als zehn Jahren mit dieser Art der Kriegführung, und auch in anderen Ländern werden Visionen vom Cyberkrieg entwickelt und futuristische Planungspapiere geschrieben. Der stellvertretende US-Verteidigungsminister John Hamre bezeichnete den Krieg gegen Jugoslawien bereits im April als den ersten Cyberkrieg, den die USA führen.[4]

Ein Blick hinter die Kulissen, soweit er möglich ist, relativiert dieses Bild in mehreren Richtungen: Für den Ausgang des Kosovo-Krieges waren die Cyberattacken relativ unbedeutend, und auch die Kriege der Zukunft werden nicht unblutig im Internet stattfinden. Neu ist allerdings, daß sich mit politisierten Hackergruppen bisher ungewohnte Kriegsparteien auf dem virtuellen Schlachtfeld tummelten. Dies zeigt, wie unkontrollierbar solche Pläne der staatlichen High-Tech-Eliten sind, wenn sie in die Realität umgesetzt werden. Zum übergreifenden amerikanischen Konzept des »Informationskrieges« gehört aber nicht nur die Manipulation von Bankkonten, sondern vor allem der Medien. Dies ist das eigentlich Entscheidende am Kosovo-Krieg: Wichtig ist nicht mehr der Sieg auf dem Schlachtfeld, das es in diesem Luftkrieg ohnehin nicht gab, sondern die Manipulation seiner medialen Repräsentation.

»Es macht Spaß, zu sehen, wie High-Tech an der Front eingesetzt wird.«

Bill Gates bei den US-Marines[6]

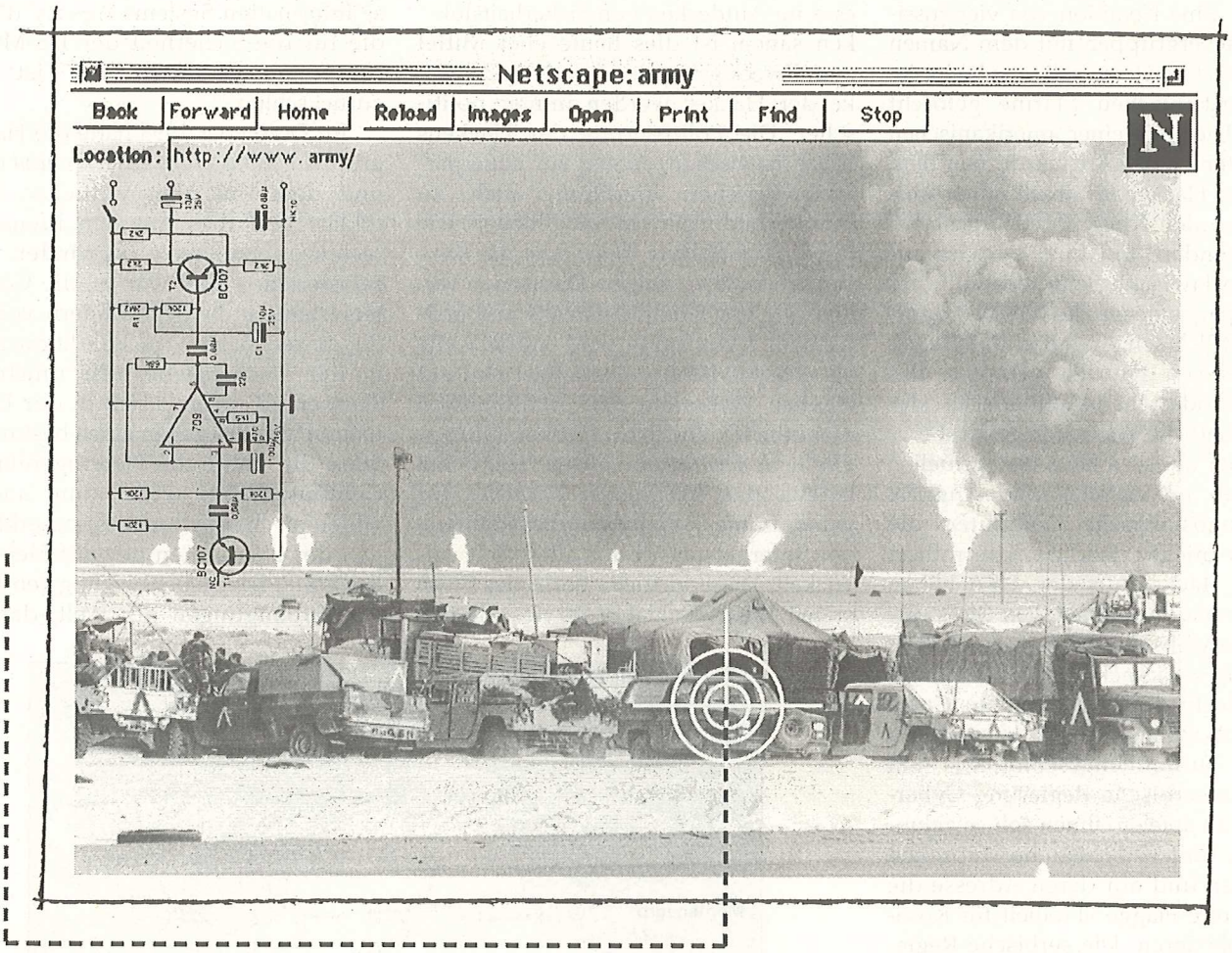
Kurz vor Ostern meldete die NATO einen jugoslawischen Angriff aus dem Cyberspace. Die »Attacke«, die von einem Belgrader Computer ausging, war allerdings bei genauerem Nachlesen lediglich eine Massensendung von tausenden Emails, die das elektronische Postfach des Militärbündnisses für andere Besucher mehrere Tage lang unzugänglich machte. Frank Rieger, Sprecher des *Chaos Computer Club (CCC)*, hält es sogar für wahrscheinlicher, daß die NATO sich einen Computervirus wie »Melissa« eingefangen hat.[7] Dieser Virus, der die Adreßverzeichnisse von Email-Programmen benutzt, um sich selbsttätig zu verbreiten, hatte im März bereits im Pentagon sein Unwesen getrieben.[8]

Dennoch: Nach den veröffentlichten Informationen wurden die internen Datennetze der westlichen Militärinstitutionen, aber auch das öffentliche World Wide Web, von serbischer Seite ins virtuelle Visier genommen. Nach einem Bericht von *US News* existiert in Belgrad ein Netz von mehr als tausend StudentInnen und SchülerInnen in sechs Computerzentren, die die kriegsbedingten Ferien nutzen, um im Internet gegen die NATO aktiv zu werden. Der größte Teil ihrer Tätigkeit besteht aus dem Füttern von Newsgroups und der Pflege ihrer umfangreichen Webseite, aber der Mail-Müll könnte ebenso wie die Viren von hier gekommen sein.[9] Nach Informationen von Infoworld.com wurden mindestens fünf neue Computerviren mit diesen Emails auf die NATO-Rechner übertragen.[10]

Bei einer anderen Art der Angriffe auf die öffentlichen Server der NATO wurde die Internet-Funktion »Ping« genutzt, mit der an einen Rechner ein kleines Datenpaket gesendet wird, das dieser an den Absender zurückschickt. Ende März wurde die NATO – wie bereits verschiedene andere Institutionen vor ihr – Opfer massenhafter Ping-Anfragen, was dazu führte, daß die Rechner überlastet waren und die Datenleitungen verstopften.[11] Diese Angriffe kamen nach Aussagen des Pentagon ebenfalls aus Serbien, aber nicht unbedingt von Rechnern der serbischen Regierung.[12] Genau wie die massenhafte elektronische Post nutzt diese Art der Angriffe reguläre Funktionen aus, die bei entsprechend häufigen Aufrufen den Rechner zu stark beschäftigen. Bekannt sind solche Angriffe als »Denial of Service Attacks«.

Über diese recht simple Art der Störungen hinaus gehen die Angriffe auf diverse Webseiten. Hacker aus Serbien sind in Webserver aus NATO-Staaten eingedrungen und haben die dort abrufbaren Internet-Seiten verändert. Die serbische Hackergruppe *CHC* etwa ersetzte Anfang April die Webseiten zweier US-Regierungseinrichtungen sowie der britischen Stadt Croydon durch eine Anti-NATO-Seite, in der diese als »National American Terrorist Organisation« bezeichnet wurde.[13]

Alle diese Angriffe richteten sich gegen die öffentliche Darstellung der NATO oder von NATO-Staaten im World Wide Web. Die Kriegführungsfähigkeit der Militärallianz war dabei nicht gefährdet, denn die internen Kommunikations- und Kommandonetze verlaufen über ganz andere Kanäle. Die Kommunikation zur Leitung der Kriegseinsätze ist nicht direkt über das



Internet oder andere öffentliche Netze zugänglich, und die Sicherheitsvorkehrungen sind hier weitaus größer als bei einem Webserver oder Mailboxrechner. Zudem laufen auf den Militärcomputern teilweise Programme und Betriebssysteme, die auf dem freien Markt nicht erhältlich sind und bei denen es daher schwierig ist, sicherheitsrelevante Informationen zu bekommen.

Einen Schritt weiter als die Web-Hacker sind daher Versuche, in die Militärcomputer selber einzudringen. Auch dies wurde im Kosovokrieg versucht. Einen ernsthaften Schaden hat nach Berichten der Belgrader Zeitung »Blic« ein Mitglied der serbischen Hackergruppe »Schwarze Hand« angerichtet. Er soll Ende März in einen Computer der Navy eingedrungen sein und alle Daten gelöscht haben. Obwohl das US-Verteidigungsminsiterium diesen Vorfall nie bestätigte, war der Rechner zeitweilig im Internet nicht erreichbar. Die gleiche Hackergruppe, die angeblich in der Tradition einer gleichnamigen serbischen Terrororganisation vom Anfang des Jahrhunderts steht, hatte bereits im Oktober 1998 die Webseite des gemäßigten Albanerführers Ibrahim Rugova gehackt.[14]

Internationale Hacker-Brigaden

Als Reaktion auf die Bombardierung der chinesischen Botschaft in Belgrad durch die USA haben auch chinesische Hacker mehrfach Webseiten amerikanischer Institutionen angegriffen. Mindestens zweimal wurde das Internet-Angebot der amerikanischen Botschaft in Peking durch den Text »Nieder mit den Barbaren!« ersetzt, ähnliches widerfuhr den Seiten des Energieministeriums, auf denen plötzlich zum Protest gegen die »amerikanischen Nazi-Methoden« aufgerufen wurde.[15] Dort stand auch zu lesen »Wir sind chinesische Hacker, die sich nicht um Politik kümmern, aber wir dulden es nicht, wenn wir sehen müssen, daß chinesische Journalisten getötet worden sind.«[16] Auf der Webseite des US-Innenministeriums tauchten Anfang Mai Bilder von den drei Zivilisten auf, die beim Angriff auf die chinesische Botschaft getötet worden waren.[17] Auch gegen die Internet-Darstellung des Weißen Hauses wurden Angriffe unternommen und die Seite war drei Tage lang nicht online. Obwohl der Sprecher des Weißen Hauses dies mit »Denial of Service«-Angriffen begründete, wurde die Nachricht von einem erfolgreichen Einbruch auf der Seite in verschiedenen

Hackerforen annonciert.[18]

Auch die russische Ablehnung der NATO-Angriffe wurde nicht nur vom Kreml auf dem diplomatischen Parkett vertreten. Eine russische Hacker-Gruppe mit dem Namen *From Russia With Love*[19] hat eine NATO-Webseite mit dem Vermerk »Haut ab aus dem Kosovo« versehen. Eine Koalition von vier russischen Hackergruppen mit dem Namen *Russian Hackers Union* soll eine Webseite der amerikanischen Marine gelöscht haben.[20] Die Seite einer amerikanischen Windsurfer-Zeitschrift wurde von dem russischen Hacker *SP* durch einen Aufruf ersetzt, den Krieg gegen Jugoslawien zu beenden. Ein Link verwies auf eine jugoslawische Seite, die zu einer Webkampagne gegen die NATO-Angriffe aufruft.[21] Nach Angaben des *Hacker News Network* wurden während des Krieges mindestens 14 militärische oder andere staatliche Webseiten gehackt.[22]

Von der anderen Seite der virtuellen Front gab es verschiedene Angriffe gegen jugoslawische Computer, die ebenfalls nicht staatlich kontrolliert wurden. Hacker aus den USA haben laut Informationen des *Boston Globe* versucht, die Webseite der jugoslawischen Regierung zu knacken, die als extrem sicher gilt. In der *Kosovo Hackers Group* haben sich albanische und europäische Hacker zusammengeschlossen, um gegen die serbische Regierung Cyberguerrilla zu spielen. Ihnen soll es gelungen sein, fünf verschiedene Webseiten zu löschen und auf deren Adresse die schwarz-rote Flagge »Freiheit für Kosovo« zu plazieren. Die serbische Regierung gab zwischenzeitlich auf der Webseite ihrer virtuellen Presseabteilung zu, daß sie technische Probleme hatte. Die Ursachen dafür können aber auch ganz banal zerbombte Telefonleitungen oder Kraftwerke gewesen sein.[23] Die hollandische Hackergruppe *Dutchthreat* hakkte sich in eine private serbische Webseite, auf der die NATO als »eine Bande Nazis« bezeichnet worden war. Sie ersetzten die Anti-NATO-Seite mit einer eigenen »Helft Kosovo«-Seite.[24]

In Mitleidenschaft gezogen wurden auch Webseiten in unbeteiligten Staaten. So wurde u.a. die Internet-Präsenz einer ägyptischen Regierungseinrichtung von der russischen Hackergruppe *KpZ* durch ein Bild der MTV-Comicfiguren Beavis & Butthead ersetzt, die zum »Stop der NATO-Morde« aufrufen.[25] Eine private Seite in Brasilien enthielt plötzlich einen Aufruf gegen Milosevic.[26]

Politisierte Computerfreaks als Cyberkrieger?

Während Hacker früher ihr Hauptinteresse im Aufdecken von Sicherheitslükken sahen, ist dies heute eher Mittel zum Zweck geworden – und die Zwekke der Hacker werden immer politischer. Die Politisierung des Hackens führt inzwischen, analog zur außerparlamentarischen Tradition, auch zu Bündnisbildungen und Koalitionen, wie die *Russian Hackers Union* oder die *Kosovo Hackers Group* zeigen. Diese neue Verbindung von Computerfreaks und politischem Aktivismus wird mittlerweile als »Hacktivismus« bezeichnet und auf eigenen Webseiten und Mailinglisten diskutiert.[27] Die New Yorker Gruppe *Electronic Disturbance Theater* (EDT) hat bereits das Programm *FloodNet* für gemeinsame Webseiten-Besetzungen von Internetsurfern aus aller Welt entwickelt. Diese virtuelle Form des Sit-in erzielt einen »Denial of Service«, indem alle an einer Aktion Beteiligten gleichzeitig eine Webseite besuchen, die von *FloodNet* dann automatisch immer wieder aufgerufen wird.[28] Im September 1998 kam es bereits zu einem virtuellen Schlagabtausch zwischen dem EDT, das ein Cyber-Sit-In auf der Pentagon-Webseite angekündigt hatte, und der Defense Information Systems Agency (DISA), die für die Sicherheit der US-Militärcomputer verantwortlich ist und zurückschlug.[29]

Im Dezember 1998 hatte die Hackergruppe *Legions of the Underground* China und dem Irak den virtuellen Krieg erklärt und dies mit den Menschenrechtsverletzungen begründet. Das selbsterklärte Ziel war es, die Computersysteme in beiden Ländern vollständig zu zerstören.[30] Solche Aktionen sind in der Hackerszene sehr umstritten: Zum einen spiegelt sich in der Parteinahme für oder gegen einen bestimmten Staat die politische Heterogenität der Computerfreaks wider, zum anderen widersprechen virtuelle Kriegserklärungen der klassischen gewaltfreien Hacker-Ethik. Die sieben wichtigsten Hakker-Vereinigungen der Welt, darunter

Kosovo Foto: USIA

auch der deutsche *Chaos Computer Club* und die Gruppe *Cult of the Dead Cow* verurteilten die Ankündigung der *Legions of the Underground* in einer gemeinsamen Erklärung in aller Schärfe.[31] Bislang ist der dringend nötige Diskussionsprozeß in der Hackerszene noch nicht sehr weit fortgeschritten, z.B. ist völlig unklar, ob Taktiken wie das im Umfeld des *Electronic Disturbance Theater* entwickelte *Bottom Up Information Warfare* oder der »elektronische zivile Ungehorsam« als Guerillakampf oder gewaltfreier Widerstand bewertet werden sollen bzw. ob diese Begrifflichkeiten aus der physischen Welt im Cyberspace überhaupt angemessen sind. Was auffällt ist aber, daß die Hacker seltener als früher versuchen, in die Computersysteme einzubrechen, die für militärische Operationen notwendig sind. Mit dem Hacken von Webseiten beeinflussen sie aber nur die mediale Repräsentation des Krieges, nicht seinen Verlauf. Offenbar glauben auch die Hacker, daß der computergestützte Webdiskurs über den Krieg immer wichtiger wird und die Bedeutung der realen Kriegführung abnimmt.

Bankraub für den Frieden? Umstrittener Cyberkrieg der CIA

Ende Mai gelangten die Information über die Cyberangriffe der CIA auf die internationalen Bankkonten des jugoslawischen Präsidenten Slobodan Milosevic an die Öffentlichkeit. Milosevic soll nach Erkenntnissen der Geheimdienste Millionenbeträge bei Banken unter anderem in Rußland, Griechenland und Zypern deponiert haben. US-Präsident Bill Clinton hat laut Newsweek den Hackern der CIA die Genehmingung erteilt, in die Computer dieser Banken einzubrechen, um das Geld auf den privaten Auslandskonten des jugoslawischen Präsidenten »zu verplempern«, so ein US-Beamter. Im Gegensatz zu den bisher genannten Aktionen, die sich direkt gegen eine der Kriegsparteien richteten oder lediglich einen Webserver manipulierten, sind in diesem Fall die Bankencomputer von unbeteiligten Staaten unter Beschuß der USA geraten. Der NATO-Partner Griechenland wäre damit unter virtuelles »friendly fire« geraten. Das Weiße Haus weigerte sich, die Meldung zu kommentieren, und nicht einmal die NATO-Verbündeten waren in die Pläne eingeweiht. Das Vorhaben war laut Newsweek Teil eines umfassenderen Planes, der auf einem Vorschlag des nationalen Sicherheitsberaters Sandy Berger beruhte. Da die US-Regierung ebenso wie der Kongreß und die Öffentlichkeit vor einem Bodenkrieg zurückschreckte, Milosevic aber mit Luftangriffen offenbar nicht beizukommen war, griff der amerikanische Sicherheitsapparat auf ein Mittel zurück, das bereits Tradition hat: Verdeckte Operationen. Neben eher traditionellen Methoden[32] waren auch die Hackerangriffe der CIA in die Banken vorgesehen.[33]

Der Realitätsgehalt dieser Geschichte ist umstritten: Laut Aussagen des Chaos Computer Club ist es technisch möglich, über das internationale Bankensystem Swift Überweisungen zu fälschen. Geheimdienste wie amerikanische *National Security Agency (NSA)* seien dazu in der Lage.[34] Einige US-Geheimdienstmitarbeiter, die von den Plänen wußten, äußerten sich dagegen skeptisch über die Möglichkeit der geplanten Cyberangriffe. Um in gut gesicherte Bankencomputer einzudringen, müßten CIA-Agenten zunächst selber jede dieser Banken besuchen, ein eigenes Konto einrichten und danach sorgfältig darüber Buch führen, wie die Institution arbeitet. Erst wenn Schwachstellen in der Datensicherheit gefunden seien, könne die NSA ihre Rechenzentren einsetzen, um die hochentwickelte Verschlüsselung und die vorgeschalteten Schutzrechner (»Firewalls«) zu überwinden.[35]

Hintergrund und politische Folgen

CCC-Sprecher Rieger warnte davor, diese Art der virtuellen Nebenschauplätze für eine ungefährliche Erweiterung des Schlachtfeldes zu halten. Die USA, Deutschland und andere westliche Staaten seien aufgrund ihrer fortgeschrittenen Digitalisierung und Vernetzung weitaus verwundbarer gegenüber solchen Attacken als die Transformationsländer in Osteuropa. »Die Eskalationsmechanismen sind kaum beherrschbar«, so Rieger.[36] Mitglieder der Geheimdienstausschüsse von Kongreß und Repräsentantenhaus in den USA, die von Sicherheitsberater Berger Mitte Mai in einer geheimen Sitzung über die virtuellen Banküberfälle der CIA gegen Milosevic informiert worden waren, äußerten sich ebenfalls besorgt. Eine solche Aktion gegen ausländische Banken würde nicht nur gegen mehrere internationale Verträge verstoßen und NATO-Mitglieder wie Griechenland gegen die USA aufbringen, es könne auch die führende Rolle der USA im weltweiten Bankgeschäft untergraben. Außerdem sei dieser Bruch der Souveränität sogar von verbündeten Staaten ein gefährlicher Präzedenzfall und lade zur Nachahmung, also zu Angriffen auf US-Banken, geradezu ein.[37]

Monate nach dem Kosovokrieg kam dann ein laues Dementi aus dem Pentagon: Man habe den elektronischen Bankraub und andere weitergehende Cyberkriegs-Optionen erwogen, aber nach einer Prüfung durch die Rechtsabteilung des Ministeriums davon Abstand genommen.[38] Lediglich eine elektronische Täuschung des serbischen Luftabwehrsystems sowie Störungen des Telefonnetzes sind demnach durchgeführt worden.[39] Die völkerrechtlichen Implikationen solcher virtuellen Kriegführung sind nämlich bislang völlig unklar, und die US-Streitkräfte wollten sich nicht der Gefahr aussetzten, hinterher als Kriegsverbrecher angegriffen werden zu können. Die USA würden einen serbischen Hacker, der ähnliches an einer New Yorker Bank versucht, im übrigen als »Cyberterroristen« bezeichnen.

Eine mögliche Eskalation von Cyberangriffen und -gegenangriffen kann sich unter Umständen zu einer ernsten Bedrohung der USA entwickeln, die immerhin die am weitesten vernetzte Gesellschaft der Welt sind. Ein von Hackern veranstalteter elektronischer Börsencrash ist seit einigen Jahren der Alptraum der amerikanischen Sicherheitspolitiker, der von den Behörden kräftig genährt wird.[40] Allein in der US-Exekutive beschäftigen sich mehr als 15 Ministerien und Behörden konzeptionell und operativ mit Fragen der »Computerkriegführung« oder Computersicherheit, neben dem Verteidigungsministerium, der CIA und dem FBI unter anderem auch die Ministerien für Energie, Justiz, Wirtschaft, Finanzen oder Transport sowie verschiedene Abteilungen des Weißen Hauses.[41] Zur Abwehr der neuen Verwundbarkeiten der Informationsgesellschaft wurde erst im vergangenen Jahr mit der Präsidenten-Direktive 63 das *National Infrastructure Protection Center (NIPC)*[42] eingerichtet,

das zur Bundespolizei FBI gehört, aber auch dem Pentagon unterstellt werden kann.[43] Die Zuständigkeiten sind bisher nur ansatzweise geklärt. Abgeordnete des US-Kongresses warnten bereits davor, daß die Hacker der verschiedenen staatlichen Stellen sich bei ihren Aktivitäten gegenseitig im Weg stehen könnten.[44] Während an der elektronischen Verteidigung gegen Hackerangriffe bereits überall in den USA gearbeitet wird, gibt es für die Entwicklung offensiver Computerkriegsfähigkeiten, also Hackerprogramme, ferngesteuerte Computerviren und ähnliches, bisher keine Grundsatzentscheidung des Präsidenten.[45]

Im Hintergrund arbeiten bereits seit den achtziger Jahren verschiedene staatliche Stellen in den USA an der Erforschung dieser Methoden. Mitarbeiter von CIA und NSA verzeichneten nach eigenen Angaben »beachtliche Erfolge dabei (...), geheime militärische Computersysteme in der Sowjetunion und anderen Ländern zu penetrieren«[46]. Auch die Streitkräfte beteiligen sich seit Ende der achtziger Jahre an der Erforschung und Entwicklung von Computerviren, die auch als »nicht-tödliche Waffen« bezeichnet werden. Die staatlichen »Informationskrieger« beziehen dabei einen großen Teil der offensiv verwendbaren Software aus Hackerkreisen.[47]

Seit 1994 existiert bereits eine *School for Information Warfare and Strategy* an der *National Defense University* in Washington D.C., in der Offiziere der Streitkräfte für Informations- und Cyberkriege ausgebildet werden. Bereits 1995 war »Information Warfare« das Leitbild für alle Forschungs- und Entwicklungspläne der US-Streitkräfte[48], und 1996 wurde es in das zentrale Planungspapier der Vereinigten Stabschefs (die »*Joint Vision 2010*«) aufgenommen.[49] Die US Army hat ihre Doktrin für Informationskriege bereits 1996 mit dem neuen Field Manual 100-6, »*Information Operations*«, formuliert.[50] Die Befehlshaber der Regionalkommandos wurden mittlerweile aufgefordert, ihre Einsatzpläne daraufhin zu überprüfen, inwieweit diese Techniken konventionelle Waffen ersetzen können. Alle diese Vorhaben zur offensiven Informationskriegführung unterliegen höchster Geheimhaltung und wurden bisher im Kongreß nicht öffentlich diskutiert.[51] Angehörigen der Streitkräfte war es bis letztes Jahr verboten, den Begriff «offensive computer operations« in öffentlichen Debatten zu verwenden.[52] Im Oktober 1998 wurde erstmals ein offizielles Dokument zur US-amerikanischen Informationskriegs-Strategie veröffentlicht, die Joint Doctrine for Information Operations (Joint Publication 3-13)[53].

Informationskrieg ist mehr als Cyberkrieg

Den Krieg um das Kosovo hat die NATO vor allem mit der Zerstörung der jugoslawischen Kommandostrukturen durch rohe Gewalt gewonnen, indem sie gezielt die Kommando- und Kommunikationseinrichtungen der jugoslawischen Streitkräfte bombardiert hat.[54] Diese Spielart des Informationskrieges, die in den USA *Command and Control War (C²-War)* genannt wird, macht die gegnerischen Truppen führungslos und schneidet sie von Aufklärungs- und anderen Daten ab.[55] Blind und auf sich selbst gestellt ziehen sie sich in der Regel zurück oder ergeben sich ohne größeren Widerstand, so zumindest die Erfahrung aus dem Golfkrieg 1991. Die von den Einheiten für psychologische Kriegführung (*PsyOps*) massenhaft verteilten Handzettel »Sie sind ein NATO-Ziel« haben ihr übriges dazugetan. Die paar Millionen Dollar dagegen, um die der jugoslawische Präsident durch die CIA-Hacker unter Umständen erleichtert worden ist, sind dagegen psychologisch wichtig, aber nicht kriegsentscheidend. Zu einem Informationskrieg gehört im amerikanischen Verständnis nämlich weit mehr als nur das Eindringen in gegnerische Computernetze.

Laut dem offiziellen Wörterbuch des Pentagon umfaßt Informationskrieg »Aktionen, die unternommen werden, um die Informationsüberlegenheit zu erlangen, indem die Informationen, informationsbasierten Prozesse, Informationssysteme und computerbasierten Netze beeinträchtigt werden, während die eigenen Informationen, informationsbasierten Prozesse, Informationssysteme und computerbasierten Netze ausgenutzt und verteidigt werden«[56]. Demnach wird die *gesamte* »Informationsumgebung« nun zentral für die militärischen Planungen. Es gilt also, nicht nur die Computernetze des Gegners lahmzulegen, sondern auch seine Sensoren zu täuschen, die Bevölkerung zu beeinflussen und an der Heimatfront für die richtigen Kriegsbilder zu sorgen. Das Ziel ist die Kontrolle der globalen Informationssphäre und aller ihrer Teilbereiche im Umfeld eines Krieges. Die Ausweitung des Krieges auf den Cyberspace ist nur ein Bereich von den vielen Informationsarenen, die durch Informationsoperationen auf neue Art ins Interesse der Militärs rücken. Neben diesen neuen, von den Medien begierig aufgenommenen virtuellen Aufgaben werden auch so alte Techniken wie die Bombardierung gegnerischer Kommandostrukturen oder die psychologische Kriegführung unter dem Oberbegriff »Informationsoperationen« zusammengefaßt. Besonders die mediale Repräsentation des Krieges im Fernsehen wird als zentral angesehen.[57] Der damalige Vorsitzende der Vereinigten Stabschefs, General Colin Powell, brachte dies zur Zeit des Golfkrieges 1991 bereits auf den Punkt: »Wenn alle Truppen in Bewegung sind und die Kommandeure an alles gedacht haben, richte deine Aufmerksamkeit auf das Fernsehen, denn du kannst die Schlacht gewinnen oder den Krieg verlieren, wenn du mit der Story nicht richtig umgehst«[58]. In der Pentagon-nahen Denkfabrik RAND Corporation in Santa Monica wird inzwischen über die Aufstellung von »Special Media Forces« nachgedacht.[59]

In diesem erweiterten Verständnis des Informationskrieges reicht auch eine entsprechend glaubwürdig durchgesickerte Meldung über Computerattacken, wenn dadurch der Gegner unter Druck gesetzt werden kann. Die Banken-Geschichte der CIA könnte daher auch eine gezielte Falschmeldung gewesen sein. Nach der Doktrin der Informationsoperationen ist es aber vor allem für die NATO eminent wichtig, sich öffentlich als unangreifbar darzustellen. Insofern haben die Hacker-Angriffe zwar keinen militärischen, aber einen massiven Image-Schaden bei der NATO hinterlassen. NATO-Sprecher Jamie Shea mußte Ende Mai zugeben, daß die aufwendig gemachte NATO-Webseite zeitweise nur sporadisch erreichbar war – eine peinliche Situation für ein Militärbündnis, das gerade dabei ist, die Überlegenheit seiner High-Tech-Streitkräfte vorzuführen.[60]

Hinweise des Autors:

Eine Menge Links, viele Literaturhinweise und einige Texte zum Thema »Militär in der Informationsgesellschaft« sind auf der Homepage des

Autors verfügbar: http://userpage.fu-berlin.de/~bendrath.
Dort kann auch die deutschprachige Mailingliste »Infowar.de« abonniert werden.

Andere Internet-Seiten zum Thema:

http://www.infowar.com: *Infowar.com, die größte Seite zum Thema. Winn Schwartau sammelt einfach alles!*

http://www.epic.org/security/infowar/resources.html: *Electronic Privacy Information Council, Infowar Resources: behandelt vor allem Probleme des Datenschutzes und der Verschlüsselung, haben einen langen Bericht zum Thema verfaßt.*

Weitere Lesetips:

Arqilla, John / David Ronfeld (Hg.): In Athena´s Camp. Preparing for Conflict in the Information Age, Santa Monica 1997: *Eine Zusammenstellung der wichtigsten Texte aus der militärnahen Debatte der letzten Jahre.*

Bendrath, Ralf: Militärpolitik, Informationstechnologie und die Virtualisierung des Krieges, in: Peter Bittner, Jens Woinowski (Hg.): Mensch – Informatisierung – Gesellschaft, Münster: Lit Verlag, 1999 (gekürzt als »Krieg im Cyberspace« in: Frankfurter Rundschau, 1.4.1999, S. 24): *Überblick über die Entwicklung in den USA, mit Fokus auf das Verhältnis Militär-Politik*

Klischewski, Ralf/Ingo Ruhmann: Ansatzpunkte zur Entwicklung von Methoden für die Analyse und Bewertung militärisch relevanter Forschung und Entwicklung im Bereich Informations- und Kommunikationstechnologie, Studie für das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Bonn 1995: Ausführliche Darstellung des Themas, mit Schwerpunkt auf Führungs- und Informationssystemen

Libicki, Martin: What is Information Warfare?, ACIS Paper Nr. 3, Washington D.C., August 1995, http://www.ndu.edu/ndu/inss/actpubs/act003/a003cont.html: Ein Klassiker, der verschiedene Arten von Informationskrieg unterscheidet.

Nye, Joseph S., jr./William A. Owens: America´s Information Edge, in: Foreign Affairs, 3./4. 1996, S. 20-36: Paradigmatisch für die amerikanische Strategie der weltweiten Informationsdominanz.

Henry, Ryan/C. Edward Peartree: Military Theory and Information Warfare, in: Parameters, Herbst 1998, S. 121-35, http://carlisle-www.army.mil/usawc/Parameters/98autumn/ henry.htm: Ein Artikel, der sich mit den verschiedenen Theorieschulen des Informationskrieges und ihren Zukunftsvisionen auseinandersetzt.

---

1 Gregory L. Vistica: »Cyberwar and Sabotage« in: Newsweek, 31.5.1999, S. 22
2 Zum Beispiel Tom Clancy / Steve R. Pieczenik: Netforce, Berkley Publishing Group, 1999
3 Zum Beispiel James Bond: Goldeneye
4 http://www.infowar.com/mil_c4i/99/mil_c4i_042399a_j.shtml
5 Ralf Bendrath ist Politikwissenschaftler und Redakteur der ZivilCourage. Er promoviert an der Freien Universität Berlin über »Das Militär in der Informationsgesellschaft« und betreibt eine Internet-Mailingliste zu diesem Thema. Näheres unter http://userpage.fu-berlin.de/~bendrath.
6 FR, 18.11.1997
7 SZ, 10.4.99
8 http://www.infowar.com/mil_c4i/99/mil_c4i_042399a_j.shtml
9 U.S. News & World Report, 10.5.1999, http://www.usnews.com/usnews/issue/990510/10info.htm
10 Elizabeth de Bony: NATO reinforces against Net attack from Serbs, InfoWorld Electric, 2.4.1999, http://archive.infoworld.com/cgi-bin/displayStory.pl?99042.einato.htm
11 CNN, 31.3.1999, http://www.cnn.com/WORLD/europe/9903/31/nato.hack/
12 http://www.infowar.com/mil_c4i/99/mil_c4i_042399a_j.shtml
13 Betroffen waren in den USA das Los Alamos National Laboratory und das Ohio Department of Development, http://freespeech.org/resistance
14 Royal United Services Institute, Newsbrief, Mai 1999, S. 39.
15 Spiegel Online, 10.5.1999, http://www.spiegel.de/netzwelt/politik/0,1518,21796,00.html
16 Florian Rötzer: Chinesen protestieren auch im Internet, telepolis, 10.05.99, http://www.heise.de/tp/deutsch/inhalt/te/2834/1.html
17 Spiegel Online, 10.5.1999, http://www.spiegel.de/netzwelt/politik/0,1518,21796,00.html
18 Sehr übersichtlich ist z.B. das Digital R3sist4nc3 Archive of Hacked Websites, http://freespeech.org/resistance.
19 Eine Anspielung auf den James Bond-Film »Liebesgrüße aus Mokau«
20 SZ, 10.4.1999; http://freespeech.org/resistance/nmimc1/med_navy_mil.htm.
21 Die Protestseite ist http://www.alert.org.yu/stop-nato.html, vgl. http://freespeech.org/resistance/windsurfer/www_americanwindsurfer_com.html.
22 http://www.hackernews.com/archive/ crackarch.html
23 SZ, 10.4.1999
24 Ellen Messmer: Kosovo cyber-war intensifies, in: Network World Fusion, 12.5.1999, http://www.nwfusion.com/news/1999/0512kosovo.html
25 http://freespeech.org/resistance/kpz/nato.html. Das gleiche Bild wurde von KpZ einen Tag später auf einer NASA-Seite hinterlassen.
26 http://freespeech.org/resistance/genetic/ berlin_genetic_com_br.html
27 http://hacktivism.tao.ca
28 Vgl. Stefan Wray: The Electronic Disturbance Theater and Electronic Civil Disobedience, 17.6.1998, http://www.nyu.edu/projects/wray/EDTECD.html; EDT-Homepage: http://www.thing.net/~rdom/ecd/ ecd.html
29 Winn Schwartau: Cyber-civil disobedience. Inside the Electronic Disturbance Theater's battle with the Pentagon, Network World, 11.1.1999, http://www.nwfusion.com/news/0111vigcyber.html
30 Vgl. Elvi Claßen: Infopeace im Cyberspace?, in: ZivilCourage, Nr. 1/99, S. 14.
31 LoU strike out with international coalition of Hackers: A joint statement by 2600, the Chaos Computer Club, the Cult of the Dead Cow, !Hispahack, L0pht Heavy Industries, Phrack and Pulhas, 7.1.1999, http://www.ccc.de/CRD/CRD19990107.html
32 Die CIA sollte danach albanische Rebellen für Sabotageaktionen ausbilden, mit denen die serbische Bevölkerung gegen ihren Präsidenten aufgebracht werden sollte. Zu den Ausbildungszielen gehörten u.a. Häusersprengungen, der Diebstahl von Lebensmittelvorräten oder die Verunreinigung von Benzinlagern.
33 Gregory L. Vistica: »Cyberwar and Sabotage« in: Newsweek, 31.5.1999, S. 22
34 zdf-news, 2.6.1999
35 Gregory L. Vistica: »Cyberwar and Sabotage« in: Newsweek, 31.5.1999, S. 22
36 zdf-news, 2.6.1999
37 Gregory L. Vistica: »Cyberwar and Sabotage« in: Newsweek, 31.5.1999, S. 22
38 Bradley Graham: Military Grappling With Guidelines For Cyber Warfare. Questions Prevented Use on Yugoslavia, Washington Post, 8.11.1999.
39 Immerhin gelang es der US Air Force nach eigener Darstellung, den Serben durch einen Hack in die Luftverteidigungssysteme falsche Ziele auf die Bildschirme zu spielen. Lisa Hoffman: Special Report. U.S. opened cyber-war during Kosovo-Fight, Washington Times, 25.10.1999.
40 Das beliebte Schlagwort dafür ist »elektronisches Pearl Harbour«, das an den Überfall der japanischen Luftwaffe auf die US-Navy im Zweiten Weltkrieg erinnert, vgl. http://www.soci.niu.edu/~crypt/other/harbor.htm
41 Vgl. z.B. Executive Order 13010 von Präsident Bill Clinton, 15.7.1996, wo die an der Presidential Commission on Critical Infrastructure Protection (PCCIP) beteiligten Einrichtungen aufgezählt werden, http://www.pccip.gov/eo13010.html.
42 http://www.fbi.gov/nipc/index.htm
43 Vgl. National Security Council: White Paper. The Clinton Administration´s Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, Mai 1998, http://www.whitehouse.gov/WH/EOP/NSC/html/NSCDoc3.html
44 Bradley Graham: In Cyberwar, A Quandry Over Rules And Strategy, in: International Herald Tribune, 9.7.1998
45 David A. Fulghum: Cyberwar Plans Trigger Intelligence Controversy, in: Aviation Week&Space Technology, 19.1.1998, S. 55.
46 Jay Peterzell: Spying and Sabotage by Computer, in: Time, 20.3.1989, zit. nach Ute Bernhardt / Ingo Ruhmann: Der Krieg der elektronischen Waffen – Elektronische Kriegsführung, in: dies. (Hg.): Ein sauberer Tod. Informatik und Krieg, Marburg 1991, S. 123.
47 Douglas Waller: Onward Cyber Soldiers, in: Time Magazine, 21.8.1995
48 Vgl. Ralf Klischewski/Ingo Ruhmann: Ansatzpunkte zur Entwicklung von Methoden für die Analyse und Bewertung militärisch relevanter Forschung und Entwicklung im Bereich Informations- und Kommunikationstechnologie, Studie für das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Bonn 1995, S. vi.
49 Vgl. John M. Shalikashvili: Joint Vision 2010, Joint Chiefs of Staff, Washington D.C. 1996, http://www.dtic.mil/doctrine/jv2010/jv2010.pdf, S. 16
50 U.S. Army Training and Doctrine Command: Field Manual 100-6, Information Operations, August 1996, http://www.fas.org/irp/doddir/army/fm100-6
51 Bei einer Anhörung des Senates zur defensiven Seite der Informationskriegführung im Juni 1998 antwortete der CIA-Direktor George Tenent auf die Frage, ob offensive Fähigkeiten entwickelt würden, nur mit einem Satz: »We're not asleep at the switch in this regard«, zit. nach Bradley Graham: In Cyberwar, A Quandry Over Rules And Strategy, in: International Herald Tribune, 9.7.1998.
52 Vgl. David A. Fulghum: Cyberwar Plans Trigger Intelligence Controversy, in: Aviation Week&Space Technology, 19.1.1998, S. 53.
53 http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf
54 vgl. z.B. tagesschau-dossier, 25.5.1999, http://www.tagesschau.de/ts/archiv/1999/Mar/23/ kosovo/M/chronologie/R/05-25-angriffe.html; NATO Press Conference, Given by Mr Jamie Shea and Major General Walter Jertz, 6.5.1999, http://www.nato.int/kosovo/press/p990506c.htm
55 Kerry A. Blount/Lauren D. Kohn: C2-Warfare in FM 100-6, in: Military Review, Nr. 4, Juli-August 1995, S. 66-69
56 DoD Dictionary of Military and Associated Terms, http://www.dtic.mil/doctrine/jel/doddict/data/i/02944. html, Übersetzung R.B.
57 U.S. Army Training and Doctrine Command: Field Manual 100-6, Information Operations, August 1996, http://www.fas.org/irp/doddir/army/fm100-6
58 Zit. nach: McKenzie Wark: Virtual Geography. Living with Global Media Events, Bloomington, Indianapolis 1994, S. 41, Übersetzung R.B.
59 John Arquilla / David Ronfeldt: The Emergence of Noopolitics. Towards an American Information Strategy, Santa Monica 1999, S. 50f.
60 Press Conference of the NATO Spokesman, Jamie Shea and Air Commodore David Wilby, 31.5.19991

Hans-Georg Ehrhart/Matthias Z. Karádi

Krieg auf dem Balkan[1]

Lage, Interessen, Optionen, Lehren und Perspektiven

Im März 1999 fielen die ersten NATO-Bomben auf Belgrad. Genau ein Jahr zuvor fragten wir in einem Beitrag, ob der Balkan zu brennen beginne und plädierten angesichts der sich anbahnenden Gewalteskalation für eine komplexe Präventionspolitik im Kosovo-Konflikt.[2] Kurz darauf tobte bereits der Bürgerkrieg zwischen jugoslawischen Sicherheitskräften und der Befreiungsarmee für das Kosovo (UCK). Während sich die internationale Gemeinschaft nur mühsam zu politischen, wirtschaftlichen und ersten militärischen Maßnahmen durchrang, gab sich der jugoslawische Präsident Milosevic gesprächsbereit und betrieb gleichzeitig eine gegen die Kosovaren gerichtete Unterdrükkungs- und Vertreibungspolitik.[3] Seine Ablehnung des Friedensabkommens von Rambouillet führte schließlich zum Krieg der NATO gegen die Bundesrepublik Jugoslawien.

1. Wie ist die Lage?

Politisch

Was hätte das für ein rauschendes Fest werden können! Die NATO beabsichtigte, ihren fünfzigsten Geburtstag als der Stabilitätsanker der europäischen Sicherheit zu begehen. Doch der Krieg auf dem Balkan hat der Jubilarin die Festtagsstimmung gründlich verdorben. Ihr Gipfeltreffen vom 23. bis 25. April 1999 in Washington beging die NATO nicht als Friedensgarant sondern als Kriegspartei.[4]

Die NATO führt Krieg, auch wenn ihre Repräsentanten dieses Wort tunlichst vermeiden. Sie sprechen lieber von »humanitärer Intervention«, von »militärischen Luftschlägen« und »chirurgischen Eingriffen«. Nicht das jugoslawische Volk sei das Ziel, sondern der Despot in Belgrad. Mit anderen Worten: Die NATO befinde sich nicht im Krieg, sondern sie vollführe eine »Polizeiaktion« zur Bestrafung Milosevics aus, quasi eine präventive Maßnahme zur regionalen Friedenssicherung. Zugleich wächst jedoch die Nervosität unter den Verbündeten. Denn bislang hat die NATO kaum eines ihrer Ziele erreicht. Darüber können auch die Erfolgs- und Treffermeldungen auf den täglichen Pressekonferenzen in Brüssel nicht hinwegtäuschen. Mit der zunehmenden Zahl ziviler Opfer stellt sich die Frage nach der Verhältnismäßigkeit der Mittel. Die westliche Allianz ist gleich einer ganzen Reihe von Fehlkalkulationen erlegen. Es zeichnet sich ab, daß die Allianz ihre Ziele durch die Bombardements nicht erreichen wird, so daß mittlerweile in der NATO eine Diskussion über den Einsatz von Bodentruppen begonnen hat. Zugleich beginnt man zu ahnen, daß die NATO selbst nicht unbeschadet aus dem Konflikt hervorgehen könnte.

Die neunziger Jahre werden in die Chroniken eingehen als das Jahrzehnt der Balkankriege. Dabei verlagerten sich die Kriege im ehemaligen Jugoslawien von Norden nach Süden: Es begann 1991 in Slowenien und Kroatien, 1992 folgte Bosnien und 1999 erreichte der Krieg schließlich Serbien, Montenegro und das Kosovo. Lediglich Mazedonien blieb bislang als einzige ehemals jugoslawische Teilrepublik vom Krieg verschont. Offiziell besteht das ehemalige Jugoslawien heute aus fünf Staaten: Slowenien, Kroatien, Bosnien-Herzegowina, Mazedonien und der Bundesrepublik Jugoslawien. Aber in der Realität sind es mindestens neun Teile, denn Bosnien ist geteilt in eine Serbische Republik und die Föderation, die ihrerseits aufgeteilt ist in kroatisch und bosniakisch kontrollierte Gebiete. Die Bundesrepublik Jugoslawien wiederum besteht aus Serbien, dem Kosovo und dem zunehmend nach Unabhängigkeit strebenden Montenegro. Und selbst in Serbien gibt es die ehemals autonome Provinz Vojvodina und den muslimisch besiedelten Sandschak. Auch Mazedonien wiederum könnte man in einen slawischen Teil und einen albanisch geprägten Teil im Westen aufteilen. Damit sind zwölf verschiedene ethnisch definierte Gebiete im Spiel, die bei einer Neuordnung des Balkans zu berükksichtigen wären. Viele davon streben wiederum nach Vereinigung mit den Nachbarstaaten: Neben »Großserbien« ist auch »Großkroatien« und »Großalbanien« für viele Menschen in der Region ein anzustrebendes Ziel. Angesichts solcher Komplexität ist davon auszugehen, daß eine friedliche Neuordnung des Balkans viele Jahre dauert, enorme Summen kostet und nur über die langfristige Aussicht auf Integration in die euro-atlantischen Strukturen Erfolg verspricht. Dennoch gibt es dazu keine Alternative.

Rechtlich

Stellen die militärischen Schläge der NATO eine die Souveränität Jugoslawiens verletzende, völkerrechtlich verbotene Gewaltanwendung dar? Oder sind sie zur Durchsetzung fundamentaler Werte der internationalen Gemeinschaft gerechtfertigt? Laut Kapitel VII der UN-Charta ist einzig und allein der UN-Sicherheitsrat dazu befugt, militärische Zwangsmaßnahmen gegen einen souveränen Staat anzuordnen. Dennoch macht man es sich im Falle Kosovo zu einfach, wenn man sich lediglich auf diese legalistische Haltung zurückzieht, zumal man sich über den Charakter der Vereinten Nationen keine Illusionen machen sollte. Sie sind eben nicht ausschließlich ein weltweites System Kollektiver Sicherheit, sondern in erster Linie ein Konzert der Großmächte. Denn bis heute hat das Gewaltmonopol »in der Charta und in der institutionellen Ausgestaltung der Weltorganisation keine Basis. Bestenfalls kann man von einem ‚Autorisierungsmonopol' der UNO sprechen, dessen Bedeutung aber durch die Ermessensfreiheit des Sicherheitsrats eingeschränkt ist«.[5]

Ist der NATO-Krieg gegen Jugoslawien ein Rechtsbruch oder ein Präzedenzfall? Entwickelt sich gar ein Völkergewohnheitsrecht hin zur humanitären Intervention?[6] Und unter welchen Voraussetzungen ist eine solche rechtmäßig? Können aus den menschenrechtlichen Verpflichtungen des Völkerrechts vielleicht sogar verbindliche Rechtspflichten abgeleitet werden, die mit

A 2nd Bomb Wing, Barksdale Air Force Base, La., B-52H deployed to RAF Fairford, U.K. in support of Operation Allied Force taxis down the runway past a row of Air Launch Cruise Missiles (ALCMs) after landing from a mission.
U.S. Air Force photo by Staff Sergeant Jim Howard

anderen zwingenden Normen des Völkerrechts (etwa dem Gewaltverbot der UN-Charta) konkurrieren? So verpflichtet die vierte Genfer Konvention von 1949 die Unterzeichnerstaaten – also auch Jugoslawien – dazu, keine Kriegsverbrechen an der Zivilbevölkerung zu verüben. In der »Konvention über die Verhütung und Bestrafung des Völkermordes« von 1948 heißt es in Artikel 1: »Die Vertragsschließenden Parteien bestätigen, daß Völkermord, ob im Frieden oder im Krieg begangen, ein Verbrechen gemäß internationalem Recht ist, zu dessen Verhütung und Bestrafung sie sich verpflichten.«[7] (Herv. durch die Verf.) Auch der Internationale Gerichtshof in Den Haag hat das Völkermordverbot und seine Durchsetzung als völkerrechtliche Verpflichtung bezeichnet, die verbindlich für alle Staaten gelte. Nun sollte man mit dem Terminus »Völkermord« vorsichtig umgehen, aber wenn auch nur die Hälfte der Berichte über Greueltaten aus dem Kosovo stimmt, muß man konstatieren, daß dort ein Völkermord im Gange ist. Die Völkermorddefinition in Artikel II der Konvention trifft auf die Vorgänge im Kosovo sicherlich zu: »In dieser Konvention bedeutet Völkermord eine der folgenden Handlungen, die in der Absicht begangen wird, eine nationale, ethnische, rassische oder religiöse Gruppe als solche ganz oder teilweise zu zerstören: (a) Tötung von Mitgliedern der Gruppe; (b) Verursachung von schwerem körperlichem oder seelischem Schaden an Mitgliedern der Gruppe; (c) vorsätzliche Auferlegung von Lebensbedingungen für die Gruppe, die geeignet sind, ihre körperliche Zerstörung ganz oder teilweise herbeizuführen; (d) Verhängung von Maßnahmen, die auf die Geburtenverhinderung innerhalb der Gruppe gerichtet sind; (e) gewaltsame Überführung von Kindern der Gruppe in eine andere Gruppe.«[8] Auch UNO-Generalsekretär Kofi Annan hat im Zusammenhang mit dem Kosovo den Begriff »Genozid« gebraucht. Fest steht, daß nicht erst seit den UNO-Einsätzen in Bosnien und Somalia ein Paradigmenwechsel im Völkerrecht stattfindet, nach dem Menschenrechte nicht mehr zu den »inneren Angelegenheiten« eines Staates gehören.

Eine weitere Frage, die sich in diesem Zusammenhang stellt, ist, ob durch die NATO im Kosovo nicht ein gefährlicher Präzedenzfall geschaffen wurde, auf den sich auch andere »Ordnungsmächte« berufen können. Droht gar ein zügelloser und militanter Humanismus zur Durchsetzung der Menschenrechte? Denn wer definiert letztendlich, wann und ob eine humanitäre Intervention gerechtfertigt ist? In diesem Zusammenhang ist auch der Vorwurf der Doppelmoral zu diskutieren. Warum greift die NATO im Kosovo ein, duldet aber beispielsweise die Unterdrückung der Kurden durch die Türkei? Auch wenn es berechtigt und notwendig ist, auf diese Doppelstandards hinzuweisen, bleibt diese Argumentation letztlich wohlfeil, wenn sie nach dem Motto verfährt: »Wenn wir nicht überall intervenieren, dann nirgends.«

Wenn man den Argumenten einer Weiterentwicklung des Völkerrechts im Sinne einer humanitären Intervention bei Völkermord und schweren Verbrechen gegen die Menschlichkeit folgt, würde dies in der Konsequenz bedeuten, daß daraus eine Interventionspflicht abzuleiten wäre. M.a.W.: Die UNO, die NATO oder die vielzitierte »coalition of the willing« wird bei zukünftigen Kosovos, Ruandas oder Bosniens eingreifen müssen. Daraus folgt eigentlich, daß humanitäre Interventionen nicht selektiv erfolgen dürfen. Eine weitere Schwierigkeit besteht darin, daß höchstwahrscheinlich auch in Zukunft Atom- und Großmächte nicht zu den »Adressaten« einer humanitären Intervention gehören werden. Um der Willkür nicht Tür und Tor zu öffnen ist vorgeschlagen worden, die Bedingungen, die eine humanitäre Intervention rechtfertigen, festzulegen.[9] Dazu gehören u.a.:

- alle diplomatischen und politischen Mittel der friedlichen Streitbeilegung müssen ausgeschöpft worden sein oder sich als offensichtlich aussichtslos erweisen, um die Gewaltanwendung als »ultima ratio« als gerechtfertigt erscheinen zu lassen;

- der Grundsatz der Verhältnismäßigkeit muß gewahrt sein, d.h. eine zur Abwehr völkerrechtswidriger Handlungen ergriffene Maßnahme muß geeignet, erforderlich und verhältnismäßig i.e.S. sein, die völkerrechtswidrige Handlung zu unterbinden, und

- die Maßnahme muß von einem »legitimen« Organ beschlossen werden, wobei ein kollektives Vorgehen von Staaten eine höhere Glaubwürdigkeit besitzt als unilaterale Aktionen und Beschlüsse eines Systems Kollektiver Sicherheit eine höhere

Autorität genießen als Aktionen von Bündnissen oder »coalitions of the willing«.

Wendet man diese Kriterien auf den Jugoslawienkrieg an, so ist zu konstatieren, daß zumindest die zweite Bedingung nicht zutrifft. Die Luftangriffe der NATO haben sich im Sinne des ursprünglichen Zieles als ungeeignet erwiesen, und der Grundsatz der Verhältnismäßigkeit wird mit der Fortdauer des Krieges zunehmend in Frage gestellt. Auf jeden Fall bleibt die grundsätzliche Frage, wer denn, wenn nicht die UNO, die Geltung dieser Kriterien überprüfen soll.

Militärisch

Die Militärmaschinerie von Slobodan Milosevic ist zwar geschwächt, aber noch lange nicht ausgeschaltet. Auch wenn ein Großteil der jugoslawischen Luftwaffe mittlerweile am Boden zerstört oder im Luftkampf abgeschossen wurde, ist beispielsweise die serbische Luftabwehr noch längst nicht vollständig zerstört worden. Darüber hinaus sind auch die Armee und die jugoslawische Sonderpolizei noch weitgehend intakt.

Mit der Verlegung der Apache-Kampfhubschrauber plant die NATO massive Luftangriffe gegen die serbischen und jugoslawischen Verbände, die direkt im Kosovo operieren. Ein weiteres Ziel der NATO-Bombardements sind die serbischen Treibstofflager und Raffinerien, von denen ein Großteil bereits zerstört wurde. Die NATO und mittlerweile auch die EU drängen jedoch auf ein Ölembargo gegen Jugoslawien, um die jugoslawische Armee vollständig vom Treibstoff abzuschneiden. Mittels einer Seeblockade soll verhindert werden, daß in Montenegros Häfen weiter Öl gelöscht wird.

Humanitär

Über die Hälfte der 1,8 Millionen Kosovo-Albaner sind mittlerweile vertrieben oder befinden sich auf der Flucht. Die systematische Vertreibung der Kosovaren ist die größte humanitäre Katastrophe in Europa seit dem Ende des Zweiten Weltkrieges. Bereits vor dem Krieg sind nach Schätzungen des UNHCR etwa 170.000 Kosovaren geflohen. In den sechs Wochen des Luftkrieges sind weit mehr als 600.000 Kosovo-Albaner

A M1A2 Abrams tank from the 1st Armor Division crosses the Sava River into Bosnia, December 31, 1995. Foto: US Army

vor allem nach Albanien, Mazedonien und Montenegro geflüchtet. Mehrere Hunderttausend Kosovaren befinden sich innerhalb des Kosovo auf der Flucht bzw. sind von serbischen Einheiten eingekesselt. Es scheint dem serbischen Kalkül zu entsprechen, eine gewisse Zahl von Albanern im Kosovo als menschliche Schutzschilde für die jugoslawischen Armee- und Polizeiverbände gegen NATO-Luftangriffe und als Geiseln für den möglichen Bodenkrieg festzuhalten.

2. Welche Ziele und Interessen verfolgen die Akteure?

NATO

Das Engagement der NATO im Kosovo-Konflikt entwickelte sich sehr zögerlich. Noch im März 1998 beschied der NATO-Rat den albanischen Wunsch nach Entsendung von Streitkräften negativ. Die NATO wollte sich noch nicht in den jugoslawischen Sumpf hineinziehen lassen. Ende Mai wurden Prüfungsaufträge zur präventiven Verlegung von NATO-Truppen nach Mazedonien und Albanien an den Militärausschuß der NATO übermittelt. Am 11. Juni 1998 erteilten die Verteidigungsminister den Militärs einen Planungsauftrag, der die ganze Bandbreite möglicher militärischer Einsatzoptionen für das Kosovo bzw. die Bundesrepublik Jugoslawien umfaßte. Im Spätsommer wurden gemeinsame Manöver mit den albanischen und den mazedonischen Streitkräften abgehalten sowie ein Verbindungsbüro im Rahmen der Partnerschaft für den Frieden in Tirana eröffnet. Mit diesen Maßnahmen sollten einerseits Skopje und Tirana der Unterstützung der NATO versichert werden. Andererseits sollte Druck auf Belgrad ausgeübt werden, um es zu einer einvernehmlichen Regelung des Kosovo-Konflikts zu bewegen.

Vor dem Hintergrund der anhaltenden serbischen Offensive und der durch sie ausgelösten Flüchtlingsströme steigerte die NATO im Oktober 1998 den Druck, indem sie mit dem Aktivierungsbeschluß den Oberbefehlshaber ermächtigte, Luftschläge anzuordnen. Dem amerikanischen Sonderbotschafter Richard Holbrooke gelang es in letzter Minute, eine Übereinkunft mit Milosevic zur Beendigung des siebenmonatigen Feldzuges gegen die UCK zu erzielen. Belgrad akzeptierte, den größten Teil seiner Truppen aus dem Kosovo abzuziehen, humanitäre Hilfe für die Binnenflüchtlinge zuzulassen und das Abkommen durch OSZE-Beobachter zu Lande sowie mit unbemannten Flugkörpern aus der Luft überwachen zu lassen. Zum Schutz der OSZE-Beobachter wurden – gegen den ausdrücklichen Willen Belgrads – NATO-Truppen nach Mazedonien entsandt. In der Folgezeit zielte die Politik der NATO auf die Ein-

haltung dieses Abkommens, welches jedoch seit November 1998 von beiden Seiten verletzt wurde.

Als dieses Vorhaben zu scheitern drohte, entwarfen die Mitglieder der Kontaktgruppe einen Friedensplan, der den Konfliktparteien Anfang Februar in Rambouillet zur Annahme vorgelegt wurde. Dieser sieht u.a. ein hohes Maß an Autonomie für die Kosovo-Albaner und die Stationierung einer 28.000 Soldaten umfassenden internationalen Friedenstruppe unter Führung der NATO im Kosovo vor (KFOR). Eine bewaffnete Friedenstruppe lehnte Milosevic aber ebenso grundsätzlich ab wie die Forderung, ihr ganz Jugoslawien zugänglich zu machen.[10] Belgrad sollte nun durch die Androhung militärischer Gewalt zur Unterzeichnung des Friedensplans gebracht werden. Seit Beginn der Luftschläge wurden im- und explizit folgende Ziele verfolgt:

- Die Unterzeichnung des Friedensabkommens von Rambouillet durch die BRJ sollte erzwungen werden. Dabei stellte sich von Beginn an die Frage, was passieren sollte, wenn Milosevic nicht einlenkt.

- Eine humanitäre Katastrophe sollte verhindert werden. Daß Milosevic die Vertreibungspolitik mit den NATO-Luftschlägen intensivierte, darf nicht überdecken, daß er diese Politik bereits vorher zielstrebig verfolgte, aber nicht in diesem Maße durchführen konnte. Selbst durch die Anwesenheit der OSZE-Beobachter ließ er sich nicht davon abhalten. Gleichwohl ist angesichts von über 700.000 Flüchtlingen seit März 1998 zu konstatieren, daß das humanitäre Ziel nicht erreicht werden konnte.

- Milosevics Fähigkeit zur Kriegführung gegen die Kosovaren soll reduziert werden. Dadurch erhofft man sich ein Einlenken Belgrads oder gegen Milosevic gerichtete Reaktionen aus dem jugoslawischen Militär. Zudem wird langsam aber sicher das Kräfteverhältnis zugunsten der UCK verändert. Schließlich werden die Bedingungen für einen Bodeneinsatz von NATO-Truppen günstiger.

- Nachdem deutlich wurde, daß die beiden ersten Ziele nicht und das dritte nur partiell erreicht werden konnten, wurde die möglichst schnelle und gesicherte Rückkehr der Vertriebenen, Flüchtlinge und Deportierten in den Zielkatalog aufgenommen. Bis dahin engagiert sich die NATO bei der Organisation der Verteilung der Flüchtlingshilfe in Albanien.

- Die Flüchtlingswelle in die Nachbarstaaten gefährdet das strategische Ziel, das regionale Eskalationsrisiko einzudämmen und das Umfeld zu stabilisieren. Wenn der Jugoslawienkrieg auf Mazedonien und Albanien übergreift oder, nach seinem Ende, sich die Befürworter eines Großalbaniens durchsetzen sollten, besteht die Gefahr, daß Bulgarien sowie die beiden NATO-Mitglieder Griechenland und Türkei in die Auseinandersetzung verwickelt werden. Ein zentraler Teil der Südflanke der NATO könnte destabilisiert werden.

- Der NATO geht es auch darum, ihre Glaubwürdigkeit und Handlungsfähigkeit bei der Bewältigung ihrer neuen Rolle – dem Export von Stabilität »out of area« und Wahrung zentraler nationaler Interessen – unter Beweis zu stellen. Ähnlich wie im Bosnien-Krieg will die mächtigste Militärallianz der Welt gerade im Jahr ihres fünfzigsten Geburtstages nicht als Papiertiger dastehen, sondern ihre führende Rolle bei der Gestaltung der europäischen Sicherheit untermauern. Gleichwohl hat sie sich in eine problematische Lage manövriert, indem sie einerseits den letzten Schritt – den Einsatz von Bodentruppen auch gegen den Willen Belgrads – von vornherein ausgeschlossen hat. Andererseits ist es fraglich, wie lange die Geschlossenheit der Allianz währt, wenn das Bombardement noch fortdauert und politische Erfolge ausbleiben.

- Obwohl die NATO bislang eine erstaunliche Geschlossenheit bewiesen hat, sind die Interessenlagen der neunzehn Mitgliedstaaten natürlich nicht homogen. So hegt z.B. Griechenland aus historischen, strategischen, wirtschaftlichen und politischen Gründen eine besondere Affinität zur Bundesrepublik Jugoslawien. Das Neumitglied Ungarn muß als Nachbarstaat der BRJ Rücksicht auf die ungarische Minderheit in der serbischen Provinz Vojvodina nehmen. Frankreich ist weder an einer anhaltenden Schwächung des UNO-Sicherheitsrates interessiert noch daran, daß der Balkan unter amerikanische Kuratel kommt. Die USA wiederum verfolgen das strategische Ziel der Sicherung der europäischen Gegenküste, wobei der amerikanische Einflußbereich über den Balkan hinausreicht und perspektivisch auch den Kaukasus und die zentralasiatischen GUS-Länder umfaßt.

Sava River Crossing
Foto: US Army

Russische Föderation

Rußland betreibt notgedrungen eine widersprüchliche Politik. Einerseits kritisiert es in harschen Tönen die Luftangriffe der NATO, zieht seine Verbindungsoffiziere aus den NATO-Institutionen zurück und droht mit schwerwiegenden Folgen. Andererseits macht es z.B. auf den Feldern Wirtschaft und Rüstungskontrolle business as usual. Es verschärft den Konflikt nicht, etwa indem es Waffen an die Serben liefert. Vielmehr ist die jetzige Regierung weiterhin an einem Ausgleich mit dem Westen und an einer Lösung des Kosovo-Problems interessiert. Gleichwohl hat Präsident Jelzin die rote Linie klar definiert, indem er einen Politikwandel für den Fall des Einsatzes von Bodentruppen seitens der NATO ankündigte. Moskau hat zwar das Rahmenabkommen von Rambouillet mit verhandelt und den politischen Teil gutgeheißen, aber nicht den militärischen Annex. Ziele und Motivlage Moskaus werden vor allem von folgenden Faktoren beeinflußt:

- Der Widerspruch zwischen dem beanspruchten Weltmachtstatus und dem tatsächlichen politischen, wirtschaftlichen und militärischen Gewicht wird größer. Gab Rußland seinen Widerstand gegen das militärische Eingreifen in Bosnien noch rechtzeitig auf, so stemmte es sich vehement gegen ein militärisches Engagement der NATO im Kosovo-Konflikt. Damit ist gerade das Gremium entwertet worden, in dem Rußlands Weltmachtanspruch noch am klarsten dokumentiert wurde: der UNO-Sicherheitsrat.

- Rußland geht es um gleichberechtigte Mitsprache in europäischen Sicherheitsfragen. Wenn die NATO die zentrale Organisation für die Gewährleistung der europäischen Sicherheit wird, bleibt Moskau trotz ständigem NATO-Rußland-Rat und Kontaktgruppe bei allianzinternen Entscheidungen de facto ausgegrenzt. Dieser Zustand ist für Rußland nicht akzeptabel.

- Moskau sieht im einseitigen Vorgehen der NATO einen Präzedenzfall im Hinblick auf die zahlreichen Minderheitenprobleme innerhalb der Gemeinschaft Unabhängiger Staaten (GUS). Manche befürchten darüber hinaus, daß sich die Atlantische Allianz eines Tages in Rußland selbst militärisch einmischen könnte.

- Der russische Verbalradikalismus erklärt sich auch und vor allem angesichts eines innenpolitisch zerrissenen Landes, das sich bereits im Wahlkampf befindet (Dumawahlen Ende 1999, Präsidentschaftswahlen im Jahre 2000). Der Jugoslawienkrieg spielt den Nationalisten, Kommunisten und Panslawisten in die Hände und bringt eine kooperative Regierung, die historische und geistige Bindungen zu Serbien nicht ohne weiteres ignorieren kann, in Erklärungsnot. Die geistige Verwandtschaft und das politische Zusammenspiel zwischen den rotbraunen Kräften in der Bundesrepublik Jugoslawien, Belarus und Rußland sind zum einen eine innenpolitische Gefahr für die Regierung Primakov. Zum anderen erschweren sie die Umsetzung einer politischen Strategie, die langfristig auf die freiwillige und kooperative Rekonstitution des postsowjetischen Raumes abzielt. Vor diesem Hintergrund ist Milosevic für die russische Regierung alles andere als ein Wunschpartner.

Bundesrepublik Jugoslawien (BRJ)

Über die Absichten und Ziele der jugoslawischen Führung ist viel spekuliert worden. Ist Milosevic ein politischer Hasardeur, ein glühender serbischer Nationalist oder ein kühl kalkulierender Techniker der Macht? Die Erfahrungen aus den vorangegangenen jugoslawischen Erbfolgekriegen spricht eher für die letztgenannte Charakterisierung. Demnach können ihm folgende Motive und Ziele unterstellt werden:

- An erster Stelle steht die politische Macht. Der jugoslawische Präsident provoziert und nutzt Krisen entweder zur Machterweiterung, wie sein gescheitertes Projekt eines Großserbiens blutig illustrierte, oder er nutzt sie zur Stabilisierung seiner Macht. Indem er der NATO die Stirn bietet, profiliert er sich als starker Mann, um den sich das serbische Volk schart. Diese durch nationalistische Propaganda verstärkte Solidarisierung nutzt er zur Ausschaltung oppositioneller Kräfte in Gesellschaft, Armee und Politik. So ist zu befürchten, daß er seinen politischen Gegenspieler, den montenegrinischen Präsidenten Djukanovic, durch die Destabilisierung der Lage in Montenegro oder einen Putsch aus dem Amt treiben will. Diese jugoslawische Republik ist zudem von großer strategischer Bedeutung, sichert sie Serbien doch den direkten Zugang zum Mittelmeer.

- Ideologisches Ziel ist die Erhaltung der serbischen Nation. Nach dem Scheitern seiner Vision eines Großserbiens geht es ihm nun darum, zumindest die vollständige Kontrolle über das Territorium der Bundesrepublik Jugoslawien zu behalten. Dem läuft die demographische Entwicklung im Kosovo zuwider. Die Kosovaren haben die höchste Geburtenrate Europas. Sollte sich diese fortsetzen, wären die Serben in der Bundesrepublik Jugoslawien im Jahre 2020 in der Minderheit.[11] Aus dieser rassistischen Logik ergeben sich zwei Möglichkeiten. Die erste und bislang praktizierte Option besteht in der Vertreibung der Kosovaren, sei es durch Diskriminierung und Repression, wie vor dem Jugoslawienkrieg, oder durch gewaltsame Vertreibung und Vernichtung. Die zweite Möglichkeit sieht eine Teilung des Kosovo vor. Ihr zufolge würden die Kosovaren im unwirtlichen Süden der Provinz zusammengepfercht, Serbien erhielte den historisch bedeutungsvollen und wirtschaftlich attraktiveren Norden. In diesem Falle hätte Milosevic nur unter dem starken militärischen Druck der NATO einen Teil »heiliger serbischer Erde« preisgegeben, gleichzeitig jedoch den Frieden und den Erhalt der serbischen Nation gesichert.

Die UCK

Im Frühjahr 1996, nur wenige Monate nach dem Abkommen von Dayton, war erstmals in den westlichen Medien von der Befreiungsarmee des Kosovo (UCK) die Rede. Im Laufe des Jahres 1997 häuften sich die Anschläge und Terrorakte auf serbische Polizeistationen, aber auch auf serbische Zivilisten und albanische »Kollaborateure«. Auch wenn es die UCK nicht gibt, lassen sich mittlerweile

doch einige Aussagen über die Ziele und Interessen der Befreiungsarmee machen.

- Die UCK-Kämpfer haben aus Dayton zwei Lehren gezogen: »Nach über fünf Jahren des an Gandhi

Damage to buildings in Kosovo, Bela Crkva, Serbia
Foto: NATO

erinnernden Kampfes um Unabhängigkeit schlossen die Vereinigten Staaten mit Milosevic einen Handel über Bosnien ab, ohne auch nur für die Wiederherstellung der Autonomie des Kosovo zu sorgen. Lehre eins: Die Gewaltlosigkeit hatte nicht funktioniert. Außerdem machte das Dayton-Abkommen in Bosnien selbst große Zugeständnisse an die gewaltsam durchgesetzten ethnischen Realitäten. Lehre Nummer zwei: Gewalt zahlt sich aus.«[12]

- Gefördert wurde der bewaffnete Aufstand der UCK durch die Plünderung der albanischen Waffenarsenale als Folge der gewalttätigen Implosion im Frühjahr 1997 und durch die Brutalität der serbischen Polizeikräfte seit Februar 1998. Es halten sich auch Gerüchte, die Entstehung der UCK sei tatkräftig durch den albanischen Geheimdienst unterstützt worden. In der Befreiungseuphorie des Sommers gelang es der UCK, nahezu die Hälfte des Kosovo zu besetzen und als befreites Gebiet auszurufen. Die Reaktion der serbischen Sicherheitskräfte ließ jedoch nicht lange auf sich warten. Der massive Einsatz von Panzern und schweren Geschützen führte zur Zerstörung von Hunderten von albanischen Dörfern, zu Massakern unter der albanischen Bevölkerung und einem Massenexodus von 300.000 Zivilisten. Erst das Holbrooke-Milosevic-Abkommen vom 25. Oktober 1998[13] und die Stationierung von unbewaffneten OSZE-Beobachtern setzte dem Treiben ein vorübergehendes Ende. Doch der Waffenstillstand wurde von beiden Seiten nicht eingehalten. Ohnmächtig mußte die OSZE mitansehen, wie die Kämpfe ab Dezember wieder zunahmen. Nach dem Massaker von Racak im Januar 1999 eskalierte der Konflikt zum offenen Krieg.

- Die UCK ist alles andere als eine homogene Armee mit klaren Befehls- und Kommandostrukturen, sondern zu großen Teilen untereinander zersplittert und zerstritten. Sie verfällt bereits jetzt in mindestens drei Fraktionen. Nachdem ihr politischer Sprecher, Adem Demaci, aufgrund seiner Weigerung, das Rambouillet-Abkommen zu unterzeichnen, zurücktrat, wurde Hashim Thaci zum politischen Chef der UCK und Delegationsleiter von Paris gewählt. Zugleich hat sich der Machtkampf zwischen der UCK und der gemäßigteren LDK weiter verschärft. Thaci hat die bisherige Exilregierung unter Bujar Bukoshi für abgesetzt erklärt und die Bildung einer neuen Exilregierung unter seiner Führung bekanntgegeben. Bukoshi widersetzte sich und erklärte, ein solcher Machtwechsel müsse demokratischen Regeln folgen. Im internen Machtkampf verfügt die Regierung Bukoshi über gute Karten, da sie die Finanzquellen der Exil-Kosovaren weitgehend kontrolliert.

- Ziel der UCK ist und bleibt die Unabhängigkeit des Kosovo; es gibt jedoch auch Anhänger eines Großalbaniens unter den UCK-Kämpfern. Mit dem Krieg der NATO gegen Jugoslawien ist die westliche Allianz zu dem geworden, was sie unter allen Umständen vermeiden wollte: zur Luftwaffe der UCK. Mit den Bombardierungen der NATO dürfte die Untergrundarmee ihrem Ziel eines unabhängigen Kosovo um einiges näher gekommen sein. Nach den jüngsten Ereignissen ist es in der Tat nur schwer vorstellbar, daß das Kosovo in seiner gegenwärtigen Form Teil des jugoslawischen Staatsverbundes bleiben könnte.

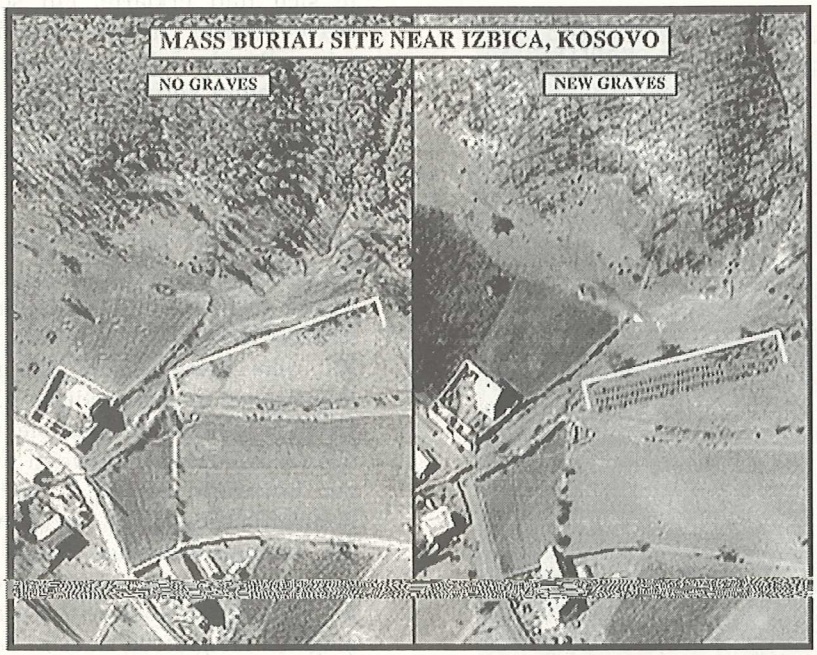
3. Welche militärischen Optionen gibt es?

Bereits in der ersten Jahreshälfte 1998 erteilten die Staats- und Regierungschefs der NATO den Militärs den Auftrag festzustellen, was sie an Streitkräften benötigen würden, um – einen entsprechenden Beschluß der Politik vorausgesetzt – eine Friedensregelung für das Kosovo militärisch durchsetzen zu können. Die NATO-Stäbe entwarfen die Streitkräfteplanung für vier Szenarien[14]:

- Option A-: Dabei wurde unterstellt, Belgrad sei bereit, mit der NATO bei der Verwirklichung eines Abkommens und der Stationierung einer NATO-Friedenstruppe zusammenzuarbeiten. Ein Szenario, welches auch das Rambouillet-Abkommen vorgesehen hatte.

- Option A: Bei diesem Szenario unterstellten die Militär-Planer der Allianz, daß die Bereitschaft Belgrads zur Zusammenarbeit durch die

Anwendung von Gewalt erzwungen werden müßte. Ein Szenario, von dem die NATO hoffte, daß es nach den ersten zwei bis drei Tagen der Luftangriffe Wirklichkeit werden könnte.



Mass Burial Site near Izbica, Kosovo
Foto: NATO

- Option B-: Dieses Szenario geht davon aus, daß die NATO einseitig, also gegen den Willen der jugoslawischen Regierung, einen Frieden im Kosovo erzwingen müsse. Die militärischen Operationen sollten sich jedoch auf das Gebiet des Kosovo beschränken. Hierfür wäre nach NATO-Plänen ein Minimum von 75.000 Soldaten erforderlich.

- Option B: Dabei ging die NATO vom worst case aus. Die Besetzung des Kosovo und die Durchführung militärischer Operationen in ganz Jugoslawien. Hierfür wären nach Auffassung der Militärs eine Streitmacht von zwei Korps mit sieben Divisionen und bis zu 200.000 Mann erforderlich.

Die NATO-Militärs forderten damals die Bereitschaft der Politiker, Bodentruppen von Anfang an bereitzustellen. Die Eskalationsfähigkeit müsse gegeben sein, da sich mit dem Einsatz von Flugzeugen allein kein dauerhafter Erfolg erzielen lasse. Im nachhinein muß man konstatieren, daß es ein Fehler der NATO-Politik war, den Einsatz von Bodentruppen von vornherein auszuschließen. Das bestärkte Milosevic in der Annahme, daß er im Falle einer Nichtunterzeichnung von Rambouillet »lediglich« NATO-Luftangriffe zu erwarten habe, die seine Macht letztlich nicht gefährden, sondern ihn im Gegenteil innenpolitisch stabilisieren würden.

Welche politischen Optionen existieren?

Auch wenn es viele noch nicht wahr haben wollen: Nach dem Ende des kalten Abschreckungsfriedens aus der Zeit des Ost-West-Konflikts ist Krieg wieder ein Mittel der Politik in Europa geworden. Das ist zu bedauern, entspricht aber der Realität. Freilich sollte Krieg nicht, wie unter Rückgriff auf ein Clausewitz-Zitat häufig behauptet, die Fortsetzung der Politik mit anderen Mitteln, sondern die Fortsetzung der Politik unter Beimischung anderer, eben militärischer Mittel sein. Im ersten Fall dankt die Politik ab und überläßt dem Militär das Feld. Genau das wollte Clausewitz nicht, weil die in jedem Krieg auftretenden »Friktionen« eine nicht kalkulierbare Eigendynamik entwickeln können, die ihn zum Äußersten treiben lassen. Das ursprüngliche politische Ziel tritt dann in den Hintergrund. Dieses zu verhindern ist die Aufgabe der Politik. Vor diesem Hintergrund gibt es im Jugoslawienkrieg grundsätzlich zwei Optionen: Entweder strebt die NATO einen Diktatfrieden gegen oder einen Verhandlungsfrieden mit Milosevic an. Für beide Optionen lassen sich – ohne Anspruch auf Vollständigkeit – pro- und contra-Argumente anführen.
Argumente für einen Diktatfrieden:

- Der territoriale Status auf dem Balkan bliebe erhalten.

- Die Vertriebenen könnten in ihre Heimat zurückkehren.

- Die Bundesrepublik Jugoslawien könnte demokratisiert und föderalisiert werden.

- Das Kosovo würde eine demokratische und multiethnische Republik.

- Die Verantwortlichen in Belgrad könnten vor das Kriegsverbrechertribunal in Den Haag gestellt werden.

Argumente gegen einen Diktatfrieden:

- Er würde von den NATO-Staaten die Bereitschaft erfordern, einen Bodenkrieg mit wahrscheinlich hohen Verlusten zu riskieren.

- Dessen Vorbereitung braucht viel Zeit, in der sich die Lage im und um das Kosovo weiter verschlechtern wird.

- Die Verhältnismäßigkeit der Mittel könnte nicht gewährleistet werden.

- Der Durchhaltewille der Serben wird als sehr hoch eingeschätzt.

- Es muß ein unkalkulierbares Eskalationsrisiko eingegangen werden (z.B. Terrorakte außerhalb Serbiens, Destabilisierung Ungarns durch Vertreibung der 400.000 ethnischen Ungarn aus der Vojvodina, Vertreibung der Binnenflüchtlinge aus dem Kosovo, Einsatz von chemischen Waffen durch die jugoslawische Armee, Eröffnung einer weiteren Front in Montenegro).

- Die von Rußland vorgegebene rote Linie würde überschritten, die jetzige Regierung zugunsten der extremistischen Kräfte geschwächt.

- Die westlichen Gesellschaften wür-

den einen lange anhaltenden und verlustreichen Krieg nicht unterstützen.

Für einen Verhandlungsfrieden sprechen folgende Argumente:

- Der gewaltsame Konflikt würde schneller beendet.
- Die Flüchtlinge könnten unter dem Schutz einer internationalen Truppe in ihre Heimat zurückkehren.
- Die Gefahr eines eskalierenden Balkankrieges wäre behoben.
- Das Verhältnis zu Rußland würde sich positiv entwickeln.
- Die finanziellen Kosten wären geringer.
- Das Vorhaben stünde auf einer einwandfreien völkerrechtlichen Basis.

Gegen eine Verhandlungslösung spricht:

- Der Brandstifter könnte sich einmal mehr als Friedensengel gerieren. Die Verbrechen blieben ungesühnt, die Bundesrepublik Jugoslawien könnte nicht an die europäischen Strukturen herangeführt werden.
- Es würde das falsche Signal an die rot-braunen Kräfte anderswo in Europa ausgesendet.
- Das Streben der Kosovaren nach staatlicher Unabhängigkeit würde mißachtet.
- Die Demokratisierung und die Wahrung der Menschen- und Minderheitenrechte könnten nur im Kosovo garantiert werden.
- Eine Reföderalisierung der Bundesrepublik Jugoslawien würde erschwert.
- Die Glaubwürdigkeit derjenigen Politiker wäre dahin, die Milosevic als Kriegsverbrecher gebrandmarkt haben.

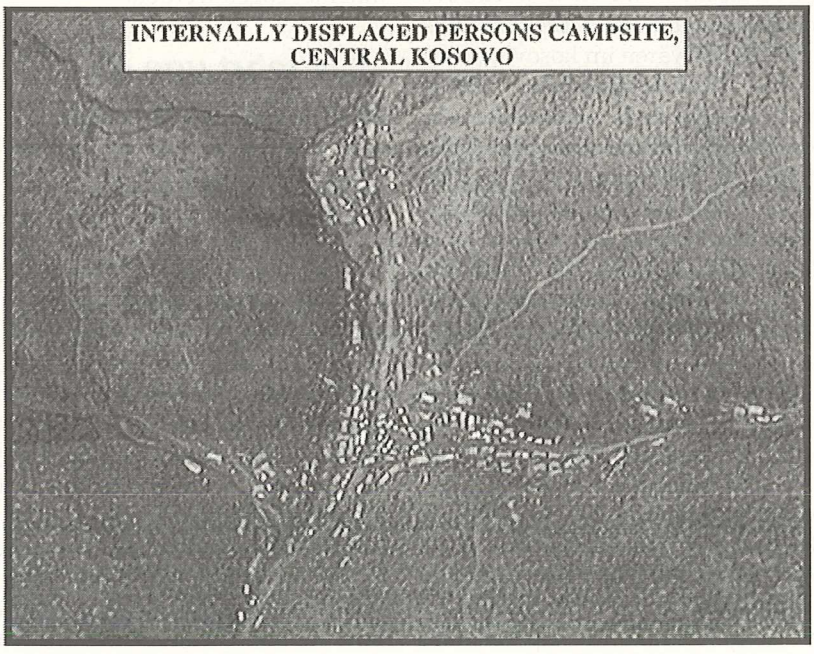
Die Aufzählung der verschiedenen Argumente zeigt, daß es keine befriedigende Lösung gibt. Als am wenigsten schlechte Option erscheint der Verhandlungsfrieden. So oder so wird sich die internationale Staatengemeinschaft auf viele Jahre auf dem Balkan engagieren müssen. Wichtig ist zunächst, daß so bald wie möglich eine Waffenruhe erreicht wird, die politischen Voraussetzungen für eine Rückkehr der Vertriebenen in das Kosovo geschaffen werden und Montenegro nicht gleichgeschaltet wird. Doch wie soll die politische Lösung konkret aussehen? In der Diskussion sind hauptsächlich folgende drei »Modelle«:

Staatliche Unabhängigkeit

Diese Option ist das erklärte Ziel vieler Kosovo-Albaner. Die Kosovaren können auf die anderen ehemaligen Republiken Jugoslawiens verweisen, die heute souveräne Staaten und Mitglieder der internationalen Gemeinschaft sind. Ein Hauptargument gegen ein souveränes Kosovo ist die Haltung Belgrads. Ihm müßten also entsprechende Anreize angeboten werden. Ein anderes Gegenargument liegt in der von Teilen der UCK vertretenen nationalistischen Idee eines Großalbanien. Ihre Verwirklichung könnte Albanien und Mazedonien in einen Bürgerkrieg stürzen. In dem einen Staat würde die heutige Clanstruktur stark zu Gunsten der Nordalbaner verändert, der andere würde wahrscheinlich daran zerbrechen, was wiederum Bulgarien, Griechenland und die Türkei in Händel verwickeln könnte. Die Serben der bosnischen Teilrepublik Srpska würden gewiß das gleiche Recht auf Anschluß einfordern, wahrscheinlich auch die Kroaten aus der Herzegowina. Die heutige Balkanordnung wäre dahin, ein weiterer Balkankrieg nicht mehr auszuschließen. Ein unabhängiges Kosovo wäre allerdings eine Möglichkeit, wenn seine Sicherheit und territoriale Integrität international garantiert und es ein Anschluß- und Vereinigungsverbot akzeptieren würde. Zudem müßte es demokratisch und multiethnisch strukturiert sein.

Teilung des Kosovo

Die Teilungsoption ist eine auf den ersten Blick naheliegende Kompromißlösung. Im Kern folgte sie der Devise »Land gegen Frieden«. Die Kosovaren erhielten einen Teil des Kosovo und ihre Unabhängigkeit, Serbien könnte den nördlichen Teil behalten und sich der »demographischen Bedrohung« der Kosovaren entledigen. Für diesen Ansatz spricht, daß er serbischen Vorstellungen eher entgegenkommen und die Wahrscheinlichkeit eines NATO-Landkrieges verringern würde. Die Gegenargumente sind jedoch überzeugender: Erstens würde einer völkischen Politik Vorschub geleistet. Zweitens lehnen die Kosovaren diese Option ab.



Internally Displaced Persons Campsite, Central Kosovo
Foto: NATO

Drittens wäre ein unabhängiges Rumpfkosovo nicht lebensfähig, es müßte also entweder von der internationalen Gemeinschaft alimentiert und gesichert werden oder den Anschluß an Albanien suchen.

Verstärkte Autonomie

Das Rahmenabkommen von Rambouillet ist nach Ansicht vieler Beobachter durch die Ereignisse überholt worden. Andere sagen, es sei für Milosevic unannehmbar gewesen. Dennoch wird es von den NATO-Staaten als Grundlage für eine Friedenslösung angesehen. Für die serbische Seite ist der Plan nicht akzeptabel, weil er das Kosovo faktisch in den Rang einer unabhängigen Republik innerhalb der Grenzen Serbiens erhebt und die Souveränität der Bundesrepublik Jugoslawien verletzt. So hätten die von den demokratischen Selbstverwaltungsorganen des Kosovo erlassenen Rechtsakte Vorrang vor denjenigen der BRJ oder Serbiens. In manchen Bereichen, etwa der unabhängigen Gerichtsbarkeit, würde das Kosovo gar über die anderen Teilrepubliken gestellt. Für die serbische Minderheit im Kosovo ist ein umfassender Minderheitenschutz vorgesehen. Sie wären im kosovarischen Parlament überrepräsentiert, hätten ihrerseits weitgehende Autonomierechte und ein Vetorecht sowohl gegen jedes ihre nationale Interessen beeinträchtigende Gesetz als auch gegen jede Änderung der Verfassung des Kosovo. Die Bundesrepublik Jugoslawien bliebe für die Grenztruppen (maximal 1.500 Mann) und – bis zum Aufbau multi-ethnischer kosovarische Ordnungskräfte – für die Polizei verantwortlich (maximal 2.500). Belgrad wäre des weiteren u.a. zuständig für Verteidigung, Außenpolitik, Währungspolitik, Binnenmarkt, Zollwesen. Ähnlich wie in Bosnien würde eine mit weitreichenden Vollmachten ausgestattete internationale Friedenstruppe für die Sicherheit im Kosovo sorgen, und eine Implementierungsmission der OSZE wäre für die Umsetzung der zivilen Bestimmungen verantwortlich. Das Kosovo wäre für zunächst drei Jahre ein internationales Protektorat. Ob das Kosovo nach Ablauf der drei Jahre im jugoslawischen Staatsverband gehalten werden kann, ist angesichts der langen Leidensgeschichte der Kosovaren zweifelhaft. Die UCK kritisiert am Rambouillet-Plan, daß er nur eine sehr vage Aussicht auf die Berücksichtigung eines Volksentscheides über die Statusfrage enthält und ihre Entwaffnung vorsieht. Zwar böte das Abkommen von Rambouillet den Kosovaren ein Höchstmaß an politischer Eigenständigkeit und Selbstbestimmung innerhalb der Grenzen der heutigen Bundesrepublik Jugoslawien, aber eben nicht die gewünschte staatliche Unabhängigkeit. Um diese zu verhindern, müßte sich die internationale Staatengemeinschaft wahrscheinlich auf einen längeren Aufenthalt einstellen als die vorgesehenen drei Jahre.

Anknüpfend an das Rambouillet-Modell hat die deutsche Regierung am 14. April 1999 einen Friedensplan vorgelegt (»Fischer-Plan«). Damit wurde – wenn auch spät – der Versuch unternommen, die Diplomatie wieder stärker ins Spiel zu bringen. Offensichtlich versucht der Westen mit einer Doppelstrategie Milosevic zum Einlenken zu bringen: Während man den militärischen Druck auf die Bundesrepublik Jugoslawien erhöht, sollen zugleich politische Initiativen auf den Weg gebracht werden. Dafür sollen Rußland und damit die Vereinten Nationen wieder stärker miteinbezogen werden.

Was lehrt uns der Jugoslawienkrieg?

»Das Hemd sitzt näher als der Rock«

Der vierte jugoslawische Erbfolgekrieg hat erneut vor Augen geführt, daß es noch ein langer Weg ist bis zur Errichtung einer stabilen europäischen Friedensordnung, die Kriege wie im ehemaligen Jugoslawien undenkbar macht. Trotz zunehmender Globalisierung dominieren in Sicherheitsfragen immer noch die Staaten, folglich bleibt ihr politischer Wille zur Kooperation eine notwendige Bedingung für jeglichen Fortschritt in diese Richtung. Das gilt insbesondere für Großmächte. Sie sind im Kosovokonflikt nicht nur an der Intransigenz der Konfliktparteien gescheitert, sondern auch an ihrer eigenen Heuchelei und Konzeptionslosigkeit. Die Leidtragenden sind in erster Linie die Menschen vor Ort. Aber auch die internationale Staatengemeinschaft hat allen Grund, über Konsequenzen für die künftige Sicherheitsgestaltung in Europa nachzudenken. Soll sie durch den Aufbau von exklusiven Einflußzonen im Dienste militärisch abgesicherter nationaler Interessen erfolgen oder durch die graduelle Schaffung eines gesamteuropäischen Sicherheitsraumes, in dem das vermeintliche Recht des Stärkeren durch die Stärke des Rechts abgelöst wird? Die Stärke des Rechts erfordert allerdings sowohl die Zustimmung der ihm unterworfenen Staaten als auch die Mittel, die Instrumente und die Bereitschaft, dem gemeinsamen Recht zur Not auch gegen Widerstreben Geltung zu verschaffen. Dazu sind die Staaten allerdings nur in Ausnahmefällen und nur dann bereit, wenn »nationale Interessen« auf dem Spiel stehen. Ergo: Das (nationale) Hemd ist ihnen immer noch näher als der (gesamteuropäische) Rock.

»Vorbeugen ist besser als schießen«

Die Notwendigkeit von Prävention gehört mittlerweile zu den Standardbekenntnissen von Politikern. Gleichwohl stellt sich in der Realität immer wieder das Problem, eine Konflikteskalation durch präventives Handeln zu verhindern. Einerseits ist es die vornehmste Aufgabe von Sicherheitspolitik, kriegerische Konflikte zu vermeiden. Gleichwohl gibt es immer wieder Krieg. Zweierlei muß in diesem Zusammenhang konstatiert werden: 1. In Sozialbeziehungen sind Konflikte etwas Normales. Es kommt auf die Art der Konfliktbearbeitung an. 2. Prävention kann scheitern. Sie setzt dreierlei voraus: die Bereitschaft, präventive Maßnahmen zu ergreifen, die damit zusammenhängenden Kosten zu tragen und die entsprechenden Instrumente zur Verfügung zu stellen. Zu beantworten sind drei Fragen: Wann soll Prävention einsetzen? Wieviel muß investiert werden? Welche Instrumente sind notwendig und müssen zur Anwendung kommen? Die Antworten auf diese Fragen sind wiederum abhängig von drei dynamischen Variablen: dem Konfliktgegenstand, der Konfliktstruktur und dem Konfliktstadium. Im Kosovokonflikt sind präventive Maßnahmen durchgeführt worden, allerdings zu spät, mit unzureichender Intensität und mit mangelhaften Instrumenten. Folglich müssen die Möglichkeiten der internationalen Gemeinschaft zur effektiven Durchführung von präventiven Maßnahmen dringend verbessert werden. Neben den in der Phase des Vorkonflikts einsetzbaren klassi-

schen Instrumenten der präventiven Diplomatie sollte eine Präventionsstrategie entwickelt werden, die friedensfördernde inner- und zwischengesellschaftliche Strukturen schafft und langfristig stabilisiert. Gleichwohl stellt sich angesichts der niemals auszuschließenden Möglichkeit der Unwirksamkeit von Prävention die Frage, was in der konkreten Gewaltsituation getan werden kann/soll/darf. Auf jeden Fall gilt: Vorbeugen ist besser als schießen!

»Lieber ein Ende mit Schrecken als ein Schrecken ohne Ende«

Hat ein Konflikt die Welle zur Gewaltanwendung überschritten, so haben Außenstehende in der Regel drei Optionen. Besteht Desinteresse am Konflikt, so verhalten sie sich neutral. Sind Interessen involviert, kann eine Eindämmungs- oder eine Kriegsbeendigungsstrategie verfolgt werden. Entscheidend ist jedenfalls die Interessenlage. Diese ist in der Regel dynamisch und wird durch vielfältige Faktoren wie z.B. Absichten, Fähigkeiten, Werte, Kosten-Nutzen-Kalkül, Rechtslage, gesellschaftliche Akzeptanz etc. beeinflußt. Obwohl der Kosovo-Konflikt bereits seit langem schwelte, begannen ernsthafte diplomatische Aktivitäten erst nach dem Umschlagen des friedlichen Widerstandes der Kosovaren in gewaltsamen. Die ersten sieben Jahre hielt sich die Staatengemeinschaft weitgehend aus dem Konflikt heraus, ab 1997/98 wurde die präventive Diplomatie unter Einschluß der Androhung militärischer Gewalt verstärkt, und seit dem 24. März 1999 führt die NATO Krieg gegen die Bundesrepublik Jugoslawien. Anders als im Bosnienkrieg wurde dieses Mal nicht gewartet, bis 250.000 Kriegstote zu beklagen waren. Gleichwohl wurde nach der Devise »Wasch mir den Pelz, aber mach mich nicht naß« gehandelt. Zur Erreichung des humanitären Ziels hätte von vornherein der Einsatz von Bodentruppen angedroht und gegebenenfalls durchgeführt werden müssen. Statt dessen wurde aber die humanitäre Katastrophe in Kauf genommen, um die eigenen Kräfte zu schonen. Auf der Strecke blieben diejenigen, um die es eigentlich ging: die Kosovaren. Unter der Prämisse einer gescheiterten präventiven Konfliktbearbeitung muß also die Folgerung gezogen werden: Lieber ein Ende mit Schrecken als ein Schrecken ohne Ende.

»Der Herr ist so stark, wie der Knecht zuläßt«

Die im Kosovokonflikt gemachten Erfahrungen zeigen, daß es offenbar weiterhin der Entschlossenheit und Führung der USA bedarf, wenn es um die Regelung schwerwiegender europäischer Sicherheitsprobleme geht, und daß dabei die NATO als wichtigstes amerikanisches Instrument politischer Einflußnahme andere Sicherheitsorganisationen wie die UNO, die EU und die OSZE marginalisiert. Obwohl die Mitgliedstaaten in jüngster Zeit im Gegensatz zum Bosnienkonflikt eine für ihre Verhältnisse erstaunliche gemeinsame Haltung an den Tag legten, war die EU offenbar nicht der geeignete Krisenmanager. Ein Grund dafür liegt in der zunächst halbherzigen Behandlung des Problems, ein anderer wohl auch in der Unfähigkeit zum Einsatz militärischer Zwangsmittel. Zwar gelang es der EU, mit der Konferenz von Rambouillet noch eine letzte diplomatische Initiative zu starten und so ein von den USA favorisiertes vorheriges militärisches Eingreifen hinauszuschieben. Doch nach dem Scheitern der Verhandlungen dominierten die militärische Logik und damit die USA. Sie stellen zwei Drittel der an den Luftschlägen beteiligten Kräfte, sie allein verfügen über ein komplettes Lagebild, folglich bestimmen sie auch die Politik. Daraus folgt zweierlei: Erstens muß die Fähigkeit der EU zur Früherkennung sich anbahnender Konflikte und zur politischen Handlungsfähigkeit bei der zivilen Konfliktbearbeitung verbessert werden. Zweitens bedarf Krisenmanagement in Europa unter Einmischung militärischer Mittel auch künftig amerikanischer Führung. Die daraus resultierende Einengung des europäischen Handlungsspielraumes erfordert dringend die Weiterentwicklung der Gemeinsamen Außen- und Sicherheitspolitik unter Einschluß militärischer Kapazitäten und strategischer Aufklärungsmittel, die gegebenenfalls unabhängig von den USA und gebunden an ein Mandat der UNO oder der OSZE eingesetzt werden können. Denn: Der Herr ist so stark, wie der Knecht es zuläßt.

»Nach dem Krieg ist vor dem Krieg«

Wenn der Jugoslawienkrieg beendet ist, herrscht noch lange kein Frieden. Von den zahlreichen Imponderabilien seien nur erwähnt: die politische Zukunft des Kosovo und der Bundesrepublik Jugoslawien, die Entwaffnung der UCK, die Revanchegelüste, die Grenzfrage, die Rückkehr der Flüchtlinge, die Traumata vieler Menschen, der politische und wirtschaftliche Wiederaufbau, die Stabilisierung der Nachbarstaaten oder Umfang, Art und Zeitrahmen des Engagements der internationalen Gemeinschaft. Notwendig ist eine komplexe Stabilisierungspolitik, welche Maßnahmen zur militärischen Absicherung des Friedens und Abrüstung ebenso umfaßt wie vertrauensbildende Maßnahmen, die internationale Einbindung der Akteure und insbesondere langfristig wirkende politische, soziale, wirtschaftliche und psychologische Maßnahmen, die allen betroffenen Individuen zugute kommen müßten. Eine solche Strategie braucht langen Atem und kostet viel Geld. Gleichwohl ist sie weitaus billiger als Krieg. Sollte eine nachhaltige Friedenskonsolidierung nicht gelingen gilt: Nach dem Krieg ist vor dem Krieg.

Was tun?

Die Lage in der Bundesrepublik Jugoslawien ist vertrackt, die weitere Entwicklung nicht absehbar. Nur eines zeichnet sich immer klarer ab: Die eigentlichen Verlierer sind zunächst einmal diejenigen, in deren Interesse man zu handeln vorgab. Dennoch: Der deutsche Friedensplan geht in die richtige Richtung. Der Versuch, Rußland und die UNO einzubinden, ist nicht nur vernünftig sondern unerläßlich. Es gibt keine Alternativen zu diplomatischen Lösungsversuchen, allerdings: It takes two to tango. Das Problem ist primär strukturell und nicht auf die Bundesrepublik Jugoslawien beschränkt. Darum ist die zur Zeit diskutierte Vorstellung eines Marshall-Plans für die ganze Region der richtige Ansatz.[15] Darüber hinaus müßte ein politischer Gesamtrahmen geschaffen werden, der die bereits bestehenden Regionalinitiativen, die sich mit grenzüberschreitenden politischen, wirtschaftlichen, gesellschaftlichen und ökologischen Fragen befassen, ebenso einbindet und für das Stabilisierungsprojekt nutzbar macht wie die Möglichkeiten von Nichtregierungsorganisationen.[16] Nach einem Waffenstillstand böten sich u.a. folgende Schritte an:

Die Autoren

Ralf Bendrath, ist Politikwissenschaftler und Redakteur der Zeitschrift »Zivilcourage«. Er promoviert an der FU Berlin über »Das Militär in der Informationsgesellschaft«.

Ute Bernhardt M.A. arbeitet bei der GMD – Forschungszentrum Informationstechnik und ist stellvertretende FIfF-Vorsitzende

Leonie Dreschler-Fischer ist Hochschullehrerin an der Universität Hamburg und Mitglied des FIfF-Vorstandes

Hans-Georg Ehrhart ist wissenschaftlicher Referent am Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH)

Marc Hermann studiert Physik und Journalistik an der Universität Hamburg. In seiner Diplomarbeit befaßte er sich mit der Minen-Detektion und besuchte im Mai 1999 humanitäre Räumarbeiten in Mosambik. Er ist zudem als freier Wissenschaftsjournalist für das Hamburger Physik-Zentrum DESY tätig.

Karen Jaehrling M.A. ist nach einem politikwissenschaftlichen Studium nun Doktorandin in der Forschungsstelle Kriege, Rüstung und Entwicklung am Institut für Politische Wissenschaft Hamburg

Matthias Z. Karádi wissenschaftlicher Mitarbeiter am Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH)

Ingo Ruhmann arbeitet seit Jahren zu Informatik und Militär und ist Mitglied des FIfF-Vorstands

Eckard Spoo ist Publizist und Autor, er ist Mitherausgeber und verantwortlicher Redakteur der Zweiwochenschrift OSSIETZKY

- Einberufung einer Gipfelkonferenz aller interessierten Staaten und internationalen Organisationen. Ziel wäre es, eine permanente und flexible multilaterale Dialogstruktur in Form eines runden Tisches für Südosteuropa zu schaffen.
- Die Staats- und Regierungschefs könnten zunächst eine gemeinsame Erklärung über regionale Stabilität und Entwicklung verabschieden sowie eine Agenda mit einem konkreten Arbeitsprogramm für grenzüberschreitende Zusammenarbeit und wirtschaftliche Entwicklung entwerfen, das auf den Folgekonferenzen evaluiert und weiterentwickelt werden müßte.
- Unter der Ägide des OSZE-Forums für Sicherheitskooperation sollten Verhandlungen über Abrüstung und regionale Rüstungskontrolle beginnen.
- Dieser Prozeß müßte einmünden in einen südosteuropäischen Pakt für Stabilität und Entwicklung, der in die OSZE zu überführen wäre, sobald die Bundesrepublik Jugoslawien die politischen Voraussetzungen dafür erfüllt.

Angesichts der Problemkomplexität ist davon auszugehen, daß eine friedliche Neuordnung des Balkans Jahrzehnte dauert, große Summen kostet und nur über die langfristige Aussicht auf Integration in die euro-atlantischen Strukturen Stabilität verspricht. Dennoch gibt es dazu keine Alternative. Demokratisierung in Serbien und in allen anderen Ländern des Balkans ist der Schlüssel zum Fortschritt. Voraussetzung dafür ist die Förderung neuer Eliten und unabhängiger Medien sowie wirtschaftlicher Aufschwung. Die Staaten auf dem Balkan haben mittel- bis langfristig keine andere Möglichkeit als die ökonomische Reintegration. Vielleicht kann die westeuropäische Integration als Modell dafür dienen, wie aus ehemaligen Todfeinden, Freunde und Partner wurden. Auch wenn der Weg dorthin weit ist, die Alternative dazu wäre Krieg, Tod und Vertreibung.

1 Dieser Beitrag erschien im Original in: Hamburger Informationen zur Friedensforschung und Sicherheitspolitik, Ausgabe 27/1999, Hamburg, Mai 1999 des Instituts für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH), Falkenstein 1, 22587 Hamburg. Nachdruck mit freundlicher Genehmigung der Autoren.

2 Vgl. Hans-Georg Ehrhart/Matthias Z. Karádi, Brennt der Balkan? Plädoyer für eine komplexe Präventionspolitik im Kosovo-Konflikt, Hamburger Informationen zur Friedensforschung und Sicherheitspolitik, Ausgabe 23/1998, Hamburg 1998.

3 Vgl. dies.:, Krieg in Sicht! Die internationale Staatengemeinschaft und der Kosovo-Konflikt, in: Vierteljahresschrift für Sicherheit und Frieden (S+F), Heft 2/1998, S. 99-108.

4 Vgl. das Washington Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, D.C. on 24th April 1999, NAC-S(99)64.

5 Winrich Kühne, Humanitäre NATO-Einsätze ohne Mandat? Ein Diskussionsbeitrag zur Fortentwicklung der UNO-Charta, Ebenhausen (SWP), März 1999, S. 9.

6 Vgl. Bruno Simma, »Die NATO-Bomben sind eine läßliche Sünde«, Interview in Süddeutsche Zeitung, 25.3.1999.

7 Vgl. den Wortlaut der Völkermordkonvention in: Gunnar Heinsohn, Lexikon der Völkermorde, Reinbek b. Hamburg 1998, S. 354-358.

8 Ebd., S. 354.

9 Vgl. zum folgenden Daniel Thürer, Die NATO-Einsätze in Kosovo und das Völkerrecht. Spannungsfeld zwischen Gewaltverbot und Menschenrechten, in: Neue Zürcher Zeitung, 3.4.1999.

10 Das Statut von KFOR hätte zwischen Belgrad und der NATO geregelt werden müssen. Die im Annex B des Vertragsentwurfs von Rambouillet vorgegebenen Formulierungen entsprechen beinahe wörtlich den Bestimmungen des Dayton-Vertrages. Insofern können sie für die jugoslawische Regierung keine Überraschung gewesen sein. Diese lehnte das ganze Kapitel VII (Implementation II) inklusive Annex aus prinzipiellen Gründen ab, während für die NATO-Staaten und die Kosovo-Albaner eine militärische Absicherung des Friedensabkommens unverzichtbar gewesen ist. Vgl. Interim Agreement for Peace and Self-Government in Kosovo (February 23, 1999), http:/www.balkanaction.org/paper/kia299.html

11 Die Hälfte aller Kosovaren ist nicht älter als 20 Jahre, 70 Prozent sind jünger als dreißig Jahre. Vgl. International Crisis Group, ICG Kosovo Briefing, February 17, 1998, S. 6f.

12 Timothy Garton Ash, Weine, zerstückeltes Land! »Gute Zäune für gute Nachbarschaft« - Balkaniens Remedur, in: Lettre INTERNATIONAL, Heft 44, Frühjahr 1999, S. 10-15, hier S. 11.

13 Vgl. Decision on OSCE Verification Mission on Kosovo, 25 October 1998, in: Helsinki Monitor 4/1998, S. 98-101.

14 Vgl. Frankfurter Allgemeine Zeitung, 1.4.1999.

15 So wurde auf dem NATO-Gipfel in Washington u.a. beschlossen, einen langfristigen wirtschaftlichen Aufbau- und Stabilisierungsprozeß in Südosteuropa in Gang zu bringen. Am 27. Mai 1999 wollen die NATO, die EU und die jugoslawischen Anrainerstaaten auf dem Petersberg in Bonn die Beratungen über einen Stabilitätspakt für den Balkan beginnen.

16 Vgl. dazu Hans-Georg Ehrhart, Preventive Diplomacy or Neglected Initiative: The Royaumont Process and the Stabilization of Southeastern Europe, in: Hans-Georg Ehrhart/Albrecht Schnabel (Eds.), The Southeast European Challenge: Ethnic Conflict and the International Response, Baden-Baden 1999, S. 197-213.

Eckart Spoo

Hilferuf für Kragujevac

22. Mai (Pfingstsamstag). In einem kleinen Speiselokal am Hamburger Hauptbahnhof treffen sich zehn Gewerkschafterinnen und Gewerkschafter, die gemeinsam nach Jugoslawien fahren wollen. Eine buntgemischte Gruppe: Der Chemie-Laborant und Betriebsrat aus Frankfurt-Höchst neben der Gewerbeschullehrerin und GEW-Delegierten aus Hamburg, der frühere VW-Arbeiter aus Braunschweig, jetzt Mitarbeiter der IG Metall, neben der (Ost-)Berliner Journalistin, die in der IG Medien aktiv ist. Manche kenne ich, einige lerne ich erst an diesem Abend kennen, wenige Stunden vor dem Abflug. Einer stellt sich als CDU-Mitglied vor: Sein Großvater, General Ludwig von Schröder, war 1941 Befehlshaber der Großdeutschen Wehrmacht in Belgrad. Den Enkel erbittert wie uns alle, daß Deutschland zum dritten Male in diesem Jahrhundert gegen Jugoslawien Krieg führt.

Initiator ist der Schauspieler Rolf Becker, Vorstandssprecher der IG Medien in Hamburg. Er hatte die Idee: »Dialog von unten statt Bomben von oben.« Im April präsentierten er und ich gemeinsam mit dem Völkerrechtslehrer Norman Paech und dem Publizisten Günther Schwarberg das Vorhaben auf einer Pressekonferenz im Hamburger Literaturhaus. Paech erwähnte die vielen internationalen Rechtsnormen, die die NATO als Aggressor bricht, auch die Vorschriften des Kriegsvölkerrechts, das z. B. das Bombardieren chemischer Betriebe mit unvorhersehbaren Folgen für die Umwelt verbietet. Schwarberg analysierte die auf uns alle einwirkende Kriegspropaganda und schlug die Gründung einer Wahrheitskommission vor. Auch Inge und Walter Jens waren zu der Pressekonferenz gekommen, verläßliche Mitstreiter gegen Rüstung und Krieg; sie hatten sich z. B. an der Anti-Raketen-Blockade in Mutlangen beteiligt und im Golfkrieg US-amerikanische Deserteure bei sich aufgenommen. Im NATO-Krieg gegen Jugoslawien müßten wir Deutsche uns von der Macht des Opportunismus befreien, sagte Walter Jens. Und wir müßten die Resignation überwinden, die sich vieler Kriegsgegner bemächtigt habe. Der Generalkonsul Jugoslawiens in Hamburg ergriff ebenfalls das Wort und sagte uns seine Unterstützung zu. Was bei der Pressekonferenz fehlte, war nur die Presse. Nachher übermittelte Rolf Becker der Deutschen Presse-Agentur eine kurze Darstellung unserer Absichten, die ich jedoch in den folgenden Tagen nirgendwo veröffentlicht fand. Hätte Walter Jens den Angriffskrieg befürwortet wie Günter Grass, dann hätte ihn das Fernsehen gewiß zu bester Sendezeit auftreten lassen.

Aber in vielen Gewerkschaftsgruppen hat unsere Initiative Zustimmung erfahren. Spenden wurden gesammelt, um die Reise zu finanzieren. Ein Rentner aus Salzgitter überwies 500 Mark.

Gedanken auf der Reise nach Jugoslawien

23. Mai (Pfingstsonntag). Im Flugzeug erhalten wir unentgeltlich die »Welt am Sonntag«. Schlagzeile: »Fülle von Beweisen für serbische Greuel«. Nach zwei Monaten Krieg bemühen sich die Aggressoren verstärkt um Beweise, die den Krieg gegen Jugoslawien nachträglich rechtfertigen sollen. Befragungsspezialisten wurden in großer Zahl in die Flüchtlingslager in Mazedonien und Albanien entsandt. Wer interessiert sich für Greueltaten der UCK? Mich widert die Kriegspropaganda an, die auf der einen Seite des Bürgerkriegs im Kosovo nur gute und auf der anderen Seite nur böse Menschen kennt. Nützt diese Propaganda, nützt der NATO-Krieg gegen Jugoslawien den hunderttausenden Kosovo-Albanern, die seit dem 24. März, seit Beginn der Bombardements, geflüchtet sind? Ob diese vielen armen Menschen wohl glauben können, was die »Welt am Sonntag« uns weiszumachen versucht: daß die NATO den Bombenkrieg ihretwegen führt?

Während des Fluges frage ich nach Antikriegsaktionen in den Städten, aus denen die Mitreisenden kommen. In einer Wohnsiedlung in Berlin-Hohenschönhausen hatte eine Mieterin ein weißes Tuch aus dem Fenster gehängt, ein Laken gegen den Krieg. Die Hausverwaltung zwang sie, das Tuch hereinzuholen. Gegen den Golfkrieg hatten noch viele mit ihren Bettüchern protestiert; da hatte sich die Hausverwaltung nicht gerührt. Warum engagieren sich diesmal vergleichsweise wenige? Weil Deutschland unmittelbar beteiligt ist? Weil Rot-Grün regiert? Weil sich viele Menschen verlassen und ohnmächtig fühlen? Weil auch der DGB-Vorsitzende Dieter Schulte – entgegen den ihn verpflichtenden Beschlüssen – die Aggression gegen Jugoslawien sogleich eilfertig unterstützt hat (und trotzdem immer noch im Amt ist)? Weil die tonangebenden Politiker und Publizisten diesen Krieg lange und gründlich vorbereitet haben (Deutschland müsse ein normaler Staat werden, Deutschland müsse erwachsen werden, Deutschland müsse Verantwortung übernehmen, Deutschland dürfe nicht tatenlos zusehen, zur militärischen Intervention gebe es keine Alternative usw.)? Wächst etwa gar Einverständnis bei den Deutschen heran, daß sie berufen seien, in Europa als zentrale Ordnungsmacht zu wirken? Oder erscheint der Krieg einfach deswegen, weil »wir« beteiligt sind, als ein guter, gerechter Krieg? Weil ein Krieg, an dem »wir« beteiligt sind, nicht böse sein kann?

Mich beunruhigt die Kriegsbereitschaft im politischen Management Deutschlands vor allem im Zusammenhang damit, daß eben jetzt deutsche Konzerne sich aufschwingen, die Vormachtstellung auf dem Weltmarkt einzunehmen: Allianz im Versicherungsgewerbe, Deutsche Bank durch Erwerb von Bankers Trust im Kreditgewerbe, Hoechst durch Verschmelzung mit Rhone-Poulenc in der Pharmaindustrie usw. Schon vor einigen Monaten haben Robert Erlinghagen und Manfred Sohn in OSSIETZKY über die zunehmende Gereiztheit zwischen USA und Euro-Land geschrieben. Mich beschäftigt die Überlegung, ob der Krieg, in den die

USA die westeuropäischen NATO-Staaten hineingezogen haben, aus der Rivalität imperialistischer Hauptmächte zu erklären ist. Oder war Deutschland die treibende Kraft?

Zwischenaufenthalt in Budapest, seit einigen Wochen Hauptstadt eines NATO-Staates, dessen Medien zuvor unter deutsche Oberhoheit genommen worden sind. In der kleinen deutschsprachigen Zeitung »Pester Lloyd« lese ich über das Wirken der staatlichen Privatisierungsgesellschaft. Vom 25. Mai an können Aktien der ungarischen Telekommunikationsgesellschaft Matáv gezeichnet werden. Ausführlich stellt das Blatt die Möglichkeiten von Kleinanlegern dar. Im letzten Absatz finde ich die lakonische Anmerkung, es stehe bereits fest, »daß das amerikanisch-deutsche Konsortium Magyar-Com als strategischer Investor 59,58 Prozent der Matáv-Aktien kontrollieren wird, denen 40,42 Prozent in Streubesitz gegenüberstehen".

Das Blatt berichtet auch über ein militärisches Ereignis: »Es war ein feierlicher Anlaß in diesen Tagen, in denen das Frontland Ungarn täglich bemüht ist, seine militärische Bereitschaft und Bündnistreue zu demonstrieren. Der Verteidigungsminister, der von den Kleinlandwirtepartei delegierte kleine Rechtsanwalt Szabó (wer dachte noch vor einem Jahr, daß die Führung dieses Portefeuilles überhaupt wichtig sein könnte?), der Chef des Generalstabes, Generaloberst Végh, und andere Würdenträger begaben sich nach Kecskemét, um sich ein Bild von der Kampfbereitschaft der ungarischen Luftwaffe zu machen. Die Stadt liegt 70 km südlich von Budapest und besitzt einen der noch benützten Militärflughäfen des Landes. (Der andere ist in Pápa, der dritte, Taszár, wurde längst den Amis überlassen.) Also wurden in Anwesenheit der hohen Gäste die bereitstehenden Jagdfliegerpiloten alarmiert. (...) Nur ein kleines Problem ergab sich: Sie konnten nicht ihre Mig-29-Kampfmaschinen besteigen und in die Höhe donnern, um mit ihren Raketen einen imaginären Feind vor den Augen ihrer Vorgesetzten zu verjagen. Der Luftraum oberhalb Kecskemét war nämlich gerade wieder einmal besetzt – den benutzten eben die amerikanischen Tankflugzeuge, um F-15-Bomber mit frischem Kerosin aufzuladen. Also warteten die hohen Tiere, die Piloten und die Presse da unten über eine Stunde, bis dann auch die Ungarn zum Zuge kamen und über ihr Kecskemét aufsteigen konnten. Was wird sich wohl der Minister über sein Gewicht in der Politik gedacht haben?«

Mit Ungarn sind auch Tschechien und Polen im März NATO-Mitglieder geworden. Bisher hatte die NATO auf dem Balkan nur ein Mitglied: Griechenland, das als wenig zuverlässiger Verbündeter gilt. Hunderttausende Gewerkschafter beteiligten sich dort an einem Streik, als die Bombardierung Jugoslawiens begann. Jetzt sind Truppen aus NATO-Ländern in Albanien und Mazedonien stationiert, Slowenien, Kroatien, Bosnien, Bulgarien, Rumänien haben ihnen Überflug- und andere Rechte eingeräumt. Nur Rest-Jugoslawien sträubt sich noch gegen die schnelle Eroberung.

Ein Bus aus Jugoslawien holt uns ab; mit den beiden Fahrern wird er uns während der ganzen Reise zur Verfügung stehen. Die Straßen sind gerahmt von Akazien in der vollen Pracht ihrer weißen Blütendolden. Anfangs regnet es. Aber je näher wir der Grenze kommen, desto klarer wird der Himmel. Wir wissen: Bombenwetter.

Kollege Horst sagt mir, seiner Frau sei es gar nicht recht, daß er mitfährt. Beide Töchter hätten ihn für verrückt erklärt. In uns beiden werden Erinnerungen an die Bombennächte wach, die wir als Kinder erlebt haben. Und nun fahren wir am 50. Jahrestag des Grundgesetzes, das jeden Angriffskrieg verbietet, seine Vorbereitung unter hohe Strafe stellt, in ein Land, das unter maßgeblicher deutscher Mitwirkung bombardiert wird. Die verfassungsbrecherischen Politiker sind heute in Berlin versammelt, um den Bundespräsidenten zu wählen. Welche Heuchelei, wenn sie das Grundgesetz feiern.

Auf beiden Seiten der Grenze werden wir von Männern in Tarnuniformen kontrolliert. Langwierige Prozeduren. Nur zwei oder drei andere Autos passieren während dieser Zeit. Es ist dunkel geworden. Mir kommt ein Tag im Jahre 1991 in den Sinn. Bei einem Treffen der überparteilichen Bürgerinitiative für Sozialismus in Hannover entstand die Idee, Unterschriften für die Forderung nach Abrüstung Deutschlands zu sammeln – nachdem sogar die Hardthöhe festgestellt hatte, Deutschland sei von keiner Seite bedroht. Zugleich beunruhigten mich damals die Anstrengungen des eben vereinten Deutschland, Jugoslawien zu zerstückeln – zunächst durch Unterstützung des slowenischen und kroatischen Separatismus. Teile und herrsche. Ich begann um Sarajewo zu fürchten. Sarajewo, das kürzlich erst Olympiastadt gewesen war. Sarajewo, einst die gemeinsame Stadt von Orthodoxen und Katholiken, Muslimen und Juden, bevor die deutschen Aggressoren im zweiten Weltkrieg die Juden vernichteten und sich mit Katholiken und Muslimen gegen die Orthodoxen, die Serben zusammentaten. Sarajewo, wo 1914 die Schüsse des Serben Gavrilo Princip das Signal gaben, auf das Deutschland geradezu gewartet hatte, um sich im lange vorbereiteten ersten Weltkrieg den »Platz an der Sonne« zu erobern. Ich schlug den Teilnehmern des Treffens vor, daß eine Gruppe europäischer Intellektueller und Gewerkschafter nach Sarajewo reisen sollte, um dort durch ihre Anwesenheit den Frieden zwischen Menschen verschiedener Sprache, verschiedener Religion, verschiedener Kultur zu schützen. Meine Anregung fand freundliches Gehör, mehr nicht. Offenbar konnte sich 1991 niemand vorstellen, was Sarajewo bevorstand. Eine führende SPD-Politikerin nannte auch unsere Abrüstungsinitiative überflüssig, denn Deutschland entwickele sich doch jetzt zur Zivilgesellschaft; unseren Protest gegen den »Jäger 90« (später »Eurofighter 2000«) könnten wir uns schon deswegen sparen, weil man sich in Bonn längst einig sei, das neue Waffensystem nicht zu bauen. Ach, dieser ewige Opportunismus, dieser immer gleiche Selbstbetrug. – Wir fuhren nicht nach Sarajewo. Der »Eurofighter« wird gebaut. Jetzt fahren wir Richtung Belgrad.

Wir haben nicht bemerkt, daß wir in einer großen Stadt angelangt sind. Der Bus hält in totaler Dunkelheit. An der Seite blinkt eine Taschenlampe auf. So finden wir den Eingang ins Hotel. In ganz Novi Sad (300 000 Einwohner), der Hauptstadt der Vojvodina, ist durch Graphitbomben der NATO der Strom ausgefallen.

Der zwölfte Angriff

24. Mai (Pfingstmontag). Um 6 Uhr früh Entwarnung. Um 23 Uhr, vor unserer Ankunft, war Alarm gegeben worden. In Novi Sad schlugen diesmal keine Bomben ein, aber in 20 Kilometer Entfernung.

Zwei Kollegen des jugoslawischen

Gewerkschaftsbundes, die beide jahrelang in Deutschland gearbeitet haben, begleiten uns ab jetzt. Der eine, Sveta, war Vertrauensmann bei DEMAG in Düsseldorf und leitet jetzt in Belgrad die Gewerkschaft für öffentliche Verwaltung und Handwerk; der andere, Miroljub, hat jahrelang beim DGB-Bundesvorstand die jugoslawischen Arbeiter in Deutschland betreut; die Stelle wurde inzwischen eingespart

Wir besichtigen die zerstörte petrochemische Fabrik. Sie liegt auf einem Gelände von etwa zwei mal zwei Kilometern. Elf Angriffe haben sie zum großen Teil zerstört. Sechs Tage lang hat sie gebrannt, die Rauchsäule war 300 Meter hoch. Die Bombenkrater haben 25 Meter Durchmesser. Der Schaden wird auf eine Milliarde US-Dollar beziffert. Hier und in dem zweiten petrochemischen Werk in Pancevo haben zwanzigtausend Menschen ihre Arbeitsplätze verloren. Ob die Fabriken je wieder aufgebaut werden können, wird sich erst nach Bodenuntersuchungen herausstellen, die Monate dauern. Wir werden vor dem Berühren der weit verstreuten riesigen Kesselteile und anderen Metalltrümmer gewarnt wegen Strahlungsgefahr durch Uranmunition (abgereichertes Uran). Auch das Klärwerk ist beschädigt. Gift fließt in die Donau. Es fehlen Pumpen für die Reparatur des Klärwerks, wie Meister Vladimir Ilic berichtet. Und auch dies erwähnt er: Acht von zehn Arbeitern, die Blut für Verletzte spenden wollten, wurden abgewiesen: Ihr Blut enthalte zu viel Gift.

In dem Arbeiterwohnviertel Detelinara besuchen wir eine Grund- und Hauptschule, die dreimal angegriffen wurde. Der Rektor kann sich die wiederholten »punktgenauen« Angriffe auf seine Schule nicht erklären. In zwei benachbarten Wohnblocks sind viele Wohnungen zerstört. Milun Duric, ein 68jähriger Dreher, berichtet uns, wie er in seiner Wohnung den Luftangriff erlebte und sich an einem Teppich aus dem Fenster abseilte, um Kinder aus dem verschütteten Keller zu retten. Er hat hier 33 Jahre gewohnt und regelmäßig mit einem Teil seines Arbeitseinkommens die Wohnung abbezahlt, bis sie sein Eigentum war. Jetzt hat er nichts mehr.

Ein Schaden von siebzig bis achtzig Millionen Dollar ist durch die völlige Zerstörung des modernen Fernsehsenders von Novi Sad entstanden, der ein wichtiges Glied der europäischen Fernsehkette war. Dieser Sender hat täglich Programme in sechs Sprachen ausgestrahlt und versorgte die zahlreichen ethnischen Gruppen. Seine Arbeit für die inter-ethnische Verständigung ist mit dem europäischen Fernsehpreis ausgezeichnet worden. Bei einem Treffen mit jugoslawischen Kolleginnen und Kollegen im Gewerkschaftshaus von Novi Sad erfahren wir, daß es in der Vojvodina bis zum Ausbruch des Krieges zwischen den 26 verschiedenen ethnischen Gruppen keine Zusammenstöße gegeben habe. Die systematischen Angriffe auf die Fernsehstationen können keinen anderen Zweck haben, als den Aggressoren die Propaganda-Oberhoheit zu verschaffen. Getroffen wird nicht nur die Informationsfreiheit der jugoslawischen Bevölkerung, sondern auch unsere, denn über die Opfer der Bombardements erfahren wir in Deutschland nicht durch die NATO, sondern meist nur durch das jugoslawische Fernsehen, wenn das deutsche von ihm Aufnahmen übernimmt.

Alle drei Brücken über die Donau sind zerstört. Unter der zerbombten »Freiheitsbrücke« verlief die Hauptwasserleitung, durch die Novi Sads südliche Stadtteile mit Trinkwasser versorgt wurden. Das über Jugoslawien hinaus bekannte herzchirurgische Zentrum von Novi Sad mußte, von Verkehr, Strom und Wasser abgeschnitten, seine Arbeit einstellen. Die »Freiheitsbrücke« war nach dem Sieg über die deutsche Wehrmacht gebaut worden, die 1941 die alte Brücke zerbombt hatte.

Wir sind mit unserem Bus zwanzig Minuten unterwegs in Richtung Belgrad, als im Norden in etwa 25 Kilometern Entfernung hohe schwarze Rauchwolken aufsteigen. Aus den Radionachrichten erfahren wir, daß die Raffinerie, die wir vorhin besucht haben, wieder bombardiert wurde.

Eine humanitäre Katastrophe

25. Mai. In Belgrad haben wir uns ein Bild von den Folgen der Bombenangriffe machen können, z.B. bei der chinesischen Botschaft und der unmittelbar daneben liegenden Musikschule. Nach Mitternacht sind wir zur Belgrader Donaubrücke gegangen, auf der sich jeden Abend eine Menschenmenge versammelt mit der angesteckten Zielscheibe »Target«. Es gibt Alarm, auf einmal stehen wir allein auf der Brücke. Die Menschen glauben nach all ihren Erfahrungen, daß die NATO-Piloten auch Brücken mit Menschen darauf bombardieren werden. Wir gehen die zehn Minuten zu unserm Hotel »Moskwa« im Zentrum der Stadt, ziemlich schnell, aber nicht in den Luftschutzkeller, sondern bleiben auf dem Zimmer, öffnen die Fenster und sehen zum Himmel hinauf.

Zehn Minuten vor 4 beginnt die Flak zu schießen. Es hört sich an wie Geprassel, bald näher, dann wieder ferner. Ein sirrendes, leise pfeifendes Geräusch über uns: Die Maschinen überfliegen Belgrad in großer Höhe. Dann unerwartet der Einschlag, nahe, sehr hart, ganz anders als bei Bomben. Das Innenministerium, das schon einmal bombardiert worden war, ist von einer Rakete getroffen.

Am nächsten Morgen sehen wir uns die Ruine des völlig zerstörten Fernsehsenders an. Ein Techniker, der das Bombardement trotz hohen Blutverlustes überlebt hat, erzählt uns, er habe wenige Minuten vorher die Etage, in der seine Kolleginnen und Kollegen getötet wurden, verlassen. Er habe alle gut gekannt. Aber sechs seien immer noch vermißt. Nichts sei bisher von ihnen gefunden worden – als wären sie durch die Hitze verdampft. 130 Kolleginnen und Kollegen des Senders wurden verletzt, einige sehr schwer. Sie liegen noch in den Krankenhäusern.

Unmittelbar am Sender liegt das Belgrader Kindertheater vor einer Kirche, auf der anderen Seite der Straße. Vom Kirchendach haben sie Leichenteile geborgen. Wir legen an der Ruine des Senders für die 16 Toten Blumen nieder, neben ein Schild mit dem Motto unserer Reise »Dialog von unten statt Bomben von oben«.

Kragujevac, die Stadt der Zastava-Automobilwerke, ist seit der Bombardierung des Betriebes die Stadt der Arbeitslosen. Von den 200 000 Einwohnern haben durch die elf Angriffe auf das Werk 37 000 Beschäftigte ihre Arbeitsplätze verloren. Hinzu kommen die indirekt Betroffenen der Zulieferbetriebe, für deren Produkte es keine Abnehmer mehr gibt. Beim Begrüßungsgespräch im Gewerkschaftshaus schildert die lokale Vorsitzende Rusica Milosavljovic die Folgen der Bombardements für die Stadt und spricht von einer humanitären Katastrophe. Das

Gespräch findet während eines Alarms statt. Wir nehmen wahr, daß sich die etwa 30 versammelten Zastava-Kolleginnen und Kollegen durch zwei entfernte Detonationen nicht irritieren lassen. Eine Frau zuckt die Achseln: »Wir versuchen, normal weiterzuleben.«

Wir übergeben eine von unserer Initiative gesammelte Spende, 10 000 Mark. Nichts im Vergleich zu den Bombenschäden, aber unser Beitrag wird verstanden als Zeichen der Solidarität aus einem der Aggressorstaaten, dem Land, dessen Wehrmacht an diesem Ort vor einem halben Jahrhundert das größte Massaker in Jugoslawien während der deutschen Okkupation verübt hat. In der Gedenkstätte für die Opfer legen wir ein Blumengebinde nieder: »Den Opfern der deutschen Wehrmacht, der Nato und der Bundeswehr.«

Am 21. Oktober 1941 wurden hier siebentausend Menschen, darunter 300 Schüler, klassenweise mit ihren Lehrern, als »Geiseln« erschossen. Ein Gedenkstein erinnert an den deutschen Soldaten, der sich weigerte, mitzuschießen und deshalb mit erschossen wurde.

Das Gelände der Gedenkstätte wurde gleich zu Beginn des NATO-Krieges getroffen, das Museum am 14. Mai durch eine in der Nähe einschlagende Rakete schwer beschädigt. Die Direktorin Slavica Kominac verweist auf die Symbolik einer durch Bombensplitter beschädigten Skulptur mit dem Titel »Der Faschismus ist überwunden«. Sie erinnert an den Besuch des Museums durch Petra Kelly Mitte der achtziger Jahre, die ins Gästebuch schrieb, die Grünen würden sich dafür einsetzen, daß sich solche Verbrechen nicht wiederholen.

Bei der Renovierung des Museums soll ein Raum angegliedert werden: für die Dokumentation der NATO-Bombardements.

Wegen des andauernden Alarms müssen wir die Besichtigung des zertrümmerten Zastava-Werkes auf morgen verschieben. Es ist ein traumhaftes Sommerwetter, die Akazien verblühen gerade. Rote Mohnfelder in der Hügellandschaft, bunte Häuser in den Feldern, ein weiter Blick. Was für ein schönes Land! Hoch oben das Sirren von Flugzeugen. Sehr fern schießt die Flak.

Wenn die schnellen Sterne kommen

In der Nacht vom 26. zum 27. Mai. Die Summe der bisherigen Eindrücke zeigt uns, in welchem Maße sich der NATO-Krieg gegen die Zivilbevölkerung richtet. Die Bombardements zerstören die Nervenzentren der Produktion und der Versorgung. Zum Beispiel Kragujevac, die Automobilfabrik Zastava: Die Trümmer des Werks werden zwar von den Arbeitern so gut wie möglich aufgeräumt, aber ohne jede Aussicht auf Wiederinbetriebnahme in absehbarer Zeit.

Alarm. Alle verlassen das Gelände, mehrere hundert Arbeiter, die mit Aufräumarbeiten beschäftigt waren. Sie grüßen zurück, als wir sie mit dem Bus überholen. Auch das Kraftwerk auf dem Betriebsgelände ist irreparabel zerstört. Es hat auch die Stadt versorgt, mit Strom und Wärme. Die Bevölkerung fürchtet den Winter, denn die Wohnungen in den Hochhäusern haben keine Kamine für Feuerstellen.

Einige von uns besuchen die Familie Pavlovic. Vater Radomil (52) hat 35 Jahre bei Zastava gearbeitet, Sohn Slobodan (27) sechs Jahre. Beide sind jetzt arbeitslos. Die Mutter Milanka ist zukkerkrank. Ihr mußten am 7. April beide Beine amputiert werden, zwei Tage vor dem schweren Angriff auf Kragujevac. Wegen der vielen Schwerverletzten, die ins Krankenhaus aufgenommen werden mußten, wurde Milanka Pavlovic viel zu früh nach Hause entlassen. Bei Alarm und Luftangriffen muß sie in der Wohnung bleiben, weil der Lift bei Stromausfall nicht funktioniert und während der vielstündigen Alarmzeiten nicht benutzt werden darf. Ihre Beinstümpfe haben sich entzündet. Es fehlt an Medikamenten, wie überall in Jugoslawien infolge des Embargos. Spezialmedikamente wie Insulin müssen kühl gelagert werden, was aber nicht möglich ist, wenn der Kühlschrank keinen Strom hat.

Bei »Zastava« als staatlichem Betrieb besteht noch ein Selbsthilfenetz, das Privatbetrieben fehlt. Für den arbeitslosen Vater und seinen Sohn gibt es ein Arbeitsausfallgeld der Firma von 230 Dinar gleich 25 Mark im Monat. Es ist für drei Monate garantiert. Das Arbeitsamt zahlt monatlich 100 Dinar, also rund zehn Mark, zunächst für ein halbes Jahr.

Bei der Abfahrt aus Kragujevac sehen wir eine lange Menschenschlange vor einem Tabakladen. Die Ursache erfahren wir drei Stunden später in Nis (300 000 Einwohner). Hier ist die größte Tabakfabrik Jugoslawiens (2500 Beschäftigte) total zerstört worden. 1995 hatte die Fabrik neue Maschinen vom Hersteller Hauni aus Hamburg gekauft.

Die Wasserpumpenfabrik in Nis (1500 Beschäftigte) wurde sowohl von Spreng- wie auch von Splitterbomben getroffen. Metallteile aus den Lagern des Werkes flogen bis zu einem Kilometer weit und durchschlugen Wände und Dächer von Wohnhäusern. Wegen der vielen Blindgänger aus Kassettenbomben wurde das Betriebsgelände gesperrt. Es ist fraglich, ob und wann in dem größten Pumpenwerk des Balkans wieder produziert werden kann, auch um die Lieferverträge mit Ägypten und den Golfstaaten zu erfüllen.

Im Industriegelände von Nis liegt ein Werk neben dem anderen in Trümmern. Auch die Technische Hochschule wurde beschädigt. Der Vizedekan der Fakultät für Elektronik (2000 Studenten), Professor Milun Jevtic, der in Bochum studiert hat, führt uns durch die verwüsteten Räume. Der Detonationsdruck hat Regale mit Büchern durch die Fenster geschleudert. Im Eingangsfoyer ist eine nicht explodierte Kassettenbombe ausgestellt, die 130 Splitterbomben enthielt. Studenten haben die Frage »Kada?« daraufgemalt – »Wann?« Von den amerikanischen Herstellern ist Januar 2005 als Verfallsdatum aufgestempelt. Wie in Nis sind in ganz Jugoslawien die Schulen und Hochschulen seit Kriegsbeginn geschlossen.

Eine Brücke über die Nisava wurde am 9. Mai, dem Feiertag der Befreiung vom Hitlerfaschismus, so schwer getroffen, daß sie nur noch für Fußgänger und Radfahrer passierbar ist. Dabei wurde auch die Wasserleitung zum Stadtzentrum durchtrennt, das benachbarte griechische Konsulat und eine dahinterliegende Prothesenfabrik beschädigt. Umliegende Privathäuser sind nun unbewohnbar.

Eine Splitterbombe ging in der Mittagszeit auf dem Marktplatz von Nis nieder, 20 Menschen wurden getötet und 50 verletzt. Der örtliche Vorstand der Gewerkschaft berichtet von 1925 getroffenen Gebäuden, darunter 18 Schulen. Während unseres Besuchs schlagen drei weitere schwere Bomben in Nis ein.

In der kleinen Bergbaustadt Aleksinac erschüttert uns das Ausmaß der Zerstörung. Siebzehn Menschen sind bei einem Angriff getötet und 36 verletzt worden. 36 Häuser wurden dem Erdboden gleichgemacht. Allein in der Straße Dujan Trivunac sind 120 Wohnungen nicht mehr bewohnbar, die meisten ausgebrannt. Viele Menschen haben sowohl ihr Heim und ihren Hausrat als auch ihre Arbeit verloren. Das Bergwerk und viele kleine Betriebe liegen wegen Strommangels still. Die Einwohner sind vor allem auf die Hilfe von Jugoslawen im Ausland angewiesen. Der Vorsitzende der örtlichen Rotkreuzstation, Miodrag Vojnovic, teilt uns erbittert mit, daß das Deutsche Rote Kreuz seit Beginn des Krieges keine Hilfe mehr leistet. Immerhin haben wir unterwegs mehrere Lastwagen mit Hilfsgütern aus Griechenland und einen Truck aus Rußland gesehen.

Eins der vielen Kinder, die sich zu uns drängen, antwortet auf die Frage, was es den Verantwortlichen für die Bombenkriege sagen würde: »Ich kann nichts sagen, ich will nur schlafen.« Die achtjährige Jana nennt die Flugzeuge am Nachthimmel »schnelle Sterne«. In einem Luftschutzbunker hat das Serbische Rote Kreuz das Kindertheater »Smeschko« (Lächeln) eingerichtet. Die Kinder haben den Beton der Wände bemalt. Vojnovic macht uns auf die Inschrift eines der Bilder aufmerksam: »Wir werden siegen, denn wir lieben unser Land, wir haben kein anderes.«

Auch die Fähren gibt es nun nicht mehr

27./28. Mai. Am vorletzten Tag unserer Reise sehen wir in Belgrad immer neue Zerstörungen, hören immer mehr Flugzeuge und Detonationen. Wir erfahren in Gesprächen mit vielen Menschen, wie der Krieg das ganze Volk in seinen Würgegriff nimmt. Tomislav Banovic, der Vorsitzende des serbischen Gewerkschaftsbundes sagt, die materiellen Schäden nach 64 Tagen Bombardement durch die NATO seien bereits größer als alle Zerstörungen während des 2. Weltkrieges in Jugoslawien.

Viermal ist das Belgrader Krankenhaus Dr. Dragisa Misovic am Bulevar Mira (Friedensboulevard) von NATO-Bomben getroffen worden. Es ist benannt nach einer Ärztin, die von den Nazis erschossen wurde. Der stellvertretende Chefarzt Dr. Miodrag Lazic, dem es fernliegt, die massenmörderische Naziokkupation zu verharmlosen, erwähnt während unserer Begrüßung: »Hitler hat in Jugoslawien kein Krankenhaus getroffen.«

Im Krankenhaus Dr. Dragisa Misovic ist die einzige jugoslawische Klinik für lungenkranke Kinder. Wir sehen zerborstene Mauern, die verbogenen Bettgestelle der kleinen Patienten, beschädigte medizinische Geräte, die sämtlich deutsche Fabrikate sind. Krankenschwestern suchen in den Trümmerhaufen nach Behandlungsberichten, die für die richtige Medikation der Langzeitpatienten unentbehrlich sind. Die Neurologie ist total zerstört, sie war vor kurzem renoviert worden. Alle 810 Patienten mußten evakuiert werden. Die meisten der 1200 Beschäftigten können ihre Aufgaben nicht mehr wahrnehmen.

Wir treffen uns mit verschiedenen Mitgliedern der bürgerlichen Opposition und aus gewerkschaftlichen Gruppen. Alle stimmen in dem Unverständnis für die Begründungen der NATO-Aggression überein. Hier einige Beispiele:

»Sind das die Menschenrechte, die wir jetzt von der NATO bekommen? Das erste Menschenrecht ist das Recht auf Leben.«

»Durch die Bombardements ist die sich öffnende Gesellschaft wieder geschlossen. Der Krieg begünstigt erst die Entwicklung einer Diktatur.«

»Es wird vielleicht wieder Strom geben, wenn wir die NATO hereinlassen, aber wir verlieren Freiheit und Würde.«

»Wenn der Westen weiterbombt, werdet ihr noch viel mehr Flüchtlinge bekommen, auch aus Serbien.«

»Die NATO am Himmel, Milosevic am Boden – ohne Hoffnung und Hilfe sind wir wie in einem Sandwich. Zwei arrogante Mächte erdrücken uns von oben und unten.«

Wissenschaftler und Vertreter der Grünen berichten uns über nicht absehbare ökologische und gesundheitliche Schäden durch die Bombardierung der chemischen Werke und durch die Verwendung neuartiger Waffen. Professor Dr. Luka Radijar berichtet, daß der bisher ohnehin schon zu hohe Phosgengehalt der Luft in der Umgebung des petrochemischen Kombinats Pancevo durch die Bombardierung um das Zehntausendfache stieg. »Mein Enkelkind in einer Hochhauswohnung im 16. Stock hat kein Wasser, keinen Strom, und die Mutter hat keine Milch. Was hilft dieser Krieg den Albanern im Kosovo, dessen Dörfer und Städte dermaßen zerstört und vergiftet sind, daß dort auf lange Zeit kein Leben mehr möglich ist?«

Im Land wächst die Angst vor völliger Isolation, nachdem schon seit langer Zeit durch das Embargo z.B. wissenschaftliche Kontakte eingeschränkt sind. Mit Beschämung hören wir, daß wir als erste deutsche Gewerkschaftergruppe seit Beginn der 90er Jahre begrüßt werden. Daß der DGB alle Kontakte eingefroren hat, befremdet die jugoslawischen Kolleginnen und Kollegen. Das Hotelpersonal in Belgrad verabschiedet uns mit Tränen. Es sind Tränen der Angst vor der ungewissen, bedrohlichen Zukunft. »Zeigt uns, daß wir nicht allein sind.« Und hier, wie zum Schluß fast aller Gespräche: »Berichtet die Wahrheit.«

Das Volk fürchtet, mundtot gemacht zu werden. Die Unterbindung der Satellitenübertragungen von Rundfunk- und Fernsehsendungen hat zur Folge, daß die Weltöffentlichkeit kaum noch etwas vom NATO-Terror erfährt. Rolf Becker: »Man verbindet dem Opfer den Mund, damit man es nicht schreien hört.« Die Abschnürung des Landes setzt sich dadurch fort, daß wichtige Informanten z.B. aus Gewerkschaften und Oppositionsgruppen keine Einreisemöglichkeit mehr in die Bundesrepublik bekommen. Unser Begleiter Sveta wollte am 29. Mai nach Düsseldorf fahren, um den DGB-Vorstand zu informieren und um solidarische Hilfe zu erbitten. Die deutschen Behörden verwehrten ihm die Einreise.

Auf der Rückfahrt passieren wir noch einmal Novi Sad, wo wir am ersten Tag unserer Reise die zerstörten Donaubrücken gesehen hatten. In der letzten Nacht sind auch die Anlegestellen der Fährboote, mit denen die Verbindung zwischen den Stadtteilen an beiden Ufern mühsam aufrechterhalten wurde, zerbombt worden.

Resümee auf der Rückreise

28. Mai. Meine Notizen sind mit denen meiner Mitreisenden in gemeinsame Berichte eingeflossen, die wir täglich nach Deutschland übermittelt haben und die ich jetzt für meinen Bericht in OSSIETZKY verwende. Auf der Rükkreise verfaßt Rolf Becker ein Resümee,

dem alle zustimmen:

»Dialog von unten statt Bomben von oben« – Ziel unserer Reise war es, Informationen aufgrund eigener Beobachtungen und unmittelbarer Kontakte mit Kolleginnen und Kollegen in Jugoslawien zu gewinnen und an unsere Kolleginnen und Kollegen in der Bundesrepublik Deutschland weiterzugeben. Wir wollten dazu beitragen, den gewerkschaftlichen Auftrag »Konflikte auf zivilem Wege ohne militärische Gewalt zu lösen« (DGB-Grundsatzprogramm) zu verwirklichen.

Auf den Stationen unserer Reise – Novi Sad, Belgrad, Kragujevac, Nis und Aleksinac – haben wir die Zerstörungen von Fabriken, Kraftwerken, Krankenhäusern, Schulen und Hochschulen, Wohnvierteln, Verkehrswegen und Brücken gesehen und in Gesprächen mit Beschäftigten zerstörter Betriebe, Ausgebombten, Rote-Kreuz-Helfern, Ärzten, Wissenschaftlern und Vertretern von Gemeinden und Gewerkschaften erfahren, was die Bombardements der NATO für die Menschen in Jugoslawien bewirken.

Der »saubere Krieg« der NATO ist kein »Krieg gegen Milosevic«, sondern ein Krieg gegen die Zivilbevölkerung. Die Zentren der Versorgung liegen in Trümmern, die Arbeitsplätze sind für Jahrzehnte vernichtet, die Gesundheit vieler Menschen in noch nicht abschätzbarem Umfang geschädigt, die Jugend ist ihrer Perspektive beraubt.

Und ein Ende des NATO-Terrors ist nicht in Sicht.

Der Auftrag, den uns die Menschen mit auf die Heimreise geben, ist einfach: Tragt dazu bei, den Krieg auch nur um einen Tag zu verkürzen. Laßt uns nicht allein. Helft die Wahrheit über unsere Lage zu verbreiten.

Es wird schwer sein, diesen einfachen Auftrag zu erfüllen. Wir bitten unsere Kolleginnen und Kollegen in Betrieben und Gewerkschaften und alle Menschen, die guten Willens sind, uns zu unterstützen. Wir fordern alle humanitären Organisationen in der Bundesrepublik Deutschland auf, die Not und das Leid der Bombenopfer zu lindern

Spendenkonto: »Hilfe für Kragujevac« (J. Bergmann), Konto 1230 499 335 bei der Hamburger Sparkasse, BLZ 200 505 50.

Dieser Beitrag ist ein Nachdruck der Zeitschrift Ossietzky mit freundlicher Genehmigung des Authors.

Ingo Ruhmann

Information Warfare an der Grenze[1]

Wenn sich der Pulverdampf gelegt hat, ist es nach kriegerischen Auseinandersetzungen Zeit für die Analyse, zugleich aber auch für die Verklärung von Erfolg und Mißerfolg. Oft genug ist zwischen beiden nur schwer eine Trennlinie zu erkennen. Seit die Medienwirkung von Konflikten sich von der psychologischen Kriegführung abgesetzt hat und – runderneuert unter der für viele neue und technikgestützte Operationen genutzten Sammelbezeichnung Information Warfare – ihren Weg in militärische Operationshandbücher gefunden hat, gehört auch die mediale Nachbereitung von Kriegen in die Kategorie der Aufräumoperationen.

Während sich die Öffentlichkeit wieder weitgehend anderen Themen zugewandt hat, mühen sich die Militärexperten zu erklären, aus welchen Gründen der Kosovo-Krieg zwar durch einen Luftkrieg entschieden wurde, dieser zugleich aber die Grenzen überlegener Luftstreitkräfte mehr als deutlich vor Augen führte. Im folgenden wird es daher darum gehen, welchen Stellenwert die zur Begründung für neue Rüstungsanstrengungen gern angeführte technologische, heute also meist informationstechnische Überlegenheit in diesem Konflikt hatte. Die mediale Seite von Information Warfare wurde vereinzelt untersucht[2]. Hier wird es um Information Warfare zunächst in einem generellen Sinne gehen, wobei militärischen Planungsszenarien der Kosovo-Krieg in seinem Ablauf gegenübergestellt wird. Daran schließt sich eine Betrachtung der Einsätze von High-Tech-Waffen an. Ebenso wird aber auch versucht, nach den Elementen von Information Warfare im engeren Sinne im Kosovo-Krieg zu fahnden, also nach dem Einsatz von Informationstechnik zur Erreichung militärischer Dominanz. Zentral ist bei dieser Betrachtung die Technik als Ausgangspunkt, politische und ethische Betrachtungsebenen stehen dahinter zurück.

Bevor also der Versuch unternommen werden kann, die Rolle von High Tech und Information Warfare im Kosovo-Krieg zu beleuchten, sollte zur Vermeidung von Mißverständnissen in Erinnerung gerufen werden, wie sich NATO-, vor allem aber US-Militärs den Ablauf eines solchen Konflikts unter Information Warfare-Prinzipien vorstellen[3]. Begonnen würde mit einer massiven Aufstockung der Aufklärungskapazitäten für die operative Planung und, um die Einheiten zur elektronischer Kampfführung operativ und technisch auf den erforderlichen Stand zu bringen. Folgen würde darauf die Einwirkung auf das Bild des Gegners von sich selbst in den Medien allgemein und durch technisch abgestützte psychologische Kriegführung in Form von Eingriffen in Computernetze und Datenbanken. Die ersten konventionellen Kampfhandlungen bestünden aus der umfassenden Zerstörung der gegnerischen Luftabwehr, der sich dann eine Zerstörung strategischer und schließlich taktischer Ziele anschließen würde. Reorganisationsversuche des Gegners wären durch das dauerhafte Niederhalten der Kommunikationsinfrastruktur im Ansatz zu verhindern. Am Ende derartiger Szenarien steht die Aufgabe eines völlig desorganisierten Gegners.

Analysiert man den Kosovo-Krieg entsprechend solcher Planungs-Blaupausen, so läßt sich leicht erkennen, daß der Ablauf der alliierten Kampfhandlungen diesen Vorgaben in einigem Umfang folgte. Doch nach dem Einlenken Milosevics ist – trotz oder gerade wegen teilweise deutlicher Kritik aus den Reihen der Militärs während des Kriegsverlaufs – die Bereitschaft der Akteure stark gesunken, sich mit dem Einsatz von Information Warfare-Elementen auseinanderzusetzen. Doch auch ohne eingehende offizielle Analysen lassen sich mehrere auffallende Diskrepanzen zwischen Anspruch und Wirklichkeit festhalten.

1. Zu keinem Zeitpunkt des Konflikts gelang es alliierten Luftstreitkräften, die jugoslawische Luftabwehr außer Gefecht zu setzen und damit die Vorbedingung jeder weiteren auf Luftüberlegenheit beruhenden Operationen zu erfüllen. Statt des-

sen wurden allein die B1-Bomber im gesamten Verlauf des Kampfhandlungen mit über 30 Raketen beschossen[4]. Ob die Entscheidung bewußt getroffen wurde, das integrierte Luftverteidigungssystem nicht zu zerstören[5] oder damit nur ein Unvermögen kaschiert wurde, ist nicht auszumachen.

2. Die Unterdrückung der verbliebenen Luftabwehr wurde dadurch behindert, daß es an Electronic Warfare-Spezialisten mangelte[6], die durch Restrukturierungen im Zuge der Entwicklung von Information Warfare in zentralen Einheiten zusammengelegt worden waren. Die Anpassung von Electronic Warfare-Systemen an neue Frequenzen dauerte deutlich länger als vor einigen Jahren[7]. Eine Reihe spezialisierter Flugzeuge wurde zu Aufgaben genutzt, die nicht der Ausrüstung entsprachen: Flugzeuge zur Koordinierung von Bodentruppen und zur Luftraumüberwachung wurden zur Koordination der Luftoperationen eingesetzt[8]. Da die Luftraumüberwachung auch durch die NATO-AWACS geleistet wurde, ist dies – trotz der höheren Anforderungen im dicht belegten Luftraum über der Adria – ein Indiz für Defizite bei der militärischen Luftraumüberwachung und der Koordination der Operationen. Auch dies ein eklatanter Widerspruch zu den Anforderungen von Information Warfare-Szenarien nach einer überlegenen Kommando- und Kontroll-Infrastruktur.

3. Die Zerstörungen am jugoslawischen Kommunikationsnetz erwiesen sich als nicht ausreichend, um die jugoslawische Kommando- und Kontrollstruktur aufzubrechen, was wiederum nicht mit den Zielen eines Information Warfare in Einklang zu bringen ist. Zwar läßt sich darüber streiten, ob die auf jugoslawischer Seite zur Vertreibung der Kosovaren eingesetzten paramilitärischen Einheiten überhaupt in eine Kommandostruktur eingebunden waren, doch ist die halbwegs koordinierte Operationsfähigkeit der regulären jugoslawischen Verbände nicht mit den Zielen eines Information Warfare in Einklang zu bringen.

4. Selbst bei der in der Luftkriegführung nicht gerade neu erfundenen Zerstörung strategischer Ziele wurde durch mangelnde Aufklärung und vor allem durch die Erfordernis, außerhalb der Reichweite der Luftabwehr zu operieren, das Ziel einer »unblutigen« Kriegführung verfehlt. Statt dessen wurden Brücken beschossen, die gerade von Zügen und Bussen passiert wurden. Die Opfer derartiger Attacken führten unter dem Blickwinkel des Information Warfare zu einem Mediendebakel für die Alliierten, das noch durch den Beschuß von Botschaften und Krankenhäusern verstärkt wurde.

5. Die Überprüfung der alliierten Erfolgsmeldungen erwies sich für die NATO als wenig schmeichelhaft. Statt Panzer waren von der »intelligenten« Munition oftmals Panzerattrappen getroffen worden, in denen Öfen eine Infrarotsignatur erzeugen. Das Problem aus Sicht von Information Warfare ist dabei nicht die Zielauswahl der Waffen, sondern die offensichtlichen Defizite bei der Zielaufklärung.

Zusammengefaßt bedeutet dies: Luftabwehr und Kommandonetz der jugoslawischen Armee blieben hinreichend operationsfähig, die Unterdrückung der Luftabwehr durch Electronic Warfare erwies sich als so schwierig, daß sich Operationen in niedriger Höhe verboten. Die Folge war eine verminderte Treffergenauigkeit, die wiederum mediale Mißerfolge produzierte. Im Vergleich zu allen Elementen der Information Warfare Doktrin lassen sich also gravierende Defizite ausmachen.

Bei diesen Ergebnissen verwundert nicht, daß gerade Militärexperten Belgrad zum Sieger der ersten Kriegsphase erklärten[9]. Nach zwei Monaten Krieg wurden zunächst Gründe für die Diskrepanzen zwischen Anspruch und Wirklichkeit gesucht[10]. Angeführt wurde, daß die gut ausgebildete jugoslawische Armee den optimalen Nutzen aus ihren Fähigkeiten gezogen hatte. Am Ende waren dann US-Militärs mit dem Vorwurf schnell bei der Hand, dies sei »coalition warfare at its worst«[11] gewesen, nur sei der Kosovo-Krieg als Fehler nicht groß genug gewesen, um daraus zu lernen. Diese auf die NATO-Alliierten gemünzten Schuldzuweisungen können kaum kaschieren, daß die Hauptprobleme keineswegs in der mangelnden Ausrüstung der europäischen Verbündeten lag, sondern darin, daß das zentrale Konzept des informationstechnisch gestützten Krieges diesmal nicht so recht aufging. Zeigen läßt sich die im Kleinen wie im Großen, also bei der gern bestaunten Waffenwirkung sogenannter Präzisionswaffen ebenso wie bei der eingehenden Betrachtung von Kernpunkten von Information Warfare-Operationen. Fraglich bleibt nur, ob hier die Begrenztheit der Einsatzmöglichkeiten von Information Warfare sichtbar wurden, oder, ob die Kampfhandlungen unter weitgehendem Verzicht auf Information Warfare-Elemente durchgeführt wurden.

Glaubenssätze: Präzision und High-Tech

Von Beginn an wurde der Kosovo-Krieg unter der zentralen Prämisse geführt, Bombardements mit Präzisionswaffen würden einen militärischen Erfolg herbeiführen können. Abgewichen wurde davon auch nicht, als den Kommentatoren dämmerte, daß weder die Technik Wunderdinge vollbringen konnte, noch, daß Kriege dadurch gewinnbar würden, daß eine Seite den Ablauf ihrer Operationen ankündigt; abgewichen wurde davon auch dann nicht, als klar wurde, daß militärische Operationen gegen die Zivilbevölkerung nicht durch Luftschläge zu unterbinden sind.

Abgesehen von allen anderen Zumutungen erweist sich immer wieder der Glaube an die Möglichkeiten von mehr oder minder »intelligenten« Präzisionswaffen als Motor unverwüstlicher Erwartungen an unblutige und schnelle militärische Erfolge. Und ebenso, wie Militärs nicht müde werden, die technischen Vorzüge ihrer Waffen zu preisen, so findet sich am anderen Ende des Spektrums derselbe Glauben an die Leistungsfähigkeit dieser Waffensysteme.

Vergessen wird dabei leider, daß der Terminus »Präzisionsbombardement« schon im Zweiten Weltkrieg regelmäßig zur Verharmlosung massiver Luftangriffe genutzt wurde. Präzise waren zu jener Zeit allenfalls Schläge wie das alliierte Bombardement der Gestapo-Zentrale in Kopenhagen. Steuerung per Video, GPS-Navigationssets und Lenkung der Bomben per Laserstrahl haben

heute die Gefahr für die Piloten vermindert, aber Wirkung und Genauigkeit von Bomben keineswegs ins Grenzenlose gesteigert oder die Gesetze der Physik aufgehoben. Folgerichtig mußte die NATO nach Untersuchung der getroffenen Militärziele die ursprünglichen Trefferzahlen deutlich nach unten korrigieren[12].

Zum Glauben an die technischen Möglichkeiten und dessen Erzeugung gehört auch, alte Technik als neue Errungenschaft zu verkaufen. Schon im Golfkrieg wurden lasergesteuerte Bomben und videogelenkte Raketen zum Medienereignis. Beides wurde zuerst eingesetzt zu Zeiten des Vietnam-Krieges. Neben einigen anderen Streitkräften nutzt auch die russische Luftwaffe seit Jahren lasergelenkte Bomben, was das russische Militär im jüngsten Tschetschenien-Konflikt als Nachweis der Präzision ihrer Bombardements anführte[13]. Während den Russen niemand Glauben schenken mag, blieb im Kosovo-Krieg völlig unhinterfragt, wodurch mittlerweile 30 Jahre alte Waffentechnik zum Ausweis von High-Tech-Kriegen werden kann.

Die Suche nach technologischen Neuerungen im Kosovo-Krieg bleibt dagegen weitgehend ergebnislos. Auch die zum Kurzschluß des jugoslawischen Elektrizitätsnetzes genutzten Graphitfäden aus den Forschungslabors für nichtlethale Waffensysteme wurden bereits im Golfkrieg eingesetzt. Von dort stammt auch die Erfahrung, daß zu kurze Fäden nicht mehr zu entfernen sind und zu unkontrollierbaren Zerstörungen der elektrischen Anlagen führen[14]. Deshalb wurden diesmal längere Fäden eingesetzt. Über den Einsatz nichtnuklearer EMP-Waffen wurde allenfalls spekuliert[15]. So ging die Demonstration von High-Tech-Waffen nicht über bekannte Technik hinaus.

Statt einer Analyse mutierten Waffentypen zum Gegenstand einer Auseinandersetzung vor allem um moralische Legitimation. Der Einsatz von Splitterbomben durch alliierte Bomber wurde zum Synonym moralischer Verwerflichkeit. Dem wurde entgegengehalten, Präzisionswaffen würden in solchem Umfang eingesetzt, daß die Arsenale fast leer seien. Die damit beabsichtigte Implikation einer präzisen Kriegführung ohne unschuldige Opfer wiederum wurde mit jedem Angriff auf Busse und Botschaften konterkariert. Doch blieb die technische Art und Weise der Kriegführung täglich neuer Anlaß der Debatte. Damit argumentierten beide Seiten zwar auf derselben irrealen Ebene eines technisch vorgeblich möglichen unblutigen Krieges. Mit dieser Debatte waren aber die eigentlich wichtigen Fragen nach Ursachen und Zielen des Krieges, den eingesetzten Mitteln und den Perspektiven jenseits militärischer Operationen erfolgreich in den Hintergrund gedrängt – zumindest dies ein Erfolg an der medialen Front von Information Warfare.

Aus dem Blickfeld: Information Warfare Operations

Im Golfkrieg wurde noch die Falschmeldung verbreitet, die Alliierten hätten mit Hilfe eingeschmuggelter Computerviren Zugang zur irakischen Luftabwehr gefunden. Derartige Meldungen sind ideale Werkzeuge im Information Warfare, weil sie den Gegner verunsichern und für die Medienberichterstattung eine hohe technologische Überlegenheit suggerieren. Im Kosovo-Krieg kam dagegen nur vereinzelt und aus unspezifizierten alliierten Quellen die Behauptung, die Computer der jugoslawischen Luftabwehr wären manipuliert worden. Auch die in der Nachbereitung des Krieges häufigeren Presseberichte über Computerhacker der NATO[16] enthalten bei genauer Analyse nicht mehr als die Nachricht, daß es der U.S. Air Force gelungen sei, in das jugoslawische Flugabwehrsystem einzudringen und dort falsche Botschaften und Ziele zu erzeugen. Außer, daß dies ein »gutgehütetes Geheimnis« sei, war allenfalls zu erfahren, daß dabei auf den Funkstrecken der Kommandonetze falsche Daten eingefügt würden[17]. Nun gibt es Manipulationen an ungesicherten Funknetzen seit dem Ersten, das Einspielen falscher Daten und Stören von Flugabwehr- und Signalnetzen seit dem Zweiten Weltkrieg. Dies wurde in den letzten 50 Jahren kontinuierlich verfeinert. Das wirklich Neue beim Information Warfare im Kosovo-Krieg bleibt aber damit im Nebel der Andeutungen von Militärkorrespondenten. Statt dessen mußte die NATO schon zu Beginn des Konflikts erklären, daß ihr E-Mailserver Ziel von 2.000 Störmails pro Tag sei, die von Jugoslawien aus versandt würden. Damit wurde nun die NATO erstmals in nennenswertem Umfang Ziel von Information Warfare Operationen.

Während die NATO 1997 erklärte, über Bosnien drei fliegende Stör- und Radiosender EC 130-E »Commando Solo« einzusetzen, die regionale Radioprogramme durch Eigenproduktionen überlagern, blieb dies von offizieller Seite im Kosovo unerwähnt. Lediglich aus Belgrad wurde diese berichtet[18]. Statt solche »intelligenten« Mittel zur Ausschaltung von Medien zu nutzen, bombardierte die NATO das Sendezentrum des jugoslawischen Fernsehens und wurde dessen Satellitenübertragung ausgesetzt, was auch dem Letzten die Rolle der Medien als Instrument der Kriegsparteien verdeutlichte. Als Indiz für eine alliierte Überlegenheit waren diese Aktionen jedoch untauglich.

Fazit

Zusammenfassend lassen sich einige Widersprüchlichkeiten aufklären, andere neu festhalten.

Schon eine kurze Analyse der Information Warfare-Elemente im Kosovo-Krieg liefert ausreichend Hinweise darauf, daß dieser kaum vorbereitet und mangelhaft koordiniert wurde. Das U.S. Verteidigungsministerium bestätigte dies in seinem »After Action Review« vom Oktober 1999, in dem es heißt: »Die Bedeutung von Fähigkeiten [zu Information Warfare Operationen] wurde während der Operation Allied Force voll erkannt, aber die Durchführung einer integrierten Information Operations Kampagne wurde verzögert durch sowohl fehlende Vorausplanung als auch fehlende startegische Führung zur Definition von Schlüsselzielen.«[19] Dies verweist ein ums andere Mal auf die schweren Versäumnisse der politischen Konfliktprävention.

Für Information Warfare im engeren Sinne bedeutsam ist die Erkenntnis, daß der Kosovo-Krieg zwar den Versuch einer Integration von Elementen in die herkömmliche Kriegführung erkennen läßt, dies jedoch insofern wenig erfolgreich war, wie wesentliche Teile nicht als Information Warfare zu klassifizieren sind oder dem sogar prinzipiell zuwiderlaufen. Hinzu kommt, daß zum einen erstmals die NATO und die USA in einem ernsthaften Sinn Ziel von Information Warfare Operationen wurden, zum anderen ein Gegner Anhaltspunkte dafür liefern konnte, wie eine relativ erfolgreiche Reaktion auf Prinzipien von Information Warfare-Operatio-

nen aussehen könnte. Damit lassen sich einige der Widersprüchlichkeiten erklären. Dies müßte zusammengenommen aber die Auseinandersetzung um die Tragfähigkeit der Ideen und Konzepte von Information Warfare herausfordern. Solange sich eine solche öffentliche Debatte aber weitgehend auf Waffentechnik beschränkt, behalten die Experten recht, die diesen Krieg für zu klein halten, um daraus Lehren zu ziehen.

Vor allem zeigte auch der Kosovo-Krieg, daß sich die Faszination der Öffentlichkeit von High-Tech-Waffen unabhängig von deren Effektivität auch weiterhin dazu nutzen läßt, ein medial positiv konnotiertes Bild einer Kriegführung zu transportieren, das auch die Gegner nur auf derselben Ebene diskutieren und damit die Wirkung dieses Themas nur weiter verstärken. Diese Debatte entlastet von deutlich unangenehmeren Fragen.

1 Dies ist die aktualisierte Fassung eines Beitrages für Heft 3/99, 1999 der Zeitschrift »Wissenschaft und Frieden« des Informationsdienstes Wissenschaft und Frieden, Reuterstr. 44, 53113 Bonn.
2 insbes.: Elvi Claßen: Medienrealität im Kosovo-Krieg; in: telepolis, 30.10.99, http://www.heise.de/tp/deutsch/special/info/6508/1.html, vgl. auch: Bernd Röhrle: Im Namen der Menschenrechte. Zur psychologischen Kriegsführung; in: Wissenschaft und Frieden, Nr. 3/99, S.: 26-29
3 vgl. auch: Ute Bernhardt, Ingo Ruhmann: Der digitale Feldherrnhügel. Military Systems: Informationstechnik für Führung und Kontrolle. in: Wissenschaft und Frieden, Heft 1/97, Dossier Nr. 24, S. 1-16
4 A Pilot's Best Friend; in: AW&ST, 31.5.99,S. 25
5 Robert Wall: Airspace Control Challenges Allies; in: AW&ST, 26.4.99,S. 30-31, S.31
6 David Fulghum: NATO Unprepared for Electronic Combat; in: AW&ST, 10.5.99, S. 35-36
7 Electronic Atrophy; in: AW&ST, 7.6.99, S. 23
8 Robert Wall: E-2Cs Become Battle Managers With Reduce EW Role; in: AW&ST, 10.5.99, S. 38; ders.: New ABCCC Tactics Used in NATO Air Strikes; in: AW&ST, 26.4.99, S. 32
9 Paul Mann: Belgrad Called Victor in War's First Phase; in: AW&ST, 26.6.99, S. 28-30
10 John D. Morrocco: Kosovo Conflict Highlights Limits of Airpower and Capability Gaps; in: AW&ST, 17.5.99, S. 31-32
11 David Fulghum: Lessons Learned may be Flawed; in: AW&ST, 14.6.99, S. 64
12 NATO zerstörte in Serbien nur 246 Panzerfahrzeuge; in:; Süddeutsche Zeitung, 18.9.99, S. 6
13 »Bomben, nochmals Bomben«; in: Der Spiegel, Nr. 34, 1999, S. 134-135
14 David A. Fulghum: Electronic Bombs Darken Belgrade; in: AW&ST, 10.5.99, S, 35-36
15 David A. Fulghum: Microwave Weapons Await a Future War; in: AW&ST, 7.6.99, S, 30-31
16 »Die Front ist überall«; in: Der Spiegel, Nr. 37, 1999, S. 288-292; David A. Fulghum: Army Hakkers Go Airborne; in: AW&ST, 18.10.99, S. 37
17 So David A. Fulghum: Army Hackers Go Airborne; in: AW&ST, 18.10.99, S. 37
18 vgl Elvi Claßen, a.a.O.
19 U.S. Department of Defense: Joint Statement on the Kosovo After Action Review. No. 478-99, 14. Oktober, 1999, http://ww.defenselink.mil/news/Oct1999/b10141999_bt478-99.html

Karen Jaehrling

Die Bundeswehr-Kommission: Neuer Anlauf oder Staffellauf?

Die Zeit vor 10 Jahren bestimmt in diesen Wochen die Schlagzeilen. Damals begann auch für die Bundeswehr eine Zeit der Umorientierung. Dabei ging es zunächst um die deutliche Verkleinerung der Streitkräfte, denn, die nach den Umbrüchen in den Staaten des Warschauer Paktes wurden sie immer weniger für die Landesverteidigung gebraucht wurden. Dadurch stellt sich auch die Frage, ob die Wehrpflicht noch nötig sei. Beantwortet wurde sie mit sukzessiven Verkürzungen der Wehrpflichtdauer. Schon damals, aber erst recht heute sind diese Fragen Marginalien. An den großen militärpolitischen Entwicklungslinien gehen sie vorbei. Nicht Umfang und Form, sondern CharakterQualität der Streitkräfte sind entscheidend für die Marschrichtung en Charakter der deutschen Sicherheitspolitik. Die interessante Frage ist aktuell, wieviele Mittel bereit gestellt werden, um die Krisenreaktionskräfte (KRK), die schnell verfügbaren Kräfte zum Einsatz für weltweite Interventionen, personell und technisch mit dem nötigen Rüstzeug zu versorgen. Was mit den übrigen Streitkräften geschieht, ist höchstens insoweit interessant, wie sie als Aufwuchskräfte für die KRK , oder für gänzlich neue Aufgaben im Inneren der Republik , also für Aufgaben außerhalb ihres geleisteten Eides zur Landesverteidigung herangezogen werden.

Schon einmal, im Jahr 1990, wurde von der damaligen Regierung eine ExpertInnenKommission, die »Unabhängige Kommission für die künftigen Aufgaben der Bundeswehr« unter Vorsitz von Prof. HansAdolf Jacobsen, mit dem Auftrag eingesetzt, Aufgaben und Struktur der Bundeswehr nach dem Ende des Kalten Krieges einer Prüfung zu unterziehen. Im Mai diesen Jahres hat Verteidigungsminister Rudolf Scharping (SPD) die ExpertInnen Kommission »Gemeinsame Sicherheit und Zukunft der Bundeswehr« eingesetzt. In Presse und in politischen Kreisen hält sich hierfür hartnäckig die Bezeichnung »Wehrstrukturkommission«, in Anlehnung an eine frühere Kommission dieser Art und Vorsitz eines Sozialdemokraten . Bleibt es bei der Kontinuität im Titel, oder ist die Kommission auch in weiterer Hinsicht ein Überhang aus früheren Jahren? Wie unterscheiden sich Auftrag, Zusammensetzung und Einbindung der neuen Kommission vom ersten Anlauf der sog. JacobsenKommission, die militärischen Ziele und Strukturen angesichts der veränderten sicherheitspolitischen Lage zu überdenken? Auch an diesem Beispiel läßt sich untersuchen, inwieweit die neue Regierung von SPD und Bündnis 90/Die Grünen mit Traditionsbeständen in der Sicherheitspolitik bricht und eigene Akzente setzt, oder inwieweit sie im Gegenteil den Staffelstab von ihren VorLäufern übernimmt und konsequent zu Ende führt, was diese auf den Weg gebracht haben.

Um also die Frage zu beantworten, welche Ergebnisse und Impulse für die aktuell interessanten Fragen von der Kommission erwartet werden können, soll hier ein Blick darauf geworden werden, wie die Motive und Interessen der Auftraggeber die Arbeit der Kommission vorstrukturieren. Davon abgesehen – das sei an dieser Stelle deutlich gesagt – bleibt es eine interessante Frage, wie die Kommissionsmitglieder mit diesen Vorstrukturierungen umgehen. Eine Anwort hierauf wird erst nach Vorliegen des Abschlußberichtes im Frühjahr 2000 möglich sein. Die Indizien für die StaffellaufVariante sind allerdings übermächtig, und es dürfte für die Kommission schwer sein, sich dem zu entziehen.

Die Vorgeschichte: Warum eine Wehrstrukturkommission?

Die Forderung nach einer Wehrstrukturkommission zählt zum Traditionsbestand der SPDFraktion in ihrer Oppositionszeit. Seit 1989 beantragte sie wiederholt die Einsetzung einer solchen Kommission, zuletzt im Jahr 1998. Es scheint also, als sei die SPDFraktion den eigenen oppositionellen Zielen treu geblieben. Welchen Inhalten wird da die Treue gehalten? Was waren die Erwartungen und Ziele, die die SPDFraktion zu Oppositionszeiten mit einer solchen Kommission verband? Waren es immer dieselben Ziele? Im Jahr 1992 erhob die Fraktion ihre Forderung noch im gleichen Atemzug mit der Forderung nach einem System Kollektiver Sicherheit. Dies ist ein Bündnis, , also einem Bündnis, das auf gegenseitigen Gewaltverzicht seiner Mitgliedsländer untereinander und auf die gemeinsame Bekämpfung von Vertragsbrechern aus den eigenen Reihen im Inneren, und nicht auf Verteidigung oder sogar präventive Intervention gegenüber einem äußeren Feind gerichtet ist . Fünf Jahre später prägte hingegen das Interesse an der Entwicklung einer eigenständigen europäischen Verteidigungsidentität das Begehren der Fraktion : »Warum«, so fragte die Fraktion in ihrer Großen Anfrage zu ‚Lage und Zustand der Bundeswehr' »setzt die Bundesregierung keine unabhängige, gesellschaftsübergreifende Kommission ein, die Vorschläge zur Bundeswehrstruktur und zur gemeinsamen europäischen Verteidigung erarbeiten soll«. Die Begründung der SPD für ihren Antrag aus dem Jahr 1998 stellt hingegen auf das Problem der mangelnden Ausstattung der Bundeswehr für die Aufgaben der »Landesverteidigung im Bündnis« und der »internationalen Konfliktbeilegung« ab. Diesen und auch den übrigen Anträgen der Fraktion läßt sich entnehmen, daß die mangelnde Ausstattung der Bundeswehr für den Einsatz außerhalb des eigenen Territoriums zur Hauptsorge der Fraktion geworden war. Dissens hinsichtlich der allgemeinen sicherheitspolitischen Ziele der Bundesregierung und der NATO läßt sich den Anfragen hingegen kaum mehr entnehmen. Zweifel an den eigenen Zielen hat die SPD mit ihrer Schwerpunktkommission Außen und Sicherheitspolitik unter Vorsitz von Scharping ausgeräumt, die den Jahren der internen Differenzen und unbestimmten Positionen vor der Wahl ein Ende setzen sollte, und die 1997 ihr Ergebnis präsentierte. Wenn die SPDFraktion also ihre Forderung nach einer Wehrstrukturkommission aus der Opposition in die Regierung hinübergerettet hat, so ist sie nur der Form nach ihrer Politik n eigenen Zielen treu geblieben. Nur haben sich iIhre inhaltlichen Ziele haben sic bis spätestens 1997 so stark der Realpolitik der Alt-Bundesregierung angenähert, daß seitdem kaum noch erkennbar ist, wo sie Gesprächsbedarf in grundsätzlichen Fragen der Bundeswehrentwicklung besitzt. Beziehungsweise: sie Die SPD stilisiert Wehrpflicht und Streitkräfteumfang zu grundsätzlichen Fragen hoch. Bedeutet das, daß die Kommission für die SPD eigentlich überflüssig ist? Überflüssig und oder auch in anderer HinsichtForm nützlich, so jedenfalls die Vermutung des verteidigungspolitischen Sprechers der CDU/CSUFraktion, Paul Breuer. Er unterstellt, daß damit der SPD und koalitionsinterne Streit über die Militärpolitik ausgelagert werden solle. Unbenommen bleibt, daß Sicherlich ist die CDU/CSUFraktion als Opposition daran interessiert sein muß, den Eindruck der Zerstrittenheit und damit Regierungsunfähigkeit der Koalition zu erwecken. – dennoch muß dies nicht in jedem Fall falsch sein. In diesem Fall ist mindestens festzuhalten, daß eine Minderheit in der SPDFraktion sowie der kleine Koalitionspartner Bündnis 90/ Die Grünen tatsächlich Gesprächsbedarf hatte, und unterstützt hat, daß die Einsetzung einer Wehrstrukturkommission im Koalitionsvertrag verankert wird. Ob dies nun tatsächlich bedeutet, daß das Verteidigungsministerium die Zeit der Beratungen nutzt, um unbehindert von internen Diskussionen Fakten zu schaffen, bleibt zu prüfen.

Ein weiteresdrittes Motiv ist augenfälliger. Der Koalitionsvertrag sieht vor, daß vor Abschluß der Arbeit der Kommission »unbeschadet des allgemeinen Haushaltsvorbehalts keine Sach und Haushaltsentscheidungen getroffen werden, die die zu untersuchenden Bereiche wesentlich verändern oder neue Fakten schaffen«. Was sich wie ein Schutz gegen die oben angesprochene Gefahr liest, die Kommission könne von der Wirklichkeit überholt werden, war in Wirklichkeit einals Aufschub für weitere Hauhaltssenkungen im Verteidigungsbereich gedacht, den sich Verteidigungsminister Rudolf von Scharping vor seinem Amtsantritt ausbedungen hatte. War seine Hoffnung also zunächst, daß die Kommission einen Schutz vor Sparattacken des Bundesfinanzministers sein könnte, so richtete sie sich im Laufe der Beratungen für den Haushalt 2000 zusehends darauf, daß die Kommission, wenn sie ihn schon nicht kurzfristig vor Streichungen bewahren könne, mindestens Schützenhilfe für die langfristige Erhöhung des Verteidigungsetats geben würde . Dies wird auch als Grund für die Vorverlegung des Abschlußberichtes der Kommission um ein halbes Jahr, ins Frühjahr 2000, angenommen. Im Herbst 2000, ursprünglich vorgesehener Termin für den Abschlußbericht, wären die Haushaltsberatungen schon gelaufen.

Ist das Verteidigungsministerium also nun an konkreten Vorschlägen der Kommission zur Anpassung der Bundeswehrstrukturen an die Erfordernisse einer Interventionsarmee interessiert, oder sind Ministerium und SPDFraktion im Gegenteil desinteressiert bzw. bestenfalls als Zeitgewinn gegen Verkleinerungen des Bundeswehrhaushaltes und als Verlagerung interner Zwistigkeiten an der Kommission interessiert? Die Vorgeschichte legt nahe, daß dies die beiden Alternativen sind, zwischen denen sich die Haltung des Ministeriums bewegt. Der Zeitpunkt der Einsetzung, die Zusammensetzung und schließlich der Auftrag der neuen Kommission verraten hier mehr.

Die neue Kommission: Wer, Wann, Was?

Wer: Die Mitglieder der Kommission

Beim ersten Anlauf, der bereits erwähnten sog. ‚JacobsenKommission' aus dem Jahr 1990/1991, bildete die Gruppe von WissenschaftlerInnen mit Arbeitsschwerpunkt im Bereich Internationale Politik/Sicherheitspolitik die größte Gruppe. Die Gruppen ‚Politische Praxis' (Militär, Fachpolitiker) und ‚Gesellschaft' waren jeweils nur halb so groß . Beim zweiten Anlauf ist der Unterschied bereits an der Spitze sichtbar: In der neuen Kommission haben die Gruppen ‚Gesellschaft' und ‚Wissenschaft' die Plätze getauscht. Der Vorsitzende

der Kommission ist der ehemaliger Bundespräsident Richard Weizsäcker, während der alten Kommission mit Prof. HansAdolf Jacobsen ein Politikwissenschaftler vorsaß. Statt rund 10 WissenschaftlerInnen prägen nun 10 Personen des öffentlichen Lebens, also aus Kirche, Gewerkschaft, oder aus dem Bestand der ehemaligen politischen Amtsträger das Gruppenbild mit 3 Damen. Dies ist so gewollt: »Die Kommission«, heißt es in der Presseerklärung zur Einsetzung der Kommission, »ist in ihrer Gesamtheit keine Gruppe militärischer Experten, sondern ihre Mitglieder repräsentieren ein weites Spektrum politischer, wirtschaftlicher und gesellschaftlicher Bereiche, die in Beziehung zur Sicherheit unseres Landes stehen«. Eine Begrenzung auf ‚militärische Experten' ist sicherlich wenig wünschenswert. Zum einen wäre aber interessant, die Gründe dafür zu erfahren, daß man allein wissenschaftliche ‚militärische Experten' für entbehrlich hielt, um der Gruppe gesellschaftlicher RepräsentantInnen Platz zu machen, nicht aber bei der Gruppe der ‚militärischen Experten' aus der Praxis den Rotstift ansetzte. Dies ist ein zweiter und oftmals übersehener Charakterzug der Gruppe: Daß nicht nur mehr ‚Gesellschaft', sondern auch weniger ‚Wissenschaft' (bei gleichbleibend viel ‚Politischer Praxis') in der Kommission vertreten sind. Zum zweiten ist fraglich, warum bei der Ausweitung des Einzugsbereichs Menschen ausgewählt wurden, deren Bezug zur »Sicherheit hunseres Landes« bzw. zur allgemeinen Sicherheitspolitik zum Teil nicht allzu deutlich erkennbar ist. Vielstimmigkeit entsteht erst durch die Artikulation voneinander abweichender Positionen, und nicht durch das Gegenüber von ‚militärischen Experten' und Laien. Den Einbezug von ‚antimilitärischen' Gegenexperten, die sich aus kritischer Perspektive mit der Entwicklung der Bundeswehr auseinandersetzen, hat die koalitionsinterne Opposition aber offenbar nicht durchsetzen können oder wollen. Daß NichtExperten möglicherweise auch weniger ernst genommen werden, ist vielleicht ein unzeitgemäßer Verdacht. Die übrigen Indizien lassen allerding nicht vermuten, daß Mal sehen, ob die übrigen Indizien vermuten lassen, daß alle Mitglieder der Kommission so egalitär behandelt werden, wie die Presseeklärung verheißungsvoll suggeriert. Oder höchstens: Und: ob sie daß sie egalitär egal behandelt werdensind oder nicht.

Wann: Beratungszeitraum der Kommission und Zeitpolitik der Regierung

Die JacobsenKommission tagte im selbenparallel zu dem Zeitraum, in dem die neue NATOStrategie entwickelt wurde, welche fast zeitgleich zum Abschlußbericht der Kommission der Öffentlichkeit präsentiert wurde. Die JacobsenKommission hatte sozusagen die Wahl, aus dem zeitlichen Nebeneinander auch ein inhaltliches Nebeneinander zu machen, und eigene Schwerpunkte in der Arbeit zu setzen daß sie vom Ministerium ohnehin ignoriert werden würde, hatte sich von Beginn an abgezeichnet. Demgegenüber ist die neue Kommission in die zeitlichen Abläufe der neuen Regierung stärker eingebunden: Sie kam vergleichsweise zügig zustande, allerdings blieb immer noch Zeit genug, um im Ministerium eine sogenannte »Bestandsaufnahme der Bundeswehr« vorzubereiten, die zur Arbeitsgrundlage der Kommission erklärt wurde. Die bereits erwähnte Vorverlegung des Kommissionsberichtes auf Frühjahr 2000 zeugt ebenfalls von enger Anbindung und sogar noch gewachsenem Interesse des Verteidigungsministeriums an der Arbeit der Kommission. Allerdings nur, soweit sie ihm den gewünschten finanziellen Freiraum verschaffen. Auch über die Höhe des gewünschten Mittelzuwachses hat Scharping die Kommission nicht im Zweifel gelassen: Bereits in der Bestandsaufnahme ist die Zahl 5 Mrd. DM genannt. Für die Verwendung der Mittel ist hingegen der Generalinspekteur der Bundeswehr damit beauftragt, zum gleichen Zeitpunkt wie der Abschlußbericht der Kommission eine »konzeptionelle Bestimmung der künftigen Aufgabenpriorisierung« vorzulegen.

Daß der Verteidigungsminister auch ansonsten nicht gerade auf die Ergebnisse der Kommission wartet, zeigen die Entscheidungen, die bereits bis zum jetzigen Zeitpunkt im Beratungszeitraum gefallen sind: die Entscheidung, am KFOREinsatz als ‚Lead Nation' teilzunehmen, mit entsprechender Verpflichtung hinsichtlich der Anzahl der beteiligten deutschen Soldaten (8500); als Folge davon die Anordnung im Juni 1999, die Krisenreaktionskräfte des Heeres von 35 000 Soldaten um weitere 10 000 Soldaten aufzustocken, um diesen personalintensiven Einsatz überhaupt bewältigen zu können: »Die Truppe hat einen Anspruch darauf, daß angesichts der Tatsache, daß wir uns verpflichtet haben, aus guten außenpolitischen Gründen, denke ich, wegen unseres Gewichtes im Bündnis, wegen unserer Verantwortung in Europa, im Kosovo zum ersten Mal als sog. Lead Nation aufzutreten (...) daß die Auswirkungen innerhalb der Bundeswehr nicht nur erkannt, sondern auch sofort in Ordnung gebracht werden.«

Was hier sofort in Ordnung gebracht wird, ist allerdings keine Kleinigkeit und auch keine »notwendige Entscheidung«, welche sich der Minister vorbehielt, zwischenzeitlich zu treffen. Mit der ‚Lead Nation' – Entscheidung wurde aus freien Stücken ein neuer Akzent in der Sicherheitspolitik gesetzt, der die ‚Sicherheitsphilosophie' der alten Bundesregierung ihrer gerechten Vervollkommnung zuführt. Die Entscheidung ist von dem Wunsch getragen, das eigene militärische Gewicht im Bündnis zu erhöhen, um bei künftigen militärischen Operationen und anderen außen und sicherheitspolitischen Belangen größeren Einfluß zu erhalten. Ein Wunsch, den Scharping mit seinen übrigen sozialdemokratischen Kollegen in Europa teilt: Nach der USADominanz in der heißen Phase des KosovoKrieg richtet sich alles Begehren der europäischen Verteidigungseliten darauf, in Ausstattung und Ausbildung ihrer Streitkräfte dem großen Bruder nachzueifern, um diesem nicht noch einmal die Entscheidung überlassen zu müssen, welche Ziele zerbombt werden und welche nicht. Die aktuelle Suche nach der ‚europäischen Verteidigungsidentität' gestaltet sich bislang vor allem als neues Wettrüsten, um die eigene militärische und politische Macht gegenüber den Bündnispartner zu erhöhen, nicht als Bestimmung eigener sicherheitspolitischer Bedarfe und Ziele (s. auch den Beitrag von Peter Lock in diesem Heft?)

Was: Auftrag und Arbeitsgrundlage der Kommission

Den letzten Rest guten Glaubens nimmt ein Blick auf den Auftrag der Kommission. Die sogenannte »Bestandsaufnahme «, die diesen Auftrag konkretisiert, unterstreicht, daß die Kommission nicht nur zeitlich, sondern auch inhaltlich

nach Vorlage des jüngsten Strategischen Konzept der NATO arbeiten soll. Dies kündigt sich bereits in der Form an: Im Koalitionsvertrag war festgehalten worden, daß die Kommission »auf der Grundlage einer aktualisierten Bedrohungsanalyse« ihre Vorschläge zu Auftrag und Struktur der Bundeswehr erarbeiten soll. Als Arbeitsgrundlage erhielt sie stattdessen eine Bestandsaufnahme im Umfang von 180 Seiten, die in erster Linie die finanzielle Krise der Bundeswehr durchdefiniert: Heer, Marine, Logistik etc. Den Krisen außerhalb der Bundeswehr, also der eigentlichen Bedrohungsanalyse, ist genau 1 Seite gewidmet. Die Analyse übernimmt bis in einzelne Formulierungen hinein die Liste von diffusen Risiken aus den Verteidigunsgpolitischen Richtlinien (VPR) des Jahres 1992, aktualisiert um das Risiko eines Nuklearkriegs zwischen Indien und Pakistan bzw. um Risiken, die aus der Verbreitung von Massenvernichtungswaffen an weitere Staaten entstehen.

Selbst wenn man darüber hinwegsieht, daß keine noch so gelungene Umstrukturierung der Bundeswehr diesen nuklearen Risiken etwas entgegensetzen könnte (es sei denn, man dächte an die gewaltsame Verhinderung jeglicher Rüstungsexporte), ist dieser Teil der Bestandsaufnahme in jeder Hinsicht dünn. Und selbst wenn die 4000 Seiten, die nach Angabe des Ministers dieser Kurzfassung zugrunde liegen, dickere Teile dazu enthält, und diese sogar den Mitgliedern der Kommission zur Einsicht überlassen wurden – selbst dann sind Schwerpunktsetzung der Kurzfassung und die dünne Auflistung der Risiken Anhaltspunkte genug, um ihnen den Hauptauftrag der Kommission zu entnehmen. Erstens: Bedarf und Ziele oder Aufgaben der Bundeswehr liegen fest, hier geht es allein um die Mittel der deutschen Sicherheitspolitik. Zweitens: Das Mittel Bundeswehr und die Mittel für die Bundeswehr sind so zu optimieren, daß sie ein noch breiteres Spektrum an militärischen Handlungsoptionen eröffnen, als der Vordenker der Reform und Autor der VPR, Generalinspekteur Klaus Naumann, jemals zu träumen wagte.

Fazit: Begrenzt tauglich

Vorgeschichte, Zusammensetzung, Beratungszeitraum und Auftrag der Kommission lassen den Schluß zu, daß Verteidigungsministerium und SPDFraktion anfänglich der Kommission mit gemischten Gefühlen gegenüberstanden. Inzwischen hat sich , daß sich das eigentümliche Mischungsverhältnis zwischen Desinteresse und recht höchst eingegrenztem Interesse jedoch zur Mitte des Beratungszeitraums zum »InteressenPol« hin verschoben. hat, Dies ist allerdings verbunden mit einer weiteren inhaltlichen Eingrenzung: Gefragt sind insbesondere Bestätigungen des erhöhten Finanzbedarfs in den kommenden Jahren. Die Auftraggeber der neuen Kommission sind konsequenter als die der letzten. Sie nehmen selbst eine der Form nach unabhängige Kommission in die Pflicht, um dem von ihren Vorgängern angestoßenen Projekt der Interventionsarmee die letzten Hindernisse aus dem Weg zu räumen. Sowohl für den Umgang mit externer Beratung als auch für die Politikinhalte gilt: Der Traditionsbruch der neuen Regierung besteht lediglich darin, die restlichen Fesseln aus Konventionen und historisch begründeten Tabus abzustreifen, um musterschülerhaft den Geist ihrer Lehrer in die Tat umzusetzen.

Was heisst dies nun für die Experten-Kommission? Kann sie angesichts des angezogenen Tempos der Modernisierung überhaupt noch mitreden? Für eine Verlangsamung oder einen neuen Anlauf gar wären folgende Schritte nötig: Empfehlungen an eine Kommission

- Nehmen Sie den Minister beim Wort: »In der Auswahl der sicherheitspolitischen Beratungsfelder ist die Kommission frei« .
- Sie haben keine anständige Bedrohungsanalyse erhalten? Füllen Sie Lücken! Vor allem diejenigen, die vermutlich keine Analyse des Ministeriums jemals schließen wird: Beziehen Sie die Risiken des weltweiten Interventionismus ein. Kalkulieren Sie die Gefahren ein, die der ‚erweiterte Sicherheitsbegriff' mit sich bringt: Für ein Szenario, in dem sich Rußland und der Westen in einem Drittland gegenüberstehen, brauchen Sie nach Kosovo wieder nicht mehr viel Phantasie. Zeigen Sie, welche Folgeschäden die Sorglosigkeit des Westens gegenüber dem Einspruch anderer Großmächte nach sich zieht. Rechnen Sie die politischen und die menschlichen »Kollateralschäden« durch. Beispielaufgaben gibt es genug.
- Sie sollen über Mittel reden? Spielen Sie das Spiel: Es zählt zum Merkmal der deutschen Sicherheitspolitik, daß zwischen konkurrierenden Zielen nicht über den Weg der Auseinandersetzung, sondern über die Gestaltung der Mittel entschieden wird. Gestalten Sie die Bundeswehr zu einer reinen DefensivArmee um. Sie haben die Unterstützung prominenter Sozialdemokraten! Empfehlen Sie, daß freiwerdende Finanzmittel aus Streitkräftereduzierungen in den Sozialhaushalt umgeschichtet werden, nicht in die Aufrüstung der KRK. Die Mittel sind nicht absolut zu gering, sie sind es nur relativ zum Ziel, sich sämtliche Handlungsoptionen bei der Bekämpfung sämtlicher Risiken weltweit offenhalten zu wollen.
- Sie sollen »Optionen« aufzeigen? Das mag in anderen Politikbereichen sinnvoll sein. Handlungsoptionen im Verteidigungsbereich hingegen gehen generell mit Aufrüstungsmaßnahmen einher. Stellen Sie sich quer: Sagen Sie explizit, welcher Weg nicht eingeschlagen werden soll. Sie irren, wenn Sie annehmen, daß die Handlungslücken, die Sie nicht schließen, lange Zeit Lücken bleiben.
- Sie sollen frei auswählen? Machen Sie Vorschläge zur aktuellen Diskussion um eine europäische »Sicherheitsphilosophie«, die über die militärische Handlungsfreiheit der großen EUStaaten hinausweist. Internationalisierung von Politik bedeutet kein Denkverbot für Gremien auf nationaler Ebene.

Das ist naiv? Naiv war Ihre Vorgänger-Kommission, die nach ihrer selbstgewählten (!) Zurückhaltung hinsichtlich der neuen NATOStrategie und ihrer Konzentration auf die mittelfristige (nicht langfristige) Entwicklung der Bundeswehr den Staffelstab wie ein heißes Eisen an die Bundesregierung zurückgab, und hoffte, »daß der Kommissionsbericht zu einer neuen, sachlich geführten Diskussion und notwendig werdenden Entscheidungen über Fragen der Sicherheit und Landesverteidigung in Deutschland führt«.

Leonie Dreschler-Fischer

Projekt MIDAS:

Detektion von Landminenfeldern mittels Fernerkundung

Die Entdeckung und Räumung von Landminenfeldern ist eine drängende und gigantische Aufgabe, die mit den bisher eingesetzten Verfahren allein nicht bewältigt werden kann, wie Marc Hermann in seinem Beitrag dargestellt hat. Der Aufwand für die Herstellung und den Einsatz einer Mine ist um Größenordnungen geringer als die Kosten, der Zeitaufwand und das Risiko für ihre Beseitigung, so daß immer wieder neue Minenfelder entstehen, während noch Jahrzehnte alte Minenfelder aus vergangenen Bürgenkriegen auf ihre Räumung warten und mühsam und unter Lebensgefahr für die Räumtrupps wieder aufgespürt werden müssen.

Das Pilotprojekt des ITC

Im Projekt MIDAS (Mine Detection by Airborne Sensors) arbeiten wir daran, die Entdeckung von Minenfeldern und einzelnen Minen durch den Einsatz von Fernerkundungsverfahren zu beschleunigen und die Räumung der Felder weniger gefährlich zu machen. Die Partner in dem Projekt sind das International Institute for Aerospace Surveys and Earth Sciences ITC in Enschede (Leitung: J. L. van Genderen) sowie die Arbeitsgruppe CENSIS (Leitung Hartwig Spitzer) an der Universität Hamburg. Pilotprojekt für das Projekt war das EU-Projekt »Airborne Minefield Detection in Angola/Mozambique«, das von 14 Partnerinstituten unter der Leitung des ITC durchgeführt wurde und von der EU mit 10 Mio. Gulden gefördert wurde. Im Rahmen dieses Pilotprojektes entstanden Luftaufnahmen von vier verschiedenen Gebieten in Mozambique, die sich stark hinsichtlich des Klimas, der Vegetation und der Bodenverhältnisse unterscheiden. Insgesamt wurden mehr als 600 km 2 überflogen und aufgenommen. Für die Aufnahmen wurden sechs unterschiedliche Arten von Sensoren eingesetzt, um möglichst vielfältige Signaturen der Minen zu erhalten: Zwei optische Sensoren im sichtbaren und nahen Infrarot, zwei thermische Sensoren für das thermische Infrarot, zwei Sensoren im Mikrowellenbereich (P-Band und X-Band Radar). Zusätzlich zu den Minenfeldern in Mozambique wurde ein Blindversuch mit einem speziell für dieses Projekt eingerichtetem Testgelände in Belgien durchgeführt. Dieses Testfeld enthielt mehrere Minenfelder mit Antipersonen- und Antipanzerminen (Übungsatrappen), die es im Blindversuch aufzuspüren galt.

Die Ergebnisse dieses Pilotprojekts waren sehr ermutigend. Es konnte gezeigt werden,[1] daß mittels der Luftaufnahmen fast alle Minenfelder des belgischen Testgeländes anhand von Indikatoren von den erfahrenen Fotointerpretern des ITC gefunden werden konnten, und weiterhin, daß auch fast alle Minen sich in wenigstens einem der verwendeten Kanäle abzeichnen. An den Bildern aus Mozambique konnte nachgewiesen werden, daß. wichtige Indikatoren, die auf Minenfelder schließen lassen, wie Reste von militärischen Lagern, Befestigungen, Zäune, Markierungen von Pfaden durch vermintes Gebiet, ja selbst Zweige, die einzelne Minen anzeigen, sehr klar mit dem Stereoskop ausgemacht werden können. Das ITC hat einen ausführlichen Katalog von Indikatoren erarbeitet, die direkt oder indirekt auf Minenfelder hinweisen. Nachdem jetzt am ITC gezeigt wurde, daß Minenfelder und einzelne Minen mit Fernerkundungsmethoden aufgespürt werden können, stellt sich die Frage, ob und wie dieser Weg mit Methoden der Bildverarbeitung zu einem automatischen Verfahren weiterentwickelt werden kann.

Die Untersuchungen in Hamburg

In der Arbeitsgruppe CENSIS in Hamburg sind zwei Teams dabei, ein Verfahren zu entwickeln, um die Interpretation der Luftaufnahmen zu automatisieren. Eine Gruppe von Physikern unter der Leitung von Hartwig Spitzer widmet sich dem Problem, einzelne Minen anhand ihrer Signaturen zu entdecken. Wichtig sind dabei insbesondere die thermischen Kanäle, da sich in diesen Kanälen auch vergrabene Minen abzeichnen können. Da die Minen sehr klein sind, ist es notwendig, die Bilder sehr genau zu registrieren, damit eine gute Fusion der thermischen Kanäle mit den optischen Kanälen ermöglicht wird. Auch an die Kalibrierung der thermischen Sensoren müssen hohe Anforderungen gestellt werden, um den Tagesgang des thermischen Signals mit berücksichtigen zu können. Da die Ergebnisse unserer Kollegen in der Physik noch nicht veröffentlicht wurden, werde ich hier nicht näher auf dieses Teilprojekt eingehen.

In der Informatik haben wir die Teilaufgabe übernommen, die Wissensrepräsentation zur Erkennung von Minenfeldern zu formulieren. Hierbei ging es darum, das Expertenwissen zur Verwendung von Indikatoren für Minenfelder explizit zu machen. Unser Ziel dabei war einerseits, zu überprüfen, inwieweit der vom ITC vorgelegte Katalog an Indikatoren explizit gemacht wurde und ob sich unter Verwendung dieser Indikatoren auch wirklich alle entdekkten Minenfelder betätigen lassen. Andererseits war es natürlich das Ziel, die Klassifikation von Gebieten als potentielle Minengebiete zu automatisieren.

Für die Wissensrepräsentation wird davon ausgegangen, daß die nötigen geographischen Daten, wie Informationen über Geländeformen, Straßen, Ortschaften, Vegetation und Landnutzung schon in Form eines geografischen Informationssystems verfügbar sind und nicht erst von uns aus den Luftaufnahmen extrahiert werden müssen. Am ITC ist genau für solche Zwecke das Informationssystem »Minedemon« entwickelt worden. Weiterhin wird angenommen, daß. alle wichtigen Indikatoren (Umzäunungen, aufgegebene Gebäude, Oberleitungen, Fahrzeugspuren usw.) anhand der Luftaufnahmen erkannt und lokalisiert wurden. In diesem Punkt steht der Bildverarbeitung noch viel Arbeit bevor, um diese Vor-

aussetzung auch wirklich zu schaffen. Als Repräsentationssprache wurde die Beschreibungslogik CLASSIC gewählt, mit der wir schon für andere Expertensystemaufgaben sehr gute Erfahrungen gemacht haben.

Repräsentiert wurden vier unterschiedliche Kategorien von Hinweisen auf Minenfeldern:

- Militärisch-strategische Hinweise: Diese betreffen die Funktion eines Minenfeldes, nämlich einen Katalog der zu schützenden oder zu sperrenden Einrichtungen, wie Reste von militärischen Einrichtungen, wichtige zivile Gebäude, Versorgungseinrichtungen, Straßen, Brücken usw.
- Aufbau der Minenfelder: Diese Regeln beschreiben, wie sinnvollerweise ein Minenfeld einzurichten ist, damit die Minen nicht durch Erosion abgetragen werden, damit man nicht selbst durch die Minen behindert wird usw. Hierzu gehören auch typische Muster, wie Minen maschinell ausgelegt werden.
- Physikalische Regeln: Das sind Regeln, die beschreiben, wo sich Minen befinden können; beispielsweise, daß auf einem harten Felsenuntergrund keine vergrabenen Minen vorkommen können, auch nicht an steilen Hängen.
- Beobachtungen zur Landnutzung: Landflächen, die regelmäßig bestellt werden, enthalten sicher keine Minen, ebenso Pisten, auf denen man Fahrzeugspuren findet, aber Brachland inmitten guten Ackerbodens, das schon viele Jahre nicht mehr bearbeitet wurde, ist erklärungsbedürftig.

Unter systematischer Anwendung aller dieser Regeln ließen sich die vom ITC entdeckten Minenfelder automatisch bestätigen.

Zur Ambivalenz des Projekts

Wenn man sich kritisch anschaut, welche Expertise modelliert wurde, dann stellt man leicht fest, daß das Expertensystem im Kern ebenso ein Experte zum Einrichten von Minenfeldern ist wie ein Experte zur Entdeckung von Minenfeldern. Theoretisch ließe es sich also sehr leicht als Ratgeber zum Verlegen von Minen mißbrauchen. Allerdings handelt es sich hierbei um so elementares Wissen, daß die Gefahr, durch das MIDAS-System neue Minenfelder zu provozieren, vernachlässigbar ist. Eine aus unserer Sicht kritischere Gefahr ist aber, daß ein solches System als Ratgeber genommen werden könnte, um künftig Minenfelder so anzulegen, daß die Gefahr der Entdeckung durch MIDAS minimiert wird. Diese Gefahr ist real und unvermeidlich, wie bei allen Gegenwaffen. Allerdings ist das vorrangige Ziel von MIDAS, bei der Beseitigung der Millionen jetzt schon verlegten Minen zu helfen, und da kann sich ja niemand mehr auf die Erkennungsstrategie von MIDAS einstellen.

1 Genderen, J. L.van und Maathuis, B. H. P. (1988) »A European Pilot Project for the Detection of Landmines in Angola«, Proceedings, International Conference on Economic Realities of Demining, March, Washington USA, p. 28.

Marc Hermann

Eine Massenvernichtungswaffe in Zeitlupe

Eine kurze Einführung in die Landminenplage und die Versuche und Probleme, sie zu bekämpfen.

»Eine Landmine ist der perfekte Soldat: Schläft nie und verfehlt nie.« So beschrieb ein General der Roten Khmer die tückischen Waffen, die in den vergangenen 25 Jahren über eine Million Menschen getötet oder verstümmelt haben. Zwischen siebzig und hundert Millionen Landminen liegen in über sechzig Ländern dieser Erde, so schätzen UNO und Internationales Rotes Kreuz. Anti-Personen-Minen haben sehr geringe Herstellungskosten, rund drei US-Dollar pro Stück. Das macht diese tückischen Waffen besonders für Entwicklungsländer und Bürgerkriegsparteien attraktiv, aber auch die USA möchten nicht auf sie verzichten.

So hergestellt, daß sie eher verstümmeln als töten, soll mit den Minen Angst bei der gegnerischen Bevölkerung erzeugt werden und Kräfte für die

Minenräumer kurz vor ihrem Einsatz

Versorgung der Verletzten gebunden werden. Noch Jahre und Jahrzehnte nach Beendigung eines Krieges fordern sie Opfer – Opfer, die zum Teil noch nicht einmal geboren waren, als die Minen verlegt wurden. Ebenso langanhaltend sind die wirtschaftlichen und sozialen Auswirkungen der Landminenplage in den Entwicklungsländern: Die Furcht vor Minen läßt die Bevölkerung vor bewährten Handelsrouten zurückschrecken, die verstümmelten Opfer sind eine große Belastung für deren Familien, da sie nichts mehr zum Einkommen beitragen können.

Die Räumung der verminten Gebiete ist also eine wichtige Voraussetzung für den Wiederaufbau von Gesellschaft und Wirtschaft nach einem Krieg. Aber noch verläuft die Minenräumung – meistens von humanitären Organisationen durchgeführt – langsam und beschwerlich. Ungefähr 100.000 Landminen wurden beispielsweise im Jahr 1993 geräumt. Bei diesem Tempo würde die totale Räumung wenigstens 700 Jahre dauern. Da

Der Autor in einem geräumten Abschnitt des Minenfeldes in der felsigen Songo-Region in Mosambik. Minenräumfahrzeuge hätten hier keine Chance. Jeder weiße Pflock steht für eine gefundene Mine.

aber entgegen aller UN-Konventionen noch immer Minen ausgelegt werden (wie beispielsweise während des Krieges in der Kosovo-Region), wird das weltweite Räumen der Minen zur regelrechten Sisyphusarbeit.

Die drei Stufen der Minenräumung

Die Minenräumung wird in drei Stufen eingeteilt: allgemeine Inspektion, technische Inspektion und schließlich vervollständigende Inspektion und Räumung. Diese Phasen sind international weitestgehend standardisiert.

Während einer Inspektion der Stufe 1 wird zunächst jede Art sekundärer Information zusammengetragen, um herauszufinden, ob sich in einer bestimmten Region ein Minenfeld befindet. In der Regel reist ein kleines Team durch die Region oder das Land und befragt die Einheimischen. Das können ehemalige Soldaten sein, die sich noch an Minenfelder erinnern, Farmer, die den Verlust von Vieh durch Landminen beklagen, Ärzte in Krankenhäusern, die von Unfällen berichten und natürlich auch die Opfer selbst. Zusammen mit einer Angabe über die Verlässlichkeit der Information wird alles auf einer Karte zusammengefaßt.

Wurde ein Minenfeld ausgemacht, so müssen seine Grenzen so genau wie möglich lokalisiert werden. Dies geschieht bei der technischen Inspektion, in der zweiten Stufe also. Ebenfalls wird versucht, genauere Informationen über die Art der Minen herauszufinden. Das primäre Ziel dieser Phase ist, die eigentliche Minenräumung, den Gang ins Feld so einfach und sicher wie möglich zu machen und die in Frage kommende Fläche zu reduzieren.

Zuletzt also die Räumung. In dieser Phase müssen entweder Menschen ins Feld geschickt werden, die die Minen entschärfen oder räumen, oder bei geeignetem Terrain können gepanzerte Fahrzeuge die Minen zur Explosion bringen. Letztere Methode wird bei der humanitären, großflächigen Räumung selten angewandt und ist eher militärischer Natur. Über die Ergebnisse der vervollständigten Inspektion wird ein Report angefertigt, der bereits bestehenden Datenbanken zugefügt wird. Nach UN-Standards gilt eine Gebiet als geräumt, wenn von 1000 Minen höchstens vier übrig bleiben.

Die momentan gängige Methode der humanitären Minenräumung ist die Verwendung von Metalldetektoren oder der Einsatz von Sprengstoff-Spürhunden zum Finden der Minen. Die Räumung erfolgt durch speziell dafür trainiertes Personal per Hand. Die Minen werden in der Regel vorsichtig freigelegt, aus dem Feld getragen und kollektiv gesprengt.

Das große Problem, mit dem die Minenräumer bislang zu kämpfen haben, ist die unzureichende Eingrenzung des vermeintlichen Minenfeldes. Bis zu neunzig Prozent der abgesuchten Fläche gehört nicht einmal zum Minenfeld, wurde aber mit derselben Sorgfalt untersucht. Eine andere Schwierigkeit ist die Vielzahl verschiedener Minen, von denen nicht alle mit einer Suchmethode gefunden werden können. So gibt es Anti-Personen-Minen, die mit weniger als einem Gramm Metall auskommen. Ein Metalldetektor würde hier versagen und Spürhunde sind rar.

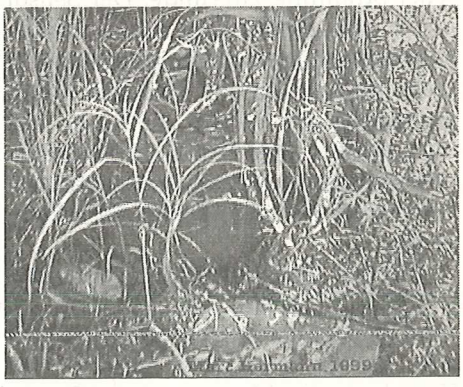
Forschungsgebiet Minen(feld)detektion

Weltweit wird an Methoden geforscht, mit denen Minenfelder oder einzelne Minen entdeckt werden können, um die Probleme zu beseitigen und die Minenräumung effektiver zu machen. Sie unterscheiden sich in den ihnen zugrunde liegenden physikalischen Methoden, in den verwendeten Algorithmen zur Datenanalyse (falls notwendig) und auch in der praktischen Durchführung. So verschieden sie sein mögen, kann man sie dennoch unter einigen einheitlichen, praxisnahen Kriterien bewerten.

Die von den Forschungsgruppen entwickelten Konzepte zur Minensuche müssen sich an drei wichtigen Kriterien messen lassen: Zuverlässigkeit, Sicherheit, Zeitaufwand. Die Kosten seien zunächst einmal außer Acht gelassen, auch wenn sie in der Praxis gewiß ein nicht unerheblicher begrenzender Faktor sind.

Das Kriterium der Zuverlässigkeit hat im allgemeinen den größten Stellenwert. Wie sehr kann man dem Ergebnis einer Suchmethode trauen? Zwei mögliche Fehleinschätzungen können auftreten: Entweder werden Minen angezeigt, wo gar keine sind (»false positives«) oder es wird kein Alarm ausgelöst und eine verminte Region wird als unvermint bewertet (»false negatives«). Letztere Fehler sind natürlich die gefährlicheren. Sie gefährden Menschenleben, während die erste Gruppe der Fehlalarme lediglich die Räumung verlängert. Das Maß der Zuverlässigkeit ist sowohl auf praktische Methoden im Felde wie auf Algorithmen anwendbar.

Die Sicherheit bei der praktischen Durchführung einer Detektionsmethode ist ebenfalls von besonderer Wichtigkeit. Hierfür muß geprüft werden, ob für die Minensuche Menschen in die Minenfelder müssen oder ob ferngesteuerte Fahrzeuge die Aufgaben übernehmen können. Möglicherweise reicht für die Detektion auch schon ein Überflug mit dem Flugzeug. Dieses Kriterium ist ebenfalls für eine spätere Minenräumung sehr wichtig.



Eine Anti-Gruppen-Mine im Gras.

Der dritte Maßstab für die Beurteilung einer Detektionsmethode ist der Zeitaufwand. Dies ist ebenfalls ein sehr praktischer Aspekt. Wieviel Fläche möglicherweise verminten Gebietes kann in einer bestimmten Zeit analysiert wer-

Ein mosambikanischer Minenräumer bereitet sich auf seinen Einsatz vor. Im Vordergrund sein Metallsuchgerät.

den? Kann die Analyse vor Ort geschehen, oder müssen die Daten aufwendig bearbeitet werden? Solche Faktoren müssen für eine Bewertung der Sicherheit einer Methode berücksichtigt werden.

Die Forschung nach dem – entsprechend den oben genannten Anforderungen – idealen Detektionsverfahren verfolgt verzweigte Wege. Grundsätzlich kann man die Verfahren danach unterscheiden, ob einzelne Minen ausgemacht werden oder großflächige Minenfelder eingegrenzt werden sollen. Die Zielsetzung wirkt sich auf die technische Umsetzung und praktische Durchführung aus.

Alle Konzepte benötigen aber zunächst eine Form der Datenaufnahme mittels Sensor. Der großen Mehrheit der Sensoren liegen die physikalischen Prinzipien des Nachweises elektromagnetischer Strahlung zugrunde. Der Sensor ist für einen bestimmten Ausschnitt des Spektrums empfindlich (oder auch für mehrere; dann spricht man von einem multispektralen Sensor). Und auch hier muß wieder zwischen zwei Verfahren unterschieden werden, nämlich zwischen passiven und aktiven Aufnahmegeräten.

Passive Sensorsysteme empfangen lediglich Strahlung, die entweder von den Objekten am Boden direkt ausgeht oder die als reflektierte Sonnen- und Umgebungsstrahlung zum Sensor gelangt. Ganz normale Fotokameras gehören zu den passiven Aufnahmegeräten, aber auch solche Sensoren, die im Infrarot- und Millimeterwellen-Bereich empfindlich sind.

In diese Gruppe fallen Thermalscanner, die die Wärmestrahlung aufzeichnen, die vom Erdboden ausgeht. Es ist zu erwarten, daß selbst vergrabene Minen sich in dieser Hinsicht von ihrer Umgebung unterscheiden.

Aktive Sensorsysteme hingegen senden selbst die Strahlung aus, für die sie empfindlich sind und messen, wieviel davon vom Erdboden zurückgeworfen wird. Dies ist zum Beispiel bei Radar- und Mikrowellensensoren der Fall. Bisweilen wird auch mit Sonardetektoren gesucht, also mit Hilfe von Ultraschall-Wellen. Momentan setzt die Forschung große Hoffnung auf in den Boden eindringende (»ground penetrating«) Radarstrahlung. Dabei wird ausgenutzt, daß die elektromagnetischen Wellen etwa eine halbe Wellenlänge tief unter die Oberfläche gehen. So könnten auch vergrabene Minen entdeckt werden. Der Nachteil: Große Eindringtiefen brauchen große Wellenlängen und damit geht eine Verringerung des Auflösungsvermögens einher.

Alle Sensoren haben gemein, daß sie auf irgendeine Weise über das vermeintliche Minenfeld bewegt werden müssen. Dabei gibt es nur zwei Möglichkeiten: am Boden oder in der Luft. Dabei liegen die Vorteile eines luftgestützten Minensuchsystems auf der Hand: Niemand wird gefährdet, und in kurzer Zeit kann man größere Landstriche abfliegen und überprüfen. Aber der Nachteil gegenüber den Sensoren in Bodennähe (bis ca. 10 Meter) ist, daß mit der zunehmenden Entfernung vom Boden das Auflösungsvermögen möglicherweise nicht ausreicht, um noch einzelne Minen zu erkennen.

Während sich Foto- und Videokameras, aber auch Scanner gut als luftgestützte Sensoren eignen, wird Radar in der Praxis eher von Fahrzeugen aus eingesetzt. In einigen Varianten können diese dann auch gleichzeitig zur Räumung eingesetzt werden. In letzter Zeit wird aber auch wieder über ein verbessertes handgetragenes System nachgedacht, das den herkömmlichen Metalldetektor ablösen soll.

Am Ende steht die Auswertung der Daten.

Bei der militärischen Minensuche muß eine Auswertung vor Ort und beinahe in Echtzeit erfolgen. Das ist momentan am ehesten durch eine optische Auswertung der Daten am Bildschirm möglich.

Der Vorteil der humanitären Minendetektion und -räumung ist, daß man sich bei Bedarf auch Zeit nehmen kann, um Konzepte zu verfeinern oder um neues Know-How einzubringen. Eine Analyse muß nicht immer direkt im Felde stattfinden, auch wenn dies das Ziel der Entwicklung sein sollte – was bei der Verwendung von handgetragenen Geräten und »Spürhund-Sensoren« im Moment ja auch der Fall ist.

Dennoch bleibt die Frage, ob und wie bei der Analyse Computer als Hilfsmittel herangezogen werden. Bei der bodengestützten Suche nach einzelnen Minen ist eine Auswertung mit Computerhilfe wünschenswert, da so durch ein schnelles Verfahren ein sofortiges Räumen der gefunden Minen ermöglicht wird. Und auch bei der großräumigen Suche nach Minenfeldern ist eine beschleunigte Auswertung ein Ziel.

Insgesamt steht die Forschung trotz einiger vielversprechender Ansätze immer noch am Anfang. Häufig wird der Fehler gemacht, daß die Konzepte ohne einen Bezug zur tatsächlichen Situation im Feld ist: fahrzeuggestützte Geräte funktionieren vielleicht in der Wüste, aber nicht in felsigen Gebirgsregionen, wie z.B. Kosovo. Feldeingrenzende Verfahren müssen ebenso in den Vordergrund rücken wie die Entwicklung handgehaltener Detektoren, die nicht nur auf Metall reagieren. In diesem Gebiet ist es besonders wichtig, daß die Forscher ein offeneres Ohr für die Wünsche der Anwender haben, damit die Landminenplage irgendwann ein Ende findet.

Ein von Pfosten markierter Pfad durch das Minenfeld bei Songo in Mosambik. Die Minenräumer müssen zuerst das Elefantengras vorsichtig roden. Stolperdrähte stellen eine weitere Gefahr dar.

Ingo Ruhmann

Die militärische Seite der KI[1]

Zu den in der Informatik umstrittenen Themen gehörte lange Zeit die Frage, in welchem Maße diese Disziplin allgemein mit militärischen Interessen in Verbindung zu bringen ist. Diese vor einer Dekade noch mit beachtenswerter Heftigkeit geführten Kontroverse2 hat seither an Schärfe verloren. Die veränderte politische Lage hat dieser Debatte einerseits ihre ideologische Dimension genommen. Die mit großem öffentlichkeitswirksamen Aufwand betriebene Demonstration militärisch genutzter Informationstechnik im Golfkrieg und die in dessen Folge unternommenen intensiven Bemühungen um eine weiter forcierte Nutzung dieser Technik bei Information Warfare und anderen Formen computergestützter Kriegsführung beendete andererseits ein Verleugnen von aus militärischen Nutzungszusammenhängen resultierenden Einflußfaktoren auf die Disziplin. Der Öffentlichkeit innerhalb und außerhalb der Fachdisziplin ist damit die militärische Bedeutung der Informatik in einem allgemeinen Sinne bewußt. Die Kenntnis um eine konkrete Nutzung und die Art von Bezügen zwischen dieser Nutzung von Informationstechnik und der Disziplin ist jedoch gering.

Verfügbare Informationen erhellen dieses Bild kaum. Einerseits macht der Einsatz von kommerziellen Standardprodukten wie etwa Office-Softwarepaketen das Militär zu wenig mehr als einem weiteren Anwender von Standardsoftware. Andererseits wenden militärische Forschungsförderungsinstitutionen substantielle Mittel auf, um an eindeutigen militärischen Nutzungsanforderungen orientierte Ergebnisse aus der Informatik zu erhalten. Über bestimmte Forschungsprojekte hinaus wurde bislang nur deutlich, daß eine Bewertung militärischer Relevanz von Forschungsarbeiten in der Informatik mit Problemen behaftet ist[3]. Auch für die KI als Teildisziplin ist diese Situation nicht anders. Im folgenden Beitrag soll es daher zunächst um einen Überblick über die Nutzung von Ergebnissen der KI für militärische Einsatzzusammenhänge sowie um eine Betrachtung der wichtigsten Fördermaßnahmen auf diesem Gebiet gehen, die durch einige Bemerkungen zur Beziehung von KI und militärischen Nutzungserfordernissen ergänzt wird. Einige der sich daraus ergebenden Fragen sollen zum Abschluß diskutiert werden.

Ausgehend von den geschichtlichen Wurzeln der Beziehung von KI und Militär werden die Ergebnisse der intensiven militärischen Förderung in den 80er Jahren betrachtet, um danach einen Überblick über die gegenwärtigen und zukünftigen Schwerpunkte in der KI-Förderung durch militärische Forschungseinrichtungen zu geben. Wie zu sehen sein wird, werden sich die Ausführungen vor allem auf Projekte in den USA konzentrieren und Arbeiten in der Bundesrepublik in den damit vorgegebenen Rahmen einordnen. Die verfügbare Materiallage erlaubt jedoch wegen der in der Bundesrepublik grundsätzlichen Zurückhaltung bei der Publizität von Ergebnissen aus militärischen Projekten für die allgemeine Öffentlichkeit keine systematische und umfassende Übersicht über militärische KI-Projekte in diesem Lande.

Zu den Wurzeln militärischen Interesses an der KI

Die Geschichte der KI konzentriert sich vornehmlich auf die Entwicklung grundlegender Ideen einiger herausragender Forscherpersönlichkeiten und auf einer allgemeineren Ebene um die bisweilen mit einigem Unterhaltungswert geführten Auseinandersetzungen zwischen Vertretern der »harten« und »weichen« KI[4]. Bei diesen Aufarbeitungen wird auf die mit der Entwicklung von KI-Methoden verbundenen Ziele eingegangen, aber allenfalls am Rande auf die Entstehungsbedingungen dieser Forschungsarbeiten. Auf welche Weise dabei auch von Beginn an militärische Interessen eine Rolle spielten und wie sich diese entwickelten, bleibt in aller Regel unbeachtet. Deshalb ist es hilfreich, auf diese Interessen und deren graduelle Entwicklung einzugehen.

Von Beginn an stellte sich die KI als ein Forschungsgebiet mit weit gesteckten Zielen dar. Ein derartiger Ansatz minderte die Bedeutung dieses Gebiets für kurzfristige produktbezogene Ergebnisse und ließ die KI vor allem als akademische Disziplin erscheinen, deren Ursprünge an wenigen Forschungsgruppen an US-Universitäten zu finden sind. Vor diesem Hintergrund ist daher bemerkenswert, in welchem Maß die KI nicht von ziviler Seite, sondern durch militärische Forschungsförderungs-Einrichtungen finanziert wurde.

Bekannt ist, daß die bis Mitte der 50er Jahre entwickelten ersten Computermodelle aus militärischen Mitteln finanziert wurden[5]. Doch auch die sich entwickelnde Fachdisziplin Informatik wurde intensiv mit Mitteln des Militärs gefördert. In den USA wurde die Förderung der Informatik hauptsächlich von fünf Organisationen geleistet – neben dem Department of Defense (DoD), das Department of Energy (DoE) und dessen Vorgänger Atomic Energy Commission, die NASA, die National Science Foundation (NSF) und das National Institute of Health (NIH). Im eigentlichen Sinne zivil waren davon bis Anfang der 60er Jahre nur die beiden letztgenannten. In der staatlichen Forschungsförderung stellte das DoD bis zum Ende der 80er Jahre mit Ausnahme dreier Jahre deutlich über 50% der Mittel[6]. Das DoD konzentrierte seinen Mitteleinsatz für die Forschungsförderung der Informatik in zunehmendem Maße auf die Advanced Research Projects Agency (ARPA, später Defense ARPA: DARPA), die lange Jahre in den USA die größte Einzelquelle für Forschungsmittel in der Informatik darstellte[7].

Wie auch andere Bereiche der Informatik in den USA konnte die KI in ihrer Anfangsphase auf die Förderung der ARPA zählen:

> *»Als noch keine Firma oder Stiftung AI erstnehmen wollte oder sich das*

leisten konnte, unterstützte die Advance Research Projects Agency (ARPA) des Verteidigungsministeriums sie durch zwei Jahrzehnte lebenswichtiger, oft sehr riskanter Forschung hindurch«[8].

Dies ist umso zutreffender, als IBM als anderer nennenswerter Förderer der KI das Interesse Ende der 60er Jahre verlor.

In der ARPA verantworteten Fachleute die Vergabe von Fördermitteln, die vordem selbst in Bereichen geforscht hatten, die sich zur Disziplin KI weiterentwickelt hatten oder aus denen grundlegende Impulse gekommen waren. Das im Bereich KI maßgebliche Information Processing Techniques Office (IPTO) der ARPA unter seinem seit 1962 amtierenden Leiter J. C. R. Licklider war hierfür ein prägnantes Beispiel. Licklider arbeitete im Zweiten Weltkrieg im Psycho-Acoustic Laboratory in Harvard an Fragen menschlichen Verhaltens in militärischen Kommunikations- und Kommandosystemen, die Experimentalpsychologie mit Ansätzen der Informationstheorie in Kontakt brachten und zu den Ausgangspunkten der Kognitionspsychologie gezählt wird. Licklider begann nach dem Krieg im Acoustics Laboratory am MIT, an dem zu dieser Zeit u.a. auch Wiener, Shannon, McCulloch, Pitts, Chomsky und Minsky arbeiteten. Licklider widmete sich dabei der Konstruktion der Benutzeroberfläche des militärischen Luftraumüberwachungssystems SAGE (Semi-Automated Ground Environment), eines der größten Computerprojekte dieser Zeit[9]. 1957 wechselte er dann zu BBN, um auch dort wieder an Problemen der Mensch-Maschine-Kommunikation zu arbeiten und wurde später einer von BBNs Vizepräsidenten. Nach seiner Ernennung zum Leiter des IPTO 1962 konzentrierte er sich auf die Unterstützung von Time-Sharing-Systemen, interactive computing und KI[10]. Neben dem MIT und Stanford wurden auch die sich bildenden KI-Forschungszentren bei RAND, Carnegie-Mellon, SRI, SDC, BBN nebst sieben weiteren »Centers of Excellence« substantiell gefördert. Auch bis zum Anfang der 80er Jahre ging der Anteil der Förderung dieser KI-Zentren durch die ARPA nicht unter 70% zurück[11], um dann in den 80er Jahren bis auf 90% anzusteigen. Vor dem Hintergrund von Lickliders Arbeiten an militärischen Kommunikationsproblemen und Verhalten von Bedienern komplexer technischer Systeme lassen sich seine Präferenzen bei der Förderung durch das IPTO als durchaus geradlinige Entwicklung sehen.

Zwar spielten schon in der Anfangsphase militärische Nutzungsvorstellungen eine deutliche Rolle, die sich vor allem auf Probleme der Mensch-Maschine-Kommunikation bezogen12. Bei der Förderung durch die ARPA ging es im Unterschied zu anderen Bereichen der *Informatik* aber zunächst weniger um Projekte mit direktem militärischen Nutzen, sondern vor allem um die Fortentwicklung der KI bei Interaktionstechniken wie Sprachverarbeitung und Fragen des Problemlösens. Viele der in derartigen Projekten gewonnenen grundlegenden Erkenntnisse waren bedeutsam für die Entwicklung vom Mehrbenutzersystemen und vor allem graphischer Benutzeroberflächen.

KI-Systeme für das Schlachtfeld

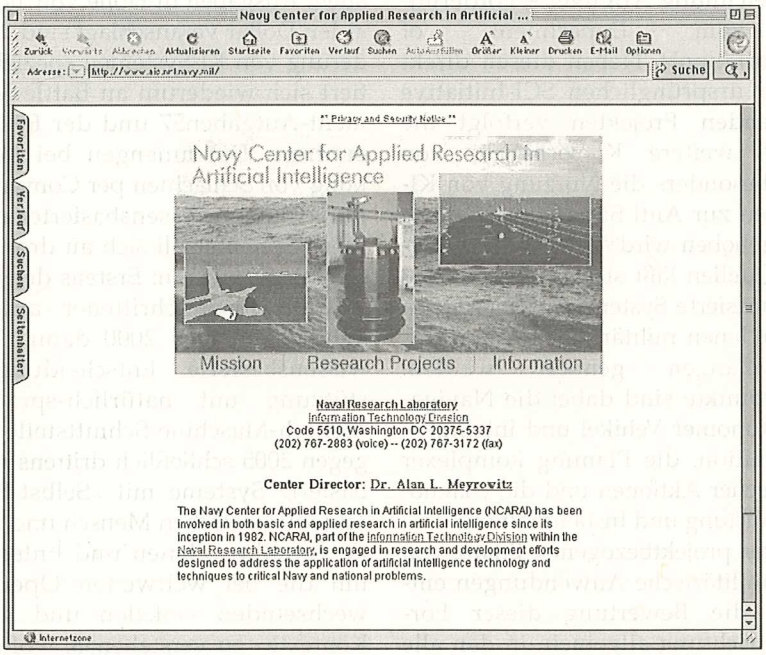
Die zunehmende Alltagstauglichkeit von KI-Systemen führte insbesondere seit den 80er Jahren auch zu konkretisierten Forschungs- und Entwicklungszielen für einem militärischen Einsatz. Die zweite Karriere der KI seit Anfang der 80er Jahre war keineswegs nur auf das gewachsene kommerzielle Interesse zurückzuführen, sondern eng mit dem Strategic Computing Programm der DARPA verbunden, das als Antwort der USA auf die »Japanische Herausforderung« durch deren Fifth Generation-Projekt konzipiert war[13].

Im Gegensatz zum japanischen Fifth Generation Project koppelte das Strategic Computing Programm weitgesteckte Forschungsvorhaben mit militärischen Nutzungszielen. Die 1983 ins Leben gerufene Strategic Computing Initiative (SCI) hatte als Forschungsziel die Entwicklung einer »completely new generation of machine intelligence technology«[14] binnen einer Dekade. Ausgehend von den Erfolgen bei Expertensystemen, Bild- und Sprachverarbeitung sollten anspruchsvolle militärische Anwendungsziele zu Fortschritten in der KI einerseits und über die dazu notwendige Rechenleistung in der Mikroelektronik andererseits führen[15]. Die KI-spezifischen Entwicklungsziele umfaßten »understanding natural language expressions, information fusion and machine learning, planing and reasoning« sowie »vision and visual image generation, speech recognition and production«[16]. Um die mit diesen Eigenschaften ausgestatteten Komponenten – sogenannte »intelligent subsystems« - in Anwendungssysteme zu integrieren, war ein weiteres Kernstück der Entwicklungsarbeiten die Kooperation verschiedener wissensbasierter Systeme.

Anders als frühere KI-Fördermaßnahmen der ARPA war das SCI-Programm auf die Anwendung neuer KI-Techniken nicht nur in allgemeinen militärischen Zusammenhängen, sondern explizit auf den Kampfeinsatz ausgerichtet, »to provide a major increase in defense capability in light of realistic scenarios of combat situations«[17]. Um – mit Ausnahme der U.S. Marines – alle Teilstreitkräfte mit Ergebnissen dieses Programms auszustatten, wurden drei Entwicklungsprojekte definiert: Autonome Vehikel, ein »Pilot´s Associate« und Battle Management-Systeme. Diese Projekte gliederten sich in verschiedenen Anwendungen auf. Dem Projekt Autonome Vehikel entsprangen sowohl das Autonomous Land Vehicle (ALV) als auch autonome Unterwasservehikel und Anwendungen für Cruise Missiles[18]. Battle-Management-Systeme entstanden sowohl – mit dem AirLand-Battle Management-System – für die Armee[19] als auch – mit dem Fleet Command Center Battle Management System der Pazifikflotte – für die Navy[20]. Hinzu kam im Projektverlauf auch ein Programm zur Entwicklung von »Smart Weapons«[21] und ein System zur Radarbildauswertung (Advanced Digital Radar Imagery Exploitation System, ADRIES)[22]. Aus allen Projekten reiften Prototypen heran, die von den beteiligten Teilstreitkräften erprobt wurden.

Die Ergebnisse dieses militärischen Interesses an wissensbasierten Systemen in den 80er Jahren sind durchaus beachtlich, wie sich an der – bedenkt man die oftmals nicht für die Öffentlichkeit bestimmten Einsatzzwecke – überraschend umfangreichen Literatur zu derartigen Systemen nachweisen läßt. Zunächst lassen sich dazu die von der DARPA selbst benannten Entwicklungserfolge anzuführen. So entstanden aus SCI-Projekten heraus die Entwicklungsumgebung KEE und deren Erweiterungen RUM (Reasoning Uncertainty Management) und ABE (A Better Environment)[23]. Zusätzlich bemerkenswert ist die Vielzahl der entwickelten wissensbasierten Systeme. Obwohl eine auf

nichtgeheime Systeme beschränkte Übersicht[24] nur ein im Einsatz befindliches militärisches XPS zur Optimierung von Luftfrachttransporten nennt, lassen sich in der Literatur eine Vielzahl weiterer wissensbasierter Systeme für militärische Anwendungen finden. Wenn



diese Übersicht auch unvollständig bleiben muß, so lassen sich daran jedoch die Schwerpunkte bei Entwicklungszielen und –erfolgen ablesen.

Analog zu zivilen Expertensystemen entstanden Diagnosesysteme für die Fehlersuche und Reparatur bei militärischen Systemen. Bei dieser Anwendung als militärspezifisch gesehen wurde der Umstand, daß in bewaffneten Konfliktsituationen viele Fehler an militärischem Gerät nicht vorhergesehen werden können[25]. Derartige Diagnosesysteme werden mittlerweile von der U.S. Army zur Wartung von Hubschraubern eingesetzt[26].

Einen weiteren Schwerpunkt stellte die Klassifikation und Analyse von Signaldaten dar. Hier zu nennen ist das aus dem SCI-Programm erwachsene XPS ADRIES zur Analyse von Radardaten in Kombination mit Daten aus anderen Quellen[27] sowie M2, ein XPS zur Prüfung von datenbasierten Hypothesen zur Aufklärungs eines Gegners und Generierung von Aussagen über diesen durch die Anwendung von Machine Learning-Verfahren[28]. Auch Unternehmen wie Martin Marietta und Hughes engagierten sich in diesem Bereich[29].

Neben der Sprachverarbeitung[30] spielten vor allem Schlachtfeld-Management-Systeme eine bedeutende Rolle. Als erfolgreich galt hierbei das XPS Battle zur Zuweisung von Waffensystemen zu Zielen, das die Bearbeitungszeit durch heuristische Suche stark reduziert. Zu den Zielen des Systems soll eine Beschreibung[31] genügen:

> *»The goal of the system is to maximise the destruction (total value D) for all targets. In an allocation plan, the destruction value for a target is the product of the target´s strategic value and the expected percentage of the target that will be destroyed in the plan. When the destruction value is maximised, the plan is considered optimal«.*

Zum Erfahrungsaustausch bei der Entwicklung derartiger Systeme und den dabei auftretenden Problemen gab es auch größere Workshops über KI-Systeme für Battle Management-Aufgaben[32], wo verschiedene weitere XPS zur Planung von militärischen Operationen (OPLANNER) und Signalanalyse (HASP-SIAP, ANALYST, AMUIDS)[33] vorgestellt wurden. Für konkrete militärische Operationen wurde das XPS ADS zum Management von militärischen Operationen nach der AirLand-Battle-Doktrin[34] und der ebenfalls aus dem SCI-Programm heraus entwickelte Prototyp ALBM (AirLand-Battle Management)[35] vorgestellt. Als ein wichtiger Forschungsbereich wurde dabei das deep modelling von Schlachtfeldern identifiziert. Auch das für militärische Aufgaben wichtige Umgehen mit Unsicherheit und Sprachverstehen wurden als Probleme genannt, die jedoch bis 1997 kaum lösbar seien. Zur Lösung der Probleme wurde die Entwicklung kooperierender XPS gefordert, von denen Grundkonzepte z.B. in dem MITRE-System ALLIES erforscht wurden[36].

Diese Kooperation verschiedener Teilsysteme aus Bildverstehen, Navigation und Planungskomponenten ist eine Voraussetzung zur Realisation von autonomen Systemen, ein Kernbereich militärischer KI-Anwendungen. Alle Teilstreitkräfte verfolgten eigene Vorhaben, die bislang unterschiedliche Reifegrade erreichten. Bereits Mitte der 80er Jahre fanden Experimente mit verschiedenen autonomen bodengestützten Robotern, Unterwasserfahrzeugen und Hubschraubern statt[37], die dabei gewonnenen Erkenntnisse wurden in Piloten-Unterstützungssystemen genutzt.

Auch in der Bundesrepublik wurden in dieser Zeit Expertensysteme zur Sensorauswertung und Unterstützung von Führungsaufgaben entwickelt. Zu nennen sind unter anderem das Experimentalsystem zur Führung von Waffensystemen Battleman von Siemens[38], das System TISFASS der IABG zur Data Fusion[39] oder das APK (Akustische Passiv-Klassifizierung) von Atlas Elektronik für Sonarsensor-Auswertung[40] auf U-Booten. Gegenstücke finden sich bei der Bundeswehr auch für andere der genannten Anwendungsgebiete wie Materialerhaltung und Fehleranalyse – so die XPS GEPARD und Proctor[41] – oder die Signalverarbeitung – wie bei MSON (Multisensorielle Objekterkennung in natürlichen Szenen), ein Kooperationsprojekt von MBB, Hochschule der Bundeswehr, der TU München, und der FhG[42].

Von fachlicher Seite fehlte es nicht an frühen Warnungen vor den sich in hochgesteckten Entwickungs-Meilensteinen der jeweiligen Projekte niederschlagenden allzu optimistischen Erwartungen[43]. Heftigere Kritik entzündete sich am Umfang konkreter militärischer Anwendungen der KI und deren Gefährdung von Menschenleben auch hierzulande[44]. Diese Auseinandersetzungen verebbten, als dem Statusbericht der DARPA nach vier Jahren[45] und den damit verbundenen Meilensteinen keine weiteren Berichte folgten. Trotzdem das ursprüngliche SCI-Programm damit letztlich vor seiner geplanten Zeitspanne auslief, wurden die meisten einzel-

nen Projekte weiterhin verfolgt. Gegenwärtig lassen sich daher die durch SCI angestoßenen Entwicklungen in der KI in verschiedenen Anwendungszusammenhängen wiederfinden.

Ergebnisse der Förderung

Auch heute verfolgt die US-Regierung eine Accelerated Strategic Computing Initiative. Verantwortlich dafür ist jedoch nicht die DARPA, sondern des U.S Department of Energy (DoE). Im Mittelpunkt dieser Initiative steht das dem DoE unterstehende Nuklearwaffenprogramm, für das eine Milliarde Dollar über fünf Jahre zur Entwicklung leistungsfähigerer Supercomputer bereitgestellt werden, um in Computersimulationen die Einsatzfähigkeit der Atomwaffen zu untersuchen, vor allem aber die Weiterentwicklung dieser Waffen trotz Teststopps zu ermöglichen[46].

Dennoch sind die mit der ursprünglichen SCI-Initiative verfolgten Projekte nicht ohne Resultate geblieben. Auch in den 90er Jahren unterstützt die DARPA weiterhin die KI in substantiellem Umfang[47]. Wissensbasierte Systeme werden in vielfacher Weise militärisch genutzt. Typisch dabei ist die Integration von KI-Techniken in herkömmliche große Softwareprojekte wie bei dem im Golfkrieg genutzten System zur Planung großer Truppenbewegungen DART (Dynamic Analysis and Replanning)[48]. Die frühesten Erfolge des SCI-Programmes lassen sich bei der Zielerkennung und Interpretation von Radardaten etwa im System ADRIES ausmachen. Auch hierbei wurden die mit derartigen Systemen gemachten Erfahrungen genutzt, um ähnliche Komponenten in verschiedene militärische Signalanalysesysteme zu integrieren. Als Erfolg gewertet wird von der DARPA auch der Pilot's Associate, dessen Prototyp schon 1991 erprobt wurde[49]. Wesentliche Leistungsmerkmale dieses Systems finden sich im Avionik-System des neuen Kampfflugzeugs F-22 wieder.

Ebenfalls erfolgreich war die Arbeit an wissensbasierten Navigationssystemen für autonome Unmanned Undersea Vehicles, von denen zwei verschiedene Prototypen entwickelt wurden[50]. Weniger erfolgreich war dagegen der Versuch, ein autonomes Landvehikel (ALV) zu entwickeln. Nachdem der seit 1985 entwickelte ALV-Prototyp auch nach Jahren nur mit geringer Geschwindigkeit auf den Straßen des Campus navigieren konnte, stellte die DARPA die Förderung 1989 ein[51]. Die Arbeit an ALV ging jedoch weiter und führte zu einer mittlerweile verbesserten Version. Das Projekt sucht nun – unter der Projektbezeichnung ALVINN – Förderhilfen vom Department of Transportation[52]. Neben diesen direkt aus der ursprünglichen SCI-Initiative stammenden Projekten verfolgt die DARPA weitere KI-Vorhaben, von denen besonders die Nutzung von KI-Systemen zur Anti Submarine Warfare hervorgehoben wird[53]. Aus den verfügbaren Quellen läßt sich festhalten, daß wissensbasierte Systeme mittlerweile in verschiedenen militärischen Einsatzzusammenhängen genutzt werden. Schwerpunkte sind dabei die Navigation autonomer Vehikel und intelligenter Munition, die Planung komplexer militärischer Aktionen und die Diagnose bei Wartung und Instandhaltung.

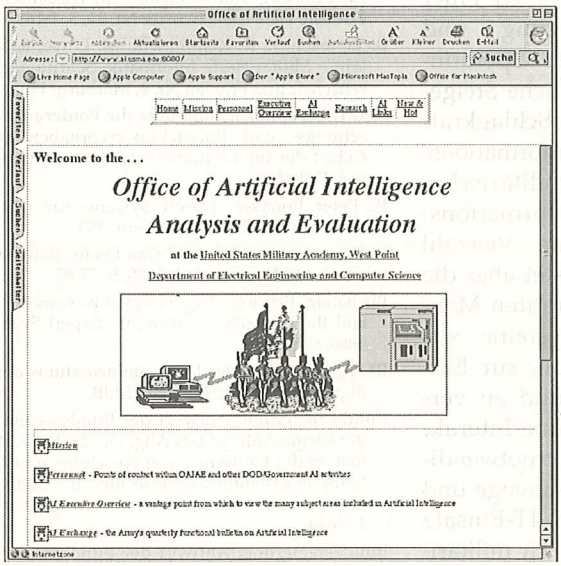
Dieser projektbezogenen Bilanz von KI für militärische Anwendungen entspricht die Bewertung dieser Forschungsrichtung allgemein in den alle zwei Jahre neu vorgelegten Dokumenten zur Forschungs- und Technologiepolitik des DoD. Die schon 1991 als militärisch bedeutsame Technologie bewertete KI wurde mit dem Ziel verfolgt, die in der Strategic Computing Initiative angelegten Schwerpunkte weiter auszubauen. Diese Forschungsziele umfaßten Bildverstehen, Autonomes Planen, Navigation, Sprach- und Textverarbeitung, Machine Learning, Wissensrepräsentation und –akquisition, Adaptive Manipulation und Kontrolle[54]. Ein Jahr später ließen sich im Grundlagenpapier des DoD zur militärischen Forschung und Entwicklung auch Weiterentwicklungen der schon in SCI angelegten Ziele erkennen – der Pilot's Associate wurde zum Crewman's Associate für Panzerbesatzungen erweitert, das autonome Landvehikel zum »Robotic Sentry«, einem autonomen Roboter-Wachposten, allein die Forschungsvorhaben zu Smart Weapons und semiautomatischer Signalverarbeitung firmierten unter ihren gewohnten Bezeichnungen[55].

Aktuelle Forschungsförderung

Aus den Erfahrungen des Golfkriegs entwickelte das DoD mit dem 1994 erschienenen Defense Science and Technology Plan56 eine umfassende Forschungsagenda der militärischen FuE-Projekte bis zum Jahr 2005. Von den darin benannten 19 Technologien gehören 12 zur Informatik, für die bis 1999 allein Ausgaben in Höhe von 14,5 Milliarden Dollar veranschlagt sind. Die Förderung von KI-Systemen speziell orientiert sich wiederum an Battle-Management-Aufgaben57 und der Fusion der enormen Datenmengen bei der Lenkung von Schlachten per Computer. Die Entwicklung wissensbasierter militärischer Systeme soll sich an drei Meilensteinen orientieren: Erstens der Demonstration fortgeschrittener autonomer Vehikel, im Jahr 2000 dann zweitens wissensbasierte Entscheidungsunterstützung mit natürlich-sprachlicher Mensch-Maschine-Schnittstelle und gegen 2005 schließlich drittens wissensbasierte Systeme mit »Selbst-Bewußtsein« für zwischen Mensch und Maschine verteiltes Planen und Entscheiden, um die bei weltweiten Operationen wechselnden »lokalen und globalen Kontexte« zu verstehen58, wofür allein bis 1999 233,2 Mio US-$ zur Verfügung stehen. Zweiter Schwerpunkt ist die Entscheidungsunterstützung durch intelligente, adaptive Mensch-Maschine-Schnittstellen und »crew associates« für Waffensysteme aller Teilstreitkräfte (Fördervolumen bis 1999: 456 Mio US-$)59 und die Unterstützung von Militärs mit wissensbasierten Unterstützungssystemen »to operate well beyond their normal mental and physical capabilities«60, wofür weitere 85 Mio US-$ zur Verfügung stehen. Hinzu kommt der Einsatz der KI in speziellen Anwendungsfeldern wie der Wettervorhersage, bei autonomen Waffensystemen und intelligenten Minen. Insgesamt fördert damit das DoD KI-Vorhaben von 1994-1999 mit deutlich über einer halben Milliarde Dollar. Das Niveau der Förderung liegt trotzdem unter dem Spitzenwert in den 80er Jahren, in denen das DoD allein im Jahr 1988 KI-Vorhaben im Umfang von 201 Mill. US-$ förderte61.

Ein beachtlicher Teil der Projekte mit längerfristigen Nutzungsabsichten wird weiterhin von der ARPA gefördert. Im ihrem laufenden Etat ist die Förderung von KI-Vorhaben auf verschiedene Projektbereiche aufgeteilt und damit nicht mehr in einer Weise koordiniert wie in den 80er Jahren. Die Arbeit etwa an autonomen Vehikeln findet heute in den

Projektbereichen »Unmanned Undersea Vehicle Systems«, »Guidance Technology« und »Advanced Land Systems Technology« statt. Unterschiedliche Arbeiten zu Battle-Management-Systemen finden sich ebenfalls im Bereich »Advanced Land Systems Technology«,



»Integrated Command & Control Technology«, aber auch im Bereich »Intelligent Systems & Software«, an dem speziell sich die Entwicklungsperspektiven der ARPA im Bereich KI am besten ablesen lassen. Die größten KI-bezogenen Forschungsprogramme bilden in diesem Bereich Arbeiten zur Mensch-Maschine-Interaktion und zu »Human Language Systems«. Dabei wird im Bereich Sprachverarbeitung auch weiterhin an der Verarbeitung und Generierung menschlicher Sprache gearbeitet, zusätzlich aber auch an der automatischen Übersetzung mit Hilfe militärischer Domain-Modelle, um die Kooperation in verschiedensten militärischen Allianzen zu unterstützen[62]. Auch der »Human Computer Interaction«-Bereich fördert Arbeiten zur Spracherkennung, darüber hinaus aber vor allem wissensbasierte multimediale Darstellungstechniken, bei denen an »Battlefield Intelligent Agents« ebenso geforscht wird wie an multimodaler Interaktion oder immersiven Virtual-Reality-Darstellungsformen realer und abstrakter Datenräume[63]. Gemeinsames Ziel aller Arbeiten ist die Reduktion der durch das explosive Wachstum an genutzten Informationsquellen gestiegenen Arbeitsbelastung von Militärs in unterschiedlichen Einsatzsituationen.

Obwohl die Arbeit an diesen weiterführenden Forschungsvorhaben auch derzeit an zivilen Forschungseinrichtungen geleistet wird, verfügt das U.S.-Militär seit den 80er Jahren auch über KI-Laboratorien der Teilstreitkräfte für spezifische bzw. nichtöffentliche Forschungsarbeiten. Die U.S. Navy nutzt seit 1982 ihr Navy Center for Applied Research in Artificial Intelligence[64], das sich derzeit neben Machine Learning und Reasoning vor allem mit Mensch-Maschine-Kommunikation befaßt. Das Air Force Institute of Technology Artificial Intelligence Laboratory[65] konzentriert sich auf den Einsatz von Fuzzy Logic in XPS und als Kopiloten-Prototyp sowie auf intelligente Interfaces. Herausragendes Projekt des 1984 gegründeten US Army AI Center[66] ist zur Zeit das Projekt Blacksmith zur wissensbasierten Entscheidungsunterstützung. Diesem Ziel widmet sich auch die Knowledge Engineering Group des US Army War College[67], die ihre Studenten systematisch in der Nutzung von wissensbasierten Unterstützungssystemen – von wissensbasierten Systemen für den Truppenaufmarsch und die Entscheidungsunterstützung allgemein über die Frequenzplanung und Minensuche bis zur Überwachung des Chemiewaffenprotokolls – unterweist. Stärker an Forschungsarbeiten ausgerichtet ist das Office of Artificial Intelligence der Militärakademie West Point[68].

Auch in der Bundesrepublik wird weiterhin an wissensbasierten Systemen auch für militärische Anwendungen geforscht, allerdings auf wesentlich geringem Niveau als in den USA:

> *»Mit dem derzeit geförderten Schwerpunkt »Intelligente Systeme« will das BMBF u. a. einen Beitrag zur Entwicklung teilautonomer, miteinander koppelbarer intelligenter Komponenten mit vielseitigen Anwendungsmöglichkeiten in der Robotertechnik leisten. Wichtige perspektivische Anwendungen sind z. B. Roboter mit Servicefunktionen in wenig attraktiven oder gefährlichen Arbeitsbereichen (...). Vom Bundesministerium der Verteidigung (BMVg) geförderte Forschungsarbeiten zu militärischen Roboteranwendungen zielen vor allem auf den Schutz des Soldaten bei gefährlichen Einsätzen und bei Übermüdungsgefahr. Hier gelten für autonome Systeme wegen ihres Einsatzes in nicht-kooperativen Umgebungen besonders hohe Anforderungen.«*[69].

Insgesamt gibt das Verteidigungsministerium hier laut Angaben der Bundesregierung jedoch nur etwa 56 Mill. Mark pro Jahr für Forschung und Entwicklung in der Informationstechnik aus – der Anteil für KI ist unbekannt. Spezifischer sind die dazu noch hinzukommenden 1,2 Mill. im europäischen Rahmen »in Teilbereichen der Informationstechnik wie Mikroelektronik, Künstliche Intelligenz«[70]. Im Gegensatz zu den USA gibt es jedoch in der Bundesrepublik so gut wie keine detaillierteren Informationen zu militärischen Forschungs- und Entwicklungsprojekten. Aussagen zu entsprechenden Vorhaben hierzulande sind daher ausgesprochen lückenhaft. Das Forschungs- und Entwicklungsprogramm des Verteidigungsministeriums ist eine Verschlußsache. Derartige Intransparenz ist sachlich nur bedingt nachvollziehbar und führt insbesondere dazu, daß dem BMVg unterstellt wird, es hätte bei seinen Fördermaßnahmen etwas zu verbergen.

Den Gegensatz zur Praxis in den USA verdeutlicht das Vorgehen des Bundesamts für Wehrtechnik und Beschaffung (BWB) bei dessen Kooperation mit dem Forschungsbereich Deduktions- und Multiagentensysteme des DFKI. So verlangte das Amt einerseits deutlich bemerkbare und in zivilen Projekten ungewöhnliche bauliche Schutzmaßnahmen gegen elektromagnetische Abstrahlung, auf der anderen Seite aber strikte Geheimhaltung über Kooperationspartner, Zweck und Umfang des Projekts. Das bei derartigen Auflagen beinahe zwangsläufige Rätseln um den Auftraggeber und dessen Ziele erhellte unter diesen Auflagen nicht das DFKI, sondern eine Antwort der Saarbrücker Landesregierung auf eine entsprechende parlamentarische Anfrage[71] und Auskünfte des Verteidigungsministeriums. Nach der Antwort des BMVg[72] geht es bei dem Projekt um Definition und Entwicklung einer vertrauenswürdigen Schnittstellenkomponente, mit der

Systeme gegen unerlaubte Manipulationen abgeschirmt und eine Möglichkeit zur Zugriffskontrolle von Datenbanken gefunden werden soll. Beschreibung und Hauptauftragnehmer entsprechend, dürfte es also um die sichere und zuverlässige Entwicklung anwendungsspezifischer Firewall-Technologie gehen.

Militärischer Nutzen der KI

Diese Übersicht über die militärische Förderung der KI zeigt ein seit Beginn dieser Disziplin ungebrochenes Interesse von Militärs in den USA an spezifischen Ergebnissen und deren Willen, zur Erreichung dieser Wünsche in vergleichsweise großem Umfang Fördermittel zur Verfügung zu stellen. Weiterhin erklärt das DoD seinen Glauben an sichere und zuverlässige wissensbasierte Systeme[73]. Diese Interessen sind nicht allein auf die USA beschränkt, sondern lassen sich auch in der Bundesrepublik ausmachen, wenn hier auch der Gesamtrahmen der entsprechenden Forschungsarbeiten deutlich geringer ist.

Wie auch im zivilen Einsatz ist zu beobachten, daß wissensbasierte Systeme im militärischen Kontext lediglich als Komponenten in größeren IT-Systemen eingesetzt werden, für die deren Funktionen allerdings von besonderer Bedeutung gehalten werden. Bemerkenswert ist dabei ein wesentliches Maß an seit dieser Zeit unverändert gebliebenen Forschungszielen. Wie schon zur Zeit Lickliders geht es der ARPA auch heute um die Vereinfachung der Mensch-Maschine-Interaktion durch maschinelles Sprachverstehen und wissensbasierte Unterstützung verschiedener, zunehmend komplexer Interaktionsformen. Mit wachsender Leistungsfähigkeit von KI-Systemen kamen die seit den 80er Jahren verfolgten Aufgaben für autonome Systeme und Entscheidungsunterstützung bei Battle-Management-Aufgaben hinzu.

Die heute in militärischen Dokumenten hervorstechende Betonung der Informationsüberlastung von Militärs wirft ein Schlaglicht auf die gestiegene Bedeutung der Informationstechnik allgemein und insbesondere von KI-Produkten als Weg zur Problemlösung für hochtechnisierte Armeen. Der von den USA forcierte – aber auch von anderen NATO-Staaten ebenfalls vorangetriebene – Einsatz von Informationstechnik beim Militär zielt darauf ab, die Wirkungsfähigkeit von Waffensystemen zu erhöhen und die Kontrolle über deren Einsatz zu verbessern. Ein mit Computerhilfe koordiniertes Vorgehen kann – wie der Golfkrieg zeigte – zu einer wesentlichen Beschleunigung und Intensivierung militärischer Operationen führen und eine erhebliche Steigerung militärischer Schlagkraft bewirken[74]. Die durch die informationstechnische Verkopplung militärischer Einheiten gesammelte Informationsmenge enthält zwar eine Vielzahl erwünschter Daten, überlastet aber die mit ihrer Verarbeitung betrauten Menschen. Wissensbasierte Systeme zur Datenfusion und -reduktion, zur Entscheidungsunterstützung und zu verbesserten Mensch-Maschine-Interaktionsformen sind daher umso notwendiger, wie einerseits die Datenmenge und andererseits – durch den IT-Einsatz bedingt – die Geschwindigkeit militärischer Operationen zunimmt. Die Warnungen von Kritikern aus den 80er Jahren, militärischen KI-Systemen keine Entscheidungen über Leben und Tod zu überlassen, sind in Anbetracht der Nutzungsformen dieser Systeme heute zwar aktueller als zuvor, finden aber kaum noch Gehör. Es ist festzuhalten, daß ohne den Einsatz oder zumindest die Hoffnung auf wissensbasierte Systeme die forcierte IT-basierte Form der Kriegsführung mit geringeren Erfolgsaussichten behaftet wäre, als dies heute von vielen Militärs gesehen wird.

Diese weiter wachsende Abhängigkeit von wissensbasierten Systemen erklärt den Hintergrund des seit Jahren thematisch weitgehend gleichbleibenden Interesses von Militärs an den Ergebnissen der KI und damit zugleich ihre konstante Förderung dieser Disziplin. Zwar hat sich für KI-Produkte nach der Anschubfinanzierungsphase der ARPA auch ein substantieller ziviler Markt entwickelt, dieser hat sich jedoch als deutlich unbeständiger erwiesen als der weiterhin bestehende militärische Produktsektor. Ohne die bei dieser Unbeständigkeit reduzierten zivilen Fördermittel treten in der KI erneut militärische Förderinteressen deutlicher zutage. Damit geht es zugleich wieder um die Verantwortung des Wissenschaftlers, sich über die Verwendungszusammenhänge seiner Forschungsergebnisse zu informieren und Rechenschaft darüber geben zu können, ob diese verantwortbar ist.

Literatur:

Bernhardt, Ute; Ingo Ruhmann: Der digitale Feldherrnhügel. Military Systems: Informationstechnik für Führung und Kontrolle; in: Wissenschaft und Frieden, Heft 1/97, Dossier Nr. 24, S. 1-16

Bickenbach, J.; R. Keil-Slawik; M. Löwe; R. Wilhelm (Hg.): Militarisierte Informatik. Schriftenreihe Wissenschaft und Frieden Nr. 4, Marburg, 1985,

BMFT: Bekanntmachung über die Förderung von Forschungs- und Entwicklungsvorhaben auf dem Gebiet der Informationsverarbeitung, Bundesanzeiger, 21.3.84

R. Peter Bonasso: Expert Systems for Intelligence Fusion; MITRE Corp., Bedford, 1984

R. Peter Bonasso: What AI Can Do for Battle Management; AI Magazine, Fall 1988, S. 77-83

Buchanan, Bruce G.: Expert Systems: working systems and the research literature; in: Expert Systems, Jan 1986, S. 32-40

BMVg: Schreiben des Bundesministeriums der Verteidigung an Oswald Metzger, MdB

Bundesregierung: Antwort der Bundesregierung auf die Kleine Anfrage des Abg. Dr.Manuel Kiper: Evaluation der Förderung von Forschung und Entwicklung in der Informationstechnik II – Softwaretechnologie und wissensbasierte Systeme, Bt.-Drs. 13/6894

Bundesregierung: Antwort der Bundesregierung auf die Kleine Anfrage des Abg. Dr.Manuel Kiper: Evaluation der Förderung von Forschung und Entwicklung in der Informationstechnik III – Telekommunikation und Wehrtechnik, Bt.-Drs. 13/6896

Chien, Yi-Tzuu; Jay Liebowitz: Expert Systems in the SDI Environment; in: Computer, Nr. 7, 1986, S. 115-122

DARPA: Strategic Computing, Washington, 1983

DARPA: Strategic Computing. Fourth Annual Report, Washington, 1988

DDR&E (Director of Defense Research and Engineering): Defense Science and Technology Strategy, Washington, July, 1992

DDR&E (Director of Defense Research and Engineering): Defense Science and Technology Strategy, Washington, September, 1994

DDR&E (Director of Defense Research and Engineering): Defense Science and Technology Strategy, Washington, May, 1996 (http://www.dtic.mil/dstp/DSTP/download/strategy.htm)

Department of Defense: Military Critical Technologies Plan, Washington D.C, May 1991

Department of Defense: Military Critical Technologies Strategy, Washington D.C, May 1996

Doherty, Will: Strategic Computing Initiative: Eine kritische Analyse, in: J. Bickenbach, R. Keil-Slawik, M. Löwe, R. Wilhelm (Hg.): Militarisierte Informatik. Schriftenreihe Wissenschaft und Frieden Nr. 4, Marburg, 1985, S.81-95

Dokumentationszentrum der Bundeswehr: Künstliche Intelligenz und Roboter (im militärischen Bereich). Bonn, 1990

Dompke, U.; Schmitz, C.: Erfordernisse und Kriterien künftiger Luftwaffen-Führungssysteme; in: Sonderforschungsvorhaben »Luftwaffe«, S. 203-225

Dreyfus, Hubert L., Stuart E. Dreyfus: Künstliche Intelligenz, Reinbek, 1987

Ebmeyer, Jürgen: Automatisierung der Funktionskette Ziel-Waffe durch Einsatz wissensbasierter Systeme; in: Heinrich Busse (Hg.): Möglichkeiten und Grenzen der Automatisierung in der Wehrtechnik. Symposium. Bundesakademie für Wehrverwaltung und Wehrtechnik, Mannheim, 1987, S. 14-1-14-8

Edwards, Tamala M.: On the Road with ALVINN; in: Time Feb. 20, 1995, S. 16

Edwards, Paul N.: The Closed World, Cambridge,

Mass., 1996

Europäische Wehrkunde: Künstliche Intelligenz für die US-Streitkräfte; in: Europäische Wehrkunde, Nr. 12, 19989, S. 755

Feigenbaum, Edward, Pamela McCorduck: Die Fünfte Computer-Generation. Künstliche Intelligenz und die Herausforderung Japans an die Welt, Basel, 1984

Flamm, Kenneth: Targeting the Computer, Washington, 1987

Flamm, Kenneth: Creating the Computer, Washington, 1988

Franklin, Jude E.; Cora Lackey Carmody; Karl Keller; Tod S. Levitt; Brandon L. Buteau: Expert System Technology for the Military: Selected Samples; in: IEEE Prodceedings, Vol 76, No 10, Oct 1988, S. 1327-1366

Galatowitsch, Sheila: DARPA: Turning Ideas into Products; in: Defense Electronics, July 1991, S. 23-41

Gilmore, John F.: Military Applications of Expert Systems; in: Future Generation of Computer Systems, Nr 6, 1985, S. 403-410

Gray, Chris Hables: The Strategic Computing Programm at Four Years: Implications and Intimations; in: AI & Society, Vol. 2, 1988, S. 141-149

Hofmann, H.W.: Einsatz moderner Informationstechnik im militärischen Bereich: Für den Verteidiger notwendig und verantwortbar; in: Informatik Spektrum, 10. Jg, Heft 1, 1987, S. 11-23

Kalinowski, Martin B.: Virtuelle Atomtests; in: FIfF-Kommunikation, Nr. 3, 1996, S. 7-13

Kawaletz, Karl-Heinz; Lothar Schulz: wissensbasierte Systeme (WBS) in der Materialerhaltung; in: Wehrtechnik, 11/94, S. 16-19

Klischewski, Ralf; Ingo Ruhmann: Ansatzpunkte zur Entwicklung von Methoden für die Analyse und Bewertung militärisch relevanter Forschung und Entwicklung im Bereich Informations- und Kommunikationstechnologie; Gutachten für das Büro für Technikfolgenabschätzung des Deutschen Bundestages, Bonn, März, 1995

Kornell, Jim: Reflections on Using Knowledge based Systems for Military Simulation; in: Simulation, Nr. 4, 1987, S. 144-148

Landesregierung des Saarlandes: Antwort zu der Anfrage der Abgeordneten Gabriele Bozok, Drs.: 11/1517

Ludvigson, Eric C.: Modernization/Readiness for Air-Land Battle 2000 (Pt.); in: Army, Green Book, 1983, S. 282-306

Mobile Computing: New wearable computer goes to the flightline; in: Defense & Security Electronics, Dez. 1995, S. 16

Nii, H.P.; Edward A. Feigenbaum: Rule-Based Understanding of Signals; in: D.A. Waterman; R. Hayes-Roth (Hg.): Pattern-Directed Inference Systems, New York, 1978, S. 483-501

McCurduck, Pamela: Machines Who Think, New York, 1979

Newell, Allen; Herbert Simon: Human Problem Solving, Englewood Cliffs, 1972

Ornstein, S. M., B.C. Smith, L.A. Suchman: Strategic Computing: An Assessment, in: Bulletin of the Atomic Scientists, Dec. 1984, S. 11-15

Pollack, Andrew: Pentagon Sought Smart Truck but it Found Something Else; in: New York Times, 30.5.89, S. 1A

Proctor, Paul: 'Expert System' Software Aims to Speed Maintenance; in: Aviation Week and Space Technology, June 10, 1996, S. 53

Simon, Herbert A.: Models of My Life, New York, 1991

Stefik, Mark: Strategic Computing at DARPA: Overview and Assessment; in: Communicatiosn of the ACM, Vol. 28, July 1985, S. 690-704

Trappl, Robert: AI- Nie. Versuch über eine wahrscheinliche zukünftige Reaktion der Öffentlichkeit; in: Rollinger/Horn: GWAI-86 und 2. 2. Österreichische Artificial-Intelligence-Tagung, Sept. 1986, Berlin, 1986, S. 1-16

Winograd, Terry: Einige Gedanken zur finanziellen Förderung durch das Militär; in: J. Bickenbach, R. Keil-Slawik, M. Löwe, R. Wilhelm (Hg.): Militarisierte Informatik. Schriftenreihe Wissenschaft und Frieden Nr. 4, Marburg, 1985, S.169-173

---

1 Dieser Beitrag erschien im Original in der Zeitschrift Künstliche Intelligenz des Fachbereichs 1 der Gesellschaft für Informatik e.V., Heft 1, 1999. Abdruck mit freundlicher Genehmigung des arenDTaP-Verlages

2 Winograd, Terry: Einige Gedanken zur finanziellen Förderung durch das Militär; in: J. Bickenbach, R. Keil-Slawik, M. Löwe, R. Wilhelm (Hg.): Militarisierte Informatik. Schriftenreihe Wissenschaft und Frieden Nr. 4, Marburg, 1985, S.169-173; Bikkenbach, J.; R. Keil-Slawik; M. Löwe; R. Wilhelm (Hg.): a.a.O.; Hofmann, H.W.: Einsatz moderner Informationstechnik im militärischen Bereich: Für den Verteidiger notwendig und verantwortbar; in: Informatik Spektrum, 10. Jg, Heft 1, 1987, S. 11-23

3 Klischewski, Ralf; Ingo Ruhmann: Ansatzpunkte zur Entwicklung von Methoden für die Analyse und Bewertung militärisch relevanter Forschung und Entwicklung im Bereich Informations- und Kommunikationstechnologie; Gutachten für das Büro für Technikfolgenabschätzung des Deutschen Bundestages, Bonn, März, 1995

4 McCurduck, Pamela: Machines Who Think, New York, 1979; Allen Newell, Herbert Simon: Human Problem Solving, Englewood Cliffs, 1972; Simon, Herbert A.: Models of My Life, New York, 1991

5 eine Aufarbeitung: Flamm, Kenneth: Creating the Computer, Washington, 1988, S. 34ff

6 Flamm, Kenneth: Targeting the Computer, Washington, 1987, S. 46

7 Stefik, Mark: Strategic Computing at DARPA: Overview and Assessment; in: Communicatiosn of the ACM, Vol. 28, July 1985, S. 690-704, S. 690

8 Feigenbaum, Edward, Pamela McCorduck: Die Fünfte Computer-Generation. Künstliche Intelligenz und die Herausforderung Japans an die Welt, Basel, 1984, S. 257

9 Edwards, Paul N.: The Closed World, Cambridge, Mass., 1996, S. 226

10 ebd., S. 264ff

11 ebd., S. 270, S. 296

12 ebd., S. 267

13 Feigenbaum/McCorduck, a.a.O.

14 DARPA: Strategic Computing, Washington, 1983, S. 7

15 ebd., S. 14f

16 ebd., S. 8

17 ebd., S. 19

18 DARPA: Strategic Computing. Fourth Annual Report, Washington, 1988, S. 21

19 ebd., S. 6

20 ebd., S. 10

21 ebd., S. 13f

22 ebd., S. 5

23 ebd., S. 16

24 Buchanan, Bruce G.: Expert Systems: working systems and the research literature; in: Expert Systems, Jan 1986, S. 32-40, S.35

25 Franklin, Jude E.; Cora Lackey Carmody; Karl Keller; Tod S. Levitt; Brandon L. Buteau: Expert System Technology for the Military: Selected Samples; in: IEEE Prodceedings, Vol 76, No 10, Oct 1988, S. 1327-1366, S. 1335f

26 Mobile Computing: New wearable computer goes to the flightline; in: Defense & Security Electronics, Dez. 1995, S. 16; Proctor, Paul: 'Expert System' Software Aims to Speed Maintenance; in: Aviation Week and Space Technology, June 10, 1996, S. 53

27 Franklin, a.a.O., S. 1336ff

28 ebd., S. 1344ff

29 Gilmore, John F.: Military Applications of Expert Systems; in: Future Generation of Computer Systems, Nr 6, 1985, S. 403-410, S.404f

30 vgl die Sonderveröffentlichungen von Speech Technology Feb/March 1985

31 Franklin a.a.O., S.1329

32 R. Peter Bonasso: What AI Can Do for Battle Management; AI Magazine, Fall 1988, S. 77-83

33 ebd., S. 79, auch: Nii/Feigenbaum, a.a.O.

34 Bonasso (88), a.a.O., S. 79

35 Payne

36 Bonasso (88), a.a.O., S. 80f

37 Gilmore, John F.: Military Applications of Expert Systems; in: Future Generation of Computer Systems, Nr 6, 1985, S. 403-410

38 Ebmeyer, Jürgen: Automatisierung der Funktionskette Ziel-Waffe durch Einsatz wissensbasierter Systeme; in: Heinrich Busse (Hg.): Möglichkeiten und Grenzen der Automatisierung in der Wehrtechnik. Symposium. Bundesakademie für Wehrverwaltung und Wehrtechnik, Mannheim, 1987, S. 14-1-14-8

39 Dompke, U.; Schmitz, C.: Erfordernisse und Kriterien künftiger Luftwaffen-Führungssysteme; in: Sonderforschungsvorhaben »Luftwaffe«, S. 203-225, S. 224

40 Wehrtechnik, 8/94, S. 66

41 Kawaletz, Karl-Heinz; Lothar Schulz: wissensbasierte Systeme (WBS) in der Materialerhaltung; in: Wehrtechnik, 11/94, S. 16-19

42 BMFT: Bekanntmachung über die Förderung von Forschungs- und Entwicklungsvorhaben auf dem Gebiet der Informationsverarbeitung, Bundesanzeiger, 21.3.84

43 Stefik, Mark: Strategic Computing at DARPA: Overview and Assessment; in: Communicatiosn of the ACM, Vol. 28, July 1985, S. 690-704, S. 701

44 Doherty, Will: Strategic Computing Initiative: Eine kritische Analyse, in: J. Bickenbach, R. Keil-Slawik, M. Löwe, R. Wilhelm (Hg.): Militarisierte Informatik. Schriftenreihe Wissenschaft und Frieden Nr. 4, Marburg, 1985, S.81-95; Dreyfus, Hubert L., Stuart E. Dreyfus: Künstliche Intelligenz, Reinbek, 1987; Ornstein, S. M., B.C. Smith, L.A. Suchman: Strategic Computing: An Assessment, in: Bulletin of the Atomic Scientists, Dec. 1984, S. 11-15; Trappl, Robert: AI- Nie. Versuch über eine wahrscheinliche zukünftige Reaktion der Öffentlichkeit; in: Rollinger/Horn: GWAI-86 und 2. 2. Österreichische Artificial-Intelligence-Tagung, Sept. 1986, Berlin, 1986, S. 1-16; Winograd, Terry: Einige Gedanken zur finanziellen Förderung durch das Militär; in: J. Bickenbach, R. Keil-Slawik, M. Löwe, R. Wilhelm (Hg.): Militarisierte Informatik. Schriftenreihe Wissenschaft und Frieden Nr. 4, Marburg, 1985, S.169-173

45 SCI (88) a.a.O., Gray 88, a.a.O.

46 Kalinowski, Martin B.: Virtuelle Atomtests; in: FIfF-Kommunikation, Nr. 3, 1996, S. 7-13; vgl. auch: http://www.netlib.org/utk/people/JackDongarra

47 Übersicht in Galatowitsch, a.a.O.

48 ebd., S. 25

49 ebd., S. 40

50 ebd., S. 36

51 Pollack, Andrew: Pentagon Sought Smart Truck but it Found Something Else; in: New York Times, 30.5.89, S. 1A

52 Edwards, Tamala M.: On the Road with ALVINN; in: Time Feb. 20, 1995, S. 16

53 Galatowitsch, a.a.O., S. 38

54 Department of Defense: Military Critical Technologies Plan, Washington D.C, May 1991, S. III-4

55 DDR&E (Director of Defense Research and Engineering): Defense Science and Technology Strategy, Washington, July, 1992, S. II-50

56 DDR&E (Director of Defense Research and Engineering): Defense Science and Technology Strategy, Washington, September, 1994

57 ebd., S. 7-2

58 ebd., S. 8-4

59 ebd., S. 8-5 und 13-2

60 ebd., S. 13-3

61 Europäische Wehrkunde

62 www.ito.arpa.mil/research/hls/

63 www.ito.darpa.mil/research/hci/

64 http://www.aic.nrl.navy.mil/

65 http://www.afit.af.mil/Schools/EN/ENG/LABS/AI/ai.html

66 http://www.pentagon-ai.army.mil/aic

67 http://carlisle_www.army.mil/usacsl/keg/keg.html

68 http://www.ai.usma.edu/

69 Bundesregierung, Bt.-Drs 13/6894, Frage 32

70 Bundesregierung, Bt.-Drs.: 13/6896, Frage 22

71 Saarl. Landesregierung, Drs. 11/1517

72 Schreiben des Bundesministeriums der Verteidigung an Oswald Metzger, MdB

73 DDR&E 94, a.a.O., S.8-4

74 Bernhardt, Ute; Ingo Ruhmann: Der digitale Feldherrnhügel. Military Systems: Informationstechnik für Führung und Kontrolle; in: Wissenschaft und Frieden, Heft 1/97, Dossier Nr. 24, S. 1-16

Ute Bernhardt, Ingo Ruhmann

Cyberterrorismus oder: Von der Militarisierung der Informationsgesellschaft

Die seit dem Golfkrieg stärker in das Bewußtsein der Öffentlichkeit geratene Nutzung der Informationstechnik durch das Militär führt bei einer Sachdebatte schnell zu einigen Bewertungsproblemen. Unklar bleibt bei genauerer Analyse der konkrete Nutzen, den Information Warfare mit sich bringt. Denn im Gegensatz zu anderer Technik, die ihren Nutzen durch größere Reichweite, höhere Geschwindigkeit und Durchschlagskraft oder andere Parameter sichtbar macht, ist er bei der Informationstechnik einer eindeutigen Bewertung nur schwer zugänglich und bleibt auch durch unterschiedliche Erfahrungswerte aus der Praxis widersprüchlich. Auch Cyberterrorismus läßt sich auf konzeptioneller Ebene schlüssig klären, wird aber um so nebulöser, je mehr man sich operativen Fragen widmet.

Bevor wir uns also hier den Folgen von Information Warfare und Cyberterrorismus zuwenden, werden zuerst Definitionen und historische Entwicklungslinien kurz vorgestellt, um damit die Bedeutung der Cyberterrorismus-Debatte zu erhellen. Daran anschließen werden sich einige Anmerkungen zur Übertragbarkeit dieser Debatte auf bundesdeutsche Verhältnisse sowie einige vielleicht ungewöhnliche Gedanken zur Rolle von Datenschutzkontrollinstanzen bei der Prävention von Information Warfare-Gefahren.

Information Warfare, Netwar, Cyberwar

Der Begriff Information Warfare wurde in einer seiner heutigen Bedeutung nahekommenden Weise bereits 1976 geprägt. Ersten Gedankenspielen schlossen sich Mitte der 80er Jahre Analysen von US-Militärs über den Wert und die systematische Nutzbarkeit von Daten und Informationen im Konfliktfall an. Im Zusammenhang damit erschien 1994 eine Studie der Forscher John Arquilla und David Ronfeldt der amerikanischen RAND-Corporation, in der differenzierte Ideen zur Nutzung neuer Instrumente bei der Austragung von Konflikten vorgelegt wurden . Darin wurden die heute unter Information Warfare zusammengefaßte Aktivitäten in zwei neue Begriffe für Konfliktformen gegliedert, die sich hier für die Analyse von Cyberterrorismus besonders gut eignen: Netwar und Cyberwar.

Netwar

Ein Netwar ist bei Arquilla/Ronfeldt definiert als informationsbezogener Konflikt auf der Ebene von Staaten und Gesellschaften. Netwar bedeutet, das Wissen der Bevölkerung eines Konfliktgegners und ihr Selbstbild zu stören und zu modifizieren. Dazu dient nun nicht mehr nur Propaganda, sondern »die Infiltration von Computer-Netzwerken und Datenbanken sowie der Versuch, die politische Opposition per Computer Netzwerk zu unterstützten« .

Ein Netwar ist im traditionellen Sinne kein Krieg, sondern ein Vielzweckinstrument mit Abschreckungscharakter. Abschreckung wird danach nicht länger von Atomwaffen geleistet, sondern auf Computer und ihre Netzwerke verlagert. Netwar überschreitet die Grenze herkömmlicher psychologischer Kriegsführung durch die Einbeziehung neuer Konflikt-Akteure. Nicht nur Staaten oder auf staatliche Macht abzielende Gruppen werden als Gegner benannt, sondern explizit auch Öko- oder Menschenrechtsgruppen, Gewerkschaften und andere politische wie gesellschaftliche Bewegungen. Das Konzept des Netwars beinhaltet damit bereits Formen des Cyberterrorismus. Erste Netwars fanden 1995 auf dem Internet statt, als Verbreitung von Informationen mexikanischer Zapatisten via E-Mail verbreiteten und als propagandistische Begleitung durch diplomatische Stellen zu den Grenzscharmützeln im selben Jahr zwischen Peru und Equador. Ähnliche Auseinandersetzungen hat es seither mehrfach – vor allem in den Konflikten um das Baskenland, Nordirland und Sri Lanka – gegeben.

Cyberwar

Cyberwar wird dagegen als neues Paradigma klar militärischer Auseinandersetzungen gesehen: »Cyberwar bedeutet die Durchführung und Vorbereitung militärischer Operationen nach informations-bezogenen Prinzipien. Er bedeutet die Störung und Zerstörung von Informations- und Kommunikationssystemen und das Wissen eines Gegners über die eigene Lage und Stärke« . Ein gern zitiertes Beispiel ist das Ausschalten des irakischen Kommandosystems in der ersten Angriffswelle alliierter Luftstreitkräfte im Golfkrieg, das die Iraker unwissend über die alliierten Aktionen und damit wehrlos ließ.

In diesem für alle Konfliktkonstellationen anwendbaren Konzept haben hergebrachte militärische Parameter wie Truppenstärke und Ausrüstung nur noch nachrangige Bedeutung. Das Wissen über diese Parameter wird selbst zum entscheidenden Faktor, den es zu nutzen gilt. Mit der Vorstellung, das mit computergesteuerten Waffen bevölkerte Schlachtfeld sei keine genügend konsequente Umsetzung der Informationstechnologie, geht dieser Ansatz über bereits länger bekannte Ideen hinaus.

Ein Cyberwar beginnt vor einem Konflikt mit dem Sammeln von Daten über einen Gegner und dem Manipulieren seiner Datenbasen und Informations-Infrastruktur. Im Konfliktfall bedeutet er das Stören der Informations-Infrastruktur eines Gegners durch Computerviren, eskaliert zum Ausschalten der Infrastruktur durch gerichtete Energiewaffen oder herkömmliche Präzisions-Bombardements und bedeutet innerhalb einer kriegerischen Operation die Unterdrückung des gegnerischen Kontroll- und Kommunikationsnetzes mit allen Mitteln bis hin zur konventionellen oder atomaren Generierung eines elektromagnetischen Pulses, zur Zerstörung allen elektrischen Geräts.

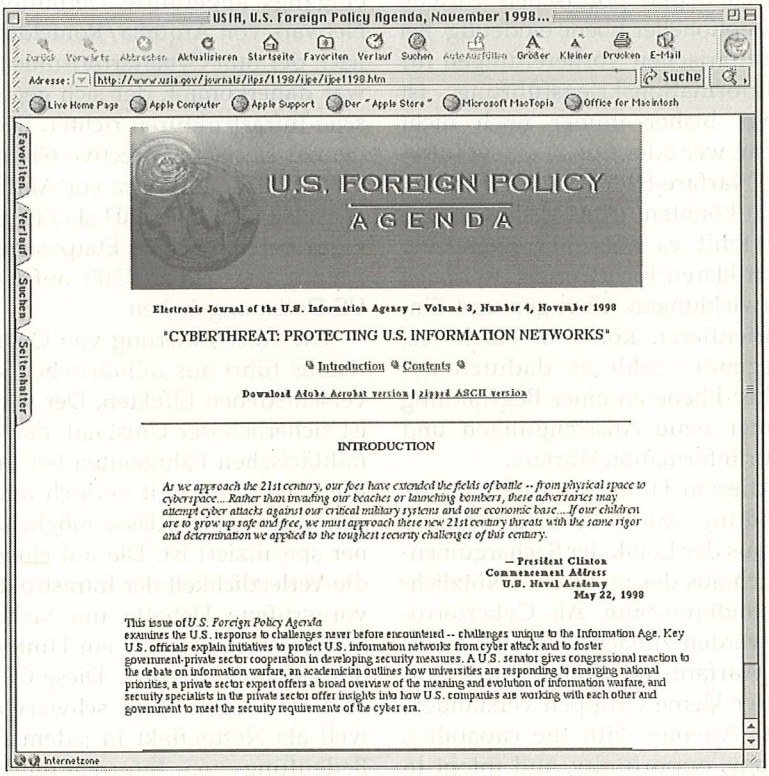
Information Warfare

Die strategische Lage nach dem Ende

der Blockkonfrontation und damit die Verlagerung militärpolitischer Schwerpunkte von atomarer Konfrontation hin zu konventionellen Kriegen führte in den USA zu dem Wunsch, technologisch gestützte militärische Überlegenheit zu demonstrieren. Auch eine Wirtschaftsmacht wie die USA hatten nie die Ressourcen, ihre Militärmacht allein auf konventionelle Mittel zu stützen. Vor dem Hintergrund der Kosten bot sich die Informationstechnik als Force Multiplyer und politisch sichere Alternative an. Mehr Informationen versprechen effektivere Kriegführung mit höherer Siegeswahrscheinlichkeit, IT-gestützte Technik verspricht Ersatz für Soldaten in riskanten Einsatzszenarios und aus entsprechenden Förderprogrammen sollen schließlich wirtschaftspolitische Impulse und damit technologischer und ökonomischer Vorsprung resultieren.

Folgerichtig ist Information Warfare heute recht weit gediehen und gehört zu den Vorhaben, die von US-Militärs operativ umgesetzt werden. Schon 1973 faßte die US Air Force ihr Electronic Warfare Center mit dem Cryptologic Support Center zum Air Force Information Warfare Center zusammen. Hier werden von der Fusion von Satellitenbildern mit Radardaten über Missionsplanungssoftware bis zu Electronic-Warfare-Systemen verschiedene IT-Systeme entwickelt. Das Joint Electronic Warfare Center der U.S.-Streitkräfte wurde in Joint Command and Control Warfare Center umbenannt und zusätzlich mit Aufgaben der psychologischen Kriegführung, operativen Sicher-heit und der Destruktion von Kommandonetzen betraut . Programme zu gerichteten Energiewaffen werden dort ebenso verfolgt wie die Sammlung aller verfügbaren Daten über Waffen- und Kommandosysteme eines potentiel-len Gegners und deren Schwachstel-len. Diese Constant Web-Datenbank zu gegnerischen Kommandosystemen ist auf einem Netzwerk in 67 Ländern verteilt realisiert.

Von der militärischen Forschung und Entwicklung bis zu den Operationen auf dem Schlachtfeld richten die US-Streitkräfte ihre Aktivitäten an Information Warfare-Prinzipien aus. Die Vorschriften der US-Streitkräfte für die Landkriegsführung – in den Grundlagen beschrieben im Field Manual 100-5 – wurde erweitert um Information Warfare-Elemente, deren Umsetzung im Field Manual 100-6 geleistet wurde. Die Ausrüstung einer voll digitalisierten »Experimental Force« (EXFOR) Einheit ist soweit gediehen, daß sie schon bei ihrem ersten Manöver im Sommer 1994 bereits den Eindruck erwecken konnte, für potentielle Aggressoren als zur Abschreckung taugliches Kriegsspiel



nutzbar zu sein. Der Kommandeur des Joint Command and Control Warfare Centers sah daher in der Abschreckung den Zweck von Information Warfare . Erweitert wurde dies durch Überlegungen, den für Information Warfare grundlegenden Wissensvorsprung bereits zur Formierung neuer Allianzen nutzen. Nach der Ablösung des Nuklearschirms der USA als Basis für Allianzen soll nun die selektive Weitergabe dominanten Wissens in Zukunft denselben Zweck erfüllen: »Ebenso, wie nukleare Dominanz der Schlüssel für eine Koalitionsführerschaft in der alten Ära war, so wird Informationsdominanz der Schlüssel im Informationszeitalter sein« . Genauso wie auf dem Schlachtfeld geht es politisch nicht um neue netzwerkartige Strukturen, sondern um die selektive Verteilung zentralisierten Herrschaftswissens nach dem »need-to-know«-Prinzip.

Gegner gesucht

Information Warfare, das Eindringen und Zerstören gegenerischer Datennetze, transformiert das Ausspähen von Sicherheitslöchern, also das Hacken von Computersystemen und deren Abwehr in militärische Aktivitäten. Militärs, die zur Demonstration von Sicherheitslükken in die Rechner von Bundesbehörden eindringen, demonstrieren nicht allein deren Verletztlichkeit. Sie arbeiten zugleich an Arbeitsbeschaffungsmaßnahmen für sich selbst. Denn wer ist besser in der Lage, die Sicherheit der nationalen IT-Infrastruktur zu schützen als eben jene, die diese Infrastruktur zum Kriegsgebiet machen wollen? Auf diese Weise verfremden Information Warrior die ursprüngliche Hackerethik vom Ausspähen anderer, um die Opfer auf die gefundenen Sicherheitslücken aufmerksam zu machen.

Was die Betroffenen bisweilen als moderne Variante der Schutzgelderpressung begreifen, wenden Information Warrior auf ganze Nationen an – ihre eigenen zuerst. Den Militärs erlaubt das Forcieren von Information Warfare als systematische Steigerung der IT-Unsicherheit überdies ein Zurückdrängen nichtmilitärischer Lösungskonzepte. Im Gegensatz zu Gelegenheitshackern und professionellen IT-Sicherheitsberatern geht es bei Information Warfare eben nicht um die systematische Reduktion von Verletztlichkeit, sondern deren selektive Nutzung. Wie das Beispiel Kryptographie zeigt, sind Militärs kein

Faktor von Sicherheit, sondern von Unsicherheit. Ihre Interessen stehen in scharfem Kontrast zu denen der zivilen Gesellschaft.

Solange sich Information Warfare als militärisches Ausnutzen von Schwächen eines Gegners begreifen ließ, waren die militärischen und politischen Vorteile auf konzeptioneller Ebene eindeutig. Bei allen militärischen Vorbereitungen für eine Informationskriegsführung ist allerdings bisher immer noch nicht erkennbar, wer oder was in einem Information Warfare-Szenario Gegner der USA sein könnten. Ohne glaubwürdige Gegner fehlt es aber auf operativer Ebene an klaren Richtwerten, an denen sich Entwicklungen, Übungen und Einsätze orientieren könnten. Noch viel grundlegender fehlt es dadurch auf politischer Ebene an einer Begründung für immer neue Anstrengungen und Mittel für Information Warfare.

Vor diesem Hintergrund erhält die Hinwendung zum Cyberterrorismus sowohl aus der Logik der Sachargumente als auch aus der politischer Nützlichkeit besonderen Sinn. Als Cyberterrorismus werden zunächst generell Information Warfare-Aktivitäten durch Einzelne oder kleine Gruppen verstanden, genauer:«Anyone with the capability, technology, opportunity, and intent to do harm« . Mit den heute im Internet frei angebotenen Manipulationswerkzeugen ist so gut wie jeder technisch nicht völlig laienhafte Internet-Nutzer zu schwerwiegenden Eingriffen in IT-Systeme in der Lage. Diese Ausweitung erhöht schlagartig die Zahl potentieller Gegner und steigert die Bedrohung.

Um die so aufgebaute Bedrohungskulisse nicht grenzenlos werden zu lassen, wird die Schadensbedrohung eingegrenzt auf Infrastruktursysteme, deren Ausfall in einer technisierten Gesellschaft zu erheblichen Problemen führt. Diese sind laut des Critical Infrastructure Assurance Office (CIAO):

1. Information and Communications,
2. Electrical Power Systems,
3. Gas and Oil Transportation and Storage,
4. Banking and Finance,
5. Transportation,
6. Water Supply Systems,
7. Emergency Services,
8. Government Services

Nicht unerwähnt bleiben sollte, daß in dieser Aufzählung das Militär außen vor bleibt. In dieser Sichtweise kehrt die eingangs angeführte Definition eines Netwars von Arquilla/Ronfeldt wieder, nach der nun Cyberterrorismus als Netwar daherkommt, der sich gegen kritische Infrastrukturen richtet. Die Presidential Decision Directive 63 vom Mai 1998 gibt ihren Schutz vor Anriffen auf diese bis zum Jahr 2003 als Ziel vor. Der dafür bereit gestellte Etatposten wurde Anfang 1999 um fast 50% auf 1,46 Mrd. US-Dollar angehoben.

Die Akzentuierung von Cyberterrorismus führt aus militärischer Sicht zu verschiedenen Effekten. Der wichtigste ist sicherlich der Umstand, daß zu den militärischen Fähigkeiten bei Information Warfare damit endlich auch eine genügend große Klasse möglicher Gegner spezifiziert ist. Die mit einer durch die Verletzlichkeit der Infrastruktur hervorgerufene Debatte um Sicherheitsmängel riskiert zwar ein Hinterfragen des Gesamtkonzeptes. Diese Gefahr ist aber deswegen nicht schwerwiegend, weil als Nettoeffekt in jedem Fall die Bedeutung von Information Warfare weiter steigt. Cyberterrorismus stellt sich somit als Bedrohungsszenario dar, das im Kontext mit Information Warfare entsprechenden Aktivitäten zusätzliche Glaubwürdigkeit verleiht.

Problem oder Lösung?

Die Verletzlichkeit der Informationstechnik und der mit Hilfe dieser Technik gesteuerten Infrastruktur ist ein keineswegs neues Phänomen. Auch die Auseinandersetzung von Militärs mit derartigen Fragen ist älteren Datums. So stellte das Orange Book des U.S. Department of Defense die erste ausführliche Aufarbeitung von IT-Sicherheitsrisiken dar und blieb lange Zeit Grundlage jeder Sicherheitsabschätzung.

Verschärft wurde seit der Herausgabe des Orange Books die IT-Sicherheitslage durch die Abkehr von kostspieligen Softwareentwicklungen für spezielle Nutzergruppen. Dank des »Commercial off the Shelf«-Programms zum Einsatz preisgünstiger kommerzieller Standardsoftware verfügen Militärs ebenso wie Betreiber kritischer Infrastrukturen heute über dieselben IT-Systeme wie jene Privatpersonen, die als potentielle Angreifer auf diese Systeme gesehen werden. Zumindest prinzipiell kann jeder auf diese Weise zu Hause die Manipulationen an solchen Rechnern erproben, die mit derselben Software ausgestatteten sind wie das Ziel einer cyberterroristischen Attacke.

Der Einsatz von Standardsoftware macht ihre Nutzer abhängig von den Lieferanten und deren eingebaute Sicherheitsmaßnahmen. Mangels Sourcecode der eingesetzten Software lassen sich weder Sicherheitslücken gezielt aufspüren noch strukturelle Sicherheitsdefizite durch eigene Modifikationen an der Software ausgleichen. Der Einsatz des Internets als preisgünstiger öffentlicher Infrastruktur eröffnet Angreifern zusätzliche Sicherheitslöcher, gegen die auch technische Gegenmaßnahmen nur begrenzt wirksam sind.

In der Bundesrepublik brauchte es gewisse Zeit und Anstöße, bis die Einsicht in derartige Verwundbarkeiten Fuß fassen konnte. Die Bundesregierung vertrat in Ihrer Antwort auf eine Kleine Anfrage noch im Mai 1997 die Auffassung, eine der Kommission des US-Präsidenten zum Schutz kritischer Infrastrukturen vergleichbare Gruppe sei »nicht erforderlich« . Wenige Wochen später allerdings ging vom Bundesinnenministerium die Initiative zur Etablierung eines heute vom Bundesamt für Sicherheit in der Informationstechnik (BSI) federführend koordinierten Arbeitskreises kritische Infrastrukturen zur Untersuchung genau dieser Fragen aus.

Vor dem Hintergrund der Defizite in der IT-Sicherheit ist ein solch schneller Meinungswandel nur zu begrüßen. Dies deshalb, weil sich darin eine neue Linie des Umgangs mit dem Problem erkennen läßt. Sieht man nämlich Cyberterrorismus aus einer einfachen administrativen Perspektive, ist das Problem schon lange gelöst. Die Bundesrepublik verfügt seit den 80er Jahren über mehr als genügend gesetzliche Grundlagen, um gegen Cyberterrorismus vorzugehen (vgl. Kasten »Cyberterrorismus – strafrechtlich gesehen«).

Der schöne gesetzliche Schein hinterläßt jedoch zwei grundlegende Fragen, nämlich, auf welche Weise erstens die sensitiven IT-Systeme geschützt sind und wer zweitens in der Lage ist, Angriffe auf diese Systeme zu erkennen und zu ahnden. Öfter schon endete die Fahndung nach Hackern in Kinderzim-

mern, als in den Kreisen politischer oder organisierter Krimineller. Wo aber die Unterscheidung zwischen Terrorismus und Jugendstreich versagt, weil beispielsweise Manipulationen an IT-Systemen kinderleicht sind, liegt Grundsätzliches im Argen.

Die Arbeitsgruppe im BSI könnte also von der Erkenntnis zeugen, daß gegen IT-Sicherheitsprobleme tiefer angesetzt werden müßte. Somit ist nun das Augenmerk auf Problemlösungsmöglichkeiten zu richten. Die Betonung, daß es mehr als eine beste Lösung gibt, geschieht hier aus zwei Gründen: Erstens ist unmittelbar einsichtig, daß die sehr verschiedenartigen Sicherheitsbedürfnisse unterschiedlicher IT-Anwender zwangsläufig zu Lösungsansätzen führen, die nicht unbedingt dekkungsgleich sein müssen. Zweitens und wichtiger noch ist aber der generelle Blickwinkel, unter dem IT-Sicherheitsprobleme gesehen werden. An den deutlich verschiedenartigen Voraussetzungen in den USA und der Bundesrepublik lassen sich Gefahren veranschaulichen.

Cyberterrorismus: Vorhandene Ansätze in der Bundesrepublik

Wie in den USA auch, werden geprüfte IT-Systeme als ein besonders geeignetes Mittel gegen Attacken gesehen. Geprüfte IT-Sicherheit wird jedoch zumeist verstanden als die durch ein Zertifikat des BSI oder vergleichbarer privater Institutionen nachgewiesene Konformität eines IT-Systems mit bestimmten Sicherheitskriterien. Mit diesem Gütesiegel wird das IT-System dann in der Praxis eingesetzt, wo untaugliche Rahmenbedingungen oder Modifikationen des Systems in der Einsatzzeit das festgestellte Sicherheitsniveau ausgehebelt werden kann.

In Behörden ist es zum Teil den Rechnungshöfen vorbehalten, den Betrieb von IT-Systemen im Einsatz zu überprüfen. In der Bundesrepublik gibt es neben dem Arbeitskreis des BSI und den Rechnungshöfen eine lang etablierte Ebene der Kontrolle von DV-Verfahren, die jedoch im Zusammenhang mit der Bekämpfung des Cyberterrorismus bislang unbeachtet geblieben ist. Die einzige Instanz jedoch, die in der Bundesrepublik mit der systematischen Kontrolle von IT-Systemen in der Planung und im Einsatz betraut ist, sind die Datenschutzbeauftragten.

Allzu leicht vergessen wird, daß Datenschutz nicht allein dem Schutz personenbezogener Daten dient, sondern die Datenschutzgesetze dazu auch Vorschriften zur IT-Sicherheit enthalten. Beispielhaft ist dies der in dieser oder ähnlicher Form auch in den Landesgesetzen nachgebildete §9 BDSG mit den im Anhang dazu aufgeführten technischen und organisatorischen Maßnahmen zur IT-Sicherheit. Um Mißbrauch zu verhindern und aufzuklären, verlangt der Datenschutz effektiven Zugriffsschutz, personalisierte und aufgabenbezogene Zugriffsrechte, auditierbare Dateizugriffe, für schutzwürdige Bereiche umfassende Dokumentation und vor allem keine Anbindung an offene Netze, sofern die Sicherheit nicht gewährleistet werden kann. Jeder Datenschutzbeauftragte wird eine Internet-Anbindung rügen, die keine der Sicherheitsklassifikation entsprechenden Sicherheitstechnologie aufweist. Einige, wie der Schleswig-Holsteinische Datenschutzbeauftragte, setzen für Prüfungen auch Hacker-Tools gegen IT-Systeme ein, um deren Sicherheitsmechanismen zu testen. Wenn sich jede Behörde an derartige Sicherheitsregularien hielte, wären Manipulationen an IT-Systemen via Internet und andere Zugriffe auf Daten nur schwer machbar und diese außerdem rekonstruierbar.

Daß die Realität so nicht aussieht, muß nicht betont werden. Zum Teil werden die Warnungen der Datenschützer nicht befolgt, zum Teil stellen sie Verstöße bei Prüfungen fest. Wichtig festzuhalten sind aber zwei prinzipielle Ansätze des Datenschutzes in diesem Land: Erstens die Analyse des Schutzniveaus von IT-Systemen von Behörden vor deren Einsatz und zweitens deren periodische Kontrolle. Diese Rechte gelten für abgeschottete DV-Anlagen ebenso wie für die Internetanbindung von Behörden. Defizite in der Bundesrepublik sind allerdings dort zu beobachten, wo im nicht-öffentlichen Bereich weder eine Vorab- noch eine anlaßunabhängige Datenschutzkontrolle möglich ist.

Die USA haben die Internet-Anbindung von Behörden dagegen vielfach vorangetrieben, ohne auf Risiken zu achten. Wer wie die USA die elektronische Steuererklärung ermöglicht und das Finanzamt mit dem Internet verbindet, ohne adäquate technische Sicherheitsfeatures zu implementieren, wird erhebliche Sicherheitsprobleme bekommen. Zugunsten der erreichten Produktivitätsgewinne lassen sich solche IT-Lösungen aber nicht zurücknehmen, die Sicherheitsrisiken bleiben. Hier zeigt sich – nicht zuletzt dank des Datenschutzes – die deutsche Vorsicht doch etwas realitätstauglicher.

Was die USA nun mit dem CIAO aufbauen, kommt der Praxis der hiesigen Datenschutzbeauftragten nicht einmal nahe. Insofern rächt sich die Nachlässigkeit der USA in puncto Datenschutz auch in Fragen der IT-Sicherheit. Ohne Datenschutzgesetze gibt es dort keine ähnlich strengen Kontrollen der IT-Sicherheit und geringere Sicherheitsbedenken. Ohne solche Bedenken wurden durch Internet-Anbindungen von Behörden erhebliche Risiken eingegangen. Ohne Datenschutzgesetze wiederum besteht kein Zwang zu datenschutz- und nutzerfreundlichen Technologien. Wie die Aktivitäten zeigen, soll statt dessen Sicherheit durch Sicherung vor Nutzern hergestellt werden.

Cyberterrorismus: Bekämpfung in den USA

Die in den USA genutzten Mittel zur Verminderung von IT-Sicherheitsrisiken umfassen nach einer Erklärung vom 22. Januar 1999: »developing tools that can identify potentially threatening activities, Intrusion detection systems, Information Sharing and Analysis Centers, Recruiting a Cyber Corps« . Alle diese Aktivitäten sind Sicherungsmaßnahmen gegen Mißbrauch. Was dabei dagegen gänzlich fehlt, sind sichere IT-Systeme. Weder wird eine regelmäßige Kontrolle von Systemen im Einsatz vorgesehen, noch generell verbesserte Prüfungen. Dies ist um so bemerkenswerter, als bei den in großer Zahl eingesetzten Betriebssystemen wie DOS oder Windows 98 ohne Zusatzsysteme – im Gegensatz zu Unix oder Windows NT – die Sicherheitslücken fundamental sind. Nach deutschem Rechtsverständnis können darin nicht einmal Daten ausgespäht werden, weil diese keine obligatorischen Sicherungen gegen unbefugten Zugang – wie eine Authentisierung durch Paßwort – kennen, ein Ausspähen aber voraussetzt, daß Daten wenigstens in minimaler Weise gegen unbefugten Zugriff gesichert sind. Erst bis zum Jahr 2010 wollen die USA die Defizite in der verfügbaren Sicherheitstechnologie auf-

arbeiten, wofür allein Forschungsmittel in Höhe von sieben Milliarden Dollar erforderlich gehalten werden .

Einerseits findet so eine Konzentration auf die Beobachtung von Nutzern statt, um zu verhindern, daß sie die zahlreich vorhandenen IT-Sicherheitslücken ausnutzen. Alle Erfahrung im IT-Sicherheitsbereich zeigen aber, daß jede rein nutzerorientierte Maßnahmen letztlich erfolglos bleiben wird. Obendrein bleibt eine solche Orientierung auf Nutzer die Erklärung schuldig, wer mit welcher Befugnis gegen wen tätig werden will. Trotz aller Internationalisierung der IT-Branche beruht Cyberterrorismus auf technischer Kompetenz, die dort existiert, wo IT entwickelt, hergestellt und breit genutzt wird. Vor der Bedeutung zwischenstaatlicher Attacken wird Cyberterrorismus deshalb lange Zeit vor allem ein Binnenproblem hochentwickelter Informationsgesellschaften sein.

Andererseits wird die Entwicklung von Sicherheitstechniken nur halbherzig vorangetrieben und bezieht nicht einmal die grundlegende Ebene von Betriebssystemen und Protokollen mit ein. Dies ist ein riskantes Spiel, das die Ursachen der Probleme unbeachtet läßt, denn: IT-Sicherheit ist unteilbar, eingebaute oder nicht beseitigte Lücken rächen sich. IT-Sicherheit muß daher im Interesse der zivilen und militärischen Sicherheit vollständig und umfassend sein. Der Einbau von Hintertüren für Information Warfare-Attacken schlägt auf die zurück, die sie eingebaut oder zugelassen haben. Darin schließlich liegt die generelle Gefahr, IT-Sicherheit vorrangig unter militärischen Aspekten zu sehen.

Zivile Gegenkonzepte zu Information Warfare

Was wir auch unabhängig von Information Warfare benötigen, ist eine Reduktion der Verletztlichkeit der Informationsgesellschaft. Neben einer frühzeitigen Abschätzung der Risiken kann dazu vor allem eine Verbesserung der IT-Sicherheit beitragen. Mit dem Orange Book stammen die ersten IT-Sicherheitskriterien aus dem Pentagon, die mittlerweile mit den Common Criteria nur leicht zivilisiert wurden. Definition und Bewertung von IT-Sicherheit ist damit kaum je unter zivilen Gesichtspunkten entwickelt worden. Wenn die Zuverlässigkeit, die Sicherheit und die Verfügbarkeit der Infrastruktur der Informationsgesellschaft von Sicherheitsmaßnahmen abhängen, dann können wir deren Definition und Bewertung ernsthaft nicht Militärs oder Geheimdiensten überlassen . Die eigentliche Frage ist also die nach den zivilen Anforderungen für Bewertungskriterien und ihrer Bedeutung im Alltag.

Folgerung aus der Debatte um Information Warfare kann nur die konsequente Politisierung und Zivilisierung der IT-Sicherheit sein . IT-Sicherheit ist in zivile Hände zu legen und entsprechend ziviler Anforderungen zu entwickeln, statt sie weiterhin unter militärischen Aspekten zu sehen. Wir brauchen auch keine Militärs, um zu verdeutlichen, worin die Verletzlichkeit der Informationsgesellschaft liegt. Wie eingangs erwähnt, gab es schon vor der Erfindung des Begriffs Information Warfare eine rege Debatte sowohl um die Folgen fehlender Sicherheit als auch um Sicherheitslücken. Warum sollten aus Hackern erst Soldaten werden müssen, um diese Sicherheitslücken ernst zu nehmen?

Die Sicherheit und der Schutz einer verletzlichen Informationsgesellschaft sind besser in den Händen ziviler Institutionen aufgehoben. NGOs und Berufsverbände waren es, die in den letzten 20 Jahren auf die Brisanz des Thema aufmerksam gemacht haben. Sie müssen auch in Zukunft an dieser Debatte beteiligt werden, statt die Sicherheit der Informationsgesellschaft staatlichen Institutionen mit zweifelhaften Ruf und militärischen Interessen zu überlassen. Statt es als Risiko zu begreifen, Sicherheitslücken offenzulegen, sollten im Gegenteil Informationsbörsen ausgebaut werden, um die betroffenen Systemadministratoren zu unterstützen. Die Offenlegung von Standards und Sicherheitsfeatures schützt vor unliebsamen Überraschungen. NGOs wie zum Beispiel Menschenrechtsgruppen oder Netzaktivisten als Kriegsgegner in einem Netwar zu begreifen, geht in die falsche Richtung. Mit ihrer Arbeit der letzten Jahre bieten sie am ehesten die Gewähr dafür, die Informationsgesellschaft demokratischen und zivilen Prinzipien entsprechend zu entwickeln und deren Verletztlichkeit im Interesse der Allgemeinheit zu vermindern. Werden solche Aktivitäten nicht unterstützt und solche Gruppen nicht eingebunden, wird nicht die Sicherheit zunehmen, sondern allenfalls die Sicherung vor mißbräuchlicher Nutzung. Information Warfare nötigt uns daher die Entscheidung ab, ob das Ziel eine zivile Informationsgesellschaft sein soll oder nicht.

Fazit

Der Vergleich der Herangehensweisen zwischen den USA und der Bundesrepublik zeigt zwei Kulturen im Umgang mit Daten und deren Sicherheit. Als Einflußfaktor auf die sehr unterschiedlichen Ansätze schon in der Problemwahrnehmung und erst recht bei der Problemlösung läßt sich eine in Europa insgesamt größere Vorsicht beim Umgang mit Daten erkennen, die als Effekt eine frühere und stärkere Wahrnehmung von Sicherheitsfragen zur Folge hatte.

Der Schutz IT-gestützter ziviler wie militärischer Infrastrukturen erfordert eine angemessene Prioritätensetzung. Grundlegend muß die Reduktion der IT-Sicherheitsdefizite sein, ebenso wie die Berücksichtigung nichttechnischer Alternativen zur Information Warfare-Abwehr wie die Verminderung der Anfälligkeit von IT-Systemen auf nichttechnische Weise, etwa durch internationale Schutzabkommen, vertrauensbildende Maßnahmen der Offenheit oder andere Mittel. Die Reglementierung und Beobachtung der Nutzer ist dagegen kein taugliches Mittel.

Cyberterrorismus ist eine Gefahr, die sich dadurch vermindern läßt, daß IT-Systeme vor ihrem Einsatz und in der Praxis stärker als bisher auf Sicherheitsmängel geprüft werden. Die einzige systematische Kontrolle dieser Art leistet in Deutschland der Datenschutz, der dadurch zur Verminderung von Gefahren bereits spezifische Beiträge geleistet hat. Wie beim modernen Datenschutz auch, geht es also letztlich um die Frage, ob Sicherheit eher durch die Kontrolle menschlichen Verhaltens zu erzielen ist oder durch angemessene technische Maßnahmen. Ein Bedrohungsszenario wie der Cyberterrorismus, das von böswilligem menschlichen Verhalten ausgeht, wird besser beraten sein, die heute und in absehbarer Zukunft verfügbaren technischen Maßnahmen einzusetzen und auszubauen, um Sicherheit herzustellen.

FIfF e.V. FIfF Überall

FIfF–Vorstand

- **Prof. Dr. Reinhard Keil-Slawik (Vorsitzender)**
  U-GH Paderborn
  Fürstenallee 11
  33102 Paderborn
- **Ute Bernhardt (stellv. Vorsitzende)**
  Am Alten Bahnhof 6
  App. 78
  64293 Darmstadt
- **Peter Bittner**
  Karl-Liebknecht-Straße 34 A
  64347 Darmstadt
- **Dagmar Boedicker**
  Daiserstraße 45
  81371 München
- **Prof. Dr. Leonie Dreschler-Fischer**
  Nienstedtener Strasse 36
  22609 Hamburg
- **Eva Hornecker**
  Neustadtswall 22
  28199 Bremen
- **Werner Hülsmann**
  Medemstade 64
  21775 Ihlienworth
- **Ingo Ruhmann**
  Rittershausstraße 11
  53113 Bonn
- **Prof. Dr. Britta Schinzel**
  Friedrichstr. 50
  79098 Freiburg i. Br.
- **Ralf E. Streibl**
  Universität Bremen
  FB 3 – Informatik
  Bibliothekstrasse 1
  28359 Bremen

Beirat

Prof. Dr. Wolfgang Coy (Berlin); **Prof. Dr. Leonie Dreschler-Fischer** (Hamburg); **Prof. Dr. Christiane Floyd** (Hamburg); **Prof. Dr. Klaus Fuchs-Kittowski** (Berlin); **Prof. Dr. Thomas Herrmann** (Dortmund); **Prof. Dr. Wolfgang Hesse** (Marburg); **Prof. Dr. Michael Grütz** (Konstanz); **Ulrich Klotz** (Frankfurt); **Prof. Dr. Hans-Jörg Kreowski** (Bremen); **Prof. Dr. Herbert Kubicek** (Bremen); **Prof. Dr. Hans-Peter Löhr** (Berlin); **Dipl.-Ing. Werner Mühlmann** (Oppung); **Prof. Dr. Frieder Nake** (Bremen); **Prof. Dr. Rolf Oberliesen** (Bremen); **Dr. Hermann Rampacher** (Bonn); **Prof. Dr. Arno Rolf** (Hamburg); **Prof. Dr. Alexander Roßnagel** (Kassel); **Prof. Dr. Gerhard Sagerer** (Bielefeld); **Dr. Gabriele Schade** (Ilmenau); **Prof. Dr. Dirk Siefkes** (Berlin); **Dr. Marie-Theres Tinnefeld** (München); **Dr. Gerhard Wohland** (Wankheim)

Regionalgruppe Freiburg

Ab Dezember 1999 trifft sich die Freiburger Regionalgruppe regelmäßig am zweiten Dienstag im Monat um 20 in der „Schwarzwaldstube" (5. OG, Institut für Informatik und Gesellschaft, Friedrichstr. 50, 79 098 Freiburg).

Beim Gründungstreffen am 3. November wurden folgende Themenvorschläge und möglicherweise zu bearbeitende Fragen diskutiert:

Ethische Konflikte von InformatikerInnen in der Berufspraxis: Wie kann in einem Arbeitsvertrag gefaßt werden, daß wir als InformatikerInnen z. B. nicht im Bereich der Rüstung arbeiten wollen? Gibt es InformatikerInnen die eine solche Klausel in ihrem Arbeitsvertrag haben? Wenn ja, wie sieht sie aus? Wir planen, eine Sammlung von Klauseln im Web zu veröffentlichen, um deren Integration in neue Arbeitsverträge zu erleichtern. Was sind weitere kritische Arbeitsgebiete für InformatikerInnen, die sich ihrem Gewissen verpflichtet fühlen?

Chipkartenprojekte in Freiburg: Welche Funktionalitäten der Chipkarten sind geplant? Welche Interessen stehen dahinter? Wie können wir mitwirken?

Weitere Themenvorschläge sind willkommen! Wir hoffen auf weitere rege Teilnahme und freuen uns auf das nächste Treffen! Eine Anmeldung (subscribe) auf unserer neuen Mailliste (fiff-fr@telematik.iig.uni-freiburg.de) ist möglich.

Kontakt: jendricke@gmx.de

Neuer Jahrestagungsband 1998 (Darmstadt)

Neu erschienen ist ein Band mit Beiträgen zur 14. Jahrestagung des FIfF 1998 in Darmstadt, die unter dem Motto stand: „Mensch sein in einer informatisierten Gesellschaft". Der 188 Seiten starke Band wurde herausgegeben von Peter Bittner und Jens Woinowski und erscheint unter dem Titel „Mensch – Informatisierung – Gesellschaft" als erster Band der Reihe *Kritische Informatik* im Lit-Verlag Münster. Er ist zu einem Preis von 39,90 DM über das FIfF-Büro oder im Buchhandel unter der ISBN 3-8258-3930-3 erhältlich.

Termine

24. – 26. 01. 2000:
International BOBCATSSS Symposium on Library and Information Science at the Jagiellonian University (Krakau, Polen). Nähere Informationen unter http://v.hbi-stuttgart.de/HyperNews/get/IEthics.html

14. – 16. 04. 2000: Klausurtagung von wissenschaftlichem Beirat und Vorstand zum Thema »Verletzlichkeit der Informationsgesellschaft« in Oberursel

18. – 19.2.2000: „Grundrechte in der Informationsgesellschaft – Zwischenbilanz rot-grüner IT-Politik": Tagung von FIfF, DVD, CILIP, Humanistische Union, Humboldt-Universität Berlin

Vielzweck-Schnipsel

Kopieren, ausfüllen und einsenden an: FIFF e.V. Medemstade 64 21775 Ihlienworth

FIfF

Das möchte ich:

- ❒ ***Ich möchte ❒ aktives / ❒ förderndes Mitglied des FIfF werden*** *(Mindestjahresbeitrag ist für Verdienende* ***60,– Euro (117,35 DM)*** *für Studierende und Menschen in vergleichbarer Situation* ***15,– Euro (29,34 DM)*** *pro Jahr.*
- ❒ ***Ich möchte die FIfF-Kommunikation zum Preis von 20,– Euro (39,15 DM) jährlich frei Haus abonnieren.***
- ❒ ***Ich überweise den Beitrag auf das Konto 413 83 600 bei der Volksbank Cuxhaven-Hadeln, BLZ 241 618 14.***
- ❒ ***Der Mitglieds- bzw. Abobeitrag soll per Lastschriftverfahren von meinem Konto abgebucht werden*** *(s. u.).*
- ❒ ***Ich möchte meine neue/korrigierte Anschrift mitteilen*** *(siehe unten).* ***Meine alte/falsche Anschrift:***

  Straße: _____ *Wohnort:* _____
- ❒ ***Ich möchte dem FIfF etwas spenden:***
- ❒ *Verrechnungsscheck über* _____ *DM liegt bei* ❒ *Spendenquittung am Ende des Kalenderjahres erbeten*
- ❒ ***Ich möchte mehr über das FIfF wissen, bitte schickt mir:*** _____
- ❒ ***Ich möchte gegen Rechnung, zuzüglich Portokosten, bestellen:*** _____
- ❒ ***Ich möchte das FIfF über einen Artikel/ein Buch informieren:*** ❒ ***Zitat*** *(siehe unten)* ❒ ***Kopie*** *(liegt bei)*
- ❒ ***Ich möchte zur FIfF-Kommunikation beitragen mit:*** ❒ ***einem Manuskript zur Veröffentlichung*** *(liegt bei)* ❒ ***einer Anregung*** *(siehe unten)*

  Bemerkungen/Ergänzungen: _____
- ❒ ***Ich möchte einen richtigen Brief schreiben. Der Vielzweck-Schnipsel ist nichts für mich.***

Die/der bin ich:

Name: _____ *Straße:* _____

Wohnort: _____ *ggf. Mitgliedsnummer:* _____

Telefon (privat): _____ *(Arbeit):* _____ *E-Mail:* _____

Einzugsermächtigung

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

Name: _____ *Jahresbeitrag:* _____ *DM, erstmals* _____

Konto-Nr.: _____ *BLZ:* _____ *Geldinstitut:* _____

Straße: _____ *Wohnort:* _____

Datum: _____ *Unterschrift:* _____

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

Adressen

Aachen
Prof.Dr.Dietrich Meyer-Ebrecht
Lehrstuhl für Meßtechnik
RWTH Aachen
52056 Aachen
Tel.: (0241) 80 78 60
Fax: (0241) 88 88 200
Mail@LfM.RWTH-Aachen.De

Berlin
TU Berlin
Irina Piens
Schmidtstraße 3
10179 Berlin
piens@prz.tu-berlin.de

FU Berlin
Lukas Faulstich
Mehringdamm 119
10965 Berlin
Tel.: (030) 69 50 92 24

Bonn
Ingo Ruhmann
Rittershausstrasse 11
53113 Bonn
ingo@ruhmann.ki.shuttle.de

Braunschweig
TU Braunschweig
Fachschaft Informatik
AStA-Fach
Katharinenstraße 1
38106 Braunschweig

Bielefeld
c/o Angewandte Informatik
Technische Fakultät
Universität Bielefeld
Postfach 100 131
33502 Bielefeld
fiff-bi@TechFak.Uni-Bielefeld.DE

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

Darmstadt
Jens Woinowski
Rhoenring 141
64289 Darmstadt
Tel.: (06151) 16 61 82 (d)
(06151) 71 81 50 (p)
woinowsk@iti.informatik.tu-darmstadt.de

Erlangen/Fürth/Nürnberg
Klaus Thielking-Riechert
Sommerstraße 10
90762 Fürth
k.thielking@link-n.cl.sub.de

Freiburg
Uwe Jendricke
Bernhardstrasse 1B
79098 Freiburg
Tel. & Fax: 0761/25665
jendricke@telematik.iig.uni-freiburg.de

Frankfurt
Ingo Fischer
Dahlmannstraße 31
60385 Frankfurt am Main

Hamburg
Simone Pribbenow
Hein-Köllisch-Platz 5
20359 Hamburg
Tel.: (040) 54715-366
pribbeno@informatik.uni-hamburg.de

Hannover
Bernhard Pfitzner
Rosenbergstraße 14a
30163 Hannover

Heilbronn
Michael Müller
FH Heilbronn, FB
Max-Planck-Straße 39
74081 Heilbronn
Tel.: (07131) 50 43 64
michael.mueller@fh-heilbronn.de

Jena
Prof. Dr. Eberhard Zehendner
Institut für Informatik
Friedrich-Schiller-Universitaet
07740 Jena
Tel: (03641) 946385
Fax: (03641) 946372
zehendner@acm.org

Kaiserslautern
Frank Leidermann
Institut für Technol. und Arbeit
Universität Kaiserslautern
Gottlieb-Daimler-Str.
67663 Kaiserslautern
Tel. 0631/205-3742
fleider@sozwi.uni-kl.de

Karlsruhe
Thomas Freytag
Institut AIFB
Universität Karlsruhe
76128 Karlsruhe
Tel.: (0721) 6084063 (d)
(0721) 815416 (p)
tfr@aifb.uni-karlsruhe.de

Kiel
Hans-Otto Kühl
Alte Kieler Landstraße 118
24768 Rendsburg
Tel.: (04331) 201-2187

Koblenz
Dr. Michael Möhring
Uni Koblenz-Landau
FB Informatik
Rheinau 3–4
56075 Koblenz
Tel.: (0261) 9119477
Fax: (0261) 37524
moeh@infko.uni-koblenz.de

Köln
Manfred Keul
Landsbergstraße 16
50678 Köln
Tel.: (0221) 317911
100031.12@compuserv.com

Konstanz
Volker Schuchhardt
Jungerhalde 78
78464 Konstanz
Tel: (07531) 874098 (d)
(07531) 34921 (p)
v.schuchhardt@cgk.sni.de

Lahn-Dill
Fiff-Regionalgruppe Lahn-Dill
c/o Markus Thielmann
Fritz-Philippi-Straße 7
35767 Breitscheid
Tel.: (02777) 1271
mt@donut.de

Leipzig
Dr. Rolf Stranzky
Freiburger Allee 9
04416 Markkleeberg
Tel.: 0341/35879-23
Fax: 0341/35879-26

München
Bernd Rendenbach
Leerbichlallee 19
82031 Grünwald
Tel.: (089) 6410547

Münster
Werner Ahrens
Franz-Daspestr. 36
48231 Warendorf

Oldenburg
Universität Oldenburg
Fachschaft Informatik
Ammerländer Heerstraße
26129 Oldenburg
Fachschaft.Informatik@informatik.uni-oldenburg.de

Paderborn
Harald Selke
Heinz Nixdorf Institut
U-GH Paderborn
Fürstenallee 11
33102 Paderborn
Tel.: (05251) 606518
hase@uni-paderborn.de

Regensburg
Paul Hilmer
Zollerstraße 13
93053 Regensburg
Tel.: (0941) 706542
Fax: (0941) 706540
P.Hilmer@LINK-R.de

Stuttgart
Kurt Jaeger
Schozacher Straße 40
70437 Stuttgart
Tel.: (0711) 8701309
(0711) 90074-23
Fax: (0711) 7289041
pi@lf.net

Tübingen
Jochen Krämer
Sand 13
72076 Tübingen
Tel.: (07071) 29-5957
fiff@informatik.uni-tuebingen.de

Ulm
Universität Ulm
Fachschaft Informatik
Bernhard C. Witt
Oberer Eselsberg
89081 Ulm
wittbe@pcpool1.informatik.uni-ulm.de

FIfF

Geschäftsstelle
FIfF e.V.
Medemstade 64
21775 Ihlienworth

Tel.: (04755) 911 154
Fax: (04755) 911 026

E-Mail:fiff@fiff.de

Dienstags 10 bis 16 Uhr,
Donnerstags 10 bis 16 Uhr

Volksbank Cuxhaven-Hadeln
Kontoverbindung: 413 83 600
BLZ 241 618 14

Überregionale Arbeitskreise des FIfF

AK »RUIN« (Rüstung und Informatik)

Ingo Ruhmann
Rittershausstraße 11
53113 Bonn
ingo.ruhmann@acm.org

AK »FIfF in Europa«

Dagmar Boedicker
Daiserstraße 45
81371 München
Tel.: (089) 7256547

AK »Informationstechnik für eine lebenswerte Welt«

Ralf Klischewski
Universität Hamburg
FB Informatik
Vogt-Kölln-Straße 30
22527 Hamburg
Tel.: (040) 54715-367
Fax: (040) 54715-311
klischew@informatik.uni-hamburg.de

FIfF im Netz

Das ganze FIfF

http://www.fiff.de

Mailing-Liste

Beiträge an:
fiff-l@fiff.de
An- und Abbestellungen an:
fiff-l-request@fiff.de

Regionalgruppen

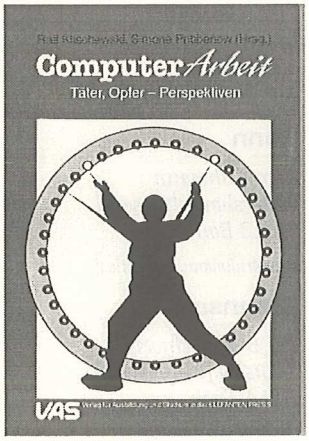
Bremen:
http://fiff.informatik.uni-bremen.de
Konstanz::
http://www.puk.de/fiff-kn
München:
http://hyperg.uni-paderborn.de/fiff/regional/muenchen
Tübingen:
http://www-fiff.informatik.uni-tuebingen.de

F..I..f..F..

Ute Bernhardt, Ingo Ruhmann (Hrsg.): Ein sauberer Tod: Informatik und Krieg.

Informations- und Kommunikationstechnik – seit ihren Anfängen politisch geformt · Computer auf dem Schlachtfeld · Dual-Use: zivil geforscht – militärisch genutzt? · »Wehrtechnik und Landesverteidigung« – Zur Forschung in der Bundesrepublik · Weiter so oder umsteuern? · u.v.a.

320 Seiten, Marburg 1991, 20,– DM



Ralf Klischewski, Simone Pribbenow (Hrsg.): ComputerArbeit. Täter, Opfer – Perspektiven

Das demokratische Potential der Neuen Fabrik · Maschinelle Intelligenz – Industrielle Arbeit · Arbeitnehmer und Betriebsräte zur Informatik im Betrieb.

190 Seiten, Berlin 1989, 19,80 DM

Ute Bernhardt, Ingo Ruhmann (Hrsg.): Computer, Macht und Gegenwehr – InformatikerInnen für eine andere Informatik

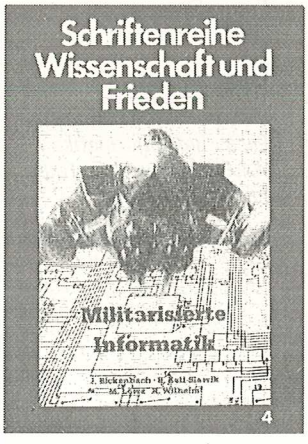
Protected Mode · Computersicherheit: militärisch oder zivil · Computer und Umwelt · Technologiepolitik und Technikfolgenforschung · Partizipative Entwicklung von Systemen ·
EU: Grundrechte als Handelshemmnisse? · u.v.a.

216 Seiten, Bonn 1991, 12,80 DM

Jutta Schaaf (Hrsg.): Die Würde des Menschen ist unverNETZbar.

Netzknoten Frankfurt · Automatisierung des Zahlungsverkehrs · Rüstungshaushalt und Informationstechnik · Verfassungsverträglichkeit als Kriterium der Technikbewertung · Ethik und Technik · Theorie der Informatik · u.v.a.

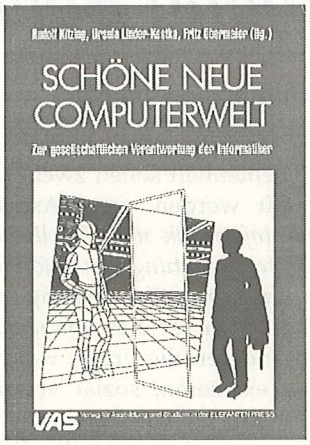
300 Seiten, Bonn 1990, 12,80 DM



J. Bickenbach et. al. (Hrsg.): Militarisierte Informatik

Erschienen in der Schriftenreihe Wissenschaft und Frieden, Nr. 4, 1985. Dieses Buch war vergriffen, doch sind einige Restexemplare aufgetaucht, die jetzt über das FIfF-Büro zum Preis von 10,– DM erhältlich sind.

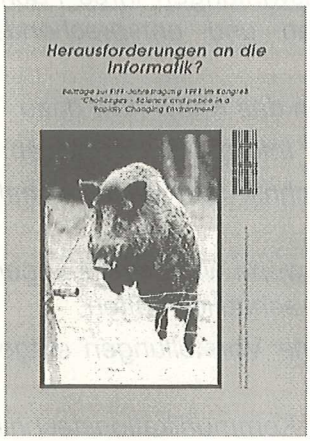
Bibliothek



Rudolf Kitzing, Ursula Linder-Kostka, Fritz Obermaier (Hrsg.): Schöne neue Computerwelt – Zur gesellschaftlichen Verantwortung der Informatiker

Beherrschbarkeit von Systemen, ihre Verletzlichkeit und die Verantwortung von Informatikern · Neue Wege in der Informatik · Psychosoziale Folgen des Computereinsatzes

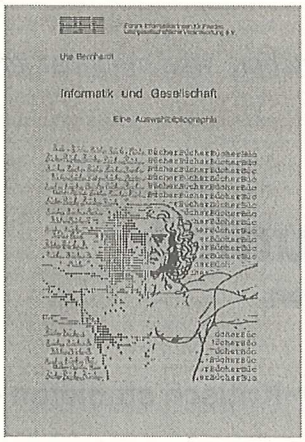
256 Seiten, Berlin 1988, 19,80 DM



Heiko Dörr (Hrsg.): Herausforderungen an die Informatik? – Science in a Rapidly Changing Environment

Wissenschaft und Ethik · Computergestützte und Elektronische Kriegsführung · Curricula und Forschungs- & Entwicklungs-Ansätze in der Informatik – den Anforderungen des 21. Jahrhunderts gerecht werden · Computertechnologie – ein angemessenes Mittel gegen die Armut der 3. Welt? · (Kredit-)Kartenzahlung im Licht von Daten- und Verbraucherschutz · Vernetzung von Friedensgruppen · Texte in englisch und deutsch

126 Seiten, Bonn 1992, 12,80 DM



Peter Bittner, Jens Woinowski (Hrsg.): Mensch – Informatisierung – Gesellschaft

Kritische Informatik, Band 1, Beiträge zur 14. Jahrestagung des FIfF 1998 in Darmstadt unter dem Motto: „Mensch sein in einer informatisierten Gesellschaft", 188 Seiten,

Münster: Lit-Verlag, 1999, Preis: 39,90 DM

Ute Bernhardt: Informatik und Gesellschaft. Eine Auswahlbibliographie

Ein thematisch gegliederter Einstieg in die Literatur zu Informatik und Gesellschaft

26 Seiten, Bonn 1990, 3,– DM

Jochen Krämer et. al. (Hrsg.): »Schöne Neue Arbeit«

Die Zukunft der Arbeit vor dem Hintergrund neuer Informationstechnologien. Der Tagungsband zur 12. Jahrestagung des FIfF in Tübingen 1996

Talheimer, 1997, 35,– DM

Hans-Jörg Kreowski et al.: Realität und Utopien der Informatik

Aus dem Vorwort: »Realität und Utopien der Informatik werden im vorliegenden Sammelband aus unterschiedlichen Sichten dargestellt, um die aktuelle Diskussion im Spannungsverhältnis von Informatik und Gesellschaft zu unterstützen und voranzubringen. Zusammengestellt sind ausgewählte Beiträge der 10. Jahrestagung des „Forums Informatikerinnen und Informatiker für Frieden und gesellschaftliche Verantwortung" (FIFF), die vom 7. bis 9. Oktober 1994 in Bremen unter dem Motto „1984 plus 10 – Realität und Utopien der Informatik" stattfand.«

Münster: agenda Verlag, 1995, 28,- DM

Alle Bücher sind erhältlich über: FIfF-Geschäftsstelle, Medemstade 64, 21775 Ihlienworth

Gesucht: Beiträge

FIfF-Kommunikation 1/2000:
»Kritisch studieren – und dann?«

In diesem Themenheft sollen zwei Fragestellungen miteinander verknüpft werden, zwei Aspekte dessen, was unter Namen wie *Informatik und Gesellschaft/Kritische Informatik/Sozialorientierte Gestaltung von Informatiksystemen*, oder *»neue Sichtweisen der Informatik«* Eingang in die Diskussion gefunden hat. Zum einen ist dies *Informatik und Gesellschaft* in der Lehre, zum anderen die Frage, welche Möglichkeiten in der Berufspraxis existieren, sozial verantwortungsvoll zu handeln. Es geht also um das Verhältnis von Theorie und Praxis. Unsere Umfrage in einigen Mailinglisten stellte eine Art »Versuchsballon« zum zweiten Aspekt dar. Die eingegangenen Antworten haben uns darin bestärkt, diese schwierige Frage anzugehen. Diese Antworten werden (anonymisiert) ebenfalls in Form einer Auswertung in das Themenheft eingehen oder können von den AutorInnen zu Artikeln erweitert werden.

Für das Themenheft können wir uns Artikel vorstellen, die sich z.B. mit den nachfolgend genannten Fragestellungen auseinandersetzen. Von besonderem Interesse sind für uns dabei die Beiträge, die das Theorie-Praxis-Verhältnis reflektieren.

Wie lassen sich Inhalte aus dem Bereich Informatik und Gesellschaft in der Lehre vermitteln? Welche Erfahrungen gibt es mit verschiedenen Lehrkonzepten und Themenbereichen? Gibt es Lehrkonzepte, die diese Thematik in andere Veranstaltungen (auch der klassischen Kerninformatik) integrieren? Wieviel Interesse besteht bei Studierenden dafür – ist es schon da, bzw. wie läßt es sich wecken?

Die ethischen Leitlinien der GI stärken den Stellenwert gesellschaftlicher Verantwortung. Doch wie sieht es aus mit der Wirklichkeit im Berufsalltag? Welche Möglichkeiten gibt es, in der Berufspraxis sozial verantwortungsvoll zu handeln? Wie unterscheiden sich selbständige und abhängige Tätigkeiten? Gibt es einen Markt für gesellschaftlich verantwortungsvolle Tätigkeit in der Informatik, z.B. Beratung? Gibt es Firmenpolitiken, die ein solches Handeln fördern oder für sich beanspruchen? Welche Möglichkeiten bieten Gewerkschaften?

Verändert sich durch die Berufspraxis das eigene Verhältnis zum Thema *Informatik und Gesellschaft* bzw. zur Informatik? Was ist dran an Mythos der Desillusionierung? Wie sehen Berufstätige im Nachhinein die Thematisierung von *Informatik und Gesellschaft* im Studium – prinzipiell bzw. in der geschehenen Form? Haben sie Vorschläge, wie dies thematisiert werden könnte, um besser auf die Berufspraxis vorzubereiten? Welche Unterschiede gibt es in Einstellung, Handlungsmöglichkeiten und (Lebens-, Berufs-) Situation zwischen BerufspraktikerInnen in den neuen Bundesländern und den alten?

Wir erhoffen uns zum zweiten Themenkomplex Beiträge vor allem von BerufspraktikerInnen, die sich diesen Fragen stellen und die (im Kleinen wie im Großen) auf vorhandene Handlungsmöglichkeiten hinweisen bzw. deren Einschränkungen analysieren.

Einreichungen für Beiträge bitte an Eva Hornecker und Peter Bittner an die Adresse: Eva Hornecker, Forschungszentrum artec, Universität Bremen, Postfach 330440, 28334 Bremen, E-Mail: eva@artec.uni-bremen.de. Redaktionsschluß ist der 31.12.1999.

Was will das FIfF?

Im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V. haben sich InformatikerInnen zusammengeschlossen, die sich nicht nur für die technischen Aspekte, sondern auch für die gesellschaftlichen Auswirkungen ihres Fachgebiets verantwortlich fühlen und entsprechende Arbeit leisten wollen:

- *Kritik üben, denn wir haben das Know-how dazu*
- *uns für eine Abrüstung der Informatik engagieren*
- *uns am Diskurs über Technik und Wissenschaft beteiligen*
- *die Öffentlichkeit warnen, wenn wir Entwicklungen in unserem Fachgebiet für schädlich halten*
- *möglichen Gefahren eigene Vorstellungen entgegensetzen*
- *die Informations- und Kommunikationstechnik nicht gegen, sondern für den Menschen gestalten*
- *uns für eine zivile und gerechte Welt einsetzen; eine Welt, in der die Grundrechte aller Menschen gewahrt werden, eine Welt, die menschenwürdig ist*
- *last not least nicht alles machen, was machbar ist*

Geplante

Themen-schwerpunkte

für die FIfF-Kommunikation

1/2000 »Kritisch studieren – und dann?«

zuständig: *Eva Hornecker, Peter Bittner*

2/2000 »Informationstechnik und Behinderung«

zuständig: *Ralf E. Streibl*

Die FIfF-Kommunikation bittet um Beiträge!

Die FIFF-Kommunikation lebt
von der aktiven Mitarbeit ihrer LeserInnen!
Interessante Artikel sowie Fotos und Zeichnungen zur Illustration (mit Quellengaben) 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.

Impressum

Die FIfF-Kommunikation ist das Mitteilungsblatt des »Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.« (FIfF). Die Beiträge sollen die Diskussion unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige AutorInnen-Meinung wieder. Nachdruck genehmigung wird nach Rücksprache mit der Redaktion in der Regel gerne erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

Heftpreis: 6 DM. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 25 DM/Jahr (inkl. Versand) abonnieren.

Erscheinungsweise: einmal vierteljährlich

Erscheinungsort: Medemstade

Auflage: 2000

Herausgeber: Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)

Verlagsadresse: FIfF-Geschäftsstelle, Medemstade 64, 21775 Ihlienworth, Tel. (04755) 911 154

ISSN: 0938–3476

Druck: Druckpartner Hemmoor

Layout: Frank Meiners

Titelbild: mit freundlicher Genehmigung des Bonner Friedensforums

Redaktionsadresse: FIfF-Kommunikation, Medemstade 64, 21775 Ihlienworth, Tel. (04755) 911 154, Fax (04755) 911 026
E-Mail: fiffko@uni-paderborn.de

FIfF-Überall: In dieser Rubrik der FIfF-Kommunikation ist jederzeit Platz für Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an: hubert@cs.tu-berlin.de

Lesen, Schluß-PFIFF: Beiträge für diese Rubriken bitte per Post an Claus Stark (Heilbronn) oder per E-Mail an: stark@secorvo.de

Redaktionsschluß für die Ausgabe 1/2000: 15. 1. 2000

Redaktions-Team FIfF-Kommunikation 4/99: Markus Hoff-Holtmanns, Harald Selke (verantwortlich)

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 bekanntzugeben!

Die Niederlage der Informationen

von Detlef Borchers

Immer schon war der Krieg ein Problem der Datenverarbeitung. Wer über die falschen Informationen verfügt, kennt seinen Gegner nicht und ist auf dem besten Wege in die Niederlage. Das wußte schon der Philosoph Shun Tsu 500 v. Chr. in seiner »Kunst des Krieges«. Heute ist man eigentlich einen Schritt weiter, heute kann die Datenverarbeitung den Krieg ersetzen. Ein Arbeitspapier von NATO-Militärinformatikern beschreibt das Szenario: »Ein groß angelegter Konflikt konnte vermieden werden; eine regionale Krise, entstanden in einer bereits aufgewühlten Region, drohte die NATO und viele Nationen in eine Situation zu ziehen, in der die Waffengewalt nötig wurde, um eine politische Situation zu erreichen. Die Information Superiority errang einen ihrer ersten Siege und führte zur Beendigung der Feindlichkeiten in Bosnien.«

Das Militär feierte in Bosnien den ersten richtigen Sieg in einem Informàtionskrieg, im sogenannten Information Warfare. »Präsident Milosevic wurde gezeigt, welche Auswirkungen IFOR-Aktionen auf das serbische Militär und die Kampfkraft seiner Truppen haben würde. Die überzeugende Darstellung der hochwertigeren Informationen hatte den gewünschten Effekt.« Information Superiority nennt sich eine Strategie, bei der die gesammelten Daten über den Gegner mit »Knowledge Management« so verdichtet werden, daß sie haushoch überlegen sind. Diese Daten präsentiert man dann dem Gegner, welcher an ihnen erkennt, daß er keine Chance hat und den geplanten Angriff abbläst.

Was in Bosnien funktionierte, blieb im Kosovo ohne Wirkung. Nun stehen die Militärinformatiker, die Verfechter der Information Superiority vor einem Rätsel. Sie trafen sich in Brüssel auf Einladung der Firma Lotus, um über das Konzept zu beraten. Die Beratungen fielen ernüchternd aus; allzu offensichtlich war das Bombardement der chinesischen Botschaft ein Beweis, dass die angestrebte Überlegenheit der Daten nicht gegeben war. Doch wo war der Fehler? Lag er im Cronos-System, das die Aktionen der NATO koordiniert? Oder in der Datenlieferung?

»Wenn wir überlegen sind, dürfen wir uns nicht allein auf Datensammlungen wie Echelon verlassen, sondern müssen viele Levels von Echelon installieren, aus denen zusammen die überlegenen Daten extrahiert werden. Wir müssen unsere Echelons skalieren können«, forderte ein Teilnehmer. Die Sammlung überlegener Daten fördert so zunächst einmal nur weitere Sammlungen von Daten: Echelon nennt sich das Abhören des internationalen Datenverkehrs im großen Stil, bei dem die Daten sogenannte »Dictionary-Computer« durchlaufen, die wie Filter funktionieren. Die Vorlage zur Arbeitstagung war da etwas klüger: »Der menschliche Faktor, die Unfähigkeit oder Unwilligkeit, die Informationen intelligent zu nutzen, ist das Hauptproblem. Eigentlich hätte Milosevicz längst die Informationen akzeptieren müssen.«